HACETTEPE ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ

Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

MİKRO-ÖĞRENME NESNELERİNİN TASARIM TABANLI ARAŞTIRMA YÖNTEMİYLE TASARLANMASI VE DEĞERLENDİRİLMESİ: İLKÖĞRETİMDE SİBER GÜVENLİK ÖRNEĞİ

Muhammet Osman ÖZLÜ

Yüksek Lisans Tezi

Ankara, 2024

Liderlik, araştırma, inovasyon, kaliteli eğitim ve değişim ile

Daha ileriye... En İyiye...

HACETTEPE ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ

Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

MİKRO-ÖĞRENME NESNELERİNİN TASARIM TABANLI ARAŞTIRMA YÖNTEMİYLE TASARLANMASI VE DEĞERLENDİRİLMESİ: İLKÖĞRETİMDE SİBER GÜVENLİK ÖRNEĞİ

DESIGN AND EVALUATION OF MICRO-LEARNING OBJECTS USING DESIGN-BASED RESEARCH METHOD: AN EXAMPLE OF CYBER SECURITY IN PRIMARY EDUCATION

Muhammet Osman ÖZLÜ

Yüksek Lisans Tezi

Ankara, 2024

Kabul ve Onay

Eğitim Bilimleri Enstitüsü Müdürlüğüne,

Muhammet Osman ÖZLÜ'nün hazırladığı "Mikro-Öğrenme Nesnelerinin Tasarım Tabanlı Araştırma Yöntemiyle Tasarlanması ve Değerlendirilmesi: İlköğretimde Siber Güvenlik Örneği" başlıklı bu çalışma jürimiz tarafından **Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalında Yüksek Lisans Tezi** olarak kabul edilmiştir.

Jüri Başkanı	Prof. Dr. S. Sadi SEFEROĞLU
Jüri Üyesi (Danışman)	Prof. Dr. G. Alev ÖZKÖK
Jüri Üyesi	Prof. Dr. Serçin KARATAŞ
Jüri Üyesi	Prof. Dr. Yasemin DEMİRASLAN ÇEVİK
Jüri Üyesi	Doç Dr. Gökhan DAĞHAN

Bu tez Hacettepe Üniversitesi Lisansüstü Eğitim, Öğretim ve Sınav Yönetmeliği'nin ilgili maddeleri uyarınca yukarıdaki jüri üyeleri tarafından 30 / 04 / 2024 tarihinde uygun görülmüş ve Enstitü Yönetim Kurulunca ..... / ..... / ..... tarihi itibarıyla kabul edilmiştir.

Prof. Dr. İsmail Hakkı MİRİCİ

Eğitim Bilimleri Enstitüsü Müdürü

Öz

Siber güvenlik, Bilgi ve İletişim Teknolojileri (BİT) ile bunların içerdiği bilgilerin hasara, yetkisiz kullanıma veya değişikliğe ya da saldırıya karşı korunduğu faaliyetler zinciri olarak tanımlanabilir. Bu çalışmada, siber güvenlik farkındalığına yönelik siber güvenlik mikro öğrenme nesnelerinin mikro öğrenme stratejisi temel alınarak tasarlanması, geliştirilmesi ve değerlendirilmesi amaçlanmıştır. Araştırma, Eğitsel Tasarım Tabanlı Araştırma (ETTA) modeliyle ortaokul 6. sınıf öğrencileri ile iki mezo döngü olacak şekilde gerçekleştirilmiştir. Her döngü (a) *Analiz ve İnceleme*, (b) *Tasarım ve Geliştirme* ve (c) *Değerlendirme ve Yansıma* mikro döngülerinden oluşmaktadır. *Analiz ve İnceleme* mikro döngüsünde, Siber Güvenlik Farkındalığı kazanımları (a) *E-Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlerin Farkına Varabilme*; (b) *E-Postalarda Yazım Hatası İçeren Tehditlerin Farkına Varabilme*; (c) *E-Postalarda Şifre Hedefli Tehditlerin Farkına Varabilme*, (ç) *E-Posta Güvenlik Ayarlarını Kullanabilme*; oluşturulmuştur. Birinci mezo döngü sürecinde, Siber Güvenlik Farkındalığı kazanımları odaklı ölçütler geliştirilerek, Siber Güvenlik Mikro Öğrenme Nesneleri Dereceli Puanlama Anahtarı (SGF-DPA) geliştirilmiştir. Geliştirilen dereceli puanlama anahtarı ile öğrencilerin Siber Güvenlik farkındalığı her iki döngü sonucunda değerlendirilmiştir. İlk mezo döngünün sonunda, SGF-DPA puanları ve öğrenci yansımaları doğrultusunda süreç yeniden düzenlenmiştir. Elde edilen bulgularla, ikinci mezo döngüde, öğrenme nesnelerine karakter eklenmesi, durağan yapıdan hareketli video yapısına geçilmesi, dinamik görsellerin kullanılması kararlaştırılarak yeniden düzenlenmiştir. Öğrencilerin SGF-DPA puanları incelendiğinde İkinci mezo döngüde belirgin bir yükselişin olduğu görülmüştür. Ulaşılan sonuçlara göre, tasarım tabanlı araştırmanın, araştırma amacına uygun olarak yürütüldüğü; siber güvenlik mikro öğrenme nesnelerinin amaca uygun özelliklere sahip olduğu söylenebilir.

Anahtar sözcükler: siber güvenlik, mikro-öğrenme, sosyal mühendislik, tasarım-tabanlı araştırma yöntemi

Abstract

Cyber security can be defined as the chain of activities in which Information and Communication Technologies (ICT) and the information contained therein are protected against damage, unauthorised use or modification or attack. In this study, it is aimed to design, develop and evaluate cyber security micro learning objects for cyber security awareness based on micro learning strategy. The research was carried out in two meso-cycles with 6th grade secondary school students with the Educational Design Based Research (EDBR) model. Each cycle consists of (a) Analysis and Review, (b) Design and Development and (c) Evaluation and Reflection micro-cycles. In the Analyse and Review micro cycle, Cyber Security Awareness gains (a) Being aware of threats based on unknown links and content in e-mails; (b) Being aware of threats containing spelling mistakes in e-mails; (c) Being aware of password-targeted threats in e-mails; (d) Using e-mail security settings. In the first meso cycle process, Cyber Security Micro Learning Objects Rubric (SGF-DPA) was developed by developing criteria focused on Cyber Security Awareness outcomes. With the developed rubric, students' Cyber Security awareness was evaluated at the end of both cycles. At the end of the first meso cycle, the process was reorganised in line with the SGF-DPA scores and student reflections. With the findings obtained, in the second meso cycle, it was decided to add characters to the learning objects, to switch from a static structure to a moving video structure, and to use various effects. When the SGF-DPA scores of the students were analysed, it was observed that there was a significant increase in the second meso cycle. According to the results obtained, it can be said that the design-based research was conducted in accordance with the research purpose; cyber security microlearning objects have appropriate features for the purpose.

Keywords: cyber security, phishing, micro-learning, social engineering, design-based research

Teşekkür

Bu çalışmada bana değerli bilgileriyle yol gösteren, saat fark etmeksizin destek olarak bu çalışmayı yapmamı sağlayan, gelecekte imza atacağım başarılarda katkısını her zaman hissedeceğim sevgili danışmanım Sayın Prof. Dr. G. Alev ÖZKÖK'e; manevi desteği ile bu çalışmanın bitmesinde büyük katkıları olan, desteğini her zaman hissettiren Sayın Kürşat ÖZKÖK'e çok teşekkür ederim.

Tez jürimde yer alarak ve çalışmama getirmiş oldukları katkılardan dolayı, Sayın Prof. Dr. S. Sadi SEFEROĞLU, Sayın Prof. Dr. Serçin KARATAŞ, Sayın Prof. Dr. Yasemin DEMİRASLAN ÇEVİK ve Sayın Doç. Dr. Gökhan DAĞHAN'a teşekkürlerimi sunarım. Değerli yorumları ve getirdiği katkıları ile çalışmama destek olan kıymetli arkadaşlarım Beyza ÖZATA ve Taha YILDIZ'a çok teşekkür ederim.

Bu uzun soluklu süreçte bana anlayış gösteren, her zaman yanımda olan, sıkıntılarımı paylaşan sevgili eşim Özlem ÖZLÜ'ye ve biricik oğlum İbrahim Baybars ÖZLÜ'ye teşekkürlerimi sunarım. Desteklerini hiçbir zaman esirgemeyen sevgili annem Selamet ÖZLÜ ve babam Mustafa ÖZLÜ'ye, kardeşlerim Gökçe Nur ÖZLÜ ve İlbilge ÖZLÜ'ye, her zaman huzur veren patili dostumuz Kuki'ye sonsuz teşekkürler.

İçindekiler

Tablolar Dizini

Şekiller Dizini

Simgeler ve Kısaltmalar Dizini

APWG: Anti Phishing Working Group

BİT: Bilgi İletişim Teknolojileri

ETTA: Eğitsel Tasarım Tabanlı Araştırma

IWS: Internet World Stats

MEB: Milli Eğitim Bakanlığı

SGF-DPA: Siber Güvenlik Farkındalığı Dereceli Puanlama Anahtarı

SGMÖN: Siber Güvenlik Mikro Öğrenme Nesnesi

TTA: Tasarım Tabanlı Araştırma

TÜİK: Türkiye İstatistik Kurumu

Bölüm 1

Giriş

Problem Durumu

Dijital teknolojilerin hızlı gelişimi, çalışma, iletişim kurma, öğrenme ve nihayetinde internete bağlı yeni bir dünyada birlikte var olma biçimimize önemli değişiklikler getirmiştir. En büyük bilgi kaynağı olma özelliğini taşıyan internet teknolojileri sayesinde bireyler günümüzde sınırsız iletişim özgürlüğüne sahip olabilmekte ve bilgiye düşük maliyetlerle çok hızlı şekilde ve kolaylıkla erişebilmektedirler. İnternet kullanıcılarının sayısı ve internete olan bağımlılık dünya genelinde giderek artmaktadır (Mohd Zaharon vd., 2021; Muniandy vd., 2017). Bunun sonucu olarak, internet teknolojisindeki hızlı gelişme, toplumu internete bağımlı hale getirmiştir.

Internet World Stats'ın (2023) raporuna göre, dünya genelinde yaklaşık 5,4 milyar, Türkiye'de ise yaklaşık 72,5 milyon İnternet kullanıcısı bulunmaktadır. Türkiye İstatistik Kurumu'nun (2023), hane halkı bilişim teknolojileri kullanım araştırması sonuçlarına göre ülkemizde 2023 yılında evden internete erişim imkânı olan hanelerin oranı bir önceki yıla göre 1,4 puan artarak %95,5 olmuştur. Yapılan araştırmalar (TÜİK, 2021), gençlerin ve çocukların internet kullanım oranlarının oldukça yüksek olduğunu göstermektedir. Ülkemizde 6-15 yaş grubundaki çocukların internet kullanım oranı 2013 yılında %50,8 iken, 2021 yılında %82,7 olarak görülmektedir. Cinsiyete göre incelendiğinde; erkek çocukların İnternet kullanım oranı 2013'te %53,7 iken 2021'de %83,9'a, kız çocuklarının oranı ise 2013'te %47,8'den 2021'de %81,5'e yükseldiği anlaşılmaktadır. Aynı yaş grubundaki çocukların %90,1'i hemen her gün, %8,5'i haftada en az bir defa internet kullanırken, yalnızca %1,4'ü haftada bir defadan az internet kullanmaktadır. Bu veriler ışığında internet teknolojisinin bireysel ve toplumsal olarak hayatı etkilediği söylenebilir.

İnternet, insanların hayatlarını olumlu yönde etkilemesine rağmen, internet kullanımıyla ilgili ortaya çıkan sorunlar da vardır (Rahman vd., 2020). Bilgisayar ve

internetin kullanılmaya başlandığı ilk yıllarda internet bir tehdit olarak algılanmamıştır. Yirmi birinci yüzyılın başlarından itibaren internetin ve teknolojik araçların hayatımızı ele geçirmesiyle siber tehdit unsuru da ortaya çıkmıştır (Blythe, 2013). Son yıllarda bilgisayar ve mobil cihazların kullanımındaki artış, kullanıcıları siber saldırı türlerine karşı daha savunmasız hale getirmiştir (Hamdani & Mustafa, 2021).

Dünya genelinde ve ülkemizde internet ortamında güvenliği sağlamak, internette işlenen suçları engellemek ve bu suçları işleyenlere yaptırımlar oluşturmak amacıyla, kanunların düzenlenmesine ve bu konuda yasal çalışmalara öncelik verilmektedir. Yapılan düzenleme ve çalışmalar internetin olumlu yönlerinin düzenlenmesi, olumsuz yönlerinin engellenmesi açısından önem arz etmektedir. Bu durum, kullanıcıların internet ortamında güvenlik gereksinimlerinin artmasına neden olmaktadır. İnternette duyulan güvenlik kaygıları siber güvenlik kavramını ortaya çıkarmıştır.

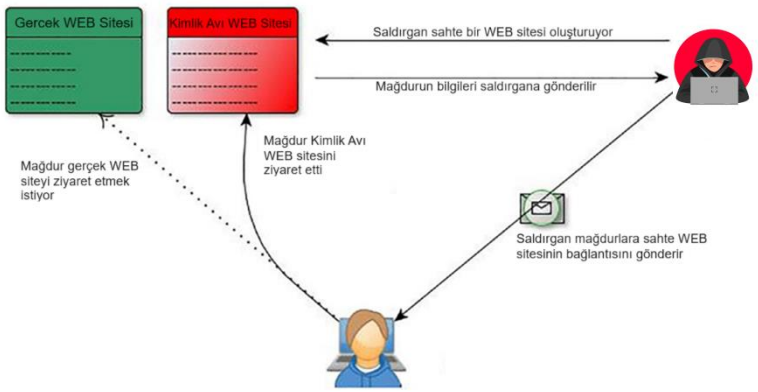
Erken dönem siber saldırılar genellikle kullanıcıları hedef alan parola veya kredi kartı bilgilerini ele geçirmeyi amaçlayan basit saldırılardan oluşmaktadır (Onashoga vd., 2019). Günümüzde siber saldırılar yaygın ve giderek daha etkili hale gelmiştir. Son yıllarda, internetin karmaşıklığı arttıkça, saldırganların kullanıcıların değerli ve özel bilgilerini elde etmek için geliştirdikleri yöntemler de gelişmiştir (Perrault, 2018). İletişimin en kolay yolu olmasına rağmen, internetin kötüye kullanılması bazı insanları suç işlemeye teşvik etmiş, bazılarının da mağdur olmasına sebep olmuştur. Bu durum, internet kullanıcıları arasında endişe yaratmaktadır. İnternet kullanımının artmasıyla birlikte, insanlar bilgilerinin güvenliği konusunda giderek endişelenmektedirler (Mohd Zaharon vd., 2021).

Siber tehditler, bilgisayar sistemlerine veya ağlarına zarar vermek ya da bilgileri ele geçirmek amacıyla gerçekleştirilen veya gerçekleştirilebilecek kötü niyetli faaliyetlerdir (Al-Hamar & Kolivand, 2020). Bu tehditler finansal kayıplara, veri kaybına, itibar kaybına ve hatta insanların güvenliğine yönelik tehlikelere neden olabilir (Kamruzzaman vd., 2016). Siber güvenliği tehdit eden unsurlardan biri olan Kimlik Avı-Oltalama (Phishing), yaygın ve kullanıcıların sıklıkla karşılaştığı tehditlerdendir (Şekil 1). Araştırmalar, internet

kullanıcılarının genellikle maruz kaldıkları e-postalardaki siber saldırılardan ve bunların tehlikelerinden habersiz olduklarını göstermektedir (Arachchilage & Love, 2013). Bu tür saldırılara maruz kalanlar arasında her yaş grubundan internet kullanıcısı bulunmasına rağmen, çocuklar ve gençler en savunmasız grubu oluşturmaktadır (Kumaraguru, vd., 2010).

Şekil 1

Siber Saldırı Stratejisi



E-postalara düzenlenen siber saldırılar, mağdurun merak ve korku gibi duygularını kullanarak, kredi kartı numarası, kimlik bilgileri ve kişisel bilgilerini ele geçirmeyi amaçlayan sosyal mühendislik tehdididir (Tchakounte vd., 2020; Yeboah-Boateng & Amanor, 2014). Herhangi bir bilgisayardan gelen sahte e-postadan indirilen eklentiler, kullanıcının farkında olmadan bilgisayarına yerleşerek bilgilerinin kısa sürede ele geçirilmesine imkân yaratmaktadır (Coventry vd. 2014). Bu tür saldırılar, internete bağımlı yaşam tarzı ve teknolojinin karmaşık yapısı nedeniyle her internet kullanıcısı için kalıcı bir tehdit haline gelmiştir. İnternete bağımlılık arttıkça, çeşitli siber saldırılar ve güvenlik ihlalleri ile karşılaşma olasılığı da artmaktadır (Liang & Xue, 2010).

Saldırıların başarısı, saldırganların sosyal medya, e-posta, web sitesi gibi kanalları kullanarak kendilerini ne kadar iyi ve meşru bir hizmet olarak sundukları ile son kullanıcının

saldırıyı tespit etme ve uygun şekilde hareket etme becerisi ile bağlantılıdır. Örneğin, hedef alınan kullanıcıların bir e-postadaki yazım hatalarını veya yanlış alt alan adını ne kadar iyi tespit edebildiği saldırının başarılı olma olasılığını önemli ölçüde düşürebilmektedir. Bu soruna karşı etkili savunma sağlayan son derece teknik çözümler mevcut olsa da bu çözümler tamamen koruma sağlayamamaktadır. Çünkü saldırılar, teknik önlemleri aşmayı amaçlamakta ve sisteme giriş noktası olarak insanları kullanmaktadır (Hamdani & Mustafa, 2021).

İnternet kullanıcılarının çoğunluğu siber saldırıları tespit etmede yetersizdir. Case ve King (2016), yürüttükleri 5 yıllık araştırmada öğrencilerin %21'inin ortalama bir ay içinde oltalama e-postası aldığını bildirdiğini tespit etmiştir. Çalışma süresince oltalama e-postalarına yanıt veren öğrenci sayısında %50'lik bir artış olduğu ortaya konmuştur. Vishwanath ve arkadaşları (2011), üniversite öğrencilerinden oluşan örneklemde, öğrencilerin tanıdıkları kişilerden gelen oltalama e-postalarındaki aciliyet ipuçlarıyla kandırılma olasılıklarının daha yüksek olduğunu bulmuştur. Alsharnouby ve arkadaşları (2015), üniversite öğrencilerinin kendilerine sunulan oltalama web sitelerinin yalnızca %53'ünü başarılı bir şekilde tespit edebildiğini bulmuştur. Göz izleme yazılımı kullanarak, öğrencilerin web sitesinin sahte olduğunu gösteren potansiyel ipuçlarına çok az zaman harcadıkları tespit edilmiştir.

Veri kullanım oranları ve internet tüketiminin artmaya devam etmesiyle siber farkındalığa duyulan ihtiyaç zorunlu hale gelmiştir (Mohd Zaharon vd., 2021). Bu tür sorunların büyük etki yaratmaması için erken önlem alınması gerekir. Bu bağlamda, internet kullanıcılarının siber güvenlik eğitimi alması zorunlu hale gelmiştir (Rahman vd., 2020).

Siber güvenlik, elektronik ortamda saklanan verilerin suç teşkil eden saldırılara karşı korunmasını veya bu verilerin sahiplerinin izin ve bilgisi dışında kullanımının engellenmesini sağlamak için alınan önlemleri ifade etmektedir (Rahman vd., 2020). Anderson ve arkadaşları (2009), siber güvenlik kavramının günümüzün dijital dünyasında giderek artan bir öneme sahip olduğunu belirtmektedir. Siber güvenlik, dijital verilerin güvenliğine yönelik

tehditlere karşı mücadele eden ve birçok yöntem ve teknolojiyi kapsayan geniş bir alandır. En önemli unsurlarından biri, Bilgi ve İletişim Teknolojilerinin (BİT) kullanımı sırasında ortaya çıkabilecek riskleri yönetmektir. Bu riskler, siber saldırılarla ilişkili veri kayıpları, finansal zararlar, itibar kaybı ve hatta insan hayatına yönelik tehditler olabilir. Siber güvenlik, bu riskleri azaltmak veya ortadan kaldırmak için çeşitli önlemler ve yöntemler sunmaktadır (Dhillon & Backhouse, 2001).

Siber tehditlerle mücadelede alınması gereken önlemler arasında, güçlü şifreler kullanmak, güncel yazılımlar ve güvenlik yamalarını kullanmak, güvenlik yazılımları ve donanımlarını kullanmak, veri yedeklemesi yapmak, ağ trafiğini izlemek ve güvenlik bilincini artırmak gibi adımlar bulunur. Güvenlik önlemlerinin standart biçimi, kriptografi, şifreleme, erişim kontrolü, parola, antivirüs ve güvenlik duvarı gibi unsurları içeren teknik önlemlerdir. Bu çözümler çeşitli siber saldırılara karşı koruma sağlasa da bilgisayar güvenliğinin yalnızca bir yönünü kapsamaktadır. Bilgisayar güvenliğinin bu yönü, teknolojiyi kullanarak güvenlik mimarisi tasarımına, geliştirilmesine, uygulanmasına ve yürütülmesine odaklanmaktadır. Siber saldırıları tespit etmeye yönelik araçlar etkili bir savunma sağlayamayabilir (Sun vd., 2017). Bu nedenle, araştırmacılar (Kumaraguru vd., 2010; Sheng vd., 2010), kullanıcıların siber güvenlik kavramlarını ve siber saldırı savunma yöntemlerini öğrendikleri ve temel savunma becerileriyle donatıldıkları siber güvenlik eğitimini, siber güvenliğin en etkili aracı olarak görmektedir.

Bilgisayar güvenliğinin diğer yönü ise insana odaklanmaktadır. Luo ve arkadaşları (2013), bireylerle ilişkili bilgi güvenliği faktörlerinin göz ardı edilemeyeceğini savunmaktadır. Benzer şekilde, Chou ve Jones (2018), siber güvenlik eğitiminin gerekliliğine vurgu yaparak, öğrencilere siber güvenlik konusunda yeterli kuramsal ve uygulamalı eğitimin verilmesinin önemine dikkat çekmektedir. Siber suç vakalarının birey, kuruluş, zaman ya da mekân fark etmeksizin meydana gelebilmesi nedeniyle siber güvenlik eğitimi zorunlu hale getirilmelidir (Rahman vd., 2020). Siber ortamda karşılaşılan tehditlere karşı geliştirilen yöntemler, eğitimlerin temelini oluşturabilir.

Siber saldırıları azaltmak için tespit, önleme ve kullanıcı eğitimi birlikte kullanılmalıdır (Vayansky & Kumar, 2018). Tespit otomatiktir ve kötü niyetli bağlantıları, yazım hatalarını veya kimlik avı e-postalarının diğer ortak özelliklerini tespit etmek amacıyla e-postaları taramak için kullanılır. Otomatik tespit ve önleme temel saldırıları durdurabilirken, iyi hazırlanmış bir siber güvenlik eğitimi her ikisinden de daha başarılı sonuç verebilir (Grubbs, 2022).

Günümüz dijital yerlileri olan öğrenciler, siber saldırılarla ilgili bilgi ve deneyim eksikliği nedeniyle yetişkinlere kıyasla daha büyük risk altındadır (Sun vd., 2017). Özellikle, bu saldırı türlerine karşı en savunmasız kitle öğrencilerdir. Siber güvenlik farkındalığı eğitimi, siber tehditlerin tehlikesi açıklanarak, olası saldırıları nasıl tespit edip bildirecekleri gösterilerek başlatılmalıdır. Öğrencilerde siber güvenlik farkındalığı, siber saldırıların kontrolünü sağlamak için arttırılmalıdır. Siber saldırı tekniklerine karşı farkındalık geliştirmek için simülasyonlar ve eğitsel çoklu ortam materyalleri, kullanıcıların kendi risklerini anlamalarına yardımcı olur. Bu farkındalık, öğrencilerin yanı sıra hedef alınan aileleri için de gereklidir. Bu eğitim süreci, çevrimiçi, yüz yüze, harmanlanmış veya karma eğitim yöntemiyle yürütülebilir (Al-Hamar & Kolivand, 2020).

Siber tehdit, öğrencilerin uygulamaya konulan güvenlik önlemlerine aşina olmaları için eğitilmesiyle azaltılabilir. Onlara güvenliğin işbirlikçi bir çaba olduğu ve herkesin sorumluluğunda olduğu anlatılmalıdır. Aksi takdirde, siber saldırıların yarattığı tehdit hızla büyüyebilir ve bu da hem bireysel hem de kurumsal düzeyde ciddi sonuçlara yol açabilir (Al-Hamar & Kolivand, 2020). Öğrencilerin siber güvenlik öğrenme sürecine daha etkili bir şekilde motive etmek ve katılımlarını sağlamak için çeşitli yenilikçi öğrenme teknikleri ve yaklaşımları kullanılabilir. Bu araştırmada, siber güvenlik eğitiminde, mikro içeriklerin kullanılması, öğrenme çıktılarını ve öğrencilerin derse katılımını artırmak etkili ve yenilikçi yaklaşımlardan biri olan mikro öğrenme stratejisi kullanılmıştır.

Mikro öğrenme stratejileri, öğrencilerin siber güvenlik çevrimiçi modüllerini hızlı bir şekilde almalarını sağlar. Bu strateji, öğrenci merkezli ve etkileşimli olması, iyi planlanmış

modüller ve eğitim sunma kabiliyeti sunar. Bu şekilde, dijital yerlilerin ihtiyaç ve talepleriyle uyumlu daha kısa öğretim materyalleri ve öğrenme etkinlikleri sunulur (Jomah vd., 2016). Ayrıca, siber güvenlik eğitiminde mikro öğrenme stratejisi, video, metin, görüntü ve ses içeren mini dersler gibi çeşitli teknoloji türleri arasında podcastler, sosyal medya, infografikler, oyunlaştırma gibi daha fazla imkanlar sunmaktadır. (Shabadurai vd., 2022).

Son yıllarda öğrenme ortamlarındaki değişiklikler, geleneksel öğrenme ve öğretme süreçlerinde de değişimlere yol açmıştır. Geleneksel öğrenme faaliyetlerinin ve kuramsal yaklaşımların etkinliği tartışılır hale gelmiştir. Bu değişimin gerektirdiği ihtiyaçlar sonucunda, geleneksel öğrenme modelleri yerini yeni öğrenme modellerine bırakmaya başlamıştır (Lau vd., 2019). Öğretme ve öğrenme sürecindeki değişim çok çeşitli yeni öğrenme yöntem ve tekniklerinin ortaya çıkmasına neden olmuştur. Bunlardan biri olan *mikro öğrenme*, geleneksel öğrenme yaklaşımlarından teknoloji destekli öğrenme yaklaşımlarına geçiş sürecinde web 2.0 teknolojisi ile ortaya çıkmıştır. Özellikle COVID-19 salgınının ortaya çıkışı, küresel ölçekte öğrenme ve öğretme sürecinde bir paradigma değişikliğine neden olmuştur. COVID-19 salgını sırasında, mikro öğrenme başlangıçta öğrencilerin uzun saatler süren çevrimiçi öğrenmeden kaynaklanan can sıkıntısı, yorgunluk ve bıkkınlık gibi sorunlarını çözmek için çevrimiçi destek olarak düşünülmüştür (Fitria, 2022). Araştırmalar, mikro öğrenmenin özellikle COVID-19'un başlangıcından bu yana popülerlik kazandığını ve COVID-19'un etkilerini hafifletmek için etkili bir öğretim stratejisi olduğunu göstermiştir (Sankaranarayanan vd., 2022).

Öğrenmeden mikro öğrenmeye geçiş ihtiyacı, insanların kısa süreli hafızasının ve görsel-işitsel kanalın işlem gücünün sınırlı olması nedeniyle bireylerin dikkat oranlarında ve konsantrasyon seviyelerinde bir azalma gözlemlenmesinden kaynaklanmaktadır (Shaffer vd., 2003). Son yıllarda yapılan çalışmalar, mikro öğrenmenin öğretim içeriğinin daha iyi anlaşılmasını kolaylaştırdığını, ilgiyi artırdığını, esneklik sağladığını ve öğrenenler tarafından kolayca kabul edildiğini göstermiştir. Mikro öğrenme, bilgi hacmini ve karmaşıklığını azaltarak, yeni öğretim modellerini geliştirerek ve öğrenenlere kendi

öğrenme zamanlarını, yerlerini ve hızlarını seçme fırsatı sunarak geleneksel öğrenmeden farklılaşır (Bruck, 2005). Araştırmalar, (Korstange vd., 2020; Mohammed vd., 2018), mikro öğrenmenin öğrencilerin öğrenme becerilerini geleneksel yöntemlere kıyasla %18 oranında artırdığını göstermiştir. Mikro öğrenme, bilgi miktarını azaltarak ve materyalleri daha çekici ve etkileşimli hale getirerek bilişsel aşırı yüklenme sorununu ele almayı amaçlar. İnsan beyninin dikkat süresi sınırlarını aşarak bilişsel aşırı yüklenmeyi önlemeyi hedefler (Fernandez, 2014). Kısa ve odaklanmış modüller kullanarak bilgiyi yaymak, daha büyük konuları daha küçük parçalar halinde sunmak mikro öğrenmenin temel amacıdır (Alqurashi, 2017).

Mikro öğrenmenin farklı boyutlarına odaklanan ve eğitim teknolojisinin yeni ortaya çıkan çeşitli konularını ele alan yeterli sayıda çalışma bulunmaktadır (Lai & Bower, 2020). Mikro öğrenme, kısa süreli (3-5 dakika) öğretim parçalarından ve öğrencilerin kolayca tüketebileceği spesifik öğrenme hedeflerinden oluşan bir e-öğrenme yaklaşımıdır. Bu iki özelliğin birleşimi, mikro öğrenmenin mesleki eğitimde kullanılmasını teşvik etmektedir (Göschlberger, 2017). Mikro öğrenmede, öğrenciler tanımlar, formüller, kısa paragraflar, kısa video bölümleri, mini podcastler, flash kartlar veya sınavlar gibi mikro içeriklere ulaşmak için mikro çoklu ortam materyallerinden yararlanır (Zhang & Ren, 2011). Araştırmacılar mikro öğrenme hakkında farklı görüşlere sahip olsalar da genellikle elektronik didaktik veya mobil öğrenme gelişiminin yeni bir aşaması ile ilişkilendirilmektedir (Hug, 2007).

Hug'un (2005) yedi boyutlu çerçeveyi sunmasından bu yana, birçok araştırmacı mikro öğrenme kavramını genişletmek için bilgi birikimine teorik ve ampirik çalışmalarla katkıda bulunmuştur. Hug (2005) mikro öğrenmeyi yedi boyuta dayalı bir öğretim çerçevesi olarak tanımlamıştır. Bu boyutlar; (1) kısa, ölçülebilir zaman, çaba ve zaman tüketimiyle ilgili öğrenme süresi, (2) küçük öğrenme üniteleri, basit konular ve dar konular içeren öğrenme içeriği, (3) modüller setini ve informal öğrenme gibi öğrenme modelinin türünü ifade eden müfredat, (4) parçalara, bölümlere ve bilgi kırıntılarına odaklanan öğrenme formu, (5) ayrı,

bağlantılı, konumlandırılmış veya harmanlanmış faaliyetlere odaklanan öğrenme süreci, (6) öğrenme nesneleri, yüz yüze ve çoklu ortam kullanan öğrenme ortamı ve (7) davranışçı, yapılandırmacı ve sosyal öğrenme perspektiflerini içeren öğrenme tipidir.

Uluslararası alan yazında çok sayıda tanım ile karşılaşmaktayız. Bunlar; (a) küçük öğrenme birimlerine ve kısa süreli odaklanmış etkinliklere dayanan bir öğrenme yaklaşımıdır (Hug, 2005; Hug vd., 2005; Lindner, 2007; Leong vd., 2021); (b) çalışanların öğrenme ihtiyaçlarını çevrimiçi olarak destekleyen içerik tabanlı bir e-öğrenme yaklaşımıdır (Giurgiu, 2017); (c) zaman ve mekândan bağımsız olarak erişim kolaylığı sağlayan küçük ve esnek eğitim içeriği bölümleri geliştirme metodolojisidir (Gabrielli, vd., 2005); (ç) mikro içerikler veya mikro çoklu ortam ile küçük öğrenme birimlerine ve kısa süreli faaliyetlere odaklanan bir öğretim tekniğidir (Neuhold & Lindner, 2007;Souza & Amaral, 2014); (d) kısa eğitim faaliyetleri için küçük, tutarlı ve kendi kendine yeten içeriği iletmek için dijital medyayı kullanan bir öğretim modelidir (Göschlberger, 2017); (e) kısa lokmalık derslerle tasvir edilen küçük parçalar halinde öğrenmedir (Jahnke vd., 2020); (f) özlü ve odaklanmış olacak şekilde tasarlanmış küçük öğrenme etkinliklerinden oluşan bir öğrenme sürecidir (Kadiev, 2021); (g) kısa eğitim faaliyetleri için küçük, tutarlı ve bağımsız içerik sunmak üzere dijital medyayı kullanan bir eğitim yaklaşımıdır (Hug, 2012); (ğ) da hedef ve sonuç odaklı, tek başına anlamlı bir öğrenme birimidir (Khan, 2019); (h) kısa, hedefe yönelik ve hızlı bir şekilde özümsenebilen ve öğrenilebilen öğrenme birimlerinden faydalanan teknoloji destekli bir öğrenme tarzıdır (Kovachev vd., 2011);

Ayrıca, Buchem ve Hamelman (2010), mikro öğrenmenin tanımını çeşitli kavramlara bağlayarak genişletmiştir; (a) mikro içerik: kısa ve öz bir biçimde sunulan bilgileri ifade eder; (b) Web 2.0: Mikro öğrenmenin açık ve parçalı bir dijital ortamda gerçekleştiği yer; (c) farklı geçmişlere, ilgi alanlarına ve öğrenme hedeflerine sahip öğrenciler arasında sosyal etkileşimi kolaylaştırma becerisi ile karakterize edilen sosyal yazılım; (ç) yapılandırılmış bir e-öğrenme ortamında da gerçekleşebildiği e-öğrenme 2.0; (d) öğrenenlerin bireysel öğrenme ortamına sahip olmalarını sağlayan kişisel öğrenme ortamı; (e) mikro öğrenmenin

dijital, mikro çoklu ortamlarında resmi yapıların ötesinde gerçekleştiği informal öğrenme ve (f) İş temelli öğrenme, mikro eğitimin kısa iş temelli eğitim formatlarına atıfta bulunabileceği iş temelli öğrenme ile de ilgilidir.

Mikro öğrenmenin öğrenme ve öğretimle doğrudan ilgili temel faydaları üzerine yapılan çalışmalar (Leong vd., 2021); (a) kavramların daha iyi hatırlanmasına yol açtığını (Giurgiu, 2017; Shail, 2019), (b) öğrenciler için daha iyi katılım sağlamaya yardımcı olduğunu (De Gagne vd., 2019; Nikou, 2019), (c) öğrencilerin motivasyonunu artırdığını (Nikou & Economides, 2018; Halbach & Solheim, 2018; Shail, 2019), (ç) işbirlikçi öğrenmede ilgi çekici ve yararlı olduğunu (Zhang & Ren, 2011) ve (e) öğrenme becerisini ve öğrenci performansını geliştirdiğini göstermektedir(Mohammed vd., 2018; Jomah vd., 2016).

Mikro öğrenme, mobil uygulamalardan video akışına ve oyunlara kadar farklı uygulamaları kapsamakta (Becker vd., 2015; Bogoch vd., 2012; Chaves vd., 2017; Lane vd., 2016) ve öğrencilerin kendi kendilerine öğrenmelerini motive etmektedir (Bell, 2010; Cosnefroy & Carré, 2014). Çoklu ortam materyallerinin örneklerinden videonun, mikro öğrenme stratejisi için etkili bir araç olduğu söylenebilir. Yousef ve arkadaşları (2014) videonun hem öğretim yöntemlerini hem de öğrenme çıktıları açısından mikro öğrenmede etkili bir araç olduğunu savunmuşlardır. Delen ve arkadaşları (2014) video tabanlı mikro öğrenme nesnelerinin geleneksel öğrenme ortamına kıyasla daha etkili bir araç olduğunu iddia etmişlerdir. Brecht ve Ogilby (2008) araştırmasında öğrencilerin %68,5'inin video temelli mikro öğrenme aracılığıyla daha iyi öğrenebildiğini belirtmişlerdir.

Mikro öğrenmenin aynı zamanda öz-yönetimli yaşam boyu öğrenmeyi güçlendirme (Buchem & Hamelmann, 2010) ve öğrenen özerkliğinin gelişimini destekleme potansiyeline sahip olduğu vurgulanmıştır (Nikou & Economides, 2018; Khong & Kabilan, 2022). Khong ve Kabilan (2022) bu öne çıkan özelliklerin, daha küçük parça boyutu, tek konu ve özerk mikro öğrenmenin öğrenme sürecine dahil edilmesinin daha kolay olduğuna işaret ettiğini belirtmişlerdir. Benzer şekilde, Jomah ve arkadaşları (2016), mikro öğrenmenin öğrenci

merkezli, erişimi kolay, etkileşimli ve iyi tasarlanmış özellikleri nedeniyle etkili bir öğrenme stratejisi olduğunu ifade etmişlerdir.

Her bir mikro öğrenme dersinin içeriğinin yüksek kalitede olması için, içeriğin konuyla ilgili, pratik olması ve öğrencilerin belirli bir dereceye kadar aşina oldukları bir dersi zorlaması önemlidir (Paul, 2016). Bu nedenle, mikro öğrenme dersleri öğrencilerin daha önce öğrendikleri dersleri daha iyi anlamalarını sağlayabilir. Bu durum, mikro öğrenme materyallerinin öğrenenler arasındaki etkileşimi teşvik edecek şekilde seçilmesinin ve öğrenenler arasında hem bireysel hem de iş birliğine dayalı çalışmaya olanak tanıyan mikro öğrenme görevlerinin tasarlanmasının önemini vurgulamaktadır.

Skalka ve Drlik (2018), uluslararası alan yazında, eğitim ortamlarında kullanılabilecek mikro öğrenme etkinlikleri üzerine deneysel çalışmaların yeterli düzeyde olmadığı olduğu belirtmiştir. Benzer şekilde, Trowbridge ve arkadaşları (2017) mikro öğrenme etkinlikleri için net bir kılavuz olmadığı tespit edilmiştir. Shabadurai ve arkadaşları (2022) mikro öğrenme perspektifinin ve içerik tasarımının hala bilinmediği de vurgulamıştır. Sankaranarayanan ve arkadaşları (2022) gerçekleştirdikleri bibliyometrik analizde, mikro öğrenmenin eğitimde önemli bir öğrenme stratejisi haline gelmeye hazır olduğu tespit edilmiştir. Leong ve arkadaşları (2021) mikro öğrenmeyi gelecek vaat eden bir araştırma alanı olarak görmektedir. Ulusal alan yazında, mikro öğrenme yaklaşımının sınıf içi öğrenme ve öğretme sürecine dahil edilmesine ilişkin sınırlı deneysel araştırma olduğu gözlemlenmiştir. Bunun nedenlerinden biri, mikro öğrenmenin örgün eğitimde nispeten yeni ancak gelişmekte olan bir yaklaşım olmasıdır.

Öğrenme nesneleri, öğrenenlerin yönetebildiği, etkileşim sağlanabilen ve uygun dönütler ve pekiştireçler verilebilen bilgi yığınlarının oluşturduğu öğrenme birim kümeleridir (Özkök & Yılmaz, 2020). Mikro öğrenme, öğrenme nesnesini küçük birimlere ayıran yenilikçi bir öğretim modeli olması nedeniyle, İlköğretim ikinci kademe Bilişim Teknolojileri ve Yazılım Dersi kapsamında, siber güvenlik farkındalığının öğrenilmesi ve öğretilmesinde tercih edilmiştir. Bu araştırma, mikro öğrenmenin temel yönlerini keşfederek siber güvenlik

farkındalığı eğitimi bağlamında nasıl başarılı bir şekilde uygulanabileceğine dair öngörü sağlamayı ve öğrenme çıktılarının iyileştirilmesini amaçlamaktadır. Siber güvenlik mikro-öğrenme nesneleri sınırlı öğrenme hedefleri ve kısa aktivitelerle mikro düzeyde organize edilmiş bir öğrenme stratejisi temelinde oluşturulmuştur.

Araştırmanın Amacı ve Önemi

Bu araştırmanın temel amacı, ilköğretim düzeyinde siber güvenlik mikro-öğrenme nesneleri tasarlamak, geliştirmek ve öğrencilerin siber güvenlik farkındalık düzeylerini, siber güvenlik farkındalık ölçütleriyle değerlendirmektir. Bu ölçütler; (a) E-postalardaki kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık; (b) E-postalardaki yazım hatası kaynaklı tehditlere yönelik farkındalık, (c) E-postalardaki şifre hedefli tehditlere yönelik farkındalık; (d) E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık'dir.

Araştırmada, Milli Eğitim Bakanlığı'nın (MEB, 2018) yayınlamış olduğu İlköğretim ikinci kademe Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programında; *6. Sınıf seviyesinde,* "Bilişim suçlarına karşı alınabilecek önlemler ve stratejiler geliştirir" hedefi (MEB, 2018) kapsamında geliştirilen *(a) E-postalardaki kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlerin farkına varabilme, (b) E-postalardaki yazım hatası kaynaklı tehditler farkına varabilme, (c) E-postalardaki şifre hedefli tehditlerin farkına varabilme, (ç) E-posta güvenlik ayarlarını kullanabilme* kazanımları odağında siber güvenlik mikro-öğrenme nesnelerinin geliştirilmesi amaçlanmıştır.

Siber güvenlik ile ilgili araştırma ve çalışmalar incelendiğinde, büyük kısmının teknik çözümlere odaklandığı, insan odaklı çalışmaların yeterli düzeyde olmadığı görülmektedir. Chou ve Jones (2018), siber güvenlik eğitiminin gerekliliğine vurgu yaparak, öğrencilere kuramsal ve uygulamalı siber güvenlik eğitiminin önemine dikkat çekmektedir. Örgün eğitimde, öğrencilere çeşitli teknolojileri kullanmayı öğretirken karşılaşabilecekleri tehditlere karşı farkındalık sağlanmaması önemli bir eksikliktir (Javidi & Sheybani, 2018). Bu nedenle, siber güvenliği farklı açılardan inceleyen araştırmalara ihtiyaç duyulmaktadır. Siber

Güvenlik Mikro-Öğrenme Nesneleri geliştirme ve değerlendirme araştırması, öğrencilerin siber güvenlik farkındalık düzeylerini belirleyeceği için alan yazındaki bu eksikliğe katkı sağlayacağı öngörülebilir.

Araştırma Problemi

Mikro-öğrenme stratejisini temel alan siber güvenlik öğrenme nesnelerinin tasarım ve değerlendirme süreci nasıl gerçekleşmiştir?

Alt Problemler

1. E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditler mikro-öğrenme nesneleri, öğrencilerin siber güvenlik farkındalıkları açısından ne düzeydedir?

2. E-postalarda yazım hatası kaynaklı tehditler mikro-öğrenme nesneleri, öğrencilerin siber güvenlik farkındalıkları açısından ne düzeydedir?

3. E-postalarda şifre hedefli tehditler mikro-öğrenme nesneleri, öğrencilerin siber güvenlik farkındalıkları açısından ne düzeydedir?

4. E-posta güvenlik ayarlarının kullanımı odaklı mikro-öğrenme nesneleri, öğrencilerin siber güvenlik farkındalıkları açısından ne düzeydedir?

5. Öğrencilerin, birinci ve ikinci mezo-döngü öğrenme-öğretme sürecinde tasarlanan siber güvenlik mikro-öğrenme nesnelerine yönelik olumlu ya da olumsuz görüşleri nelerdir?

Sayıltılar

Araştırmaya katılanların kullanılan veri toplama araçlarına samimi ve doğru cevaplar vereceği varsayılmıştır. Öğrencilerin, ait oldukları şubelerdeki diğer öğrencilerle benzer özelliklerde olduğu düşünülmektedir.

Sınırlılıklar

Araştırmanın uygulandığı sınıf bünyesinde bulunan bilgisayarlar sayılarının öğrenci sayılarına oranla azlığı öğrencilerin sürece katılımında motivasyonlarını olumsuz yönde etkilemiştir. Fiziksel imkanların yetersizliği öğrencilerin öğrenme nesnelerinin siber güvenlik farkındalığına etkisi açısından sınırlılık getirmiştir.

Tanımlar

Oltalama (Phishing). Saldırganın güvenilir birinin ya da kurumun kimliğine bürünerek alıcının bir bağlantıya tıklaması, kötü amaçlı bir dosyayı indirmesi ya da normalde paylaşmayacağı verileri paylaşmasını sağlamaya çalıştığı bir elektronik aldatma türü olarak tanımlanmaktadır (Coronges vd., 2012).

Sosyal Mühendislik. Hassas bilgileri açığa çıkarmak veya kısıtlı alanlara erişim izni vermek için kişileri etkilemek ve manipüle etmek olarak bilinir (Uebelacker & Quiel, 2014).

Bağlantı manipülasyonu (Link manipulation). Evrensel URL adreslerine benzer yanlış yazılmış URL adresleri saldırganlar (phishers) tarafından kullanılan aldatma yöntemlerinden biridir (Onashoga vd., 2019).

E-Posta/Spam. En yaygın kimlik avı tekniğidir. Milyonlarca kullanıcıya aynı e-posta gönderilir ve kişisel bilgilerin doldurulması istenir (Onashoga vd., 2019).

İnternet sitesi sahteciliği (Website forgery). Adres çubuğunu değiştirmek ve meşru bir web sitesinin içeriğini taklit etmek şeklinde yapılan oltalama saldırılarıdır (Onashoga vd., 2019).

SMS oltalama (SMSishing). Kısa Mesaj Hizmeti (SMS) yoluyla yapılan bir kimlik avı saldırısı biçimidir (Tchakounte vd., 2020).

Sesli oltalama (Vishing). Sesli arama yoluyla yapılan bir kimlik avı saldırısı biçimidir.

Mızrak oltalama (Spearphishing). Belirli bir kişi veya kuruluş grubuna yönelik olarak tasarlanan (Tchakounte vd., 2020), hedeflerin sınıflandırıldığı, kişiselleştirilmiş, belirli göndericileri taklit edebilen ve tespit sistemlerini atlamak için farklı teknikler kullanabilen saldırı türleridir (Al-Hamar & Kolivand, 2020)

Bölüm 2

Araştırmanın Kuramsal Temeli ve İlgili Araştırmalar

Bu bölümde araştırma da geliştirilen siber güvenlik odaklı mikro-öğrenme nesnelerini kapsayan kuramsal temele ve ilgili araştırmalara yer verilmiştir.

Araştırmanın Kuramsal Temeli

Mikro-Öğrenme

Mikro öğrenme, öğrenenlere kısa, kolayca sindirilebilir bilgi parçaları sunmaya odaklanan modern bir öğrenme yaklaşımıdır. Öğrencilerin ezici ve akılda tutulması zor olabilecek büyük miktarda bilginin aksine, kendilerine küçük parçalar halinde sunulduğunda bilgileri daha iyi tutabilmeleri fikrine dayanmaktadır. Zaman içinde küçük dozlara ayrılan bilgiye, öğrencilerin sürekli maruz kalmasını sağlar ve unutma oranını azaltır. Buna ek olarak, mikro öğrenme, insan zihninin bilgiyi işleme ve tutma kapasitesinin sınırlı olduğunu ve bilgiyi küçük, yönetilebilir parçalar halinde sunmanın daha etkili olduğunu belirtmektedir. Öğrenme içeriğinin genellikle kısa, odaklanmış dersler veya etkinlikler şeklinde küçük, yönetilebilir birimler halinde sunulmasını içeren pedagojik bir yaklaşımdır. Bu yaklaşım, öğrencilerin zaman ve dikkatlerine yönelik artan talepler, mobil cihazların yükselişi ve çevrimiçi öğrenme kaynaklarının mevcudiyeti nedeniyle son yıllarda popülerlik kazanmıştır.

Bilişsel kuram, mikro öğrenmenin dayandığı en etkili kuramlardan biridir ve mikro öğrenmenin dayandığı önemli bir kuramda "unutma eğrisi/forgetting curve "dir (Ebbinghaus, 1885). Bu kuram, insanların zaman içinde bilgiyi unutma eğiliminde olduğunu ve unutma oranının, bilginin tüketilmesinden sonraki ilk birkaç gün içinde en yüksek olduğunu belirtir. Bu, "aralık etkisi/spacing effect" olarak bilinir (Ebbinghaus, 1885), burada bilgi bir kerede sunulmak yerine zamana yayıldığında daha kolay tutulur. Mikro öğrenme, bilgiyi zaman içinde sunulabilecek daha küçük, yönetilebilir parçalara ayırarak bu ilkeden yararlanır ve öğrencilerin bilgiyi daha iyi tutmasına ve hatırlamasına olanak tanır.

Mikro-öğrenme, küçük öğrenme birimlerine ve kısa süreli etkinliklere dayanan bir öğrenme yaklaşımıdır. (Hug vd., 2005; Lindner, 2007; Nikou & Economides, 2017) Bu kullanışlı küçük adımlı öğrenme, “mobil cihazların her yerde bulunmasını, yakınlığını ve kullanılabilirliğini” güçlendirir (Bruck vd., 2012) günümüzün yoğun çalışma ortamında aşırı bilgi yükünü önlemek için “işle bütünleşik öğrenmeyi” (Decker, vd., 2017) desteklemektedir (Khong & Kabilan, 2022).

Mikro öğrenmenin modern tanımı, mikro öğrenmenin, bilgi ve uygulamaya yönelik etkileşimli aktiviteleri içeren küçük parçalar halinde öğrenmeyi sağlayan aktivite odaklı bir yaklaşım olduğunu belirtmektedir. Mikro-öğrenme, eğitim içeriğini kısa, iyi planlanmış birimler halinde, genellikle öğrencinin uzun süreli dikkatini gerektirmeyen mobil uygulamalar aracılığıyla sunar (Skalka vd., 2021). Mikro-öğrenmede öğrenciler öğrenmelerindeki ilerlemeyi kontrol ederler ve öğrenme içeriğine zaman ve mekan kısıtlaması olmaksızın mümkün olduğunca sık erişilebilirler (Reynolds & Dolasinski, 2020). Shail'e (2019) göre mikro öğrenme, öğrencinin beyninin bilgiyi alma şeklini taklit eden küçük bilgi parçacıkları sunar ve mikro-öğrenme içeriğinin kısa süresi, daha uzun derslerden kaynaklanan bilişsel yorgunluğu azaltır. Giurgiu (2017) tarafından yapılan bir araştırma, öğrenme içeriğini küçük parçalar halinde sunmanın bilginin kalıcılığını %20 artırdığını ortaya çıkarmıştır. Bu nedenle mikro öğrenme, öğrenme deneyimini ve sonuçlarını geliştiren umut verici bir öğrenme dağıtım yöntemi gibi görünmektedir (Nikou, 2019).

Hug (2005) mikro öğrenmeyi yedi boyuta dayalı bir öğretim çerçevesi olarak tanımlamıştır. Bu boyutlar; (1) Kısa ölçülebilir zaman, çaba ve zaman tüketiminin derecesi olan öğrenme süresi, (2) Küçük öğrenme üniteleri, basit konular ve dar konular içeren öğrenme içeriği, (3) Modüller setini ve informal öğrenme gibi öğrenme modelinin türünü ifade eden müfredat, (4) Parçalara, bölümlere ve bilgi kırıntılarına odaklanan öğrenme formu, (5) Ayrı, bağlantılı, konumlandırılmış veya entegre faaliyetlere odaklanan öğrenme süreci, (6) Öğrenme nesneleri, yüz yüze ve multimedya kullanan öğrenme ortamı ve (7) Davranışçı, yapılandırmacı ve sosyal öğrenme perspektiflerini içeren öğrenme tipidir.

Mikro öğrenme parçacıklarının tasarlanması, geliştirilmesi, uygulanması ve değerlendirilmesi beklenen öğrenme çıktılarına ulaşmak için bir çerçeveye uyması gerekmektedir (Berkowitz, 2017). Bu amaçla, Khan (2019) bir dizi standardizasyon ilkeleri sıralamıştır. Bu ilkelere göre, rastgele üretilen her bilgi parçası veya küçük bileşen mikro-öğrenme olarak adlandırılmaz. Bu ilkeler; 1) pedagojik (öğretme, öğrenme ve öğrenme çıktıları ile ilgili, etkileşim ve katılım), 2) teknolojik (öğrenme ortamı, yazılım ve mobil bilgisayarlar), 3) arayüz tasarımı (kullanım kolaylığı, gezinilebilirlik, mobil uyumluluk), 4) değerlendirme (tek öğrenme hedefi; öğrenenler ve değerlendirilebilir ve izlenebilir çıktılar), 5) yönetim (tasarım ve yeniden tasarım için yönetilebilirlik), 6) Kaynak desteği (dijital kütüphaneye uygunluk, arşivleme, eğitimler, podcastler, bağlantılar, belgeler ve sözlükler), 7) etik (çeşitlilik, erişilebilirlik, siyasi ve sosyal açıdan tarafsızlık, kişisel haklar, telif hakları konuları), 8) kurumsal (kurumsal destek, sorumluluk alma ile ilgili ve maliyet etkinliği) olarak sıralanır.

Polasek ve Javorcik (2019) tarafından yapılan bir çalışmada, bilgisayar mimarisi ve işletim sistemi temellerinin öğretilmesinde mikro öğrenme uygulaması araştırılmıştır. Bu çalışmada, geleneksel ders tabanlı bir sınıfa ya da mikro öğrenme sınıfına rastgele atanan 26 birinci sınıf öğrencisi, final sınavında geleneksel ders tabanlı sınıftakilere göre daha iyi performans göstermiştir. Mikro öğrenme sınıfında ayrıca daha yüksek öğrenci katılımı ve memnuniyet seviyelerinin yanı sıra daha düşük stres ve kaygı seviyeleri tespit edilmiştir. Araştırmacılar, mikro öğrenmenin etkili bir öğretim yaklaşımı olabileceği ve öğrencilerin öğrenme çıktılarını ve katılımını artırma potansiyeline sahip olduğu sonucuna varmıştır.

Han (2019) tarafından yapılan bir başka çalışmada, North China Electric Power Üniversitesi'nde İngilizce bilmeyen öğrencilerinin öğrenme çıktılarını iyileştirmek için, kolayca anlaşılabilir ve akılda kalıcı olacak şekilde tasarlanmış kısa, özlü dersler verme yöntemi olan mikro öğrenme incelenmiştir. Araştırmacı, ana dili İngilizce olmayan 70 öğrenciyle bir çalışma yürütmüş ve mikro-ders öğretiminin öğrencilerin İngilizce dinleme ve konuşma becerileri üzerinde önemli bir olumlu etkisi olduğunu tespit etmiştir. Araştırmacı,

mikro-ders yönteminin öğrencilerin öğrenme çıktılarını iyileştirmek isteyen eğitimciler için faydalı bir araç olabileceğini öne sürmüştür.

Zarshenas ve arkadaşları (2022), mikro-öğrenmenin hemşirelik öğrencilerinin öğrenme ve öz yeterlilikleri üzerindeki etkisini araştırmıştır. Araştırmacılar, hemşirelikle ilgili belirli konularda kısa ve odaklanmış öğrenme modülleri alan bir mikro öğrenme grubuna rastgele atanan 64 hemşirelik öğrencisini içeren girişimsel bir çalışma yürütürken, yüzyüze kontrol grubu geleneksel yüzyüze eğitim almıştır. Araştırmacılar, katılımcıların öğrenme çıktılarını ve öz yeterlilik düzeylerini müdahaleden önce ve sonra ölçmüştür. Sonuçlar, mikro-öğrenme grubunun yüzyüze kontrol grubuna göre önemli ölçüde daha yüksek öğrenme çıktılarına ve öz yeterlilik düzeylerine sahip olduğunu göstermiştir. Mikro öğrenme grubu ayrıca yüzyüze kontrol grubuna kıyasla daha yüksek düzeyde katılım ve motivasyon bildirmiştir. Araştırmacılar, mikro öğrenmenin öğrenciler için etkili bir öğretim yöntemi olabileceği ve öğrenme çıktılarını ve öz yeterliliklerini geliştirebileceği sonucuna varmıştır.

Kasuma ve diğerleri (2021) tarafından daha önce yapılan bir diğer çalışmada, öz yeterliliğin öğrencilerin öğrenme başarısında kilit bir faktör olduğu, özellikle de öz yeterlilik düzeyi yüksek olan öğrencilerin daha ilgili ve motive oldukları ortaya konmuştur. Çalışmada, mikro öğrenmenin eğitime dahil edilmesinin öğrenciler için daha verimli ve etkili öğrenme deneyimleri sağlayabileceğini öne sürülmüştür. Burada incelenen bulgular, mikro öğrenmenin özellikle örgün eğitim, yükseköğretim ve mesleki gelişim bağlamlarında bilgi kalıcılığını artırmak için etkili bir yöntem olabileceğini göstermektedir. Bunun nedeni, öğrenme içeriğini anlaşılması ve akılda tutulması kolay küçük, yönetilebilir birimler halinde sunma kabiliyetinin yanı sıra esnekliği ve rahatlığı gibi diğer ek faydalardır. Bununla birlikte, mikro öğrenme pedagojisinin en uygun tasarımını ve uygulamasını belirlemek ve bağlam ve öğrenci popülasyonu açısından nasıl değişebileceğini anlamak için daha fazla araştırmaya ihtiyaç vardır.

Shabadurai ve arkadaşları (2022) özel bir üniversitede çalışanların çevrimiçi eğitimi için mikro boyutlu içerik tasarımını araştırmıştır. Anket ve odak grup görüşmesine

dayanarak, video öğesinin mikro öğrenmenin en popüler öğesi olarak kabul edildiğini, bunu statik metin ve infografiklerin izlediğini bulmuşlardır. Bunun yanı sıra, çalışma aynı zamanda mikro öğrenme için ideal mikro boyutlu içerik uzunluğunu da belirlemiştir; bu uzunluk 5-7 dakika arasındadır, bunu 7-10 dakika ve 3-5 dakika takip etmektedir. Verilere göre, çalışmaya katılanlar en az ilgiyi ortalama üç dakikadan kısa olan daha kısa içeriklere göstermiştir. Çalışmaya katılanlar ayrıca "kısa sürenin" mikro öğrenmenin en avantajlı özelliği olduğunu ve bunu odaklanmış, bağımsız, etkileşimli ve duyarlı diğer özelliklerin izlediğini düşünmektedir.

Choo ve Abdul Rahim (2021) eczacılık öğrencilerinin mikro öğrenmeye ilişkin algılarını ve performanslarını araştırmıştır. Konuları daha küçük parçalara ayırarak ve Google Formlar aracılığıyla çevrimiçi sınavlarla öğrenme performansını değerlendirerek bir mikro öğrenme yaklaşımı kullandılar. Bu, bilginin öğrenciler için hızlı, özlü ve konu merkezli olacak şekilde uyarlanabilen kısa öğrenme içeriği aracılığıyla sunulduğu mikro öğrenmenin odaklanmış özelliği ile uyumluğu olduğunu tespit etmişlerdir.

Chai-Arayalert ve Puttinaovarat (2020), öğrencilerin sınırlı dikkat süreleri nedeniyle uzun süre çalışmaya zorlanmadıklarında mikro öğrenmenin sonuçlarının daha iyi olduğunu bulmuştur. Kapsamlı içeriğin öğrencilerin sıkılmasına ve içeriği tam olarak anlayamamasına neden olabileceğini bulmuşlardır. Bu bulgu, içerik tasarımı perspektifinden bakıldığında, mikro öğrenmenin, isteğe bağlı içerik edinimini kolaylaştırmadaki pratikliği ve çeşitliliğine ek olarak, esas olarak içeriğin hızlı bir şekilde alınmasındaki verimliliği açısından yararlı olduğunu göstermiştir.

McKee ve Ntokos (2022) çevrimiçi mikro öğrenmenin bilgisayar oyunları yükseköğretiminde öğrenci katılımı üzerindeki etkisini incelemiştir. Çalışma, iki öğrenci grubunu karşılaştırmak için yarı deneysel bir tasarım kullanmıştır: biri mikro öğrenme tabanlı eğitim alırken, diğeri geleneksel ders tabanlı eğitim almıştır. Araştırmacılar, bir anket ve öğrenci davranışlarının gözlemlenmesiyle ölçüldüğü üzere, mikro öğrenme temelli eğitimin öğrenci katılımı üzerinde olumlu bir etkisi olduğunu bulmuşlardır. Çalışma ayrıca, daha kısa

video içeriğinin, daha uzun videolara kıyasla öğrenci katılımı üzerinde daha büyük bir etkiye sahip olduğunu buldu. Araştırmacılar, mikro öğrenme temelli öğretimin, bilgisayar oyunları yükseköğretiminde öğrenci katılımını artırmak için etkili bir yaklaşım olabileceği ve daha kısa videoların öğrenciler arasında katılımı teşvik etmede daha etkili olabileceği sonucuna varmıştır.

Park ve Kim (2018) e-öğrenme sisteminde mikro öğrenme içeriğinin tasarımını ve geliştirilmesini araştırmıştır. Çalışma, mevcut e-öğrenme yöntemlerini değiştirmek ve öğrencilerin öğrenme zamanını ve ortamını dikkate alan kişiselleştirilmiş içerik oluşturmak amacıyla çeşitli tasarım ve geliştirme stratejileri sunmuştur. Mevcut müfredattaki mikro öğrenme içeriğini öğrenme materyalleri olarak kullanmak ve normal müfredatı mikro öğrenme ile değiştirmek için, çalışma akılda tutulması gereken birkaç önemli faktörü vurgulamıştır. İlk olarak, mikro öğrenme içeriği geliştirme, kısa bir ünite ile öğrenme konusunun tek bir temasına sahip olacak şekilde tasarlanmalıdır; örneğin, 10 dakikayı geçmeyen kısa bir etkileşimli video. İkinci olarak, bu çalışma aynı zamanda öğrencilerin bağlamıyla ilgili ve uygun mikro öğrenme içeriklerinin geliştirilmesinin önemini vurgulamıştır.

Pascual ve arkadaşları (2020) çalışmalarında, mikro öğrenme yaklaşımının öğrencilerin öğrenme performansını artırmadaki etkinliğini göstermiştir. Çalışmada, mikro öğrenme derslerinde TED konuşma videoları, dergi makaleleri ve belgeseller kullanılmıştır. Çalışma, mikro öğrenme dersi için materyal seçiminde temel faktörleri vurgulamıştır. İlk olarak, destek materyalinin öğrencilerin zaten aşina oldukları kavramları pekiştirmesi gerekmektedir. İkinci olarak, mikro öğrenme dersinin amacı öğrencilerin ilgisini çekmek ve öğrenme içeriğiyle daha fazla ilgilenmelerini sağlamak olduğundan, materyaller hedeflenen öğrenciler için çekici olmalıdır.

Siber Güvenlik

Son yıllarda, siber güvenlik kavramı, teknolojik gelişmelerdeki hızlı yükselişin etkisiyle toplumların giderek daha fazla birbirine bağlı hale gelmesiyle önem kazanmıştır.

Bilgi ve İletişim Teknolojilerindeki (BİT) yenilikler günlük hayatımıza kolaylık getirirken, kişisel bilgilerin güvenliğine yönelik tehditleri de artırmaktadır. Elektronik sistemlerin kötü niyetli saldırılardan korunmasını kapsayan siber güvenlik, bilgisayarları, ağları, sunucuları, mobil cihazları ve saldırı sonrası veri kurtarmayı kapsayan kritik bir uygulama haline gelmiştir (Poepjes & Lane, 2012).

Siber güvenliğin önemi, kişisel bilgilerin korunması, verimliliğinin sürdürülmesi ve kurum ve kuruluşlara güven duymasının sağlanmasındaki rolü ile vurgulanmaktadır. Siber güvenliğin kökleri, İnternet'ten önce ARPANET'in kurulduğu 1970'li yıllara kadar uzanmaktadır (Simonet & Teufel, 2019). Bu tarihlerden günümüze Uygulama güvenliği, Ağ güvenliği, Güvenlik ve Nesnelerin İnterneti güvenliği olarak kategorize edilen farklı tehditleri ele almak için gelişmiştir. Siber güvenlik yalnızca verilerin güvenliğini sağlamak için değil, aynı zamanda hassas bilgiler, kişisel olarak tanımlanabilir bilgiler, korumalı sağlık bilgileri, kişisel veriler ve fikri mülkiyet saldırıları dahil olmak üzere çeşitli veri türlerinin çalınmasına ve silinmesine karşı koruma sağlamak için de gereklidir (Skripak vd., 2020). Dahası, bilgi güvenliğinin ötesine geçerek fiziksel bilgilerin korunmasını da kapsar (Villanueva vd., 2020).

Siber güvenliğin temel amaçları arasında operasyonel teknolojik sistemlerin güvenliğini artırmak, bilgi güvenliği tehditlerini ele almak, işbirliği etkileşimleri için güvenilir bir ortam yaratmak, elektronik saldırılara karşı altyapı dayanıklılığını sağlamak, siber suçları azaltmak, elektronik sistemlerdeki kusurları ortadan kaldırmak, bilgi güvenliği sistem kusurlarını onarmak ve bireyleri yeni siber saldırı teknikleri ve yöntemleri konusunda eğitmek yer almaktadır (Hadlington & Parsons, 2017; Pawlowski & Jung, 2015). Etkili siber güvenlik, temel unsurların bir araya gelmesine dayanır. Teknoloji, önlemler kullanarak siber saldırılara karşı üstün koruma sağlamada çok önemli bir rol oynamaktadır. Bireyler, temel veri koruma ilkelerine uyma, güçlü parolalar kullanma ve potansiyel risklerden kaçınma konusunda hayati bir rol oynamaktadır. Hem bireysel hem de teknolojiler tarafından yönetilen operasyon ve faaliyetleri içeren süreçler, siber güvenlik temellerinin uygulanmasına katkıda bulunur (Poepjes & Lane, 2012).

Farklı alanlara odaklanan farklı siber güvenlik modelleri:

1) Ağ güvenliği (bilgisayar ağlarının istilacı ve fırsatçı bileşenlere karşı korunması),

2) Uygulama güvenliği (Yetkisiz erişimi önlemek için cihazların ve programların güvenliğinin sağlanması) ve

3) Bilgi güvenliği (depolama aşamalarında verilerin bütünlüğünün ve gizliliğinin korunması) (Skripak vd., 2020).

Üst düzey siber güvenlik sağlamak için bilgi dosyalarının düzenli olarak yedeklenmesi, kişisel bilgiler için güvenilir web sitelerinin kullanılması, e-posta eklerinden veya bilinmeyen kaynaklardan gelen bağlantılardan kaçınılması, donanımın güvenlik yamaları ile güncel tutulması ve güvenli internet kullanımı kültürünün teşvik edilmesi gibi çeşitli mekanizmalar ve gereksinimler önerilmektedir (Poepjes & Lane, 2012). Siber güvenlik farkındalığı, bireyin öz verilerinin gizliliğini, kişilerin kimliklerini ve siber suçlulara karşı savunmasız olan diğer varlıkları korumanın önemini anlamaları için eğitilmesini içerir. İnternet kullanımı, e-posta iletişimi ve çevrimiçi etkileşimlerle ilgili riskleri ele alır. Siber farkındalık eğitimi, kullanıcılarla ilgili güvenlik ihlallerinin önlenmesinde, siber güvenlik kültürünün geliştirilmesinde ve olası siber saldırılara karşı hazırlık yapılmasında çok önemlidir (Pawlowski & Jung, 2015).

Siber güvenlik eğitimi, internet kullanıcılarının veri ihlallerini hızlı bir şekilde tespit edebilmeleri ve bunlara müdahale edebilmeleri için gereklidir (Eminağaoğlu vd., 2009). Siber güvenlik farkındalığı eğitimi, bireylere bir kurumun bilgisayar sistemlerini, verilerini, paydaşlarını ve diğer varlıklarını çevrimiçi tehditlerden ve suç faaliyetlerinden nasıl koruyacaklarını öğreten formal bir süreçtir (Poepjes & Lane, 2012). Siber güvenlik eğitiminin hedefleri arasında siber güvenlik olaylarına müdahalenin iyileştirilmesi, ihlallerin azaltılması, güvenlik araçlarının etkinliğinin artırılması, paydaşların uzmanlığının geliştirilmesi ve ortaya çıkan siber tehditlerin anlaşılması yer almaktadır (Cain vd., 2018). Siber güvenlik farkındalığının sağlanması, davranışsal bir referans noktası oluşturmayı, güvenlik

önlemlerini etkinleştirmeyi ve en başından itibaren davranışı güvence altına almayı içerir (Al-Janabi & Al-Shourbaji, 2016). Siber güvenlik farkındalık eğitimi yoluyla, genel güvenlik riskini azaltmak, siber suçlardan kaynaklanan mali kayıpları en aza indirmek, bireylerin kurumdan ayrıldığında güvenlik açıklarını önlemek ve paydaşları nezdinde olumlu bir itibar sağlamada yer alması sayılabilir (Garba vd., 2020).

Siber suçların maliyetinin giderek artması, siber güvenlik farkındalığını ve önleyici tedbirleri giderek daha önemli hale getirmektedir (Amao, 2015). Paylaşılan bilgilerin bu tehditlerden korunması, Bilgi Güvenliği Yönetimi yönergeleri doğrultusunda siber güvenlik önlemlerinin uygulanmasını gerektirir (Furnell & Vasileiou, 2022). Siber güvenliğin önemi, kişisel bilgilere yönelik artan tehditler ve verilerin, ağların ve bireylerin korunmasındaki kritik rolü ile vurgulanmaktadır. Uzaktan eğitimin büyümesi ve çevrimiçi platformlara olan güvenin artmasıyla birlikte, riskleri azaltmak ve dijital ortamların güvenliğini sağlamak için siber güvenlik farkındalığı daha da hayati hale gelmektedir.

Siber güvenlik, elektronik verilerin suç teşkil eden veya yetkisiz kullanımına karşı korunma durumu veya bunu başarmak için alınan önlemlerdir (Oxford University Press, 2014). Siber güvenlik, bilgi ve iletişim sistemleri ile bunların içerdiği bilgilerin hasara, yetkisiz kullanıma veya değişikliğe ya da keşfe karşı korunduğu ve/veya savunulduğu faaliyet, süreç, yetenek veya durum olarak da tanımlanabilir. Dolayısıyla siber güvenliğin bu çağda çok önemli bir faktör olduğu ve dijital dönüşüm çağında kritik bir hale geldiği söylenebilir (Ahmed vd., 2019; Ricci vd., 2019).

Siber güvenlik, bilgisayar bilimlerinden ortaya çıkmış, ancak diğer birçok alanda önemli bir endişe kaynağı haline gelmiştir. Siber güvenlik eğitimi ve beceri kazandırma tüm kamu ve özel kuruluşlar için kaçınılmaz bir gereklilik haline gelmiştir. Yakın zamanda gerçekleşen uluslararası siber saldırılar nedeniyle bu çaba milyarlarca dolar maddi zarara ve milyonlarca insan saatine mal olmuştur. Bu nedenle siber güvenlik eğitiminin K-12'de başlamasının gerekli olduğuna inanılmaktadır (Javidi & Sheybani, 2018). Yeni neslin siber

farkındalık sahibi olabilmesi için siber tehditler ve riskler konusunda sağlam bir temele sahip olmaları gerekir (Javidi & Sheybani, 2018).

İlgili Araştırmalar

Bu bölümde çalışmaya örnek olabilecek ilgili araştırmalara yer verilmiştir. Alan yazında Siber Güvenlik Eğitimi ile ilgili sınırlı sayıda araştırma bulunmaktadır. İlgili araştırmalara ISI Web of Science, EBSCOhost, Science Direct, ERIC ve Google Akademik üzerinden tarama yapılarak ulaşılmıştır. Söz konusu tarama yapılırken “Siber Güvenlik”, “Kimlik Avı”, “Mikro-öğrenme” anahtar sözcüklerinden yararlanılmıştır. Yapılan aramalar sonucunda tam metnine erişim sağlanan ve Siber Güvenlik bağlamlarından en az birini temel alan son 10 yılda gerçekleştirilmiş çalışmalar, aşağıda verilen ilgili başlığın altında eski tarihten yeni tarihe doğru özetlenmiştir.

Case ve King (2016) üniversite öğrencilerinin kimlik avına karşı hazır olup olmadıklarını ve risk altında olup olmadıklarını incelemiştir. Çalışma işletme fakültesi öğrencilerinin, gelecekte çalışacağı kurum ya da kuruluşlarda, çalışacakları işe yönelik yapılacak olan kimlik avı saldırılarının hedefleri olacağı düşüncesiyle, öğrencilerin kimlik avı saldırıları ile ilgili olarak eğilimlerini incelemek amacıyla yapılmıştır. Bu kapsamda araştırmacılar tarafından bir Elektronik Posta Davranışı (Electronic Mail Behavior) aracı geliştirilmiş ve ABD’de bulunan bir üniversitenin işletme fakültesi derslerine kayıtlı lisans öğrencilerine uygulanmıştır. Araştırmada kullanılan veriler beş yıl boyunca her yarıyılda anket uygulanarak toplanmıştır. Toplamda 1.668 öğrenciden elde edilen verilerle, çalışmanın her yılında kredi kartı kimlik avı e-postalarının öğrenciler arasında en yaygın saldırı türü olduğu bulgusuna ulaşılmıştır. Kimlik avı e-postasına yanıt verenler incelendiğinde, cinsiyet ile alınan kimlik avı e-postası miktarının, kimlik avı yanıtlama davranışı ile bilgi açısından anlamlı korelasyonlara sahip olduğu görülmüştür.

Sun ve Chen (2016) e-posta hedefli siber tehditleri önleme eğitiminde dinamik kavram haritalarının interaktif yanıt sistemi ile entegre edilmesinin ilkokul öğrencilerinin

motivasyonu ve öğrenme çıktıları üzerindeki etkisini incelemiştir. İnteraktif yanıt sistemi aracılığıyla dinamik kavram haritası oylama soruları sunarak öğrencilerin kendi sorularıyla ilgili bilgi kavramı çerçevesini daha iyi anlamalarına yardımcı olmayı, bölünmüş dikkat etkisini azaltırken öğrencilerin optimum etkililik için öğrenme ortamına odaklanmasına yardımcı olmayı amaçlamışlardır. 130 beşinci sınıf öğrencisi geleneksel resim ve metin materyallerinin kullanıldığı 21 erkek ve 22 kız öğrencinin bulunduğu toplam 43 öğrenciden kontrol grubu, statik kavram haritalarının kullanıldığı 22 erkek ve 21 kız öğrencinin bulunduğu toplam 43 öğrenciden oluşan deney grubu I ve dinamik kavram haritalarının kullanıldığı 21 erkek ve 23 kız öğrencinin bulunduğu toplam 44 öğrenciden oluşan deney grubu II olmak üzere üç gruba ayrılmıştır. Öğrenme motivasyonunu ölçmek için, Michigan Üniversitesi'nde Ortaöğretim Sonrası Öğretim ve Öğrenimin Geliştirilmesine Yönelik Ulusal Araştırma Merkezi tarafından geliştirilen Motivasyona Yönelik Öğrenme Stratejileri Anketinden (Motivated Strategies for Learning Questionnaire- MSLQ) öz yeterlilik ve içsel değer ölçeğini uyarlanarak 6'lı likert tipi bir ölçek kullanılmıştır. Oltalama saldırılarına karşı öğrenme başarısını ölçmeye yönelik test çalışmayı gerçekleştiren araştırmacılar tarafından eğitim materyalinin içeriğine bağımlı olarak oluşturulmuş ve 10 adet doğru/yanlış sorusu ve 18 adet çoktan seçmeli soru içermektedir. Sonuçlar, kimlik avını önleme eğitimi sırasında interaktif yanıt sistemi ile dinamik kavram haritalarının kullanılmasının, başlangıçtaki öz yeterlilikleri yüksek olan öğrencilerin öğrenme öz yeterliliğini önemli ölçüde artırdığını göstermiştir. Başlangıçta öz-yeterliği düşük olan öğrenciler için interaktif yanıt sistemi ile geleneksel resimli metinlerin kullanılması test sonrası öz yeterliliğin artmasına yardımcı olmuştur. Dinamik kavram haritaları grubundaki öğrencilerin başarısının, geleneksel resim-metin grubuna göre önemli ölçüde daha yüksek olduğu sonucuna varılmıştır. Bulgular, sınıfta interaktif yanıt sistemi ile dinamik kavram haritalarının kullanılmasının öğrencilerin öğrenme süreci üzerinde olumlu bir etkiye sahip olduğunu göstermektedir. Benzer stratejileri uygularken öğrencilerin başlangıçtaki öz yeterliklerinin de dikkate alınmasının önemli olduğu vurgulanmaktadır.

Sun ve Lee (2016) oltalamaya karşı öğrenme motivasyonunu ve başarısını artırmak için tablet PC'lerdeki kavram haritaları ile çalışma sayfalarının hangisinin daha etkili olduğunun karşılaştırıldığı bir araştırma yapmıştır. Çalışmanın amacı, öğrencilerin öğrenme motivasyonunu ve başarısını artırmak için kavram haritaları ve tablet PC'lerin kimlik avı önleme eğitimine entegrasyonunun uygulanabilirliğini değerlendirmektir. Sekizinci ve dokuzuncu sınıflardan öğrenim gören 155 öğrenciden oluşan katılımcılar, 77 öğrenciden oluşan deney grubu ve 78 öğrenciden oluşan kontrol grubu olarak ikiye ayrılmıştır. İki grup başlangıçta oltalamaya karşı aynı eğitimi almıştır. İkinci aşamada deney grubu kavram haritaları ile tablet PC de çizim yaparken kontrol grubu çalışma sayfalarını tamamlamıştır. Veri toplama aracı olarak 31 sorudan oluşan 7 puanlık likert tipi bir ölçek olan ve Motivasyona Yönelik Öğrenme Stratejileri Anketinden (Motivated Strategies for Learning Questionnaire- MSLQ) uyarlanan Oltalamaya Karşı Öğrenme Motivasyon Anketi kullanılmıştır. Çalışma, kimlik avını önleme eğitimi sırasında tablet PC'lerde kavram haritalarının kullanılmasının, başlangıçtaki motivasyonları yüksek olan öğrencilerin öğrenme motivasyonunu önemli ölçüde artırdığını ortaya koymuştur. Başlangıç motivasyonu veya ön bilgisi düşük olan öğrenciler için çalışma sayfalarının kullanılmasının son test başarılarını ve motivasyonlarını artırabileceğini vurgulanmıştır. Çalışma müfredatın, erişilebilir teknolojik medyanın öğrenme etkinliklerine entegrasyonuyla birlikte öğrencilerin öğrenme tercihlerine veya ön bilgilerine göre tasarlanması durumunda, kimlik avına karşı koruma kavramının öğretilmesindeki motivasyon ve başarının etkili bir şekilde artırılabileceği sonucunu ortaya çıkarmıştır.

Muniandy ve arkadaşları (2017), çalışmalarında Malezya’daki yükseköğrenim öğrencilerinin siber güvenlik davranışlarını incelemiştir. Bu amaçla, Malezya’daki yüksek öğrenim öğrencileri arasında kötü amaçlı yazılım, şifre kullanımı, kimlik avı, sosyal mühendislik ve çevrimiçi dolandırıcılık açısından siber güvenlik davranışlarının durumu ölçülmüştür. Öğrencilerin demografik bilgilerini ve siber güvenlik davranışlarını ölçen, Siber Güvenlik Davranış Ölçeği 128 öğrenciye uygulanmıştır. Araştırma, katılımcıların incelenen

beş siber güvenlik değişkeninin tamamında genel olarak yetersiz olduğunu göstermektedir. Bulgulara göre, katılımcıların davranışları beş siber güvenlik değişkeninin tamamında önemli ölçüde savunmasız olduğunu ve davranışları onların siber güvenlik tehditlerine maruz bırakabileceğini ortaya koymaktadır.

Sun ve arkadaşları. (2017) çalışmalarında, kimlik avını önlemeye yönelik bir eğitsel dijital oyun ile öğrencilerin sıralı davranış kalıplarını, akış deneyimini ve öğrenme performansını araştırmışlardır. Bu kapsamda, ilkokul öğrencilerine oyun tabanlı kimlik avı önleme dersi vererek, onların öğrenme davranış kalıplarını keşfetmeyi ve akış durumlarının öğrenme davranış kalıpları ve öğrenme başarıları üzerindeki etkilerini araştırmayı amaçlamışlardır. Çalışmada, Tayvan'da bir ilkokulda eğitim görmekte olan 110 öğrenciye oyun tabanlı kimlik avı ile mücadele dersi yapılmıştır. Ders kapsamında öğrenme davranış kalıpları ve öğrenme başarıları açısından öğrenciler arasındaki farklılıklar incelenmiştir. Araştırmada kullanılan veriler, eğitimden önce uygulanan sosyal ağlar ile ilgili kimlik avı bilgisine yönelik ön test, ders esnasında öğrenciler tarafından kullanılan oyun tabanlı öğrenme sisteminin log kayıtları, ders sonrasında uygulanan sosyal ağlar ile ilgili kimlik avı bilgisine yönelik son test ve akış durumu anketi ile toplanmıştır. Araştırmanın davranış kalıplarına yönelik bulguları, öğrencilerin hatalarından ders alma eğiliminde olduklarını göstermiştir. Akış durumlarına göre, akış grubunda yer alan öğrencilerin, başarısız bir oyunun ardından sonuçları akranlarıyla tartışma davranışını ve ardından ders materyalini okuma davranışını sergileyebildiği ve öğrenme görevinde başarılı olana kadar bu davranışları tekrarlamaya devam edebildiği görülmüştür. Kaygı grubunda yer alan öğrenciler de akranlarından yardım istemiş, okuma materyallerine başvurmuş, başarılı olana kadar bunu tekrarlamış ancak akış grubundan farklı olarak öğrendiklerini doğrulama davranışını göstermemiştir. Sıkılgan gruptaki öğrenciler ise akranlarına ve okuma materyallerine daha az güvenen bir davranış sergilemiş ve onlarda başarılı olana kadar tekrar tekrar denemeye devam etmişlerdir. Sonuçlar, öğrenenlerin tekrarlanan bir oyun

davranış kalıbı aracılığıyla deneme yanılma yoluyla korsan sitelere karşı bilgi edinebileceklerini göstermiştir.

Perrault (2018), araştırmasında üniversite öğrencilerinin kimlik avına ilişkin tutumlarını ve davranışsal niyetlerini ayarlamak için çevrimiçi bir test kullanmıştır. Araştırmada, eğitimcilerinin ve öğrencilerin kimlik avı konusundaki tehdit algısını ve gelecekteki kimlik avı girişimlerini belirleme konusundaki güvenlerini artırmaya yardımcı olmak için kullanabilecekleri yeni ve uygun maliyetli bir strateji belirlemesi amaçlanmıştır. Bu amaçla, çevrimiçi kimlik avı testinin öğrencilerin algılanan tehdit, öz yeterlilik ve kimlik avı hakkında daha fazla bilgi edinme niyetleri üzerinde nasıl bir etkisi olduğu ve çevrimiçi kimlik avı testinin öğrencilerin kimlik avı kavramını başkalarıyla tartışma niyetleri üzerinde ne gibi bir etkisi olduğu incelenmiştir. ABD'de bir üniversitedeki 462 öğrenci çalışmaya katılmıştır. Çalışmada kullanılan veriler, kimlik avı şiddeti, kimlik avı girişimlerine yatkınlık, kimlik avı girişimlerini belirleme konusunda öz yeterlilik, kimlik avı hakkında daha fazla bilgi edinme niyeti ve kimlik avını başkalarıyla tartışma niyeti değişkenlerini ölçen Risk Davranışı Teşhisi (RBD) ölçeği ile ön test, son test ve gecikmeli son test olmak üzere üç aşamada toplanmıştır. Ön test uygulandıktan sonra katılımcılara SonicWall Kimlik Avı IQ Testi'nden sorular sunulmuş, kimlik avı girişimi ya da büyük şirketlerden gelen gerçek iletişim e-postalarından oluşan 10 ekran görüntüsü gösterilmiştir. Katılımcılar her bir ekran görüntüsünü izledikten sonra e-postanın "meşru" mu yoksa "kimlik avı" mı olduğunu belirtmeleri istenmiştir. Bu araştırmanın sonuçlarında, üniversite öğrencilerinin kimlik avı konusundaki tutumlarını, gelecekteki kimlik avı girişimlerini belirleme konusundaki güvenlerini ve kendilerini bu tehdide karşı savunmasız hissettiklerini ortaya koymuştur.

Onashoga ve arkadaşları (2019) çalışmalarında, kimlik avı saldırısı farkındalığına yönelik Securix adında üç boyutlu oyun tabanlı bir öğrenme ortamı üzerine araştırma yapmıştır. Araştırmada internet kullanıcılarına kimlik avı saldırılarını nasıl tespit edeceklerini ve bunlardan nasıl kaçınacaklarını öğreten bir üç boyutlu video oyunu sunarak kullanıcılara kimlik avı saldırıları hakkında bilgi vermeyi ve kimlik avı saldırılarına karşı farkındalığı

artırmayı amaçlanmaktadır. Araştırmaya 50 katılımcı katılmıştır. Araştırmada kullanılan veriler, algılanan tehdit, kimlik avı saldırısının yol açabileceği muhtemel zararları, tehlikeleri, tehlike veya hasarına ilişkin algılarını, algılanan duyarlılığın kimlik avı saldırısının gerçekleşme olasılığını değerlendirmek için kullanılan bir anket aracılığıyla toplanmıştır. Sonuçlar, etkileşimli oyunun internet kullanıcılarına kimlik avı saldırılarına karşı uyanık olmak için stratejiler öğretmede etkili bir yaklaşım olduğunu ortaya koymuştur.

Weaver ve arkadaşları (2021) kullanıcıların kimlik avı e-postalarını tanımlama konusunda eğitilebileceği bir araştırma üzerinde çalışmışlardır. Kullanıcıları kimlik avı e-postalarını tespit etme konusunda eğitmek amacıyla Jigsaw çevrimiçi kimlik avı testinin etkinliğini test edilmiştir. Kullanıcıları güvenilir ipuçlarını kontrol etme ve yorumlama konusunda eğitmenin, daha sonra kimlik avı e-postalarını tanımlama becerilerini geliştirip geliştirmeyeceği ve ne ölçüde geliştireceği ile ilgilenilmiştir. Çalışmaya, 40 üniversite öğrencisi katılmıştır. Katılımcılar, her gruba eşit sayıda olacak şekilde, rastgele olarak eğitim grubuna ve kontrol grubuna ayrılmışlardır. Tüm katılımcılara ilk olarak ön test olarak sekizi kimlik avı olan ve sekizi kimlik avı olmayan 16 e-posta verilmiş, ön testten sonra, eğitim grubundaki katılımcılar Jigsaw eğitim testini tamamlamışlar ve kontrol grubundaki katılımcılar da Jigsaw çevrimiçi kimlik avı testini tamamlamak için gereken süre kadar bir bulmaca doldurma görevini tamamlamışlardır. Daha sonra tüm katılımcılara son test olarak sekizi kimlik avı olan ve sekizi kimlik avı olmayan 16 e-posta verilmiştir. Araştırma sonucunda eğitim grubunun kontrol grubuna kıyasla ön testten son teste kadar e-postaları kimlik avı olmayan veya kimlik avı olarak sınıflandırmada daha fazla gelişme gösterdiği bulgusuna varılmıştır.

Mohd Zaharon ve arkadaşları (2021), Y kuşağının kimlik avı farkındalığını etkileyen faktörler üzerine çalışmışlardır. Çalışmanın amacı, Malezya'daki Y kuşağı insanlar arasında kimlik avı farkındalığını etkileyen faktörleri belirlemektedir. Malezya da bir şehirdeki 1978-1994 yılları arasında doğmuş Y kuşağında olan beş yüz katılımcıyla çalışma gerçekleştirilmiştir. Çalışmada veri toplama aracı olarak katılımcıların yaş, cinsiyet, medeni

durum ve meslek gibi demografik özelliklerini, bağımlı değişken olarak Y kuşağının kimlik avı konusundaki farkındalığını, bağımsız değişken olarak sosyal mühendisliğin etkisini, kimlik avı karşıtı bilgiyi ve güvenlik endişesini ölçen beşli likert tipi ölçeği kullanılmıştır. Sonuçlar, Y Kuşağı kişiler arasında sosyal mühendislik etkisi ile dolandırıcılık farkındalığı arasında negatif bir ilişki olduğunu, kimlik avı karşıtı bilgi ile kimlik avı farkındalığı arasında pozitif bir ilişki olduğunu göstermiştir. Güvenlik endişeleri ile kimlik avı farkındalığı arasında da pozitif bir ilişki bulunmuştur. Bu çalışmanın bulgularına dayanarak, insanları daha fazla kimlik avı materyali ile eğiterek kimlik avı yöntemleri ve kimlik avı karşıtı bilgiler konusunda her zaman güncel kalarak sosyal mühendisliğin etkisine karşı uyanık olmaları tavsiye edilmektedir.

Grubbs (2022), kimlik avı ile mücadele için oyun tabanlı bir eğitimde demografik faktörlerin etkisi üzerine bir araştırma yapmıştır. Araştırmanın amacı, yaşın, cinsiyetin, eğitimin ve önceki eğitimin bireyin kimlik avına karşı koruma oyunu sırasında öğrenme yeteneğini nasıl etkilediğini analiz etmek ve ölçmektir. Kimlik avı eğitiminin genel etkinliğini ölçmek için video eğitimi ve oyun tabanlı eğitim yöntemleri kullanılmıştır. 500 katılımcının olduğu çalışmada, 250 katılımcıya video eğitimi, 250 katılımcıya oyun tabanlı eğitim uygulanmıştır. Araştırmada kullanılan veriler, Bilgi Güvenliği İnsan Boyutları Anketi ile toplanmış, ankette cinsiyet, alınan günlük e-posta sayısı, yaş, siber güvenlik eğitim saatleri, eğitim düzeyi ve oyun oynayarak geçirilen haftalık saat bilgileri ön test ve son test uygulanarak toplanmıştır. Sonuçlar, geniş bir demografik grupta kısa bir videonun kimlik avı önleme oyunundan daha etkili olduğunu ve hiçbir bireysel demografik faktörün oyunun etkinliği üzerinde önemli bir etkiye sahip olmadığını ortaya çıkarmış, oyun temelli eğitimin etkili olabileceğini ancak kısa bir videonun daha etkili olduğunu göstermiştir.

Witsenboer ve arkadaşları (2022), Hollanda da ilkokul ve lise öğrencilerinin siber güvenlik davranışlarının ölçümü üzerine çalışmışlardır. Bu kapsamda çalışmada öğrencilerin ilkokul ve liselerde siber güvenlik davranışlarını ne ölçüde geliştirdiklerinin araştırılması amaçlanmıştır. Çalışmaya 140 ilkokul öğrencisi ve 96 lise öğrencisi katılmıştır.

Araştırmada Bilgi Güvenliğinin İnsani Yönleri Anketinin (HAIS-Q) çalışmanın kapsamı doğrultusunda davranış boyutu ile ilgili maddeleri öğrencilerin yaş grupları dikkate alınarak uyarlanarak kullanılmıştır. Anket kullanımın değerlendirilmesi amacıyla öğrencilerle iki grup görüşmesi gerçekleştirilmiştir. Araştırma bulguları, Hollanda okul müfredatının siber güvenlik konusuna pek önem vermediğini ve öğrencilerin çevrimiçi davranışlarını çoğunlukla deneyimler, internetteki talimatlar, ebeveynler ve kardeşler aracılığıyla edindiklerini ortaya çıkarmıştır. Birçok öğrencinin zamanla daha umursamaz davranışlar geliştirdiğini belirtmiş, siber güvenlik eğitiminin, çocukların çevrimiçi donanımları kullanmaya başlamasıyla birlikte ilkokulda başlaması gerektiğini vurgulamıştır. Kimlik avı e-postalarını ve kimlik avı web sitelerini tanımanın, özellikle dikkat edilmesi gereken bir konu olduğu vurgulanmıştır.

Sun ve Lin (2022) yapmış olduğu çalışmada etkileşimli bir yanıt sistemini ters yüz sınıf eğitimine entegre etmenin öğrencilerin kimlik avına karşı öz yeterliliği, kolektif yeterliliği ve sıralı davranış kalıpları üzerindeki etkilerini incelemiştir. Ters yüz sınıf öğretimi ile entegre edilmiş farklı etkileşimli yanıt sistemlerinin öğrencilerin öz yeterliliği, kolektif yeterliliği ve sıralı davranış kalıpları üzerindeki etkisi ve bu üç boyut arasındaki ilişkiyi araştırmayı amaçlamıştır. Etkileşimli olmayan yanıt sistemi, bireysel etkileşimli yanıt sistemi ve işbirlikçi etkileşimli yanıt sistemi olmak üzere üç gruptan oluşan ve her grupta 29 yedinci sınıf öğrencisinin bulunduğu toplam 87 öğrenci araştırmaya katılmıştır. Sonuçlar, etkileşimli yanıt sistemini ters çevrilmiş sınıfa dahil ederken, akran desteği davranışının öz yeterliliği artırmada etkili olduğunu göstermiştir. İşbirlikçi etkileşimli yanıt sistemi yaklaşımının, öğrencilerin öğretmenle etkileşime geçme konusunda motive olmasına yardımcı olduğunu ortaya koymuştur. Akranlar arasındaki bilgi oluşturma davranışları ile etkileşimli yanıt sistemini kullanım davranışları arasındaki ilişkinin zayıf olduğu sonucuna varılmıştır. Öğretmenlerin öğretim için eğitim teknolojilerini kullanmanın yanı sıra, öğrencilerin öz yeterliliğini ve işbirlikçi yeterliliğini artırmak için akranlarına karşılıklı tanıma ve etkili iletişim becerileri bilgisi edinme konusunda rehberlik etmeleri önerilmektedir.

Jerrim (2023) Uluslararası Öğrenci Değerlendirme Programı (Programme for International Student Assessment -PISA) verilerini kullanarak 15 yaşındaki çocukların oltalama e-postalarına verdiği yanıtlara yönelik bir araştırma yapmıştır. Araştırma oltalama e-postalarına yanıt verme olasılığı en yüksek olan gençlerin özelliklerini ortaya koymayı amaçlamıştır. Araştırmada kullanılan veriler OECD ülkelerinde uygulanan "Tanınmış bir cep telefonu operatöründen gelen kutunuza, akıllı telefon kazananlardan biri olduğunuzu söyleyen bir mesaj aldınız. Gönderen, size akıllı telefonu gönderebilmesi için bağlantıya tıklayarak verilerinizi içeren bir form doldurmanızı ister. Sizce bu e-postaya tepki olarak aşağıdaki stratejiler ne kadar uygundur?" sorusunu içeren 2018 PISA verilerinden alınmıştır. Araştırma sonuçları her yedi gençten birinin oltalama e-postalarına cevap verme eğiliminde olduğunu ve bu oranın sosyo-ekonomik olarak düşük seviyede olan öğrenciler arasında beşte bire yükseldiğini göstermektedir. Araştırma sonuçlarına göre Türkiye de her beş gençten biri oltalama e-postalarına yanıt verme eğilimindedir. Bilişsel becerileri düşük olan gençlerin oltalama e-postalarına yanıt verme riskiyle karşı karşıya olma olasılıklarının daha yüksek olduğu vurgulanmıştır. Bu sonuçlar ışığında gençlere, özellikle de sosyo ekonomik olarak düşük seviyede bir geçmişe sahip olanlara ve akademik başarısı düşük olanlara, karşılaştıkları çevrimiçi riskler hakkında daha fazla önem verilmesi ve daha kaliteli eğitim sağlanması gerektiği vurgulanmıştır.

İlgili Araştırmaların Özet

İncelenen alan yazın siber güvenlik konusuna yönelik olarak farklı yaş gruplarındaki öğrencilerin eğitim ihtiyaçlarını vurgulamaktadır. Araştırmalarda öğrencilerin siber güvenlikle ilgili kavram bilgisi ve siber saldırılara karşı koyma konusunda yetersiz kaldıklarını belirtilmektedir. Pek çok araştırma bireylerin siber saldırılara karşı önemli ölçüde savunmasız olduğunu ve bu durumun onları siber güvenlik tehditlerine maruz bırakabileceğini ortaya koymuştur (Muniandy vd., 2017; Perrault, 2018; Witsenboer vd., 2022). Jerrim (2023) yapmış olduğu araştırmada her yedi gençten birinin siber saldırılardan olan kimlik avı e-postalarına cevap verme eğiliminde olduğunu göstermiştir. Yine Jerrim 'in

(2023) araştırmasından Türkiye de her beş gençten birinin kimlik avı e-postalarına cevap verme eğiliminde olduğu anlaşılmaktadır. Witsenboer ve arkadaşları (2022), siber güvenlik eğitiminin, çocukların çevrimiçi donanımları kullanmaya başlamasıyla birlikte ilköğretim seviyesinde başlaması gerektiğini vurgulamıştır.

Siber saldırılar hakkında bilgi edinmenin siber güvenlik farkındalığı ve bu tür saldırılara karşı koymada etkili olduğu araştırmalardan anlaşılmaktadır (Case & King, 2016; Mohd Zaharon vd.; 2021). İncelenen alan yazında siber saldırı eğitimi ve farkındalığı kapsamında; bireylerde siber güvenlik farkındalığı oluşturabilecek ve siber güvenliğe dikkat çekebilecek çevrim içi testlerin uygulanması (Perrault, 2018; Weaver vd., 2021), eğitsel dijital oyunların kullanımı (Grubbs, 2022; Onashoga vd., 2019; Sun vd., 2017), kavram haritalarının kullanımı (Sun ve Chen, 2016; Sun ve Lee, 2016), etkileşimli araçların kullanımı (Sun ve Lin, 2022) ve video kullanımı (Grubbs, 2022) gibi eğitsel faaliyetlerin araştırmalara konu olduğu görülmektedir. Grubbs (2022) kimlik avı kapsamında hazırlanmış kısa bir videonun kimlik avı önleme oyunundan daha etkili olduğunu savunmuştur. Yapılan araştırmalar öğrencilerin siber güvenlik konusundaki bilgi eksikliklerini ve siber tehditlere karşı savunmasız olduklarını vurgulamakta olmasına rağmen bu soruna çözüm sunan az sayıda araştırma bulunmaktadır. Kendi kendine öğrenmeyi destekleyen, öğretimi küçük parçalar halinde tasarlayarak öğrenmeyi kolaylaştıran mikro-öğrenme stratejiyle hazırlanmış öğretim materyallerinin bu soruna çözüm olacağı düşünülmektedir.

Bölüm 3

Yöntem

Bu bölümde araştırmanın yöntemine, veri toplama araçlarına, araştırmacının rolüne, araştırma modeline, veri analizine yer verilmiştir.

Tasarım Tabanlı Araştırma Yöntemi

Tasarım tabanlı araştırmanın (TTA) başlangıcı genellikle Brown'ın 1992 yılında tasarım deneyleri hakkında yazdığı makaleye dayandırılmaktadır. TTA yöntemleri, eğitim alanındaki yeniliklerin uygulamada nasıl, ne zaman ve neden işe yaradığını anlamak için araştırmacılara birçok fırsat sunmaktadır (Penuel, vd., 2011). TTA esnek olmasına rağmen aynı zamanda oldukça sistematiktir. Bu yaklaşımı kullanan araştırmacılar öncelikle çözülmesi gereken bir sorun tanımlamaktadır (Edelson, 2002). Hem sistematik hem de esnek olmanın birleşimi, yalnızca işe yarayan bir araştırmaya yol açmakla kalmaz, aynı zamanda araştırmacıların bunun nasıl ve neden işe yaradığını anlamasını sağlamaktadır (Cobb, vd., 2003; Hjalmarson, vd., 2021). Tasarım tabanlı araştırma (TTA), son yirmi yılda matematik ve fen eğitiminde bir araştırma metodolojisi olarak önem kazanmıştır ve amaçları ve eğitim ortamları açısından çeşitlilik göstermektedir (Cobb, vd., 2003; Corcoran vd., 2009; Daro vd., 2011; Hjalmarson, vd., 2021; Penuel vd., 2013).

Barab ve Squire (2016) tasarım temelli araştırmayı "bir yaklaşımdan ziyade, doğal ortamlarda öğrenme ve öğretmeyi açıklayan ve potansiyel olarak etkileyen yeni teoriler, eserler ve uygulamalar üretmek amacıyla bir dizi yaklaşım" olarak tanımlamaktadır. Bu, Plomp'un (2013) "analiz, tasarım, değerlendirme ve revizyon faaliyetleri, idealler ('amaçlanan') ile gerçekleştirme arasında uygun bir denge sağlanana kadar yinelenir" şeklinde tanımladığı tasarım temelli araştırmanın döngüsel doğasını ifade etmektedir (Hjalmarson, vd., 2021).

TTA, eğitim araştırmacılarına eğitim araştırmalarına rehberlik edebilecek yeni bir çerçeve sunmaktadır (Van den Akker vd., 2006; Brown, 1992; Cobb vd., 2003). Reeves

(2006) bu araştırma çerçevesini: “karmaşık sorunları gerçek bağlamlarda uygulayıcılarla iş birliği içinde ele almak; bu karmaşık sorunlara makul çözümler üretmek için bilinen ve varsayımsal tasarım ilkelerini teknolojik gelişmelerle bütünleştirmek; yenilikçi öğrenme ortamlarını test etmek ve iyileştirmek ve yeni tasarım ilkelerini tanımlamak için titiz ve yansıtıcı bir araştırma yürütmek” şeklinde üç temel ilkede özetlemektedir. TTA’nın nihai hedefi, eğitim araştırmaları ile gerçek dünya sorunları arasında daha güçlü bir bağlantı kurmaktır. Teknoloji destekli öğrenme, bilgisayar destekli öğrenme ortamlarında TTA yöntemi yaygın olarak kullanılmaktadır (Hjalmarson, vd., 2021).

TTA bağlamları anlamaya, etkili sistemlerin tasarlanmasına ve çalışma konuları için anlamlı değişiklikler yapmaya odaklanan tasarımcılar tarafından yürütülür (Barab & Squire, 2016). TTA’nın ayırt edici özelliklerinden biri, araştırmanın yinelemeli doğasıdır. Her yineleme ilerledikçe, araştırmacılar bağlama en iyi uyan çeşitli araştırma yöntemlerinden yararlanarak araştırmayı iyileştirir ve yeniden işlemektedir. Bu esneklik, nihai sonucun süreçten daha öncelikli olmasını sağlamaktadır.

Eğitsel Tasarım Tabanlı Araştırma (ETTA) Modeli

Eğitsel Tasarım Tabanlı Araştırma Modelinin yaklaşık 20 yıllık bir geçmişi vardır (Brown, 1992; Collins, 1992) ve bu süre içinde pek çok farklı terimle adlandırılmıştır. En yaygın isimlerden bazıları tasarım tabanlı araştırma (Kelly, 2003), geliştirme araştırması (Van den Akker, 1999), tasarım deneyleri (Brown, 1992; Collins, 1992), biçimlendirici araştırma (Newman, 1990) ve eğitim tasarımı araştırmasıdır (Van den Akker vd., 2006).

ETTA modeli, karmaşık eğitim sorunlarına yönelik çözümlerin yinelemeli olarak geliştirilmesinin bilimsel sorgulama için ortam sağladığı bir araştırma türüdür. Eğitim tasarımı araştırmalarından çıkan çözümler eğitim ürünleri (örneğin çok kullanıcılı bir sanal dünya öğrenme oyunu), süreçler (örneğin çevrimiçi kurslarda öğrenci öğrenimini desteklemek için bir strateji), programlar (örneğin öğretmenlerin daha etkili sorgulama stratejileri geliştirmelerine yardımcı olmayı amaçlayan bir dizi atölye çalışması) veya politikalar (örneğin yıl boyunca eğitim) olabilir. Eğitim tasarımı araştırmacıları önemli gerçek

dünya sorunlarını çözmeye çalışırken, aynı zamanda benzer sorunlarla karşılaşan diğer araştırmacıların çalışmalarını bilgilendirebilecek yeni bilgiler keşfetmeye çalışırlar.

TTA yöntemini kullanan araştırmacılar farklı yöntemler kullanabilirken, McKenney ve Reeves (2012) ETTA modelini ana hatlarıyla *analiz ve inceleme, tasarım ve geliştirme, değerlendirme ve yansıma* olmak üzere üç temel süreçte belirtmiştir. Yinelemeli yapısı, araştırmacıların çalışmalarını, ürünleri, süreçleri iyileştirmelerine ve yeni kaynakları ve eğitim yaklaşımlarını test etmelerine olanak tanıyan yinelemeli araştırma döngüleri halinde düzenlemelerine olanak tanımaktadır. ETTA modelinin verileri, "eğitim araştırmasının nasıl, ne zaman ve neden ortaya çıktığını anlamak" için kanıtlar sunmakta, sonuçların iyileştirilmesine yol açmakta ve araştırmacılar, tasarımcılar ve katılımcılar arasında yakın bir işbirliği içinde kanıtlara dayalı yeniliklerin uygulanmasını teşvik etmektedir (Tinoca vd., 2022). McKenney ve Reeves'e (2012) ETTA modelinde, tasarım, araştırma ve uygulamayı eş zamanlı olarak harmanlamaktadır.

ETTA modeli uygulayıcıların ve araştırmacıların karmaşık bir eğitim sorununa çözüm tasarlamak için iş birliği yaptığı ve birden fazla uygulama yinelemesi yoluyla değerlendirildiği uzun süreli bir yaklaşımdır (Anderson & Shattuck, 2012). ETTA konusunda deneyimli olan araştırmacılar, ETTA'nın kişiselleştirilebilirliğinin eğitim uygulamaları, politika ve teori üzerinde etki yaratabilecek daha esnek özgün araştırmalara yol açtığını öne sürmektedir (Fishman, vd., 2013; Herrington, 2012; McKenney & Reeves, 2014; Reimann, 2013). Geliştirme çalışmaları söz konusu olduğunda ETTA araştırmasının amacı, eğitim uygulamasındaki karmaşık sorunlar için araştırmaya dayalı çözümler geliştirmektir. Bu tür tasarım araştırması, eğitim uygulamasındaki karmaşık sorunlar için araştırmaya dayalı çözümler üretmek ve bu araştırmaların özellikleri ile bunları tasarlama ve geliştirme süreçleri hakkındaki bilgileri ilerletmek amacıyla eğitim araştırmalarının sistematik analizi, tasarımı ve değerlendirilmesi olarak tanımlanmaktadır.

Barab ve Squire'ın (2016) geniş tanımı, aynı zamanda eğitimsel tasarım (tabanlı) araştırmalarını da kapsar ve şöyle belirtirler: "Tasarım temelli araştırma, bir yaklaşımdan

ziyade doğal ortamda öğrenmeyi ve öğretmeyi açıklayan ve potansiyel olarak etkileyen yeni teoriler, eserler ve uygulamalar üreten bir dizi yaklaşımdır.”

Doğası gereği tasarım araştırması, eğitim uygulamalarındaki karmaşık sorunlara araştırmaya dayalı çözümler geliştirmeyi veya öğrenme ve öğretme süreçlerine ilişkin teorileri geliştirmeyi veya doğrulamayı amaçladığından eğitim uygulamalarıyla (ve dolayısıyla eğitim politikasıyla da) ilgilidir. Geliştirme çalışmaları olarak tasarım araştırması söz konusu olduğunda, aşağıdaki aşamalar ayırt edilir:

Ön Araştırma: ihtiyaç ve bağlam analizi, alan yazı taraması, çalışma için kavramsal veya teorik bir çerçevenin geliştirilmesi.

Geliştirme veya Prototip Oluşturma: her biri mikro araştırma döngüsü olan yinelemelerden oluşan yinelemeli tasarım aşaması ve araştırmanın iyileştirilmesi ve rafine edilmesini amaçlayan en önemli araştırma faaliyeti olarak biçimlendirici değerlendirme.

Değerlendirme: çözümün veya araştırmanın önceden belirlenmiş özellikleri karşılayıp karşılamadığına karar vermek için (yarı) özetleyici değerlendirme. Bu aşama da genellikle müdahalenin iyileştirilmesine yönelik tavsiyelerle sonuçlandığından, bu aşama yarı özetleyici olarak adlandırılmaktadır.

ETTA modeli, günümüzde yürütülen ve raporlanan eğitim araştırmalarının büyük çoğunluğunun kısıtlılığı sorunu için umut verici bir çözümdür (Van den Akker vd., 2006). Diğer eğitim araştırması türlerinin aksine, ETTA araştırma ve uygulama arasında doğrudan bir bağlantı sağlamaktadır ve bu nedenle anlamlı bir etkiye sahip olma şansı büyük ölçüde artmaktadır.

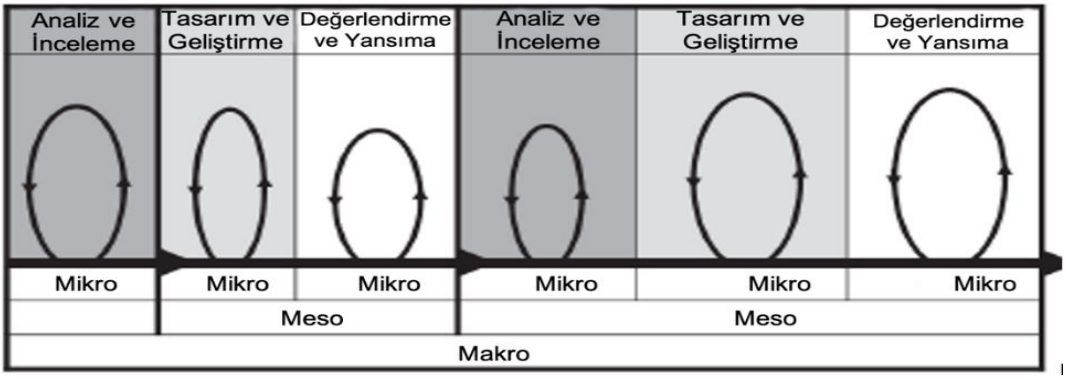
İlk olarak, ETTA uygulayıcıların ve araştırmacıların önemli öğretim ve öğrenim sorunlarının belirlenmesinde iş birliği yapmalarını gerektirmektedir. İkinci olarak, ETTA, uygulayıcıları ve araştırmacıları, mevcut tasarım ilkelerine dayalı olarak bu ve diğer ciddi sorunlara prototip çözümler geliştirmeye yönelik yaratıcı faaliyetlere dahil etmektedir. Teori, eğitim araştırmalarına yönelik diğer birçok yaklaşımda neredeyse sonradan akla gelen bir

düşünce gibi görünmektedir, ancak eğitim tasarımı araştırmalarında, ciddi sorunları ele alan prototip yeniliklerin şekillendirilmesinde birincil rol oynamaktadır. Üçüncü olarak, ETTA ilgili herkes tarafından tatmin edici sonuçlara ulaşılana kadar, hem prototip çözümlerin hem de bunların dayandığı tasarım ilkelerinin test edilmesi ve iyileştirilmesinde uygulayıcıların ve araştırmacıların yakın işbirliğini içermektedir. ETTA, araştırma projelerinin başladığı sorunların çözümünde ilerlemeyi temsil eden arzu edilen sonuçlar elde edilene kadar "tamamlanmış" sayılmamaktadır.

TTA'nın en çok kullanılan modellerinden biri McKenney ve Reeves (2012) tarafından sunulmuş olup, etkileşimli ve esnek bir şekilde uygulanan üç ana aşamayı tanımlamaktadır: analiz/inceleme, tasarım/geliştirme ve değerlendirme/yansıtma. Mevcut çalışmada kullanılan bu genel modelin bir temsili Şekil 2'de sunulmuştur. Teori ve pratiğe olan ikili odaklanma, sırasıyla kuramsal ve uygulamaya dönük çıktıları temsil eden dikdörtgenler aracılığıyla açıkça vurgulanmaktadır. Model, tek ve bütünleşik bir araştırma ve tasarım sürecini göstermektedir. Yamuk; uygulama ve yayılmayı temsil ederek, uygulama ile etkileşimin mevcut olduğunu ve kapsamın süreç içinde arttığını göstermektedir. Çift yönlü oklar, uygulamada olup bitenlerin hem devam eden temel süreçleri hem de nihai çıktıları etkilediğini ve bunun tersinin de geçerli olduğunu göstermektedir (McKenney ve Reeves, 2012).

Şekil 2

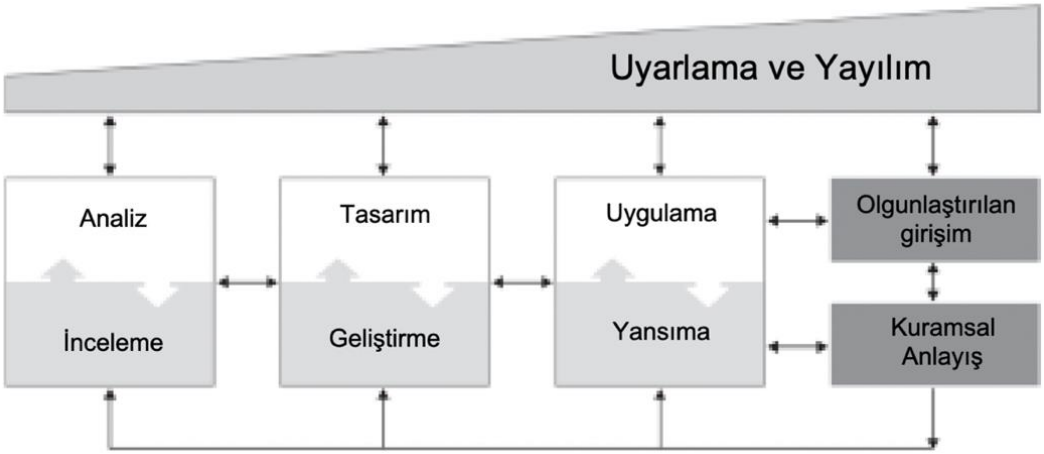
Eğitsel tasarım araştırmasında Mikro, Mezo ve Makro döngüler (McKenney ve Reeves, 2012)



Şekil 2'de gösterilen model, uygulama (yamuk) ile sürekli etkileşim içinde gerçekleşen ve hem pratik hem de bilimsel sonuçlar (dikdörtgenler) veren üç temel aşamayı (kareler) içeren esnek, yinelemeli bir süreci tasvir etmektedir. Teorik anlayış, münferit aşamaların yanı sıra genel yörüngeden de elde edilebilir. Bu nedenle, sonraki adımları atmadan önce belirli bir aşamadan elde edilen iç görüleri yazılı olarak pekiştirmek için zaman ayırmak yatırıma değerdir.

Şekil 3

Eğitsel Tasarım Tabanlı Araştırma Modeli (McKenney ve Reeves, 2012)



Şekil 3'te gösterilen jenerik modelde, dörtgenler *Analiz ve İnceleme, Tasarım ve Geliştirme, Değerlendirme ve Yansıma* olmak üzere üç temel aşamayı temsil etmektedir. Farklı bileşenler arasındaki oklar sürecin yinelemeli ve esnek olduğunu göstermektedir. Süreç yinelemeli ve esnektir, çünkü bileşenlerden elde edilen farklı sonuçlar diğerlerini desteklemektedir. İzlenen genel akışlara rağmen belirtilmesine rağmen birçok farklı yol izlenebilir olması sürecin esnek olduğunu göstermektedir.

Eğitsel Tasarım Tabanlı Araştırma Yönteminin Süreç Akışı

Eğitsel Tasarım Tabanlı Araştırma (ETTA) modeli genellikle bir sorunun ön incelemesi ile başlamaktadır (McKenney & Reeves, 2012).

Analiz ve İnceleme

ETTA modelinin bu aşamasının ana hedefi problemin tanımlanmasıdır. Bağlamsal analiz ve ihtiyaç değerlendirmesinin yanı sıra alan yazın taraması ile probleme ilişkin ilk bulgular rafine edilerek problemin nedenleri açıklanır. *Analiz ve inceleme* mikro döngüsünün temel amacı, üçüncü şahısların benzer problemlere yaklaşımları, çözüm yollarını araştırmak ve öğrenmektir. İnceleme genellikle saha ziyaretleri, profesyonel toplantılar ve bilgi paylaşım ağı kurma yoluyla gerçekleştirilir.

Analiz ve inceleme mikro döngüsünde, sürecin devamı için zemin hazırlanırken, sorunların ne olduğuna dikkat çekilmekte ve ele alına probleme örnekler verilmektedir. Daha sonra, analiz süreci, hedeflerine ve bu sürecin nasıl planlanacağına, yürütüleceğine ve anlamlandırılacağına dikkat çekilerek ayrıntılı olarak tartışılmaktadır.

Analiz ve inceleme mikro döngüsünde, ele alınacak problemin daha iyi anlaşılması için uygulayıcılarla iş birliği yapılmaya çalışılır. Problemin araştırılabilir olup olmadığını ve eğitim tasarımı araştırmasının gerçekten de hem problemin çözümüne hem de bilimsel anlayışa gerekli katkıyı yapıp yapamayacağını değerlendirmek için alan yazın taraması yapılır. Bu mikro döngü, problemin tanımı ve hedeflerin ifade edilmesi şeklinde, problemin daha iyi anlaşılma sürecidir. Buna ek olarak, problemin sınırları keşfederek, kısmi tasarım gereksinimlerinin yanı sıra ilk tasarım önerileri de ana hatlarıyla belirlenebilir. Tasarım gereklilikleri, tasarım seçimlerini çerçevelemesi gereken faktörlerdir. Bu aşamada belirlenen tasarım gereksinimleri geçici ve kısmi olup ihtiyaçların ve bağlamın anlaşılmasıyla ilgilidir.

Analiz süreci (literatür taraması, problem tanımı, bağlam analizi ve ihtiyaç değerlendirmesi) daha analitik olma eğilimindeyken ve inceleme süreci (işbirlikçi aktiviteler) daha açık uçlu olma eğilimindedir. Analiz süreci, problemin ipuçları aracılığıyla tanımlanmasına ve anlaşılmasına yardımcı olur. Analiz süreci, hedef ortamda çözüm tasarlarken yararlanılabilecek fırsatların ve kullanıl(a)mayan kaynakların aranmasına yardımcı olur. Analiz ve inceleme aşamasındaki ana görevlerin her birini nasıl ilişkilendirildiğine dair örnekler Tablo 1'de sunulmuştur.

Tablo 1

Analiz ve İnceleme (McKenney & Reeves, 2012)

	Araştırma	Görevler	Ortaya Çıkarma
Analiz	Anlamak için okur	Alan yazını tarar	Yeni fikirler üretir
	Problemi tespit eder	Problemi tanımlar	Problemi ortaya çıkarır
	Problemi araştırır	İçeriği analiz eder	Problemin nedenlerini sorgular
	Problemin ne olduğunu sorar	İhtiyaçları analiz eder	Beklentileri sorgular
İnceleme	Artı ve eksileri belirtir	Saha ziyaretleri yapar	Yeni yöntemler arar
		Toplantılar yapar	
	Geribildirim talep eder	İlgili kişilerle iletişim kurar	Farklı fikirleri sorar

Tasarım ve Geliştirme

ETTA modelinin uygulama aşaması sistematik bir problem çözme sürecidir ve aynı zamanda proje boyunca tasarımla ilgili biçimlendirici kararların alınmasına olanak tanıyacak şekilde esnek bir şekilde yinelenir (McKenney & Reeves, 2012). Tasarım ve geliştirme mikro döngüsü sistematik ve kasıtlıdır, ancak aynı zamanda yaratıcılığı, ortaya çıkan iç görülerin uygulanmasına açıklığı da içerir. Bu mikro döngü boyunca, problemin nasıl ele alınacağına ilişkin fikirler oldukça geniş ve belirsiz başlama eğilimindedir ve yavaş yavaş rafine edilir, budanır ve işlevsel hale getirilir. Tasarım mikro döngüsünde, fikirler üretilerek, her biri değerlendirilerek ve en umut verici görünenlerin potansiyel çözümler araştırılır. Sınırlı sayıda seçenek belirlendikten sonra, potansiyel çözümler bir taslaklar kademeli ayrıntılı olarak tasarlanır. Tasarımın taslakları genellikle bir prototip oluşturma süreciyle inşa edilir. İlk prototip versiyonları test edilir. Daha sonraki versiyonlar genellikle daha detaylı ve işlevseldir. Genellikle, tasarım ve geliştirme mikro-döngüsü yeni iç görülere yol açarak yeni döngüleri tetikler.

Tasarım ve geliştirme mikro döngüsü çeşitli çıktılara yol açabilir. Potansiyel çözümlerin araştırılması ve taslaklarının oluşturulması, oluşturulacak potansiyel tasarımları tanımlayan belgeler ortaya çıkarabilir. Bunlar, taslak tasarımının daha geniş tanımlarından daha ayrıntılı tasarım özelliklerine kadar değişebilir. Geliştirme süreci çözümün kendisini ortaya çıkarır bu bir öğretim tasarımı, eğitim yazılımı ya da dolaylı olarak öğretime yönelik belirli bir yaklaşım için süreç kılavuzları) temsil edilmeye uygun olabilir. Bu çıktılardan herhangi biri değerlendirme ve yansıtma konusu olabilir. Tasarım ve geliştirme aşamasındaki ana görevlerin her birini nasıl ilişkilendirildiğine dair örnekler Tablo 2'de sunulmuştur.

Tablo 2

Tasarım ve Geliştirme (McKenney & Reeves, 2012)

	Araştırma	Görevler	Ortaya Çıkarma
Tasarım	Fikirlerin niteliğini değerlendirir	Çözümleri araştırır	Farklı fikirlere açıktır
	Fikirleri daha pratik hale getirmenin yollarını arar	Çözümleri taslaklandırılır	Sınırları zorlar
Geliştirme	Dikkatini vermeyi sürdürür	Çözümleri geliştirilir	Olasılıkları değerlendirir
	Veriler tarafından yönlendirilir	Çözümleri gözden geçirir	Sezgiyle yönlendirilir

Değerlendirme ve Yansıma

ETTA modelinin yansıma ve değerlendirme mikro döngüsü, çalışmanın uygulama aşamasında meydana gelenlerin aktif ve düşünceli bir şekilde ele alınmasını içerir (McKenney & Reeves, 2012). Değerlendirme ve yansıma mikro döngüsü, tasarım fikirleri ve prototip çözümler ampirik olarak test edilir ve müdahale özelliklerinin işe yarayıp yaramadığına, nasıl ve neden yaradığına dair (teorik) anlayışı iyileştirmek amacıyla bulgular üzerine düşünülür. Bu döngünün sonucunda uygulamanın uygulandığında ortaya çıkardığı etkilerin daha iyi anlaşılması sağlanır. Buna ek olarak, uygulamanın araştırılmasıyla tasarım

dolaylı olarak test edilmiş olur. Bulgular üzerine düşünme, sonuçlar için açıklamalar ve tasarım (gereksinimler veya önermeler; ön tasarımı) ve/veya prototip çözümleri yeni veya rafine fikirler üretilmesine yardımcı olur. Değerlendirme geniş anlamda, tasarımlar veya geliştirilmiş prototiplerin her türlü ampirik testine atıfta bulunmak için kullanılmaktadır. Tasarım araştırmasının bu aşamasında yansıtma, bulguların ve gözlemlerin geriye dönük olarak değerlendirilmesini tanımlamak için kullanılır. Tablo 3, bu aşamada bunun ne anlama gelebileceğine dair örnekler vermektedir.

Tablo 3

Değerlendirme ve Yansıma (McKenney & Reeves, 2012)

	Araştırma	**Görevler**	**Ortaya Çıkarma**
Değerlendirme	Etkili yöntemler oluşturur	Araştırmanın çerçevesini çizer	Süprizlere açıktır
	Bir planı yürütür	Verileri toplar	Planlanmamış fırsatları yakalar
Yansıma	Çıkarımlar ve tümevarımlar	Bulguları analiz eder	Neden böyle olduğunu sorgular
	Anlamı belirler	Süreçleri dikkate alır	Farklı durumları sorgular

Araştırmanın Çalışma Grubu

Araştırmanın 1. Döngüsünde çalışma grubunu 2023-2024 Öğretim Yılı Bahar Dönemi'nde devlet ilköğretim kurumunda 6.sınıfta öğrenim gören 29 öğrenci oluşturmaktadır. Araştırmanın 2. Döngüsünde çalışma grubunu 2023-2024 Öğretim Yılı Bahar Dönemi'nde devlet ilköğretim kurumunda 6.sınıfta öğrenim gören 26 öğrenci oluşturmaktadır. Araştırma sürecinde 2023-2024 Öğretim Yılı Bahar Dönemi'nde ve 2023-2024 Öğretim Yılı Bahar Dönemi'nde Devlet ilköğretim kurumundan toplam 4 öğretmen katkı sağlamıştır.

Çalışma grubu özellikleri. Araştırma, 6. Sınıf öğrencileri ile art arda iki uygulama olacak şekilde yürütülmüştür. Her iki uygulamaya da 55 öğrenci katılım sağlamıştır. Araştırma sürecine ilköğretim okulundan 4 bilişim teknolojileri öğretmeni katkı sağlamıştır.

Veri Toplama Araçları

Araştırma kapsamında Siber Güvenlik mikro-öğrenme nesnesi tasarım ve geliştirme sürecinin incelenmesi amacıyla veri toplama aracı olarak *"Siber Güvenlik Farkındalık Dereceli Puanlama Anahtarı (SGF-DPA)"*, *"Öğrenci Görüşme Formu"* kullanılmıştır. Veri toplama araçları araştırma kapsamında geliştirilmiştir.

Siber Güvenlik Farkındalık Dereceli Puanlama Anahtarı (SGF-DPA)

Dereceli Puanlama Anahtarının oluşturulması. *Dereceli puanlama anahtarları*, öğrencilerin performansını değerlendirmek amacıyla kullanılan, son dönemlerde ortaya konulan formatif bir değerlendirme aracıdır. Öğretmenlerin, öğrencilerinin çalışmalarını değerlendirmelerine ve yaptıkları işlere puan vermelerine ya da değer biçmelerine yardımcı olan ve öğrencilerin ulaşmaları beklenen performans seviyelerinin ortaya konulmasını sağlayan, kullanımı kolay ve sade bir tablodur (Boston, 2002; Baya'a vd., 2009; Crawford, 2001).

Wolf ve Stevens (2007) *dereceli puanlama anahtarlarının* öğrenme hedeflerini netleştirerek, öğretim tasarımına rehberlik ettiğini, değerlendirmenin tüm öğrenciler için eşit ve doğru bir şekilde yapılmasına yardımcı olduğu, öğrencilere geri bildirim ve kendilerini değerlendirme fırsatı sunduğu gibi çeşitli yararlarının olduğunu belirtmektedir (Sarıca & Usluel, 2016). Bu çalışmada *SGF-DPA*, araştırma kapsamında geliştirilen SGMÖN'nin tasarım ve geliştirmesine rehber olması ve Siber Güvenlik farkındalığını değerlendirmek amacıyla geliştirilmiştir.

Dereceli puanlama anahtarı oluşturulurken Andrade'nin (1997) ortaya koyduğu işlem basamakları dikkate alınmıştır. Moskal'ın (2019) belirtmiş olduğu gibi *dereceli puanlama anahtarı* geliştirilirken seçilen ölçütlerin hedeflere uygun ve birbirleri ile tutarlı bir

yapıya sahip olması, puanlama düzeyinin anlamlı ve açık ifade edilmesi, ölçüt ifadelerinin puanlama düzeylerine göre tanımının açık ve anlaşılır bir dille sunulmuş olmasına dikkat edilmiştir (Sarıca & Usluel, 2016).

Dereceli puanlama anahtarı oluşturulurken Andrade (1997)'nin ortaya koymuş olduğu işlem basamakları dikkate alınmıştır. SGF-DPA işlem basamakları aşağıda verilmiştir.

SGF-DPA Oluşturma Basamakları.

1. *Siber Güvenlik Mikro-Öğrenme Nesnelerine (SGMÖN) İlişkin Alan Yazın İncelemesi (DPA, bileşenler, oluşturma süreci, vs.):* DPA'nın oluşturulma sürecinde ilk olarak alan yazındaki DPA incelenmiştir. İncelenen DPA'ında Siber Güvenlik farkındalığını içeren ölçütleri belirlenmiştir. Belirlenen ölçütler doğrultusunda, *SGF-DPA* uygulama süreci dikkate alınarak DPA'nın dört boyuttan oluşturulmasına karar verilerek, tanımların ve puanlama düzeyinin belirlenmesi aşamasına geçilmiştir.

2. *Ölçütlerin, Tanımların ve Puanlama Düzeyinin Belirlenmesi*: İncelemelerin ardından DPA ile ilgili boyutlar: (a) E-Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık; (b) E-Postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık (c) E-Postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık; (ç) E-Posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık olarak belirlenmiştir.

Puanlama 1 ile 5 arası olacak biçimde oluşturulmuştur. Düzey açıklamaları önce en üst ardından en alt düzey belirlenerek yazılmıştır. Moskal'ın (2019) belirtmiş olduğu gibi DPA'nın geliştirilirken ölçütlerin belirlenen hedeflere uygun ve tutarlı olması; puanlama düzeyinin anlamlı ve anlaşılır olması, ölçütlerin ifadesinin ve puanlama düzeylerine göre tanımının açık ve anlaşılır bir dille yazılmış olmasına dikkat edilmiştir

3. *Taslak DPA'nın Hazırlanması:* Ölçütler belirlendikten sonra araştırmacılar tarafından SGMÖN tasarlama ve geliştirme süreci göz önüne alınarak siber güvenlik farkındalığı dereceli puanlama anahtarının; (a) *E-Postalarda Kaynağı Bilinmeyen Bağlantı*

ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık; (b) *E-Postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık;* (c*) E-Postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık;* (ç) *E-Posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık* olmak üzere 4 bölümden oluşmasına karar verilmiştir. SGF-DPA'nın taslak boyutları ile öğrencilerin SGMÖN'nin tasarımında rehber olması ve öğrencilerin Siber Güvenlik Farkındalığının değerlendirilmesi amaçlanmıştır.

4. ***Taslak DPA'nın Kullanımı*:** DPA'nın geliştirme sürecinin ilk aşamasında oluşturulan taslak DPA, bir ilköğretim okulu yedinci sınıfta öğrenim gören 12 öğrencin bilişim teknolojileri dersi kapsamında SGMÖN'ne dönüt vermeleri amacıyla kullanılmıştır.

5. ***Öğrencilerden ve Ders Sorumlusundan Dönütlerin Alınması:*** DPA, öğrencilerin ve bilişim teknolojileri öğretmeninin görüşüne sunulmuştur. Dönütler doğrultusunda düzenlemelere gidilmiştir.

6. ***Taslak DPA'nın Gözden Geçirilmesi ve Düzenlemelerin Yapılması:*** DPA'nın dili öğrencilerin anlayabileceği düzeyde basitleştirilmiştir. DPA'nın niceliksel olarak çok uzun olmasından dolayı kısaltılması amacıyla her puanlamada tekrar eden giriş ayrı bir sütuna alınmıştır. Bütünlüğü bozmamak adına her boyut ayrı bir sayfada başlayacak şekilde konumlandırılmıştır. Bilişim teknolojileri öğretmeni tarafından doğruluk ölçütünü öğrencilerin değerlendirme yetkinliğinin olmadığı belirtilmiş ve bu kapsamda doğruluk ölçütü çıkarılmıştır.

7. ***Geçerlik ve Güvenirlik Çalışmalarının Yapılması:*** Düzenlemelerin ardından DPA'nın geçerlik ve güvenirlik çalışmaları yapılmıştır. Bu çalışmalar DPA'nın geçerlik ve güvenirlik çalışmaları başlığında ayrıntılı olarak açıklanmıştır.

DPA geçerlik ve güvenirlik çalışmaları.

DPA'nın geçerliği, "içerik, yapı ve ölçüt" boyutları bakımından değerlendirilmektedir (Moskal & Leydens, 2019; Sarıca & Usluel, 2016). (a) İçerik, belirlenmiş değerlendirme ölçütlerinin ilgili konu bağlamında yeterli bilgiyi sunması; (b) yapı, belirlenen değerlendirme

ölçütlerinin konu ile ilişkili olup olmadığı; (c) ölçüt ise ilgili konu bağlamında farklı uygulamalarda puanlama ölçütünün ele alınması durumunda doğru şekilde yansıtması ile ilgilidir (Moskal & Leydens, 2019; Sarıca & Usluel, 2016).Taslak DPA'nın dönütler temelinde güncellenmesini takiben oluşturulan DPA, bu boyutlar ele alınarak eğitsel bağlamda siber güvenlik farkındalığı konusunda 3 uzmanın görüşüne sunulmuştur.

Ölçütlere ilişkin ortak olarak belirtmiş olan dönütler doğrultusunda, *"Kaynağı Bilinmeyen E-postalara Dönüt Verme"* ölçütü *"E-Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık"* olarak değiştirilmiş; *"Yazım Hataları"* ölçütü ile *"Reklam ve Ödüller"* ölçütü birleştirilerek adı *"E-Postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık"* olarak değiştirilmiş; *"Kullanıcı Şifre Yönetimi"* ölçütü *"E-Postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık"* olarak değiştirilmiş; *"Ücretsiz E-posta Servis Sağlayıcı Güvenlik Ayarlarını Kullanabilme"* ölçütü *"E-Posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık"* olarak değiştirilmiştir. Düzey açıklamaları yeniden değerlendirilerek genişletilmiş ve ayırt ediciliğin arttırılması sağlanmıştır. Yazım yanlışlıkları düzeltilmiştir. Tablo 4'te düzenlenmiş *SGF-DPA'nın* boyutları ve ölçütleri görülmektedir.

Tablo 4

SGF-DPA Ölçütleri

Boyutlar	Ölçütler
E-Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık	E-postayı açma
	Gönderen adresini kontrol etme
	E-posta içeriğindeki bağlantıya tıklama
	E-postada istenen kişisel verileri gönderme
	E-posta içeriğindeki eki cihaza indirme
E-postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık	Yazım kurallarına uygunluğu kontrol etme
	E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme
	E-postayı gönderenin adresinin yazımını kontrol etme
	E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme
	E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme
E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık	E-posta şifre değiştirme sıklığı
	E-posta şifre uzunluğu
	E-posta şifresi ile klavye düzeni ilişkisi
	Kişisel verilerle şifre belirleme
	Karmaşık ve özel karakterlerle şifre belirleme
E-Posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık	Çift faktörlü kimlik doğrulama kullanma
	Telefonla doğrulama kullanma
	Kurtarma e-postası kullanma
	Güvenlik ayarları hakkında bilgi edinme
	Güncellemeleri uygulama

Gerekli güncellemeleri takiben düzeltme talep eden uzmanlara DPA tekrar gösterilmiş ve DPA'na son hali verilmiştir. Bu adım ile DPA'nın geçerlik çalışması tamamlanmıştır.

DPA'nın Güvenirliği

İki bağımsız puanlayıcı tarafından verilen puanların tutarlılığını veya uyuşmasını ifade etmektedir (Moskal & Leydens, 2019; Sarıca & Usluel, 2016). Dereceli puanlama anahtarları için iki tür güvenirlikten bahsedilebilir; Puanlayıcılar arası uyum ve puanlayıcılar arası güvenirlik.

Puanlayıcılar arası uyum, dereceli puanlama anahtarının kullanımı sonucunda puanlayıcılar arasındaki tutarlılık; puanlayıcılar arası güvenirlik ise farklı puanlayıcıların puanları arasındaki korelasyondur (Tinsley & Weiss, 2000).

Çok dereceli değerlendirmelerde iki değerlendirici arasındaki uyuşmayı hesaplamada kullanılan yöntemlerden biri kappa istatistiğinin bir türü olan "ağırlıklandırılmış kappa" yöntemidir (Şencan, 2005). Kappa katsayısından elde edilen değerler "zayıf uyuşma =< .20"; "kabul edilebilir uyuşma= .20-.40"; "orta derecede uyuşma= .40-.60"; "iyi uyuşma= .60-.80";"çok iyi uyuşma= .80-1.00" olarak yorumlanmaktadır (Şencan, 2005).

Araştırmada değerlendirici/puanlayıcı arası uyuşma yüzdesi ve Cohen Kappa katsayısı kullanılarak ölçeğin güvenirliği saptanmıştır. Uyuşma, belirli bir ölçütte değerlendirici/puanlayıcıların değerlendirmelerinde aynı puanı vermeleri anlamına gelir (Şencan, 2005).

Uyuşma oranının %70'in üzerinde olması nedeniyle değerlendirmenin güvenilir olduğuna karar verilmekte, anlamlı ve yorumlanabilir katsayılar .50 ile 1.00 arasında değişmektedir. Uyuşma oranı şans eseri denk gelme durumunu dikkate almadığından sınıflandırma kriteri ayrıca Kappa katsayısı ile de test edilmektedir (Şencan, 2005).

DPA geliştirme sürecinin ilk aşamasında oluşturulan taslak DPA, bir Ortaokul yedinci sınıfında öğrenim gören, 16 öğrencinin Bilişim Teknolojileri dersi kapsamında siber güvenlik

farkındalıklarını değerlendirmek amacıyla kullanılmıştır. Bu amaçla, öğrencilerin Bilişim Teknolojileri dersi kapsamında siber güvenlik öğrenme-öğretme süreci ve çalışmaları gözlemlenmiş, iki bağımsız değerlendirici tarafından puanlanarak ağırlıklı kappa katsayıları hesaplanmış ve DPA'na ilişkin güvenirlik sonuçları elde edilmiştir. Güvenirlik analizlerinin sonuçları Tablo 5'te sunulmuştur.

Tablo 5

SGF-DPA'nın Alt Boyutlarına Göre Puanlayıcılar Arası Uyuma İlişkin Ağırlıklı Kappa Katsayısı Sonuçları

Boyut	Ölçütler	N	κ
E-postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık	E-postayı açma	16	0.79
	Gönderen adresini kontrol etme	16	0.77
	E-posta içeriğindeki bağlantıya tıklama	16	0.74
	E-postada istenen kişisel verileri gönderme	16	0.72
	E-posta içeriğindeki eki cihaza indirme	16	0.73
E-postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık	Yazım kurallarına uygunluğu kontrol etme	16	0.61
	E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme	16	0.61
	E-postayı gönderenin adresinin yazımını kontrol etme	16	0.63
	E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme	16	0.60
	E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme	16	0.60
E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık	E-posta şifre değiştirme sıklığı	16	0.71
	E-posta şifre uzunluğu	16	0.64
	E-posta şifresi ile klavye düzeni ilişkisi	16	0.65
	Kişisel verilerle şifre belirleme	16	0.61
	Karmaşık ve özel karakterlerle şifre belirleme	16	0.61
E-posta Güvenlik Ayarlarının Kullanımına ilişkin Farkındalık	Çift faktörlü kimlik doğrulama kullanma	16	0.62
	Telefonla doğrulama kullanma	16	0.64
	Kurtarma e-postası kullanma	16	0.68
	Güvenlik ayarları hakkında bilgi edinme	16	0.67
	Güncellemeleri uygulama	16	0.62

Kappa değerleri 0.60 ile 0.79 arasındadır. Bu koşulda en düşük uyum, ***E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık*** boyutunun "*E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme*" ve "*E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme*" ölçütlerinde elde edilmişken (κ = 0.60) en yüksek uyum, ***E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık boyutunun*** "*E-postayı açma*" ölçütü için bulunmuştur (κ = 0,79).

E-Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık boyutunda; "*E-postayı açma*" ölçütünde puanlayıcılar arasında istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.79, p<.01). "*Gönderen adresini kontrol etme*" ölçütünde puanlayıcılar arasında istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.77, p<.01). "*E-posta içeriğindeki bağlantıya tıklama*" ölçütünde puanlayıcılar arasında istatistiksel olarak istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.74, p<.01). "*E-postada istenen kişisel verileri gönderme*" ölçütünde ise puanlayıcılar arasında istatistiksel istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.72, p<.01). "*E-posta içeriğindeki eki cihaza indirme*" ölçütünde ise puanlayıcılar arasında istatistiksel istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.73, p<.01).

E-postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık boyutunda; "*Yazım kurallarına uygunluğu kontrol etme*" ölçütünde puanlayıcılar arasında istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.61, p<.01). "*E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme*" ölçütünde puanlayıcılar arasında istatistiksel olarak anlamlı ve çok iyi uyuşma olduğu görülmektedir (κ = 0.61, p<.01). "*E-postayı gönderenin adresinin yazımını kontrol etme*" ölçütünde puanlayıcılar arasındaki arasında istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.63, p<.01). "*E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme*" ölçütünde puanlayıcılar arasında istatistiksel olarak anlamlı ve iyi uyuşma görülmektedir (κ

= 0.60, p>.01). “*E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme*” ölçütünde puanlayıcılar arasında istatistiksel olarak istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.60, p<.01).

E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık boyutunda; “*E-posta şifre değiştirme sıklığı*” ölçütünde puanlayıcılar arasında istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.71, p<.01). “*E-posta şifre uzunluğu*” ölçütünde puanlayıcılar arasında istatistiksel olarak anlamlı ve çok iyi uyuşma olduğu görülmektedir (κ = 0.64, p<.01). “*E-posta şifresi ile klavye düzeni ilişkisi*” ölçütünde puanlayıcılar arasında istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.65, p<.01). “*Kişisel verilerle şifre belirleme*” ölçütünde puanlayıcılar arasında istatistiksel olarak anlamlı ve iyi uyuşma görülmektedir (κ = 0.61, p>.01). “*Karmaşık ve özel karakterlerle şifre belirleme*” ölçütünde puanlayıcılar arasında istatistiksel olarak istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.61, p<,01).

E-posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık boyutunda; “*Çift faktörlü kimlik doğrulama kullanma*” ölçütünde puanlayıcılar arasında istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.62, p<.01). “*Telefonla doğrulama kullanma*” ölçütünde puanlayıcılar arasında istatistiksel olarak anlamlı ve çok iyi uyuşma olduğu görülmektedir (κ = 0.64, p<.01). “*Kurtarma e-postası kullanma*” ölçütünde puanlayıcılar arasında istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.68, p<.01). “*Güvenlik ayarları hakkında bilgi edinme”* ölçütünde puanlayıcılar arasında istatistiksel olarak anlamlı ve iyi uyuşma görülmektedir (κ = 0.67, p>,01). “*Güncellemeleri uygulama*” ölçütünde puanlayıcılar arasında istatistiksel olarak istatistiksel olarak anlamlı ve iyi uyuşma olduğu görülmektedir (κ = 0.62, p<.01).

Siber Güvenlik Farkındalığı Öğrenci Görüşme Formu

Öğrencilerin Siber Güvenlik odaklı mikro-öğrenme nesnesi kullanarak kendilerini güçlü hissettikleri yönleri belirlemek amacıyla Tablo 6’te görülen soruları içeren öğrenci görüşme formu oluşturulmuştur. Görüşme formunun son hali EK B’de yer almaktadır.

Tablo 6

Siber Güvenlik Farkındalığı Öğrenci Görüşme Formu Soruları

Aşamalar	Açıklamalar
Güçlü yönleri ve eksik yönleri	Siber Güvenlik mikro-öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmede kazandığım güçlü yönler nelerdir?
	Siber Güvenlik mikro-öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmede zayıf yönler nelerdir?
Oluşturduğu fırsatlar engeller	Siber Güvenlik mikro-öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmemi kolaylaştıran yönler nelerdir?
	Siber Güvenlik mikro-öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmemi zorlaştıran/engelleyen yönler nelerdir?

Araştırmacının Rolü

Araştırmada araştırmacı ve uygulayıcılar eşit oranda sorumluluk almış, her aşama iletişim halinde ilerletilmiştir. Tasarım tabanlı araştırmada uygulayıcılar ve araştırmacıların uzun vadeli iş birlikleri içinde olmalarını gerektirmektedir. Uygulayıcılar ve araştırmacıların uzmanlıkları, araştırma sürecinin farklı aşamalarındaki kararları etkileyebilmektedir. Bu kapsamda araştırmacı, uygulama süreci, veri toplama araçları geliştirilmesi, verilerin toplaması ve veri analizi sürecinde aktif rol oynamıştır.

Araştırma Modeli

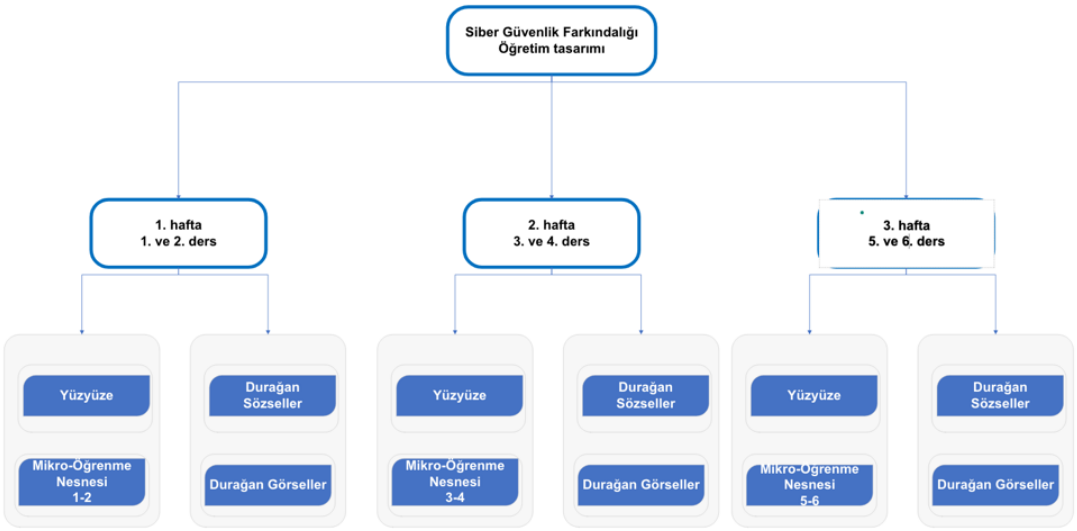
Araştırma, ilköğretim düzeyinde her bir mezo döngüde üç mikro döngü olacak şekilde iki mezo döngüde gerçekleştirilmiştir. Araştırmanın modeli, McKenney ve Reeves'in (2012) Eğitsel Tasarım Tabanlı araştırma modeli temel alınarak uygulanmıştır.

Birinci Mezo Döngü.

Araştırmanın ilk mezo döngüsü, *Analiz-İnceleme*, *Tasarım-Geliştirme* ve *Değerlendirme- Yansıma* mikro döngülerini içermektedir. Birinci mezo döngü 2023 – 2024 eğitim-öğretim yılı bahar döneminde 3 haftalık bir süreçte, haftada 2 saat olacak şekilde gerçekleştirilmiştir.

Şekil 4

Siber Güvenlik Ders Tasarımı



Tablo 7

Birinci Mezo Döngüde SGMÖN Tasarım Süreci

Mikro Döngü	Aşama	Süreç
Analiz ve İnceleme	Problemin tanımlanması	Problemin araştırmacı ve uygulayıcılar ile işbirlikli analizi
	Bilgi toplama	Problemin teorik çerçeve ve yöntemlerini belirleme
	Gerçek yaşam ile örneklendirme	Başlangıç tasarımını geliştirme
Tasarım ve Geliştirme	Mikro öğrenme nesnesi tasarlama Prototip geliştirme	Tasarımın test ve iyileştirme döngüleri Kuramsal fikirleri uygulamaya geçirme
Değerlendirme ve Yansıma	Geliştirilen prototipi uygulama Veri toplama Toplanan verileri analiz etme	Tasarımın etkililiğini değerlendirmek Ürüne tasarım ilkelerini yansıtmak

Tablo 7 incelendiğinde ilk mezo döngüdeki her bir mikro döngünün adımları ile bu adımların SGMÖN'nin oluşturulma sürecinin hangi ana ve alt ölçütlerine karşılık geldiği görülmektedir.

Analiz ve İnceleme

Analiz ve İnceleme ilk mikro döngüsü, araştırmanın bağlamına yönelik olarak kapsamlı bir şekilde problemin tanımlanması, bilgi toplama ve gerçek yaşam ile örneklendirme çalışmalarından oluşmaktadır. Bu mikro döngü, gerçek yaşamda karşılaşılan uygulanabilir bir problemin tanımlanması ile başlanmıştır. Araştırmayı uygulayacak kişiler ve araştırmacılar arasında anlamlı iş birliğinin kurulabilmesi ve araştırma bağlamının koşullarının belirlenmesi için bu döngüde iki bilgisayar öğretmeni, bir öğretim tasarımı uzmanı, bir dijital içerik geliştirme uzmanı ve bir siber güvenlik uzmanı ile üç toplantı gerçekleştirilmiştir.

İlk toplantıda, siber güvenlik kavramı üzerinde tartışılmıştır. Öğretmenler öğrencilerin kişisel verilerin gizliliğine önem vermediklerini, sosyal ağlarda dikkatli davranmadıklarını ve bu nedenle taciz, zorbalık gibi eylemlerle karşı karşıya kaldıklarını belirtmişlerdir. Muniandy ve arkadaşları (2017) yapmış olduğu çalışmada katılımcıların siber güvenlik bilgilerinin yetersiz olduğunu ve siber tehditlere maruz kalabileceklerini belirtmiştir. Jerrim (2023), 2018 PISA verilerine göre 15 yaşındaki çocuklara yönelik yapmış olduğu çalışmada Türkiye de her beş çocuktan birinin kimlik avı e-postalarına cevap verme eğiliminde olduğunu vurgulamıştır. Witsenboer ve arkadaşları (2022), siber güvenlik eğitiminin, çocukların çevrimiçi donanımları kullanmaya başlamasıyla birlikte ilköğretim seviyesinde başlaması gerektiğini vurgulamıştır. Milli Eğitim Bakanlığı'nın (MEB) yayınlamış olduğu İlköğretim ikinci kademe Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programında; *6. Sınıf seviyesinde,* "Bilişim suçlarına karşı alınabilecek önlemler ve stratejiler geliştirir" kazanımının temel alınabileceği belirtilmiştir (MEB, 2018). MEB'in ortaya koymuş olduğu kazanımlar, alan yazında vurgulanan ilköğretim seviyesindeki öğrencilerin siber güvenlik ihtiyaçları ve öğretmenlerin belirttiği sorunlar çerçevesinde siber güvenlik farkındalığına yönelik olarak e-postaları hedef alan siber tehditler problemine karar verilmiştir.

Öğrencilerin öğrenme süreçlerinde destek olacak eğitsel dijital materyallerin etkililiği konusunda çelişkili görüşlere vurgu yapılmıştır. Mikro öğrenme, geleneksel öğrenme yaklaşımlarından teknoloji destekli öğrenme yaklaşımlarına geçiş sürecinde önemli bir strateji haline gelmiştir. Mikro-öğrenme stratejisinin temelini oluşturan kısa süreli (3-5 dakika) öğretim parçalarından ve spesifik öğrenme hedeflerinden oluşan, (Göschlberger, 2017) öğrenme nesnelerinin tasarlanması hususunda görüş birliğine varılmıştır. Öğretim materyallerinin son yıllarda alan yazında pek çok araştırmaya konu olan, birçok disiplinde öğretim materyali geliştirme sürecinde incelenen mikro-öğrenme stratejisi çerçevesinde geliştirilmesine karar verilmiştir. Araştırmanın konusu ve öğrencilerin dijital araçları kullanabilme bilgi ve becerileri göz önünde bulundurularak uygulamanın ilköğretim 6. Sınıf seviyesinde Bilişim Teknolojileri ve Yazılım Dersinin uygun olabileceği görüşüne varılmıştır.

İkinci toplantıda, siber güvenlik konusunda alan yazındaki uygulama örnekleri üzerinde tartışılmıştır. Öğretimin kazanımlarına dayandırılan siber güvenlik içeriği mikro-öğrenme stratejisine uygun olarak küçük parçalara ayrılmıştır. Her bir parçanın kapsamı bir mikro öğrenme nesnesi oluşturacak şekilde planlanmıştır. Siber güvenlik içeriğinin 6 parçaya ayrılmasına karar verilmiştir. Mikro-öğrenme stratejisine göre hazırlanacak, storyboard'ların içerik kapsamının aşağıdaki gibi olması konusunda görüş birliğine varılmıştır.

E-Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık; ***Mikro-Öğrenme Nesnesi;*** Siber güvenliğin tanımına değinilmiştir. Siber tehditlerle karşılaşılabilecek araçlar vurgulanmış, kişisel verilerin siber saldırılar için tehdit unsuru olduğuna dikkat çekilmiştir. Siber ortamda karşılaşılabilecek tehditlerden bahsedilmiştir. Oltalama, virüs, zararlı yazılım, zombi bilgisayar, spam ve solucanlar gibi yaygın olarak karşılaşılan siber saldırı türleri tanımlanmıştır. Siber saldırganlar, bilgisayar korsanları (Hackers), taklitçiler (Impersonators), çevrim içi avcılar (online predators), siber pedofili (cyber stalkers), siber zorbalar (cyber bulying) tanımlanmıştır. Bu saldırganların nasıl ve hangi yollarla saldırdıkları vurgulanmıştır. Virüslerin sistemlere verdiği zararlardan

ve cihazlara bulaşma yollarına değinilmiştir. E-posta hedefli siber tehditler yoluyla sanal dolandırıcılık konusunda bilgilendirme yapılmış, siber saldırganların hedeflediği verilerden bahsedilmiştir. E-postaları hedef alan siber tehditlerin nasıl yapıldığı, e-posta saldırılarının nasıl göründüğü ve sahte e-postaların içeriği anlatılmıştır. Fiziksel postalarla e-postaların güvenlikleri karşılaştırılmıştır. E-postaların güvenlik riskleri vurgulanmıştır. E-posta hırsızlığına yol açabilecek durumlar belirtilmiştir.

E-Postalarda Yazım Hatası İçeren Tehditlere Yönelik Farkındalık Mikro-Öğrenme Nesnesi; Siber güvenlik saldırılarının nasıl yapıldığından bahsedilmiştir. Siber korsanların hangi kimliklerle ve nasıl mesaj gönderdiğine değinilmiştir. siber güvenlik tehditleri içeren e-postaların içeriği anlatılmıştır. Hedef kullanıcıların siber korsanların e-postalarını yanıtlamalarının sonuçları vurgulanmıştır. Siber güvenlik tehditleri içeren e-postalarının tespit edilme yollarına değinilmiştir. Bilgi hırsızlığı kavramı açıklanmış, saldırganların hedeflediği ve ele geçirebileceği veriler anlatılmış ve ele geçirilen verilerin hangi amaçlarla kullanılabileceği belirtilmiştir.

E-Posta Şifre Hedefli Tehditlere Yönelik Farkındalık Mikro-Öğrenme Nesnesi; Siber güvenlik saldırıları tipleri anlatılmıştır. siber güvenlik tehditlerinin yoğun yaşandığı e-postaları alındığında yapılması gerekenler vurgulanmıştır. Şifre hedefli saldırıların nasıl ve ne amaçla yapıldığından bahsedilmiştir. Güçlü şifre belirlemenin önemi ve nasıl yapılacağı belirtilmiştir. E-postaları hedef alan siber tehditlerin tespitinde yazım kurallarının önemi, e-posta içeriğindeki reklam ve ödül vaadi gibi oluşturulan tuzaklar, kişisel verilerin paylaşımının sakıncaları anlatılmıştır.

E-Posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık Mikro Öğrenme Nesnesi; Sıklıkla kullanılan ve ücretsiz e-posta servis hizmeti veren Gmail, Hotmail, Yahoomail ve Yandexmail e-posta servislerinin kullanımında yapılan hatalardan bahsedilmiştir. Gmail hesaplarının güvenlik ayarları konusunda bilgilendirme yapılmıştır. E-posta hesabının güvenlik ayarlarının önemi vurgulanmış ve yapılması gereken ayarlar anlatılmıştır. Güvenlik ayarlarından bağlı cihazların kontrolü ve yönetimi, şifre yönetimi, çift

faktörlü doğrulama, hesaba kurtarma e-postası ve telefon bilgisi oluşturma, e-posta hizmeti veren kuruluşun tespit ettiği güvenlik açıklarını görme ve giderme konularının önemi anlatılmış ve yapılması gerekenler gösterilmiştir. Kişisel verilerin gizliliği ve yapılması gereken gizlilik ayarları belirtilmiştir. Kişisel verilerin paylaşımı konusunda dikkat edilmesi gereken hususlar gösterilmiştir.

Öğretim neticesinde hedeflenen kazanımlarla Siber Güvenlik farkındalığının "*E-Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık*", "*E-Postalarda Yazım Hatası İçeren Tehditlere Yönelik Farkındalık*", "*E-Postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık*" ve "*E-Posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık*" boyutlarında değerlendirilmesine karar verilmiştir.

Üçüncü toplantıda, araştırmanın konusu ve hedef kazanımları kapsamında kullanılacak ölçme araçları tartışılmıştır. Her biri 5 maddeden oluşan 4 boyutlu 20 maddeli "Siber Güvenlik Farkındalığı Dereceli Puanlama Anahtarı" 'nın taslağı geliştirilmiştir. Geliştirilen taslak,

1. E-Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık
2. E-Postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık
3. E-Posta Şifre Hedefli Tehditlere Yönelik Farkındalık
4. E-Posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık

boyutlarından oluşmaktadır.

E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık boyutu, Downs ve arkadaşları (2007) yapmış olduğu çalışmada kimlik avı e-postalarına aldanma ve meşru e-postalara güvenme eğilimlerine yönelik olarak bir anket uygulamıştır. Weaver ve arkadaşları (2021) kullanıcıları kimlik avı e-postalarını tespit etme konusunda eğitmek amacıyla Jigsaw çevrimiçi kimlik avı testinin etkinliğini sınamışlardır. Alanyazından elde edilen bilgiler e-posta hedefli siber tehditlerin virüs içeren ekler, kullanıcıyı sahte sitelere yönlendiren bağlantılar içerdiği tespit edilmiştir. *E-postalarda*

kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalığın değerlendirilmesinin çalışmanın amacına katkıda bulunacağı görüşüne varılmış; gelen e-postayı açma, göndericinin adresini kontrol etme, e-posta içeriğindeki bağlantıları tıklama, talep edilen kişisel verileri paylaşma ve e-posta eklerini indirme davranış kalıplarının değerlendirilmesine karar verilmiştir.

E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık boyutu, Downs ve arkadaşlarının (2007) ve Weaver ve arkadaşlarının (2021) yapmış olduğu çalışmalardan e-posta içeriğindeki yazım hatalarının kimlik avı e-postalarının tespitinde etkili olduğu anlaşılmıştır. E-postalardaki metnin dil bilgisi kurallarına uygunluğunu kontrol etme, e-postadaki bağlantıların adreslerinin doğruluğunu kontrol etme, gönderici adresinin yazılışını kontrol etme, e-posta içeriğindeki reklam bağlantısındaki adresin reklam sahibinin adresi olduğunu kontrol etme ve e-posta içeriğindeki ödül bağlantısındaki adresin ödülü vadedenin adresi olduğunu kontrol etme davranışlarının değerlendirilmesine karar verilmiştir.

E-postalarda şifre hedefli tehditlere yönelik farkındalık boyutu, Muniandy ve arkadaşları (2017) çalışmasında öğrencilerin kötü amaçlı yazılım, şifre kullanımı, kimlik avı, sosyal mühendislik ve çevrimiçi dolandırıcılık açısından siber güvenlik davranışlarının durumunu ölçmüştür. Muniandy ve arkadaşlarının (2017) çalışması ve Weaver ve arkadaşlarının (2021) çalışması şifre kullanımının önemini ve kullanıcı şifrelerini ele geçirmeye yönelik kimlik avı e-postalarını ortaya koymuştur. E-posta şifre değiştirme sıklığı, tanımlanan şifrenin uzunluğu, şifrenin klavye üzerindeki tuş düzenini takip edip etmediği, şifrenin kişisel verilerden oluşup oluşmadığı, şifrenin karmaşık ve özel karakterler içermesi davranışlarının değerlendirilmesi kararlaştırılmıştır.

E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık boyutu, Shevchuk ve arkadaşları (2020) kullanıcıların çoğunun güvenlik ayarlarını kullanmadığını ve çok fazla kişisel bilgi paylaşmanın getirdiği risklerin farkında olmadığını belirterek kullanıcıları etkileyen güvenlik ayarlarına ilişkin farkındalığı tartışmıştır. Çift faktörlü kimlik doğrulama,

telefonla doğrulama, kurtarma e-postası ile doğrulama, güvelik ayarları hakkında bilgi sahibi olma ve güncellemeleri uygulama davranışlarının değerlendirilmesi görüşüne varılmıştır.

Mikro-öğrenme nesneleri hakkında öğrenci görüşlerinin hangi yöntemle toplanacağı üzerinde tartışılmıştır. "*Siber Güvenlik Farkındalığı Öğrenci Görüşme Formu*" hazırlanmasına karar verilmiştir. Öğrenci görüşme formu,

1. *Siber Güvenlik mikro-öğrenme nesneleri ile, siber saldırıları tespit etmede kazandığım güçlü yönler nelerdir?*

2. *Siber Güvenlik mikro-öğrenme nesneleri ile, siber saldırıları tespit etmede zayıf yönler nelerdir?*

3. *Siber Güvenlik mikro-öğrenme nesneleri ile, siber saldırıları tespit etmemi kolaylaştıran yönler nelerdir?*

4. *Siber Güvenlik mikro-öğrenme nesneleri ile, siber saldırıları tespit etmemi zorlaştıran/ engelleyen yönler nelerdir?* maddelerini içermektedir.

Tasarım ve Geliştirme

Bu mikro döngüde, analiz ve incelene evresinde alan uzmanları ile iş birliği halinde belirlenen gereksinimlere ve alan yazına göre tasarım ve geliştirme süreci detaylandırılmış, öngörülen süreç modeli ve adımları belirlenmiştir. Çoklu ortam materyallerinin içeriğinde kullanılacak nesneler tartışılmıştır.

Analiz ve inceleme mikro döngüsünde ulaşılan çıkarımlar ve öğretmenlerin sürece yönelik önerilerine göre siber güvenlik odaklı mikro öğrenme nesnesi yönergesini uygulama adımlarını içeren yönerge oluşturulmuştur. Öğrenciler, her dersin öğretme ve öğrenme sürecinde siber güvenlik mikro-öğrenme nesneleri ile yapılacak olan etkinlikten haberdar edilmişlerdir.

Bilişim Teknolojileri öğretmeni siber güvenlik mikro öğrenme nesnelerini sunmuştur ve daha sonra siber güvenlik örnekleri ve etkinlikleri üzerinden siber güvenlik kavramı incelenmiştir. Öğrencilerin istedikleri zaman inceleyebilecekleri öğrenme nesneleri; (a) E-

Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık, (b) E-Postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık, (c) E-Postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık, (d) E-Posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık, oluşmaktadır.

Tasarımda kullanılan renkler öğrencilerin ilgisini uyandıracak, vurgulama ve görülebilirlik açısından uygun bir renk kompozisyonu oluşturacak (Karataş, 2003) şekilde seçilmiştir. Öğrenme nesnelerinin ara yüzünde siyah beyaz ve kırmızı renklerin kullanılmasına karar verilmiştir. Kırmızı renk rekabet ve saldırı gibi duyguları anımsatırken, beyaz renk temizlik, saflık, gençlik ve masumiyetin rengidir (Karataş, 2003). Tasarımda kullanılacak görsel ve sözsel unsurlar tespit edilmiştir. Öğrencilerin seviyesine uygun, konuya dikkat çekici metinler ve ilgili görsellerin kullanılması görüşüne varılmıştır. Görsel nesnelerde, içeriğe uygun olarak, hacker, bilgisayar, kimlik avı, virüs ve bunun gibi görsellerin kullanımı benimsenmiştir. Öğretim materyalinin Microsoft Office PowerPoint uygulaması kullanılarak tasarlanmasına karar verilmiştir.

Resimli öykü taslağı (Storyboard) MS Office Powerpoint paket programı aracılığıyla öğretim tasarım uzmanı desteği ile hazırlanmıştır. Belirlenen kazanımlar kapsamında mikro-öğrenme nesnelerinin ara yüz tasarımlarına başlanılmıştır. Her bir sahnede öğrencilere sunulacak sözsel ve görseller belirlenmiş, resimli öykü taslağı üzerinde yerleştirilerek ara yüz tasarımları yapılmıştır. Analiz ve inceleme evresinde kararlaştırılan içerik taslağı çerçevesinde, resimli öykü taslağı oluşturulmuştur.

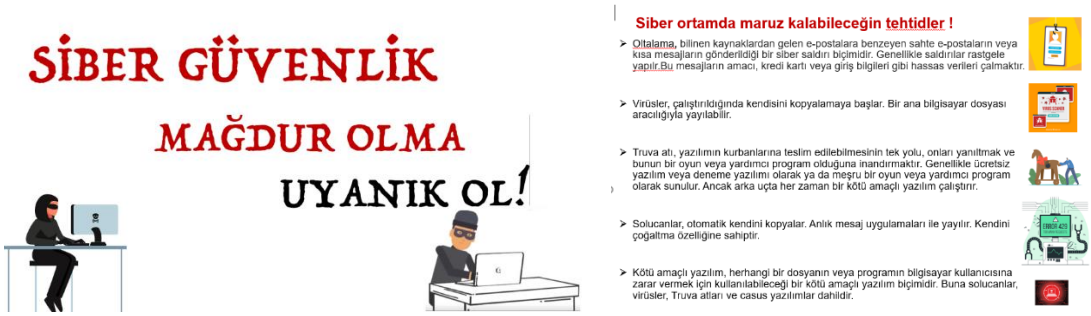
Mikro-Öğrenme Nesnelerinin tasarımı; İçerik bağlamında alan yazında yer alan tanımlamalar ışığında, kavramlara karşılık gelen görsel nesneler tespit edilmiştir. Benzer konularda hazırlanmış olan içerikler (resim, video metin vb. gibi) incelenmiştir. Yapılan araştırmalar neticesinde mikro-öğrenme nesnelerinde kullanıma uygun olduğu düşünülen sözsel ve görsel materyaller hazırlanmıştır. Planlanan içeriğe uygun olacak şekilde ara yüz tasarımları yapılmıştır. Mikro öğrenme nesneleri, öğretim programıyla uyumlu, içeriğin

doğru ve güncel, sade ve anlaşılır bir dille, öğrenciyi güdüleyici ve ilgiyi sürekli tutacak özelliklere sahip olarak (Seferoğlu, 2009) düzenlenmiştir.

E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık mikro öğrenme nesnesi tasarlanmıştır (Şekil 5). Siber güvenlik kavramına dikkat çekilmiştir. Siber tehditler konusunda öğrencileri bilgilendirecek konulara değinilmiştir. E-postaları hedefleyen siber tehditler farkındalığına yönelik içerikler tasarlanmıştır.

Şekil 5

E-Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık Mikro Öğrenme Nesnesi Tasarım Örneği



E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık mikro öğrenme nesnesi tasarlanmıştır (Şekil 6). E-postaları hedefleyen siber saldırıların nasıl yapıldığı hakkında bilgiler tasarıma eklenmiştir. Siber korsanların hedeflediği veriler ve elde edilen verilerin hangi amaçlarla kullanılabileceğinden bahsedilmiştir. Siber güvenlik tehditleri içeren e-postaların içeriğinden bahsedilmiştir.

Şekil 6

E-Postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık Mikro Öğrenme Nesnesi Tasarım Örneği

E-postalarda şifre hedefli tehditlere yönelik farkındalık mikro öğrenme nesnesi tasarlanmıştır (Şekil 7). Güçlü şifre kullanımı, şifrelerin belirli aralılarla değiştirilmesinin önemine değinilmiştir. Şifrelerde kişisel veri kullanımının sakıncalarından bahsedilmiştir.

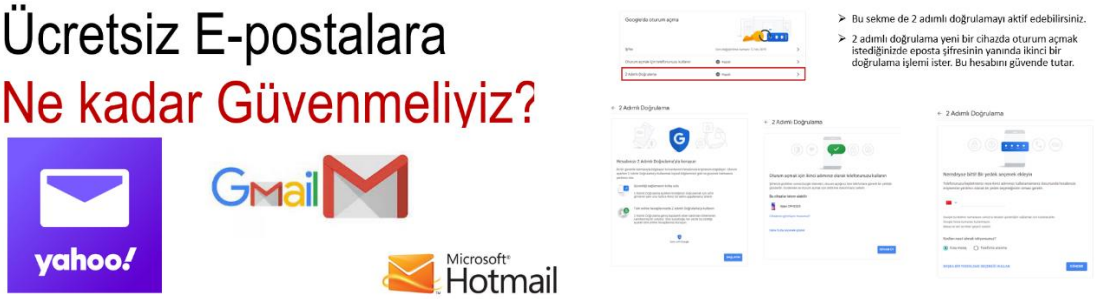
Şekil 7

E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık Mikro Öğrenme Nesnesi Tasarım Örneği

E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık mikro öğrenme nesnesi tasarlanmıştır (Şekil 8). Sınıf içerisinde örnek olarak kullanılan Gmail e-posta uygulamasının sunmuş olduğu güvenlik ayarları içeriğe eklenmiştir. Güvenlik ayarlarının kullanımı, önemi, faydalarından söz edilmiştir.

Şekil 8

E-postalarda Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık Mikro Öğrenme Nesnesi Tasarımları



Mikro öğrenme nesnelerinin ara yüzleri, yukarıda görüldüğü şekilde tasarlanmıştır. Sahne tasarımları tamamlanan mikro öğrenme nesneleri alan uzmanlarının görüşüne sunulmuş ve uygun olduğu görüşüne varılmıştır.

İkinci Mezo Döngü.

İkinci mezo döngü, birinci döngünün yansıma evresinde elde edilen bulgular ile tespit edilen problemlerin tanımlanması ile başlamıştır. *Analiz ve İnceleme*, *Tasarım ve Geliştirme*, *Değerlendirme ve Yansıma* olmak üzere üç mikro döngü tamamlanmıştır. Birinci mezo döngüde kullanılmış olan mikro öğrenme nesneleri ikinci mezo döngü sürecinde kullanılmak üzere iyileştirilmiş, tasarıma uygun geliştirme yapılmış ve değerlendirilmiştir. Mikro öğrenme nesnelerinin kullanımı neticesinde elde edilen bulgular araştırmacı tarafından yorumlanmıştır.

Bu gereksinimlerden hareketle ikinci mezo döngü 2023 – 2024 eğitim – öğretim yılı Bahar döneminde 3 haftalık bir süreçte haftada 2 saat olacak şekilde planlanarak gerçekleştirilmiştir. İkinci mezo döngüde siber güvenlik odaklı mikro öğrenme nesneleri tasarım süreci Tablo 8'de sunulmuştur.

Tablo 8

İkinci Mezo Döngüde SGMÖN Tasarım Süreci

Mikro Döngü	Aşama	Süreç
Analiz ve İnceleme	Problemin tanımlanması	Birinci mezo döngüde karşılaşılan problemler nelerdir?
		Problemin çözümü için iyileştirilmesi gereken nedir?
	Bilgi toplanması	Tasarımı iyileştirmek için gerekli veriler nelerdir?
	Gerçek yaşam ile örneklendirilmesi	Ücretsiz e-posta uygulamaları
Tasarım ve Geliştirme	Mikro öğrenme nesnelerini<n tasarlanması	Tasarım için materyallerin toplanması
		Tasarımın planlanması
	Prototip geliştirilmesi	Planlanan tasarımın geliştirilmesi
		Öğretim tasarımının tasarlanması
Değerlendirme ve Yansıma	Geliştirilen prototipi uygulama	Mikro öğrenme nesnesi uygulanır
	Veri toplama	Uygulama sonucu veriler toplanır
	Toplanan verileri analiz etme	Veriler analiz edilir

Tablo 8 incelendiğinde ikinci mezo döngüdeki her bir mikro döngünün adımları ile bu adımlarda siber güvenlik mikro öğrenme nesnelerinin geliştirilme süreci özetlenmektedir.

Analiz ve İnceleme.

İkinci mezo döngüde siber güvenlik mikro öğrenme nesnelerinin yeniden düzenleme süreci, birinci mezo döngünün değerlendirme ve yansıma mikro döngüsünde elde edilen bulgular ışığında yapılmıştır. Bu kapsamda alan uzmanları ile iki toplantı gerçekleştirilmiştir.

Birinci toplantıda; ilk mezo döngüde öğrencilerin mevcut içeriğe odaklanmakta zorluk yaşadıkları, sınıf içerişinde öğrencilerin öğretime katılımı, öğretmen ile öğrenciler arasında etkileşimin yeterli olmadığı gözlemlenmiştir. Öğrencilerin katılım sağlamada zorlanması, dikkatlerinin başka yönlere kaymasının nedenleri tartışılmıştır. Bir öğretim materyalinden öğrenciyi güdüleyici ve ilgiyi sürekli tutacak özelliklere sahip olması

beklenmektedir (Seferoğlu, 2009). Bu nedenle öğrencilerin ilgisini çekecek bir unsurun eklenmesi görüşüne varılarak, mikro-öğrenme nesnelerinde kullanılmak üzere, motivasyonu arttıracak bir karakter tasarımı yapılmasına karar verilmiştir. Siber korsanları çağrıştıran siyah korsan şapkalı ve siyah göz bantlı, hedef kitlenin yaş seviyesine uygun görünümde bir karakter tasarımı planlanmıştır.

Grubbs (2022) çalışmasında siber tehditleri önlemede kısa bir videonun daha etkili olduğunu vurgulamıştır. İçeriğin kısa videolar halinde yeniden düzenlenmesinin etkili olacağı değerlendirilmiştir. Grubbs'un (2022) önerileri doğrultusunda ikinci döngüde öğrenme nesnelerinin yeniden düzenlenmesi görüşülmüştür. Öğretimin akışında dikkatin öğretim materyalinden uzaklaşmasını önlemek için, hareketli bir içerik oluşturulmasına ve içeriğe uygun, dikkati dağıtmayacak tonda ve ritimde arka plan müziği eklenmesine karar verilmiştir. Görüş birliğine varılan değişiklikleri uygulamak için bir video düzenleme aracı kullanılması kararlaştırılmış, ilk döngüde yansı olarak tasarlanan mikro-öğrenme nesnelerinin ikinci döngüde video formatında yeniden düzenlenmesi görüşüne varılmıştır. Öğrenme nesnelerini daha gerçekçi hale getirmesi ve metinlerin ekranda çiziminin öğrenci ile etkileşimi sağlaması amacı ile el yazısı ile çizim efekti eklenmesi uygun görülmüştür. Yine öğretimi daha gerçekçi hale getirmek ve kullanılan nesneleri çizim efekti ile oluşturmak için Taşınabilir Ağ Grafiği (Portable Network Graphic- PNG) formatında kullanılan nesneler yerine, Ölçeklenebilir Vektör Grafiği (Scalable Vector Graphics- SVG) formatında nesneler kullanımına ve başlıkların SVG formatında oluşturulmasına karar verilmiştir.

Mikro-öğrenme stratejisi doğası gereği birbirinden bağımsız gibi görünen öğretim unsurlarının, anlamlı bölümlere ayrılmış bir bütünün parçalarıdır. Fernandez (2014) mikro öğrenme kullanmanın amacını, kısa ve odaklanmış üniteler kullanarak bilgiyi yaymak, daha büyük bir konunun kavramlarını kümülatif olarak daha küçük parçalar halinde göstererek öğrencilerin yeni bilgilere konsantre olmalarını ve bunları akılda tutmalarını kolaylaştırmak şeklinde ifade etmiştir. Mikro-öğrenme stratejisi öğrencilerin kendi öğrenme hızlarında, kendi belirledikleri şekilde öğrenmesi amacına uygun bir öğretim stratejisidir.

Sankaranarayanan ve arkadaşları (2022) mikro öğrenme stratejisini ilgi çekici kılan özelliğin, öğrenenlerin eğitim içeriğine ve görevlerine hızlı bir şekilde erişme yeteneği sağlayarak bilgi ve becerileri etkili bir şekilde kazanmaları ve sahip olduklarını uygulamalarına olanak tanıması şeklinde açıklamıştır. Bu nedenle ilk döngüde doğrusal olarak planlanan öğretim sürecinin ikinci döngüde sarmal olarak yapılması planlanmıştır. Geliştirilen mikro-öğrenme nesnelerinin öğretim sürecinde kullanımında Öğrenme Yönetim Sistemi (Learning Management System - LMS) kullanımına karar verilmiştir. Ara yüzlerinde kırmızı ve beyaz renklerin kullanımı uygun bulunmuştur.

Berkowitz (2017) mikro öğrenme stratejisini temel alan öğrenme nesnelerinin tasarlanması, geliştirilmesi, uygulanması ve değerlendirilmesi beklenen öğrenme çıktılarına ulaşmak için bir çerçeveye uyması gerektiğini belirtmiştir. Hug (2005) mikro öğrenmeyi yedi boyuta dayalı bir öğretim çerçevesi olarak tanımlamıştır. Bu boyutlar; (1) Kısa ölçülebilir zaman, çaba ve zaman tüketiminin derecesi olan öğrenme süresi, (2) Küçük öğrenme üniteleri, basit konular ve dar konular içeren öğrenme içeriği, (3) Modüller setini ve informal öğrenme gibi öğrenme modelinin türünü ifade eden müfredat, (4) Parçalara, bölümlere ve bilgi kırıntılarına odaklanan öğrenme formu, (5) Ayrı, bağlantılı, konumlandırılmış veya entegre faaliyetlere odaklanan öğrenme süreci, (6) Öğrenme nesneleri, yüz yüze ve multimedya kullanan öğrenme ortamı ve (7) Davranışçı, yapılandırmacı ve sosyal öğrenme perspektiflerini içeren öğrenme tipidir. Bu çerçeveye uygun olarak mikro öğrenme nesnesi yeniden düzenlenmiştir. Bu çerçevede dersin öğretim tasarımı ikinci toplantıda tartışılmıştır.

İkinci toplantıda; öğretim sürecini desteklemek, ilk döngüde düşük olan öğrenci katılımını artırmak amacıyla öğretimin sınıf içi etkinlikler ile desteklenmesi konusunda görüş birliğine varılmıştır. İkinci mezo döngüde öğrencilere animasyonlu bir tasarım kullanılmasına ve öğrenciler ile öğretmenin etkileşimini artıracak etkinlikler uygulanmasına karar verilmiştir. Çözüm tasarlama ve çözüm geliştirme mikro döngülerinde yapılan düzenlemelerle sürecin olabildiğince renkli, öğrenci ile öğretmen iletişimini artıran, mikro-öğrenme nesnelerinin etkililiğini destekleyici bir tasarım ile sürdürülmesi amaçlanmıştır.

Mikro-öğrenme nesnelerinin yeniden tasarımı için VideoScribe uygulamasının kullanımının uygun olacağına karar verilmiştir. Bu uygulama, animasyon içeren bir tasarım oluşturma imkânı sağlamakla birlikte, renkli, eğlenceli ve öğrencilerin seviyesine uygun bir dijital ortam sunmuştur.

Tasarım ve Geliştirme.

Birinci mezo döngüde olduğu gibi "*E-Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık*, *E-Postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık*, *E-Posta Şifre Hedefli Tehditlere Yönelik Farkındalık*, *E-Posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık*" konularında mikro öğrenme nesnelerinin yeniden tasarımına karar verilmiştir. Karar verilen sahne tasarımları Storyboard üzerinde yerleştirilmiş, mikro öğrenme nesnelerinin taslağı tamamlanmıştır. Hazırlanan taslak alan uzmanlarının görüşüne sunulmuş, alan uzmanları görüşleri doğrultusunda gerekli düzenlemeler yapılmıştır. VideoScribe uygulaması kullanılarak oluşturulan taslağa uygun olarak mikro öğrenme nesnelerinin prototipi oluşturulmuştur. Şekil 9 da görüldüğü üzere mikro-öğrenme nesnesi karakter tasarımı hazırlanarak taslaklar içerisinde kullanılmıştır.

Şekil 9

Mikro Öğrenme Nesnelerinde Kullanılan Karakter Tasarımı

E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık mikro öğrenme nesnesi yeniden düzenlenmiştir. Öğrenme hedeflerine uygun olacak şekilde iki adet mikro öğrenme nesnesi halinde tasarım gerçekleştirilmiştir. Birinci mikro öğrenme nesnesinde, siber güvenliğin tanımına değinilmiştir. Siber tehditlerle karşılaşılabilecek araçlar vurgulanmış, kişisel verilerin siber saldırılar için tehdit unsuru olduğuna dikkat çekilmiştir. Siber ortamda karşılaşılabilecek tehditlerden bahsedilmiştir. Oltalama, virüs, zararlı yazılım, zombi bilgisayar, spam ve solucanlar gibi yaygın olarak karşılaşılan siber saldırı türleri tanımlanmıştır. Siber saldırganlar, bilgisayar korsanları(Hackers), taklitçiler(Impersonators), çevrim içi avcılar(online predators), siber sapıklar(cyber stalkers), siber zorbalar(cyber bulying) tanımlanmıştır. Bu saldırganların nasıl ve hangi yollarla saldırdıkları vurgulanmıştır. Virüslerin sistemlere verdiği zararlardan ve cihazlara bulaşma yollarına değinilmiştir (Şekil 10).

Şekil 10

Yeniden Düzenlenen E-Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık Mikro Öğrenme Nesnesi 1

İkinci mikro öğrenme nesnesinde E-posta hedefli siber tehditler yoluyla sanal dolandırıcılık konusunda bilgilendirme yapılmış, siber saldırganların hedeflediği verilerden bahsedilmiştir. E-postaları hedef alan siber tehditlerin nasıl yapıldığı, e-posta saldırılarının nasıl göründüğü ve sahte e-postaların içeriği anlatılmıştır. Fiziksel postalarla e-postaların güvenlikleri karşılaştırılmıştır. E-postaların güvenlik riskleri vurgulanmıştır. E-posta hırsızlığına yol açabilecek durumlar belirtilmiştir (Şekil 11).

Şekil 11

Yeniden Düzenlenen E-Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık Mikro Öğrenme Nesnesi 2

E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık mikro öğrenme nesnesi yeniden düzenlenmiştir (Şekil 12). Mikro öğrenme stratejisi çerçevesinde içerik hedefleri doğrultusunda iki mikro öğrenme nesnesi oluşturulacak şekilde bölünmüştür. Birinci mikro öğrenme nesnesinde, siber güvenlik saldırılarının nasıl yapıldığından bahsedilmiştir. Siber korsanların hangi kimliklerle ve nasıl mesaj gönderdiğine değinilmiştir. Siber güvenlik tehditleri içeren e-postaların içeriği anlatılmıştır. Hedef kullanıcıların siber korsanların e-postalarını yanıtlamalarının sonuçları vurgulanmıştır (Şekil 12).

Şekil 12

Yeniden Düzenlenen E-Postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık Mikro Öğrenme Nesnesi 1

İkinci mikro öğrenme nesnesinde, Siber güvenlik tehditleri içeren e-postalarının tespit edilme yollarına değinilmiştir. Bilgi hırsızlığı kavramı açıklanmış, saldırganların

hedeflediği ve ele geçirebileceği veriler anlatılmış ve ele geçirilen verilerin hangi amaçlarla kullanılabileceği belirtilmiştir (Şekil 13).

Şekil 13

Yeniden Düzenlenen E-postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık Mikro Öğrenme Nesnesi 2

E-postalarda şifre hedefli tehditlere yönelik farkındalık mikro öğrenme nesnesi yeniden düzenlenmiştir. Siber güvenlik saldırıları tipleri anlatılmıştır. siber güvenlik tehditlerinin yoğun yaşandığı e-postaları alındığında yapılması gerekenler vurgulanmıştır. Şifre hedefli saldırıların nasıl ve ne amaçla yapıldığından bahsedilmiştir. Güçlü şifre belirlemenin önemi ve nasıl yapılacağı belirtilmiştir. E-postaları hedef alan siber tehditlerin tespitinde yazım kurallarının önemi, e-posta içeriğindeki reklam ve ödül vaadi gibi oluşturulan tuzaklar, kişisel verilerin paylaşımının sakıncaları anlatılmıştır (Şekil 14).

Şekil 14

Yeniden Düzenlenen E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık Mikro Öğrenme Nesnesi

E-postalarda güvenlik ayarlarının kullanımına ilişkin farkındalık mikro öğrenme nesnesi yeniden düzenlenmiştir. Sıklıkla kullanılan ve ücretsiz e-posta servis hizmeti veren Gmail, Hotmail, Yahoomail ve Yandexmail e-posta servislerinin kullanımında yapılan hatalardan bahsedilmiştir. Gmail hesaplarının güvenlik ayarları konusunda bilgilendirme yapılmıştır. E-posta hesabının güvenlik ayarlarının önemi vurgulanmış ve yapılması gereken ayarlar anlatılmıştır. Güvenlik ayarlarından bağlı cihazların kontrolü ve yönetimi, şifre yönetimi, çift faktörlü doğrulama, hesaba kurtarma e-postası ve telefon bilgisi oluşturma, e-posta hizmeti veren kuruluşun tespit ettiği güvenlik açıklarını görme ve giderme konularının önemi anlatılmış ve yapılması gerekenler gösterilmiştir. Kişisel verilerin gizliliği ve yapılması gereken gizlilik ayarları belirtilmiştir. Kişisel verilerin paylaşımı konusunda dikkat edilmesi gereken hususlar gösterilmiştir (Şekil 15).

Şekil 15

Yeniden Düzenlenen E-postalarda Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık Mikro-Öğrenme Nesnesi

Birinci mezo döngüde elde edilen bulguların ışığında öğretim tasarımında geliştirmeye gidilmiştir. Etkileşimli içeriklerin kullanımının araştırma kapsamında hedeflenen kazanımlara ulaşmada katkı sağlayacağı değerlendirilerek, öğretim tasarımına etkileşimli içerikler eklenmiştir. Kullanıcılarının e-postaları hedef alan siber tehditleri tespit etmede gelişme göstereceği (Waver vd. 2021) ve öğrencilerin içeriğe odaklanmasını sağlayacağı düşünülen "https://phishingquiz.withgoogle.com/" çevrim içi e-postaları hedefleyen siber tehdit testinin sınıf içi etkinlik olarak kullanımı uygun görülmüştür.

Öğrencilerin güçlü şifreler belirleme ve şifrelerin önemini kavrama konusunda dikkatlerini çekecek, şifre hedefli tehditler konusunda farkındalıklarını artıracak bir etkinlik uygulanmasına karar verilmiştir. Bu kapsamda girilen şifrenin ne kadar sürede çözülebileceğini hesaplayan, https://www.csa.gov.sg/Tips-Resource/Interactive-Tools/Password-Checker çevrim içi aracının kullanılmasının uygun olacağı görüşüne varılmıştır.

Öğrencilerin yaş grubu göz önünde bulundurularak, içeriğin pekiştirilmesini sağlayacağı ve öğrencilerin motivasyonunu artıracağı düşünülen labirent bulmaca oyununun kullanımı kararlaştırılmıştır. Oyun, verilen sorunun doğru yanıtının labirentte bulunması ve oyuncunun doğru cevaba hareket ettirilmesi mekaniği ile çalışmaktadır.

İçeriği desteklemek amacıyla sınıf içi test etkinlikleri planlanmıştır. Bu kapsamda Kahoot çevrim içi aracı kullanılarak bir test uygulanmıştır. Bunun yanında çeşitli e-posta hedefli siber tehdit görselleri sunulmuş, öğrencilerle görsellerin siber tehdit olmasının nedenleri hakkında tartışılmıştır. Wordwall çevrim içi aracı kullanılarak çeşitli sınıf içi test etkinlikleri planlanmıştır. Kavramları pekiştirmesi amacıyla kelime-kavram eşleştirme etkinliği düzenlenmiştir.

İlk döngüde öğrencilerin e-posta güvenlik ayarlarının kullanımına ilişkin farkındalık ve uygulama noktasında sıkıntılar yaşadığı gözlemlenmiştir. Bu nedenle gmail güvenlik ayarları üzerinden öğrencilerle uygulamalı bir etkinlik planlanmıştır. Planlanan bu etkinlikler ile öğrencilerin mikro öğrenme nesnelerine odaklanmaları, verilen bilginin siber güvenlik farkındalıklarının artırılması amaçlanmıştır. Tasarım ve geliştirme mikro döngü süreci Tablo 9 da gösterilmiştir.

Tablo 9

İkinci Mezo Döngüde Tasarım ve Geliştirme Mikro Döngü Aşamaları

Aşamalar	Açıklamalar
Sahne tasarımlarının gerçekleştirilmesi	Tasarımda kullanılacak nesnelerin oluşturulması Görsel ve sözsel nesnelerin sahnelere yerleştirilmesi Resimli öykü taslağının tamamlanması
Mikro Öğrenme Nesnesinin Oluşturulması	Resimli öykü taslağının Video Scribe uygulamasında tasarlanması Prototipin tasarlanması
Öğretim Tasarımı	Sınıf içi etkinliklerin planlanması

Verilerin Analizi

Araştırmada veriler öğrencilerden toplanan SGF-DPA ve siber güvenlik farkındalığı öğrenci görüşme formları gözlem kayıtları aracılığıyla toplanmıştır. Tablo 10'da döngülere göre kullanılan veri toplama araçları açıklanmıştır.

***Mikro-Öğrenme Stratejisi Odaklı Siber Güvenlik Öğrenme Nesnelerinin Siber Güvenlik Farkındalığı Dereceli Puanlama Anahtarına Göre Değerlendirilmesi*.**

Araştırmadaki tüm döngüler Siber Güvenlik Farkındalığı Dereceli Puanlama Anahtarı ile değerlendirilmiş, mikro öğrenme stratejisi odaklı siber güvenlik öğrenme nesnelerinin genel niteliklerini belirlemek için toplam puan, dereceli puanlama anahtarının alt boyutları ve ölçütler bazında alt puanlar hesaplanmıştır. 1 ile 5 arasında 5 dereceli geliştirilmiş, dereceli puanlama anahtarı doğrultusunda en yüksek 100 puan alınabilmektedir.

E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık boyutundan en yüksek 25 puan; *E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık* boyutundan en yüksek 25 puan; *E-postalarda şifre hedefli tehditlere yönelik farkındalık* boyutundan en yüksek 25 puan; ve *E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık* boyutundan en yüksek 25 puan alınabilmektedir.

Yansıma formlarının değerlendirilmesi.

Birinci ve ikinci mezo döngü sonunda öğrenciler yansıma formlarıyla değerlendirilmiştir. 55 yansıma formu, siber güvenlik mikro-öğrenme nesneleri uygulama süreci sonunda, öğrencilerin siber güvenlik farkındalık düzeyleri elektronik ortamında cevaplamışlardır. Birinci mezo döngü sonunda 29 öğrenci yansıması; ikinci mezo döngü sonunda ise 26 öğrenci yansıması alınmıştır.

Ön analiz yöntemlerinden kodlama (Miles & Huberman, 1994) ile yansımalar anlamlı parçalara ayrılarak analiz edilmiştir. Yansımaları kodlamaya, kaynağını kavramsal çerçeve, araştırma soruları, hipotezler, sorun alanları ve anahtar kavramlar olduğu belirtilen başlangıç listesi oluşturularak başlanmış, tümevarımcı kodlama tekniği (Strauss ve Corbin, 1990) ile kodlama yapılmıştır. Yansıma formlarının analiz listesi (Tablo 10) için yansıma soruları temel alınmıştır.

Tablo 10

Siber Güvenlik Farkındalık Ölçütleri

Yansıma Kod Listesi
Siber güvenlik ilişkili temel kavramları anlama
Gerçek yaşamda karşılaştığı siber tehditlerle öğrendiklerini ilişkilendirme
Gelen e-postalardaki yazım hatasının tehdit içerebileceğini anlama
E-posta güvenlik ayarlarını yapabilme
E-posta karmaşık şifreleme adımlarını oluşturma
Etkileşimli öğrenme materyali
İşbirlikli çalışma
Anlık geri bildirim
Teknik destek kaynaklı sorunlar
Süre yetersizliği
Mobil cihaz desteğinin eksikliği

Geçerlik ve Güvenirlik

Araştırmanın iç geçerliği, iç geçerliğin sorgulanmasına yönelik sorulan sorular (Miles & Huberman, 1994) doğrultusunda irdelenmiştir. İç güvenirlik için önerilen (LeCompte & Goetz, 1982) iç güvenirlik stratejilerine başvurulmuştur. Toplanan veriler betimsel analiz doğrultusunda raporlanmıştır.

Araştırmada ulaşılan nitel verinin yaklaşık %25'lik bir bölümü üzerinde gerçekleştirilen "kontrol kodlaması" (Miles & Huberman, 1994) doğrultusunda ilk aşamada araştırmacı ayrı ayrı kodlama işlemini gerçekleştirmiş, ardından bir araya getirerek kodlamaları karşılaştırmıştır. İlk kodlama işlemi sonunda yapılan güvenirlik analizi sonunda kodlayıcılar arasındaki güvenirlik % 67.21 bulunmuş, kontrol kodlaması sonucunda ise güvenirlik % 71.44 bulunmuştur.

Araştırmanın eğitsel tasarım araştırması yöntemi ile gerçekleştirilmiş olması nedeniyle dış geçerlik ilişkisi bulunmamaktadır.

Bölüm 4

Bulgular, Yorumlar ve Tartışma

Bu bölümde siber güvenlik mikro-öğrenme nesneleri tasarlama ve değerlendirme sürecine yönelik veri analizi ile elde edilen bulgular, araştırma problemlerini takip eden alt başlıklar halinde sunulmuş ve yorumlanmıştır.

Araştırma Probleminin Sınanması

Bu araştırmanın amacı öğrenme – öğretme sürecine yönelik siber güvenlik mikro-öğrenme nesnelerinin tasarlanması ve değerlendirmesidir. Bu amaç kapsamında siber güvenlik mikro-öğrenme nesnelerinin tasarlanma ve değerlendirilme süreci iki mezo döngü halinde gerçekleşmiştir. Araştırma bir ana problem ve her iki mezo döngüde olmak üzere beş alt problemden oluşmaktadır. Araştırma sürecinde alt problemler kapsamında verilerin analizleri ile elde edilen bulgular izleyen alt başlıklar halinde sunulmuş ve yorumlanmıştır.

Birinci Mezo Döngü Bulguları

Siber güvenlik mikro öğrenme nesneleri tasarlama ve değerlendirme süreci kapsamında gerçekleştirilen birinci döngü 3 mikro döngüden oluşmaktadır.

Birinci mezo döngünün 3. mikro döngüsünü oluşturan değerlendirme ve yansıma döngüsünde, Siber Güvenlik Mikro Öğrenme Nesneleri (SGMÖN) gerçek sınıf ortamında uygulanmış, öğrencilere Siber Güvenlik Farkındalığı Dereceli Puanlama Anahtarı (SGF-DPA) ve Siber Güvenlik Farkındalığı Öğrenci Görüşme Formu uygulanmıştır.

Bu kapsamda birinci mezo döngüde, siber güvenlik mikro öğrenme nesnelerinin, öğrencilerin siber güvenlik farkındalık düzeylerini *1.1. E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık, 1.2. E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık, 1.3. E-postalarda şifre hedefli tehditlere yönelik farkındalık, 1.4. E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık ölçütlerini* sınayan bir alt problem, öğrenci görüşlerini sunan diğer bir alt problem olmak üzere iki alt

problemden oluşmaktadır. Alt problemler kapsamında toplanan verilerin analizleri ile elde edilen bulgular izleyen alt başlıklar halinde sunulmuş ve yorumlanmıştır.

1. Birinci Mezo Döngüde, Tasarlanan Siber Güvenlik Mikro-öğrenme Nesneleri, Öğrencilerin Siber Güvenlik Farkındalıkları Açısından Ne Düzeydedir?

Birinci mezo döngü sürecinde tasarlanan siber güvenlik mikro öğrenme nesnelerinin değerlendirilmesi için öğrencilere uygulanan siber güvenlik farkındalığı dereceli puanlama anahtarı ile öğrencilerin siber güvenlik farkındalık ortalamaları hesaplanarak araştırma problemi kapsamında sunulmuştur.

Birinci döngüde tasarlanan siber güvenlik mikro öğrenme nesneleri 29 öğrenci tarafından değerlendirilmiş, siber güvenlik mikro-öğrenme nesneleri ortalaması ($\bar{X}$=2.65) olarak hesaplanmıştır. Alt boyutlarının ortalamaları, *E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık* boyutu için ($\bar{X}$=2.73), *E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık* boyutu için ($\bar{X}$ = 2.73), *E-postalarda şifre hedefli tehditlere yönelik farkındalık* boyutu için ($\bar{X}$ = 2.62) ve *E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık* boyutu için ($\bar{X}$ = 2.55) olarak hesaplanmıştır.

E-postalarda kaynağı bilinmeyen bağlantı ve *içerik kaynaklı tehditlere yönelik farkındalık*, *E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık*, *E-postalarda şifre hedefli tehditlere yönelik farkındalık ve E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık* boyutlarının yetersiz ve kısmen yeterli seviyeleri arasında kaldığı görülmektedir.

E-postalarda kaynağı bilinmeyen bağlantı ve *içerik kaynaklı tehditlere yönelik farkındalık* boyutu ($\bar{X}$=2.73) ve *E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık* boyutunun ($\bar{X}$=2.73) benzer ortalamaya sahip olduğu görülmektedir (Tablo 11).

Tablo 11

Birinci Döngüde Tasarlanan SGMÖN'nin SGF-DPA Boyutlarına Göre Betimsel İstatistikleri

Mikro-öğrenme Nesnesi Boyutları	Madde Sayısı	En Düşük	En Yüksek	$\bar{X}$	S.S.
E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere *yönelik farkındalık*	5	1.60	4.40	2.73	0.70
E-postalarda yazım hatası kaynaklı tehditlere *yönelik farkındalık*	5	1.60	4.40	2.73	0.70
E-postalarda şifre hedefli tehditlere *yönelik farkındalık*	5	1.60	4.20	2.62	0.67
E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık	5	1.00	3.80	2.55	0.66

Mikro-öğrenme nesneleri tasarlama süreci; *1.1. E-postalarda Kaynağı Bilinmeyen Bağlantı* ve *İçerik Kaynaklı Tehditlere Yönelik Farkındalık*, *1.2. E-postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık*, *1.3. E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık* ve *1.4. E-posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık* alt boyutları açısından ayrı ayrı incelenmektedir.

1.1. Birinci Mezo döngüde Tasarlanan E-postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditler Mikro Öğrenme Nesneleri, Öğrencilerin Siber Güvenlik Farkındalıkları Açısından Ne Düzeydedir?

Öğrencilerin, birinci mezo döngüde tasarlanan siber güvenlik mikro-öğrenme nesneleri, "*E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık*" boyutu ve ölçütlerine yönelik değerlendirme sonuçları aşağıda sunulmuştur.

Siber güvenlik mikro öğrenme nesneleri, siber güvenlik farkındalığı dereceli puanlama anahtarı düzeyleri açısından incelendiğinde, *E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık* boyutunun, %66.89 (oldukça yetersiz), %20 (yetersiz), % 3.44 (kısmen yeterli), % 4.13 (yeterli), % 4.82 (yeterince güçlü) olduğu belirlenmiştir.

Ölçütler, düzeyler açısından incelendiğinde; *E-postayı açma* ölçütünün (% 72.41) oldukça yetersiz düzeyde; *Gönderen adresini kontrol etme* ölçütünün (% 44.8) yetersiz düzeyde; *E-posta içeriğindeki bağlantıya tıklama* ölçütünün (%75.9) oldukça yetersiz düzeyde; *E-postada istenen kişisel verileri gönderme* ölçütünün (%82.8) oldukça yetersiz düzeyde; *E-posta içeriğindeki eki cihaza indirme* ölçütünün (%86.2) oldukça yetersiz düzeyde olduğu görülmektedir (Tablo 12).

Tablo 12

Birinci Döngüde Tasarlanan SGMÖN'nin E-postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık Boyutuna İlişkin SGF-DPA Düzeyleri Betimsel İstatistikleri

E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık	**1**		**2**		**3**		**4**		**5**	
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**
E-postayı açma	21	72.4	6	20.7	1	3.4	-	-	1	3.4
Gönderen adresini kontrol etme	5	17.2	13	44.8	3	10.3	6	20.7	2	6.9
E-posta içeriğindeki bağlantıya tıklama	22	75.9	5	17.2	-	-	-	-	2	6.9
E-postada istenen kişisel verileri gönderme	24	82.8	3	10.3	2	6.9	-	-	-	-
E-posta içeriğindeki eki cihaza indirme	25	86.2	2	6.9	-	-	-	-	2	6.9

Siber güvenlik farkındalığı dereceli puanlama anahtarının, *E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık* boyutu ve ölçütlerine göre ortalamaları (Tablo 13) incelendiğinde *"E-postada istenen kişisel verileri gönderme"* seviyesinin ($\bar{X}$=1.24) en düşük ve *"Gönderen adresini kontrol etme"* seviyesinin ($\bar{X}$=2.55) en yüksek ortalamaya sahip olduğu görülmektedir. Ölçütler düzeyler açısından incelendiğinde ağırlıklı olarak oldukça yetersiz ile yetersiz düzeyleri arasında toplandığı görülmektedir.

"E-postayı açma" ölçütünün ($\bar{X}$=1.41), "*E-posta içeriğindeki bağlantıya tıklama"* ($\bar{X}$=1.44), *"E-postada istenen kişisel verileri gönderme"* ($\bar{X}$=1.24), *"E-posta içeriğindeki eki*

cihaza indirme" ($\bar{X}$=1.34) ölçütleri oldukça yetersiz ile yetersiz düzeyleri arasında yer alırken; *"Gönderen adresini kontrol etme"* ölçütünün ($\bar{X}$=2.55) yetersiz ile kısmen yeterli düzey arasında yer alması dikkat çekicidir.

Ölçütlerin aldığı en düşük ve en yüksek değerler incelendiğinde *"Her gelen e-postaya istenen kişisel bilgilerimi gönderirim"* ölçütü en düşük oldukça yetersiz en yüksek kısmen yeterli düzeyinde değerlendirilmişken, diğer ölçütlerin en düşük oldukça yetersiz, en yüksek yeterince güçlü düzeyinde değerlendirildiği görülmektedir (Tablo 13).

Tablo 13

Birinci Döngüde Tasarlanan SGMÖN'nin SGF-DPA E-postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık Boyutu Betimsel İstatistikleri

E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık	**N**	**En Düşük**	**En Yüksek**	**$\bar{X}$**	**S.S.**
E-postayı açma	29	1.00	5.00	1.41	.86
Gönderen adresini kontrol etme	29	1.00	5.00	2.55	1.21
E-posta içeriğindeki bağlantıya tıklama	29	1.00	5.00	1.44	1.05
E-postada istenen kişisel verileri gönderme	29	1.00	3.00	1.24	0.57
E-posta içeriğindeki eki cihaza indirme	29	1.00	5.00	1.34	1.04

Siber güvenlik farkındalığı dereceli puanlama anahtarının alt boyutlarından olan "*E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık" boyutunun*, *"Gönderen adresini kontrol etme"* ölçütünün yetersiz düzeyde, *"E-postayı açma"*, "*E-posta içeriğindeki bağlantıya tıklama", "E-postada istenen kişisel verileri gönderme"* ve "*E-posta içeriğindeki eki cihaza indirme"* ölçütlerinin oldukça yetersiz düzeyde değerlendirildiği dikkat çekmektedir.

1.2. Birinci Mezo Döngüde, Tasarlanan E-postalarda Yazım Hatası Kaynaklı Tehditler Mikro Öğrenme Nesneleri, Öğrencilerin Siber Güvenlik Farkındalıkları Açısından Ne Düzeydedir?

Öğrencilerin, birinci mezo döngüde tasarlanan siber güvenlik mikro öğrenme nesneleri, "*E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık*" boyutu ve ölçütlerine yönelik değerlendirme sonuçları aşağıda sunulmuştur.

SGMÖN, SGF-DPA düzeyleri açısından incelendiğinde *"E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık" boyutu*, %10.34 (oldukça yetersiz), %41.37 (yetersiz), % 28.96 (kısmen yeterli) , % 4.82 (yeterli) ve % 15.86 (yeterince güçlü) olduğu belirlenmiştir. Ölçütler, düzeyler açısından incelendiğinde; "*Yazım kurallarına uygunluğu kontrol etme*" (% 44.8) kısmen yeterli düzeyde; "*E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme*" (% 41.4) yetersiz düzeyde; "*E-postayı gönderenin adresinin yazımını kontrol etme*" (%51.7) yetersiz düzeyde; *"E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme"* (%37.9) yetersiz düzeyde; *"E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme"* (%51.7) yetersiz düzeyde olduğu görülmektedir (Tablo 14).

Tablo 14

Birinci Döngüde Tasarlanan SGMÖN'nin E-postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık Boyutuna İlişkin SGF-DPA Düzeyleri Betimsel İstatistikleri

Siber Güvenlik Farkındalığı Dereceli Puanlama Anahtarı Düzeyleri										
E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık	**1**		**2**		**3**		**4**		**5**	
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**
Yazım kurallarına uygunluğu kontrol etme	6	20.7	7	24.1	13	44.8	-	-	3	10.3
E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme	2	6.9	12	41.4	6	20.7	2	6.9	7	24.1
E-postayı gönderenin adresinin yazımını kontrol etme	3	10.3	15	51.7	8	27.6	-	-	3	10.3

E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme	-	-	11	37.9	9	31.0	3	10.3	6	20.7
E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme	4	13.8	15	51.7	6	20.7	-	-	4	13.8

Siber güvenlik farkındalığı dereceli puanlama anahtarının "*E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık"* boyutu ve ölçütlerine göre ortalamaları (Tablo 15) incelendiğinde "*E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme"* ($\bar{X}$=2.13) en düşük ve "*E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme*" ($\bar{X}$=3.00) en yüksek ortalamaya sahip olduğu görülmektedir. Ölçütler düzeyler açısından incelendiğinde ağırlıklı olarak yetersiz ile kısmen yeterli düzeyleri arasında yığıldıkları görülmektedir.

"*Yazım kurallarına uygunluğu kontrol etme"* ($\bar{X}$=2.55), *"E-postayı gönderenin adresinin yazımını kontrol etme"* ($\bar{X}$=2.48), *"E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme"* ($\bar{X}$=2.13), "*E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme*" ($\bar{X}$=2.48) ölçütleri yetersiz ile kısmen yeterli düzeyleri arasında yer alırken; *"E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme"* ($\bar{X}$=3.00) ölçütünün kısmen yeterli düzeyinde yer alması dikkat çekicidir.

Ölçütlerin aldığı en düşük ve en yüksek değerler incelendiğinde *"E-postayı gönderenin adresinin yazımını kontrol etme"* ve "*E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme*" ölçütlerinin en düşük yetersiz, en yüksek yeterince güçlü düzeyinde değerlendirildiği; "*Yazım kurallarına uygunluğu kontrol etme", "E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme"* ve "*E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme*" ölçütlerinin en düşük oldukça yetersiz, en yüksek yeterince güçlü düzeyinde değerlendirildiği görülmektedir (Tablo 15).

Tablo 15

Birinci Döngüde Tasarlanan SGMÖN'nin SGF-DPA E-postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık Boyutu Betimsel İstatistikleri

E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık	N	En Düşük	En Yüksek	X̄	S.S.
Yazım kurallarına uygunluğu kontrol etme	29	1	5	2.55	1.15
E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme	29	1	5	3.00	1.33
E-postayı gönderenin adresinin yazımını kontrol etme	29	2	5	2.48	1.05
E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme	29	2	5	2.13	1.16
E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme	29	1	5	2.48	1.18

SGF-DPA 'nın alt boyutlarından olan *"E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık"* boyutunun, *"E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme", "E-postayı gönderenin adresinin yazımını kontrol etme", "E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme", "E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme"* ölçütlerinin yetersiz düzeyde; *"Yazım kurallarına uygunluğu kontrol etme"* ölçütünün kısmen yeterli düzeyde değerlendirildiği dikkat çekmektedir.

1.3. Birinci Mezo Döngüde, Tasarlanan E-postalarda Şifre Hedefli Tehditler Mikro Öğrenme Nesneleri, Öğrencilerin Siber Güvenlik Farkındalıkları Açısından Ne Düzeydedir?

Öğrencilerin, birinci mezo döngüde tasarlanan siber güvenlik mikro öğrenme nesneleri, "*E-postalarda şifre hedefli tehditlere yönelik farkındalık*" boyutu ve ölçütlerine yönelik değerlendirme sonuçları aşağıda sunulmuştur.

SGMÖN, SGF-DPA düzeyleri açısından incelendiğinde *"E-postalarda şifre hedefli tehditlere yönelik farkındalık"* boyutunun, %30.34 (oldukça yetersiz), %27.58 (yetersiz), %

12.41 (kısmen yeterli), % 8.96 (yeterli) ve % 20.68 (yeterince güçlü) olduğu belirlenmiştir. Ölçütler, düzeyler açısından incelendiğinde; *"E-posta şifre değiştirme sıklığı"* (% 41.4) yetersiz düzeyde; *"E-posta şifre uzunluğu"* (% 31) yetersiz düzeyde; *"E-posta şifresi ile klavye düzeni ilişkisi"* (%44.8) yeterince güçlü düzeyde; *"Kişisel verilerle şifre belirleme"* (% 69) oldukça yetersiz düzeyde; *"Karmaşık ve özel karakterlerle şifre belirleme"* (% 69) oldukça yetersiz düzeyde olduğu görülmektedir (Tablo 16).

Tablo 16

Birinci Döngüde Tasarlanan SGMÖN'nin E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık Boyutuna İlişkin SGF-DPA Düzeyleri Betimsel İstatistikleri

E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık	**1**		**2**		**3**		**4**		**5**	
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**
E-posta şifre değiştirme sıklığı	2	6.9	12	41.4	1	3.4	4	13.8	10	34.5
E-posta şifre uzunluğu	2	6.9	9	31.0	8	27.6	5	17.2	5	17.2
E-posta şifresi ile klavye düzeni ilişkisi	-	-	10	34.5	2	6.9	4	13.8	13	44.8
Kişisel verilerle şifre belirleme	20	69.0	5	17.2	3	10.3	-	-	1	3.4
Karmaşık ve özel karakterlerle şifre belirleme	20	69.0	4	13.8	4	13.8	-	-	1	3.4

Siber güvenlik farkındalığı dereceli puanlama anahtarının, *"E-postalarda şifre hedefli tehditlere yönelik farkındalık"* boyutu ve ölçütlerine göre ortalamaları (Tablo 17) incelendiğinde *"Kişisel verilerle şifre belirleme"* ($\bar{X}$=1.51) ölçütünün en düşük ve "*E-posta şifresi ile klavye düzeni ilişkisi"* ($\bar{X}$=3.68) ölçütünün en yüksek ortalamaya sahip olduğu görülmektedir. Ölçütler düzeyler açısından incelendiğinde ağırlıklı olarak oldukça yetersiz ile yetersiz düzeyleri ve kısmen yeterli ile yeterli düzeyleri arasında yığıldıkları görülmektedir.

"E-posta şifre değiştirme sıklığı" ($\bar{X}$=3.27), *"E-posta şifre uzunluğu"* ($\bar{X}$=3.06), *"E-posta şifresi ile klavye düzeni ilişkisi"* ($\bar{X}$=3.68) ölçütleri kısmen yeterli ile yeterli düzeyleri

arasında yer alırken; "*Kişisel verilerle şifre belirleme"* ($\bar{X}$=1.51) ve *"Karmaşık ve özel karakterlerle şifre belirleme"* ($\bar{X}$=1.55) ölçütleri oldukça yetersiz ile yetersiz düzeyleri arasında yer alması dikkat çekicidir.

Ölçütlerin aldığı en düşük ve en yüksek değerler incelendiğinde tüm ölçütlerin en düşük oldukça yetersiz, en yüksek yeterince güçlü düzeyinde değerlendirildiği görülmektedir (Tablo 17).

Tablo 17

Birinci Döngüde Tasarlanan SGMÖN'nin SGF-DPA E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık Boyutu Betimsel İstatistikleri

E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık	**N**	**En Düşük**	**En Yüksek**	**$\bar{X}$**	**S.S.**
E-posta şifre değiştirme sıklığı	29	1.00	5.00	3.27	1.48
E-posta şifre uzunluğu	29	1.00	5.00	3.06	1.22
E-posta şifresi ile klavye düzeni ilişkisi	29	1.00	5.00	3.68	1.36
Kişisel verilerle şifre belirleme	29	1.00	5.00	1.51	0.94
Karmaşık ve özel karakterlerle şifre belirleme	29	1.00	5.00	1.55	0.98

SGF-DPA 'nın alt boyutlarından olan *"E-postalarda şifre hedefli tehditlere yönelik farkındalık"* boyutunun*, "Kişisel verilerle şifre belirleme"* ve "*Karmaşık ve özel karakterlerle şifre belirleme*" ölçütlerinin oldukça yetersiz düzeyde; *"E-posta şifre değiştirme sıklığı"* ve *"E-posta şifre uzunluğu"* ölçütlerinin yetersiz düzeyde; "*E-posta şifresi ile klavye düzeni ilişkisi*" ölçütünün yeterince güçlü düzeyde değerlendirildiği dikkat çekmektedir.

1.4. Birinci Mezo Döngüde, Tasarlanan E-posta Güvenlik Ayarlarının Kullanımı Odaklı Mikro Öğrenme Nesneleri, Öğrencilerin Siber Güvenlik Farkındalıkları Açısından Ne Düzeydedir?

Öğrencilerin, birinci mezo döngüde tasarlanan siber güvenlik mikro öğrenme nesneleri, *"E-posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık"* boyutu ve ölçütlerine yönelik değerlendirme sonuçları aşağıda sunulmuştur.

SGMÖN'nin, SGF-DPA düzeyleri açısından incelendiğinde "*E-posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık"* boyutu, %31.03 (oldukça yetersiz), %26.20 (yetersiz), % 17.93 (kısmen yeterli), % 6.20 (yeterli), % 18.62 (yeterince güçlü) olduğu belirlenmiştir. Ölçütler, düzeyler açısından incelendiğinde; *"Çift faktörlü kimlik doğrulama kullanma"* (% 48.3) yetersiz düzeyde; "*Telefonla doğrulama kullanma*" (% 44.8) yeterince güçlü düzeyde; *"Kurtarma e-postası kullanma"* (% 69) oldukça yetersiz düzeyde; *"Güvenlik ayarları hakkında bilgi edinme*" (% 55.2) oldukça yetersiz düzeyde; "*Güncellemeleri uygulama"* (% 31) kısmen yeterli düzeyde olduğu görülmektedir (Tablo 18).

Tablo 18

Birinci Döngüde Tasarlanan SGMÖN'nin E-posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık Boyutuna İlişkin SGF-DPA Düzeyleri Betimsel İstatistikleri

E-posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık	**1**		**2**		**3**		**4**		**5**	
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**
Çift faktörlü kimlik doğrulama kullanma	6	20.7	14	48.3	3	10.3	1	3.4	5	17.2
Telefonla doğrulama kullanma	2	6.9	5	17.2	5	17.2	4	13.8	13	44.8
Kurtarma e-postası kullanma	20	69.0	4	13.8	5	17.2	-	-	-	-
Güvenlik ayarları hakkında bilgi edinme	16	55.2	7	24.1	4	13.8	-	-	2	6.9
Güncellemeleri uygulama	1	3.4	8	27.6	9	31.0	4	13.8	7	24.1

Siber güvenlik farkındalığı dereceli puanlama anahtarının *"E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık"* boyutu, ölçütlerine göre aldığı ortalamalar (Tablo

19) incelendiğinde *“Kurtarma e-postası kullanma”* ölçütünün ($\bar{X}$=1.48) en düşük ve *“Telefonla doğrulama kullanma”* ölçütünün ($\bar{X}$=3.72) en yüksek ortalamaya sahip olduğu görülmektedir. Ölçütler düzeyler açısından incelendiğinde “*Telefonla doğrulama kullanma*” ve ”*Güncellemeleri uygulama*” ölçütlerinin kısmen yeterli ile yeterli düzeyleri arasında; “*Çift faktörlü kimlik doğrulama kullanma*” ölçütünün yetersiz ile kısmen yeterli düzeyleri arasında; “*Kurtarma e-postası kullanma*” ve “*Güvenlik ayarları hakkında bilgi edinme*” ölçütlerin oldukça yetersiz ile yetersiz düzeyleri arasında yığıldıkları görülmektedir.

Ölçütlerin aldığı en düşük ve en yüksek değerler incelendiğinde *“Kurtarma e-postası kullanma”* ölçütünün en düşük oldukça yetersiz, en yüksek kısmen yeterli düzeyinde değerlendirildiği, *“Çift faktörlü kimlik doğrulama kullanma”*, *“Telefonla doğrulama kullanma”,* “*Güvenlik ayarları hakkında bilgi edinme*” ve *“Güncellemeleri uygulama”* ölçütlerinin en düşük oldukça yetersiz, en yüksek yeterince güçlü düzeyinde değerlendirildiği görülmektedir (Tablo 19).

Tablo 19

Birinci Döngüde Tasarlanan SGMÖN’nin SGF-DPA E-posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık Boyutu Betimsel İstatistikleri

E-posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık	**N**	**En Düşük**	**En Yüksek**	**$\bar{X}$**	**S.S.**
Çift faktörlü kimlik doğrulama kullanma	29	1	5	2.48	1.35
Telefonla doğrulama kullanma	29	1	5	3.72	1.38
Kurtarma e-postası kullanma	29	1	3	1.48	0.78
Güvenlik ayarları hakkında bilgi edinme	29	1	5	1.79	1.14
Güncellemeleri uygulama	29	1	5	3.27	1.22

Siber güvenlik farkındalığı dereceli puanlama anahtarının alt boyutlarından olan *“E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık*” boyutunun, *“Çift faktörlü kimlik doğrulama kullanma”* ölçütünün yetersiz düzeyde; “*Telefonla doğrulama kullanma”*

ölçütünün yeterince güçlü düzeyde; *“Kurtarma e-postası kullanma”* ve *“Güvenlik ayarları hakkında bilgi edinme”* ölçütlerinin oldukça yetersiz düzeyde; *“Güncellemeleri uygulama”* ölçütünün kısmen yeterli düzeyde değerlendirildiği dikkat çekmektedir.

2. Öğrencilerin, Birinci Mezo Döngüde, Öğrenme-Öğretme Sürecinde Tasarlanan Siber Güvenlik Mikro Öğrenme Nesnelerine Yönelik Görüşleri Nelerdir?

Öğrencilerin birinci mezo döngü kapsamında tasarlanan SGMÖN deneyimlerine yönelik görüşlerini belirlemek amacıyla süreçte iyi yapabildikleri/yapamadıkları ve süreçlerini kolaylaştıran/zorlaştıran etmenler sorulmuş, elde edilen bulgular Tablo 20’de sunulmuştur.

Öğrencilerin yarısından fazlası siber güvenlik ilişkili temel kavramları anlamada, dört öğrenciden biri gerçek yaşamda karşılaştığı siber tehditlerle öğrendiklerini ilişkilendirme ve gelen e-postalardaki yazım hatasının tehdit içerebileceğini anlama konusunda güçlü olduğunu belirtmişlerdir. Öğrencilerin yarısından fazlası e-posta güvenlik ayarlarını yapabilme, üç öğrenciden biri e-posta karmaşık şifreleme adımlarını oluşturma konusunda zayıf olduklarını ifade etmişlerdir. Öğrencilerin yarıdan fazlası işbirlikli çalışma ve anlık geri bildirim, yarıdan azı ise etkileşimli öğrenme materyali konusunda e-posta hedefli siber tehditleri tespit etmelerini kolaylaştırdığını belirtmiştir. Öğrencilerin tamamına yakını teknik destek kaynaklı sorunları, yarıdan fazlası süre yetersizliği ve mobil cihaz desteğinin eksikliğini e-posta hedefli siber tehditleri tespit etmelerini zorlaştırdığını belirtmiştir (Tablo 20).

Tablo 20

Birinci Döngüde Öğrencilerin SGMÖN'ne Yönelik Görüşlerine İlişkin Tema, Kod, Frekans ve Yüzdeleri

Tema	Kod	f	%
Siber güvenlik mikro-öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmede kazandığım güçlü yönler	Siber güvenlik ilişkili temel kavramları anlama	16	55.2
	Gerçek yaşamda karşılaştığı siber tehditlerle öğrendiklerini ilişkilendirme	8	27.5
	Gelen e-postalardaki yazım hatasının tehdit içerebileceğini anlama	7	24.1
Siber güvenlik mikro öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmede zayıf yönler	E-posta güvenlik ayarlarını yapabilme	17	58.6
	E-posta karmaşık şifreleme adımlarını oluşturma	9	31.0
Siber güvenlik mikro öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmemi kolaylaştıran yönler	Etkileşimli öğrenme materyali	13	44.8
	İşbirlikli çalışma	18	62.0
	Anlık geri bildirim	21	72.4
Siber güvenlik mikro öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmemi zorlaştıran/engelleyen yönler	Teknik destek kaynaklı sorunlar	25	86.2
	Süre yetersizliği	19	65.5
	Mobil cihaz desteğinin eksikliği	21	72.4
Öğrenci Sayısı		29	100

Öğrenci yorumlarından bazıları şu şekildedir:

Siber Güvenlik mikro öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmede kazandığım güçlü yönler ölçütü için;

"*Siber tehditleri tespit etmenin birden fazla yolu olduğunu öğrendim*." (Ö17).

"*E-mailime gelen mailin sahte olup olmadığını kontrol etmeyi öğrendim*." (Ö19).

"*Güçlü şifre belirleme yollarını ve gelen e-postalardaki bağlantıları kontrol etmeden açmamam gerektiğini öğrendim*." (Ö28).

Siber Güvenlik mikro öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmede zayıf yönler ölçütü için;

"*Gelen maillerin siber tehdit olduğunu anlamakta zorlanıyorum*" (Ö21).

"*Yazım hatalarını bulmakta zorlanıyorum*." (Ö31).

Siber Güvenlik mikro öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmemi kolaylaştıran yönler ölçütü için;

"*Hesabımın çalınmasını önleyebilirim*." (Ö23).

"*Kullandığım şifreyi belirli aralıklarla değiştireceğim*." (Ö24).

"*E-postalarımı kontrol etmeden açmam*." (Ö40).

Siber Güvenlik mikro öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmemi zorlaştıran/engelleyen yönler ölçütü için;

"*Hesaplarımın ve bilgilerimin çalınması*." (Ö19).

"*Mailler ile virüs gönderebilir bilgisayarıma bulaştırabilirler*." (Ö32).

Birinci mezo döngü süreci sonunda siber güvenlik farkındalığı öğrenci görüşme formunda öğrencilerin belirttiği görüşler dikkate alındığında, öğrencilerin siber güvenlik kavramında farkındalık kazanmaya ilişkin olarak yarısından fazlasında başarılı sonuçlar elde edildiği söylenebilir. Ancak öğrendiklerini günlük hayatla ilişkilendirmede zayıf oldukları anlaşılmaktadır. E-postaları hedefleyen siber tehditleri tespit etme yöntemlerinin yeterince güçlü olmadığı görülmektedir.

İkinci Mezo Döngü Bulguları

Siber güvenlik mikro öğrenme nesneleri yeniden düzenleme ve değerlendirme süreci kapsamında gerçekleştirilen ikinci mezo döngü 3 mikro döngüden oluşmaktadır.

İkinci mezo döngünün 3. mikro döngüsünü oluşturan değerlendirme ve yansıma döngüsünde, siber güvenlik mikro öğrenme nesneleri (SGMÖN) gerçek sınıf ortamında uygulanmış, öğrencilere siber güvenlik farkındalığı dereceli puanlama anahtarı (SGF-DPA) ve siber güvenlik farkındalığı öğrenci görüşme formu uygulanmıştır.

Bu kapsamda ikinci mezo döngüde, siber güvenlik mikro öğrenme nesnelerinin, öğrencilerin siber güvenlik farkındalık düzeylerini *1.1. E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık, 1.2. E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık, 1.3. E-postalarda şifre hedefli tehditlere yönelik farkındalık, 1.4. E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık* ölçütlerini sınayan bir alt problem, öğrenci görüşlerini sunan diğer bir alt problem olmak üzere iki alt problemden oluşmaktadır. Alt problemler kapsamında toplanan verilerin analizleri ile elde edilen bulgular izleyen alt başlıklar halinde sunulmuş ve yorumlanmıştır.

1. İkinci Mezo Döngüde, Yeniden Düzenlenen Siber Güvenlik Mikro Öğrenme Nesneleri, Öğrencilerin Siber Güvenlik Farkındalıkları Açısından Ne Düzeydedir?

İkinci döngü sürecinde yeniden düzenlenen siber güvenlik mikro öğrenme nesnelerinin değerlendirilmesi için öğrencilere uygulanan siber güvenlik farkındalığı dereceli puanlama anahtarı ile hesaplanan siber güvenlik farkındalık ortalamaları birinci alt problem kapsamında sunulmuştur.

İkinci döngüde yeniden düzenlenen siber güvenlik mikro öğrenme nesneleri 26 öğrenci tarafından değerlendirilmiş, siber güvenlik mikro öğrenme nesneleri ortalaması ($\bar{X}$ = 12.05); "*E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık"* ($\bar{X}$ = 2.95); "*E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık*" ($\bar{X}$ = 3.08); "*E-postalarda şifre hedefli tehditlere yönelik farkındalık*" ($\bar{X}$ = 2,96) ve "*E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık"* ($\bar{X}$ = 3.06) alt boyutlarının ortalamaları hesaplanmıştır.

"E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık" ile *"E-postalarda şifre hedefli tehditlere yönelik farkındalık"* boyutlarının yetersiz düzeyde, *"E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık"* ile *"E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık"* boyutlarının kısmen yeterli düzeyde değerlendirildiği görülmektedir. "*E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık*" ve "*E-postalarda şifre hedefli tehditlere yönelik farkındalık*"

boyutlarının yetersiz ile kısmen yeterli düzeyleri arasında kaldığı, *"E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık*" ve *"E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık"* boyutlarının kısmen yeterli ile yeterli düzeyleri arasında kaldığı görülmektedir.

"*E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık*" ($\bar{X}$ = 2.95) ile "*E-postalarda şifre hedefli tehditlere yönelik farkındalık"* ($\bar{X}$ = 2.96) boyutlarının ve *"E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık*" ($\bar{X}$ = 3.08) ile *"E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık"* ($\bar{X}$ = 3.06) boyutlarının benzer ortalamaya sahip olduğu söylenebilmektedir (Tablo 21).

Tablo 21

İkinci Döngüde Yeniden Düzenlenen SGMÖN 'nin SGF-DPA Boyutlarına Göre Betimsel İstatistikleri

Mikro-öğrenme Nesnesi Boyutları	**Madde Sayısı**	**En Düşük**	**En Yüksek**	**$\bar{X}$**	**S.S.**
E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere *yönelik farkındalık*	5	1.40	4.60	2.95	0.67
E-postalarda yazım hatası kaynaklı tehditlere *yönelik farkındalık*	5	2.00	5.00	3.08	0.89
E-postalarda şifre hedefli tehditlere *yönelik farkındalık*	5	1.40	4.60	2.96	0.90
E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık	5	1.60	4.80	3.06	0.71

Yeniden düzenlenen mikro öğrenme nesneleri, siber güvenlik mikro öğrenme nesnelerinin ana bileşenleri olan *"E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık*", "*E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık*", "*E-postalarda şifre hedefli tehditlere yönelik farkındalık*" ve *"E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık"* alt boyutları açısından ayrı ayrı incelenmektedir.

1.1. İkinci Mezo Döngüde, Yeniden Düzenlenen E-postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditler Mikro Öğrenme Nesneleri, Öğrencilerin Siber Güvenlik Farkındalıkları Açısından Ne Düzeydedir?

Öğrencilerin, ikinci mezo döngüde yeniden düzenlenen siber güvenlik mikro öğrenme nesneleri, "*E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditle*re *yönelik farkındalık*" boyutu ve ölçütlerine yönelik değerlendirme sonuçları aşağıda sunulmuştur.

Siber güvenlik mikro öğrenme nesneleri, siber güvenlik farkındalığı dereceli puanlama anahtarı düzeyleri açısından incelendiğinde, "*E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık"* boyutu, % 22.30 (oldukça yetersiz), % 27.69 (yetersiz), % 30.76 (kısmen yeterli), % 10.76 (yeterli), % 8.46 (yeterince güçlü) olduğu belirlenmiştir. Ölçütler, düzeyler açısından incelendiğinde; "*E-postayı açma"* (% 38.5) kısmen yeterli düzeyde; "*Gönderen adresini kontrol etme*" (% 34.6) yetersiz ve kısmen yeterli düzeyde; "*E-posta içeriğindeki bağlantıya tıklama*" (%34.6) oldukça yetersiz düzeyde; "*E-postada istenen kişisel verileri gönderme*" (%42.3) kısmen yeterli düzeyde; "*E-posta içeriğindeki eki cihaza indirme*" (%38.5) yetersiz düzeyinde olduğu görülmektedir (Tablo 22).

Tablo 22

İkinci Döngüde Yeniden Düzenlenen SGMÖN'nin E-postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık Boyutuna İlişkin SGF-DPA Düzeyleri Betimsel İstatistikleri

E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık	**1**		**2**		**3**		**4**		**5**	
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**
E-postayı açma	6	23.1	4	15.4	10	38.5	6	23.1	-	-
Gönderen adresini kontrol etme	1	3.8	9	34.6	9	34.6	-	-	7	26.9
E-posta içeriğindeki bağlantıya tıklama	9	34.6	7	26.9	6	23.1	3	11.5	1	3.8

E-postada istenen kişisel verileri gönderme	4	15.4	6	23.1	11	42.3	2	7.7	3	11.5
E-posta içeriğindeki eki cihaza indirme	9	34.6	10	38.5	4	15.4	3	11.5	-	-

Siber güvenlik farkındalığı dereceli puanlama anahtarının *"E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık"* boyutu ve ölçütlerine göre ortalamaları (Tablo 23) incelendiğinde, "*E-posta içeriğindeki eki cihaza indirme"* ölçütünün ($\bar{X}$=2.03) en düşük ve "*Gönderen adresini kontrol etme*" ölçütünün ($\bar{X}$=3.11) en yüksek ortalamaya sahip olduğu görülmektedir. Ölçütler düzeyler açısından incelendiğinde ağırlıklı olarak yetersiz ile kısmen yeterli düzeyleri arasında toplandığı görülmektedir.

"*E-postayı açma*" ($\bar{X}$=2.61), "*E-posta içeriğindeki bağlantıya tıklama*" ($\bar{X}$=2.23), "*E-postada istenen kişisel verileri gönderme*" ($\bar{X}$=2.76), "*E-posta içeriğindeki eki cihaza indirme*" ($\bar{X}$=2.03) ölçütleri yetersiz ile kısmen yeterli düzeyleri arasında yer alırken; "*Gönderen adresini kontrol etme*" ($\bar{X}$=3.11) ölçütünün kısmen yeterli ile yeterli düzeyleri arasında yer alması dikkat çekicidir.

Ölçütlerin aldığı en düşük ve en yüksek değerler incelendiğinde "*E-postayı açma*" ve "*E-posta içeriğindeki eki cihaza indirme*" ölçütlerinin en düşük oldukça yetersiz, en yüksek yeterli düzeylerinde değerlendirildiği; "*Gönderen adresini kontrol etme*", "*E-posta içeriğindeki bağlantıya tıklama*" ve "*E-postada istenen kişisel verileri gönderme*" ölçütlerinin en düşük oldukça yetersiz, en yüksek yeterince güçlü düzeylerinde değerlendirildiği görülmektedir (Tablo 23).

Tablo 23

İkinci Döngüde Yeniden Düzenlenen SGMÖN'nin SGF-DPA E-postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlere Yönelik Farkındalık Boyutu Betimsel İstatistikleri

E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık	N	En Düşük	En Yüksek	X̄	S.S.
E-postayı açma	26	1.00	4.00	2.61	1.09
Gönderen adresini kontrol etme	26	1.00	5.00	3.11	1.27
E-posta içeriğindeki bağlantıya tıklama	26	1.00	5.00	2.23	1.17
E-postada istenen kişisel verileri gönderme	26	1.00	5.00	2.76	1.17
E-posta içeriğindeki eki cihaza indirme	26	1.00	4.00	2.03	0.99

Siber güvenlik farkındalığı dereceli puanlama anahtarının alt boyutlarından olan "*E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık*" boyutunun, "*E-postayı açma*" ve "*E-postada istenen kişisel verileri gönderme*" ölçütlerinin kısmen yeterli düzeyde, "*Gönderen adresini kontrol etme*" ölçütünün yetersiz ve kısmen yeterli düzeylerinde, "*E-posta içeriğindeki bağlantıya tıklama*" ölçütünün oldukça yetersiz düzeyde, "*E-posta içeriğindeki eki cihaza indirme*" ölçütünün yetersiz düzeyde değerlendirildiği dikkat çekmektedir.

1.2. İkinci Mezo Döngüde, Yeniden Düzenlenen E-postalarda Yazım Hatası Kaynaklı Tehditler Mikro Öğrenme Nesneleri, Öğrencilerin Siber Güvenlik Farkındalıkları Açısından Ne Düzeydedir?

Öğrencilerin, ikinci mezo döngüde yeniden düzenlenen siber güvenlik mikro öğrenme nesneleri, "*E-postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık*" boyutu ve ölçütlerine yönelik değerlendirme sonuçları aşağıda sunulmuştur.

SGMÖN, SGF-DPA düzeyleri açısından incelendiğinde "*E-postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık*" boyutu, % 0.76 (oldukça yetersiz), % 42.30

(yetersiz), % 30 (kısmen yeterli), % 1.53 (yeterli) ve % 25,38 (yeterince güçlü) olduğu belirlenmiştir. Ölçütler, düzeyler açısından incelendiğinde; "*Yazım kurallarına uygunluğu kontrol etme*" (% 42.3) ölçütünün kısmen yeterli düzeyde; *"E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme"* (% 34.6) ölçütünün yetersiz ve yeterince güçlü düzeyde; "*E-postayı gönderenin adresinin yazımını kontrol etme*" (%46.2) ölçütünün yetersiz düzeyde; "*E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme*" (%57.7) ölçütünün yetersiz düzeyde; "*E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme*" (%46.2) ölçütünün yetersiz düzeyde olduğu görülmektedir (Tablo 24).

Tablo 24

İkinci Döngüde Yeniden Düzenlenen SGMÖN'nin E-postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık Boyutuna İlişkin SGF-DPA Düzeyleri Betimsel İstatistikleri

E-postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık	**1**		**2**		**3**		**4**		**5**	
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**
Yazım kurallarına uygunluğu kontrol etme	-	-	7	26.9	11	42.3	2	7.7	6	23.1
E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme	-	-	9	34.6	8	30.8	-	-	9	34.6
E-postayı gönderenin adresinin yazımını kontrol etme	1	3.8	12	46.2	8	30.8	-	-	5	19.2
E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme	-	-	15	57.7	4	15.4	-	-	7	26.9
E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme	-	-	12	46.2	8	30.8	-	-	6	23.1

Siber güvenlik farkındalığı dereceli puanlama anahtarının "*E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık*" boyutu ve ölçütlerine göre ortalamaları (Tablo 25) incelendiğinde "*E-postayı gönderenin adresinin yazımını kontrol etme*" ($\bar{X}$=2.84)

ölçütünün en düşük ve "*E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme*" ($\bar{X}$=3.34) ölçütünün en yüksek ortalamaya sahip olduğu görülmektedir. Ölçütler düzeyler açısından incelendiğinde ağırlıklı olarak kısmen yeterli düzeyde yığıldıkları görülmektedir.

"*Yazım kurallarına uygunluğu kontrol etme*" ($\bar{X}$=3.26) ve "*E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme*" ($\bar{X}$=3.34) ölçütleri kısmen yeterli ile yeterli düzeyleri arasında, "*E-postayı gönderenin adresinin yazımını kontrol etme"* ($\bar{X}$=2.84) ve "*E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme*" ($\bar{X}$=2.96) ölçütleri yetersiz ile kısmen yeterli düzeyleri arasında, "*E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme*" ($\bar{X}$=3.00) ölçütünün kısmen yeterli düzeyde yer alması dikkat çekicidir.

Ölçütlerin aldığı en düşük ve en yüksek değerler incelendiğinde "*E-postayı gönderenin adresinin yazımını kontrol etme*" ölçütünün en düşük oldukça yetersiz, en yüksek yeterince güçlü düzeyde değerlendirildiği, diğer tüm ölçütlerin en düşük yetersiz, en yüksek yeterince güçlü düzeyde değerlendirildiği görülmektedir (Tablo 25).

Tablo 25

İkinci Döngüde Yeniden Düzenlenen SGMÖN'nin SGF-DPA E-postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık Boyutu Betimsel İstatistikleri

E-postalarda Yazım Hatası Kaynaklı Tehditlere Yönelik Farkındalık	**N**	**En Düşük**	**En Yüksek**	**$\bar{X}$**	**S.S.**
Yazım kurallarına uygunluğu kontrol etme	26	2.00	5.00	3.26	1.11
E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme	26	2.00	5.00	3.34	1.29
E-postayı gönderenin adresinin yazımını kontrol etme	26	1.00	5.00	2.84	1.18
E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme	26	2.00	5.00	2.96	1.31
E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme	26	2.00	5.00	3.00	1.20

Siber güvenlik farkındalığı dereceli puanlama anahtarı alt boyutlarından olan "*E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık*" boyutunun, "*Yazım*

kurallarına uygunluğu kontrol etme" ölçütünün kısmen yeterli düzeyde; "*E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme*" ölçütünün yetersiz ve yeterince güçlü düzeyde, "*E-postayı gönderenin adresinin yazımını kontrol etme*", "*E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme*" ve "*E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme*" ölçütlerinin yetersiz düzeyde değerlendirildiği dikkat çekmektedir.

1.3. İkinci Mezo Döngüde, Yeniden Düzenlenen E-postalarda Şifre Hedefli Tehditler Mikro Öğrenme Nesneleri, Öğrencilerin Siber Güvenlik Farkındalıkları Açısından Ne Düzeydedir?

Öğrencilerin, ikinci mezo döngüde yeniden düzenlenen SGMÖN 'nin, SGF-DPA 'nın "*E-postalarda şifre hedefli tehditlere yönelik farkındalık"* boyutu ve ölçütlerine yönelik değerlendirme sonuçları aşağıda sunulmuştur.

SGMÖN, SGF-DPA düzeyleri açısından incelendiğinde "*E-postalarda şifre hedefli tehditlere yönelik farkındalık"* boyutu, % 16.15 (oldukça yetersiz), % 33.84 (yetersiz), % 17.69 (kısmen yeterli), % 2.30 (yeterli) ve % 30 (yeterince güçlü) olduğu belirlenmiştir. Ölçütler, düzeyler açısından incelendiğinde; "*E-posta şifre değiştirme sıklığı*" (% 46.2) ölçütünün yetersiz düzeyde; "*E-posta şifre uzunluğu*" (% 42.3) ölçütünün yeterince güçlü düzeyde; "*E-posta şifresi ile klavye düzeni ilişkisi"* (% 46.2) ölçütünün yeterince güçlü düzeyde; "*Kişisel verilerle şifre belirleme*" (% 30.8) ölçütünün kısmen yeterli düzeyde; "*Karmaşık ve özel karakterlerle şifre belirleme*" (% 46.2) ölçütünün oldukça yetersiz düzeyde olduğu görülmektedir (Tablo 26).

Tablo 26

İkinci Döngüde Yeniden Düzenlenen SGMÖN 'nin E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık Boyutuna İlişkin SGF-DPA Düzeyleri Betimsel İstatistikleri

E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık	**1**		**2**		**3**		**4**		**5**	
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**
E-posta şifre değiştirme sıklığı	3	11.5	12	46.2	2	7.7	-	-	9	34.6
E-posta şifre uzunluğu	-	-	10	38.5	5	19.2	-	-	11	42.3
E-posta şifresi ile klavye düzeni ilişkisi	-	-	10	38.5	4	15.4	-	-	12	46.2
Kişisel verilerle şifre belirleme	6	23.1	6	23.1	8	30.8	2	7.7	4	15.4
Karmaşık ve özel karakterlerle şifre belirleme	12	46.2	6	23.1	4	15.4	1	3.8	3	11.5

Siber güvenlik farkındalığı dereceli puanlama anahtarının "*E-postalarda şifre hedefli tehditlere yönelik farkındalık*" boyutu ve ölçütlerine göre ortalamaları (Tablo 27) incelendiğinde "*Karmaşık ve özel karakterlerle şifre belirleme*" ($\bar{X}$=2.11) ölçütünün en düşük ve "*E-posta şifre değiştirme sıklığı*" ölçütünün ($\bar{X}$=3.67) en yüksek ortalamaya sahip olduğu görülmektedir. Ölçütler düzeyler açısından incelendiğinde ağırlıklı olarak kısmen yeterli ile yeterli düzeyleri arasında yığıldıkları görülmektedir.

"*E-posta şifre değiştirme sıklığı*" ($\bar{X}$=3.67), "*E-posta şifre uzunluğu*" ($\bar{X}$=3.46) ve "*E-posta şifresi ile klavye düzeni ilişkisi*" ($\bar{X}$=3.53) ölçütleri kısmen yeterli ile yeterli düzeyleri arasında yer alırken; "*Kişisel verilerle şifre belirleme*" ($\bar{X}$=2.69) ile "*Karmaşık ve özel karakterlerle şifre belirleme*" ($\bar{X}$=2.11) ölçütleri yetersiz ile kısmen yeterli düzeyleri arasında yer alması dikkat çekicidir.

Ölçütlerin aldığı en düşük ve en yüksek değerler incelendiğinde "*E-posta şifre uzunluğu*" ve "*E-posta şifresi ile klavye düzeni ilişkisi*" ölçütlerinin en düşük yetersiz, en yüksek yeterince güçlü düzeyinde değerlendirilirken, "*E-posta şifre değiştirme sıklığı*", "*Kişisel verilerle şifre belirleme*" ve "*Karmaşık ve özel karakterlerle şifre belirleme*"

ölçütlerinin en düşük oldukça yetersiz, en yüksek yeterince güçlü düzeyinde değerlendirildiği görülmektedir (Tablo 27).

Tablo 27

İkinci Döngüde Yeniden Düzenlenen SGMÖN 'nin SGF-DPA E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık Boyutu Betimsel İstatistikleri

E-postalarda Şifre Hedefli Tehditlere Yönelik Farkındalık	N	En Düşük	En Yüksek	$\bar{X}$	S.S.
E-posta şifre değiştirme sıklığı	26	1	5	3.67	1.54
E-posta şifre uzunluğu	26	2	5	3.46	1.39
E-posta şifresi ile klavye düzeni ilişkisi	26	2	5	3.53	1.42
Kişisel verilerle şifre belirleme	26	1	5	2.69	1.34
Karmaşık ve özel karakterlerle şifre belirleme	26	1	5	2.11	1.36

Siber güvenlik farkındalığı dereceli puanlama anahtarı alt boyutlarından olan "*E-postalarda şifre hedefli tehditlere yönelik farkındalık*" boyutunun, "*E-posta şifre uzunluğu*" ile "*E-posta şifresi ile klavye düzeni ilişkisi*" ölçütlerinin yeterince güçlü düzeyde; "*E-posta şifre değiştirme sıklığı*" ölçütünün yetersiz düzeyde; "*Kişisel verilerle şifre belirleme*" ölçütünün kısmen yeterli düzeyde; "*Karmaşık ve özel karakterlerle şifre belirleme*" ölçütünün oldukça yetersiz düzeyde değerlendirildiği dikkat çekmektedir.

1.4. İkinci Mezo Döngüde, Yeniden Düzenlenen E-posta Güvenlik Ayarlarının Kullanımı Odaklı Mikro Öğrenme Nesneleri, Öğrencilerin Siber Güvenlik Farkındalıkları Açısından Ne Düzeydedir?

Öğrencilerin, ikinci mezo döngüde yeniden düzenlenen siber güvenlik mikro-öğrenme nesnelerinin, siber güvenlik farkındalığı dereceli puanlama anahtarının "*E-posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık*" boyutu ve ölçütlerine yönelik değerlendirme sonuçları aşağıda sunulmuştur.

SGMÖN'nin, SGF-DPA düzeyleri açısından incelendiğinde, "*E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık"* boyutu, % 14.61 (oldukça yetersiz), % 32.30 (yetersiz), % 16.92 (kısmen yeterli), % 4.61 (yeterli), % 31.53 (yeterince güçlü) olduğu belirlenmiştir. Ölçütler, düzeyler açısından incelendiğinde; "*Çift faktörlü kimlik doğrulama kullanma*" (% 42.3) ölçütünün yetersiz düzeyde; "*Telefonla doğrulama kullanma*" (% 65.4) ölçütünün yeterince güçlü düzeyde; "*Kurtarma e-postası kullanma*" (% 34.6) ölçütünün oldukça yetersiz düzeyde; "*Güvenlik ayarları hakkında bilgi edinme*" (% 38.5) ölçütünün yetersiz düzeyde; "*Güncellemeleri uygulama*" (% 53.8) ölçütünün yeterince güçlü düzeyde olduğu görülmektedir (Tablo 28).

Tablo 28

İkinci Döngüde Yeniden Düzenlenen SGMÖN 'nin E-posta Güvenlik Ayarların Kullanımına İlişkin Farkındalık Boyutuna İlişkin SGF-DPA Düzeyleri Betimsel İstatistikleri

E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık	**1**		**2**		**3**		**4**		**5**	
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**
Çift faktörlü kimlik doğrulama kullanma	4	15.4	11	42.3	6	23.1	-	-	5	19.2
Telefonla doğrulama kullanma	-	-	7	26.9	2	7.7	-	-	17	65.4
Kurtarma e-postası kullanma	9	34.6	6	23.1	5	19.2	3	11.5	3	11.5
Güvenlik ayarları hakkında bilgi edinme	6	23.1	10	38.5	5	19.2	3	11.5	2	7.7
Güncellemeleri uygulama	-	-	8	30.8	4	15.4	-	-	14	53.8

Siber güvenlik farkındalığı dereceli puanlama anahtarının "*E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık*" boyutu ölçütlerine göre aldığı ortalamalar (Tablo 29) incelendiğinde *"Kurtarma e-postası kullanma"* ve "*Güvenlik ayarları hakkında bilgi edinme*" ölçütlerinin seviyesinin ($\bar{X}$=2.42) en düşük ve "*Telefonla doğrulama kullanma" ölçütünün seviyesinin* ($\bar{X}$=4.03) en yüksek ortalamaya sahip olduğu görülmektedir. Ölçütler düzeyler açısından incelendiğinde "*Telefonla doğrulama kullanma"* ölçütünün yeterli ile yeterince güçlü düzeyleri arasında; "*Güncellemeleri uygulama*" ölçütünün kısmen yeterli ile

yeterli düzeyleri arasında; diğer ölçütlerin yetersiz ile kısmen yeterli düzeyleri arasında yığıldıkları görülmektedir.

Ölçütlerin aldığı en düşük ve en yüksek değerler incelendiğinde "*Telefonla doğrulama kullanma*" ve "*Güncellemeleri uygulama*" ölçütlerinin en düşük yetersiz, en yüksek yeterince güçlü düzeyde değerlendirildiği, "*Çift faktörlü kimlik doğrulama kullanma*", "*Kurtarma e-postası kullanma*" ve "*Güvenlik ayarları hakkında bilgi edinme*" ölçütlerinin en düşük oldukça yetersiz, en yüksek yeterince güçlü düzeyde değerlendirildiği görülmektedir (Tablo 29).

Tablo 29

İkinci Döngüde Yeniden Düzenlenen SGMÖN 'nin SGF-DPA E-posta Güvenlik Ayarlarının Kullanımına İlişkin Farkındalık Boyutu Betimsel İstatistikleri

E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık	**N**	**En Düşük**	**En Yüksek**	**X̄**	**S.S.**
Çift faktörlü kimlik doğrulama kullanma	26	1	5	2.65	1.32
Telefonla doğrulama kullanma	26	2	5	4.03	1.37
Kurtarma e-postası kullanma	26	1	5	2.42	1.39
Güvenlik ayarları hakkında bilgi edinme	26	1	5	2.42	1.20
Güncellemeleri uygulama	26	2	5	3.76	1.39

Siber güvenlik farkındalığı dereceli puanlama anahtarı alt boyutlarından olan "*E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık*" boyutunun, "*Çift faktörlü kimlik doğrulama kullanma*", "*Güvenlik ayarları hakkında bilgi edinme",* ölçütlerinin yetersiz düzeyde, "*Telefonla doğrulama kullanma*", *"Güncellemeleri uygulama*" ölçütlerinin yeterince güçlü düzeyde, "*Kurtarma e-postası kullanma*" ölçütünün oldukça yetersiz düzeyde değerlendirildiği dikkat çekmektedir.

2. **Öğrencilerin, İkinci Mezo Döngüde Öğrenme-Öğretme Sürecinde Yeniden Düzenlenen Siber Güvenlik Mikro Öğrenme Nesnelerine Yönelik Görüşleri Nelerdir?**

Öğrencilerin ikinci mezo döngü kapsamında yeniden düzenlenen SGMÖN'nin, deneyimlerine yönelik olumlu ve olumsuz görüşlerini belirlemek amacıyla süreçte iyi yapabildikleri/yapamadıkları ve süreçlerini kolaylaştıran/zorlaştıran etmenler sorulmuş, elde edilen bulgular Tablo 30'da sunulmuştur.

Öğrencilerin yarıdan fazlası gerçek yaşamda karşılaştığı siber tehditlerle öğrendiklerini ilişkilendirme, yarıya yakını siber güvenlik ilişkili kavramları anlama ve gelen e-postalardaki yazım hatasının tehdit içerebileceğini anlama konusunda güçlü olduklarını belirtmişlerdir. Öğrencilerin yarısı e-posta güvenlik ayarlarını yapabilme, yarıdan fazlası e-posta karmaşık şifreleme adımlarını oluşturma konusunda zayıf olduklarını ifade etmişlerdir. Öğrencilerin tamamına yakını etkileşimli öğrenme materyali, işbirlikli çalışma ve anlık geri bildirimin e-posta hedefli siber tehditleri tespit etmeyi kolaylaştırdığını belirtmiştir. Üç öğrenciden biri teknik destek kaynaklı sorunlar, süre yetersizliği ve mobil cihaz desteğinin eksikliğinin e-posta hedefli siber tehditleri tespit etmeyi zorlaştırdığını belirtmiştir (Tablo 30).

Tablo 30

İkinci Döngüde Öğrencilerin SGMÖN'ne Yönelik Görüşlerine İlişkin Tema, Kod, Frekans ve Yüzdeleri

Tema	Kod	f	%
Siber güvenlik mikro-öğrenme nesneleri ile, , e-posta hedefli siber tehditleri tespit etmede kazandığım güçlü yönler	Siber güvenlik ilişkili temel kavramları anlama	11	42.3
	Gerçek yaşamda karşılaştığı siber tehditlerle öğrendiklerini ilişkilendirme	14	53.8
	Gelen e-postalardaki yazım hatasının tehdit içerebileceğini anlama	9	34.6
Siber güvenlik mikro-öğrenme nesneleri ile, , e-posta hedefli siber tehditleri tespit etmede zayıf yönler	E-posta güvenlik ayarlarını yapabilme	13	50
	E-posta karmaşık şifreleme adımlarını oluşturma	16	61.5
	Etkileşimli öğrenme materyali	19	73.0

Siber güvenlik mikro-öğrenme nesneleri ile,, e-posta hedefli siber tehditleri tespit etmemi kolaylaştıran yönler	İşbirlikli çalışma	21	80.7
	Anlık geri bildirim	24	92.3
Siber güvenlik mikro-öğrenme nesneleri ile, , e-posta hedefli siber tehditleri tespit etmemi zorlaştıran/engelleyen yönler	Teknik destek kaynaklı sorunlar	10	38.4
	Süre yetersizliği	9	34.6
	Mobil cihaz desteğinin eksikliği	9	34.6
Öğrenci Sayısı		26	100

Öğrenci yorumlarından bazıları şu şekildedir:

Siber Güvenlik mikro-öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmede kazandığım güçlü yönler ölçütü için;

"*Siber güvenliğin ne demek olduğunu biliyorum ve kendimi siber saldırılara karşı koruyabilirim."* (Ö12).

"*Güçlü şifre oluşturma yollarını öğrendim ve kişisel bilgilerimi saldırılara karşı koruyabilirim.*" (Ö14).

"*Kişisel verilerimin ve hesaplarımın saldırganların eline geçmesini önleyebilirim*." (Ö47).

Siber Güvenlik mikro-öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmede zayıf yönler ölçütü için;

"*Gelen e-postada bağlantılar olması ve kişisel veriler talep etmeleri*." (Ö2).

"*Yabancı dilde gelen e-postalarda kimlik avını tespit edemem*." (Ö50).

"*Güvenlik ayarları konusunda zayıf hissediyorum*." (Ö49).

Siber Güvenlik mikro-öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmemi kolaylaştıran yönler ölçütü için;

"*Kişisel verilerimi ve hesaplarımı koruyabilmem*." (Ö50).

"*Siber güvenlik hakkında öğrendiklerim sayesinde kendimi güvende hissederim*." (Ö13).

"*E-posta ve sosyal hesaplarımı koruyabilirim*." (Ö53).

Siber Güvenlik mikro-öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmemi zorlaştıran/engelleyen yönler ölçütü için;

"*Hesaplarım ve kişisel verilerim çalınabilir*." (Ö50).

"*Hesabımı ve kişisel bilgilerimi ele geçirebilirler*." (Ö4).

İkinci mezo döngü süreci sonunda siber güvenlik farkındalığı öğrenci görüşme formunda öğrencilerin belirttiği görüşler dikkate alındığında, öğrencilerin siber güvenlik kavramında farkındalık kazanmaya ilişkin olarak büyük çoğunluğunun başarılı sonuçlar elde ettiği söylenebilir. Birinci döngünün aksine öğrendiklerini günlük hayatla ilişkilendirmede daha güçlü oldukları anlaşılmaktadır. E-postaları hedefleyen siber tehditleri tespit etme yöntemlerinde daha başarılı oldukları görülmektedir. Öğrencilerin mikro öğrenme nesnelerinin daha başarılı olduğu görüşünde hemfikir olduğu anlaşılmaktadır.

Birinci ve İkinci Mezo Döngü Bulguları Karşılaştırmalı Analizi

Bu bölümde birinci ve ikinci mezo döngüler sonucunda, siber güvenlik mikro-öğrenme nesneleri tasarlama ve değerlendirme sürecine yönelik elde edilen bulgular, karşılaştırılarak analiz edilmiştir.

Tablo 31

Birinci ve İkinci Mezo Döngü Betimsel İstatistikleri

Mikro-öğrenme Nesnesi Boyutları	**Birinci Mezo Döngü** $\bar{X}$	**İkinci Mezo Döngü** $\bar{X}$
E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık	2.73	2.95
E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık	2.73	3.08

E-postalarda şifre hedefli tehditlere yönelik farkındalık	2.62	2.96
E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık	2.55	3.06

Her iki döngü sonucunda elde edilen bulgular ışığında mikro öğrenme nesnelerinin siber güvenlik farkındalığı amacıyla kullanımının başarılı sonuçlar elde edilebileceğini söylemek mümkündür. Birinci döngü sonucunda elde edilen bulgular *E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık, E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık, E-postalarda şifre hedefli tehditlere yönelik farkındalık* ve *E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık* boyutlarının ortalamalarının yetersiz düzeyde değerlendirildiğini, ikinci döngü sonucunda elde edilen bulgular *E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık, E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık, E-postalarda şifre hedefli tehditlere yönelik farkındalık* ve *E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık* boyutlarının ortalamalarının kısmen yeterli düzeyde değerlendirildiğini göstermektedir.

İkinci döngü sonucunda elde edilen bulgular, öğrencilerin değerlendirme puanlarının birinci döngüye göre belirgin bir yükseliş olduğu söylenebilir. Bulgular ikinci döngüde, Hug'ın (2005) tanımladığı, (1) Kısa ölçülebilir zaman, çaba ve zaman tüketiminin derecesi olan öğrenme süresi, (2) Küçük öğrenme üniteleri, basit konular ve dar konular içeren öğrenme içeriği, (3) Modüller setini ve informal öğrenme gibi öğrenme modelinin türünü ifade eden müfredat, (4) Parçalara, bölümlere ve bilgi kırıntılarına odaklanan öğrenme formu, (5) Ayrı, bağlantılı, konumlandırılmış veya entegre faaliyetlere odaklanan öğrenme süreci, (6) Öğrenme nesneleri, yüz yüze ve multimedya kullanan öğrenme ortamı ve (7) Davranışçı, yapılandırmacı ve sosyal öğrenme perspektiflerini içeren öğrenme tipi boyutları çerçevesinde yeniden düzenlenen siber güvenlik mikro öğrenme nesnelerinin etkili olduğunu göstermektedir.

Birinci döngüde başarılı sonuçlar alınmasına rağmen süreçte öğrencilerin motivasyon düşüklüğü ve odaklanma sorunları yaşadığı gözlemlenmiştir. Bu durumu çözmek amacıyla ikinci döngüde siber korsanları çağrıştıran siyah korsan şapkalı ve siyah göz bantlı, hedef kitlenin yaş seviyesine uygun görünümde bir karakter tasarıma eklenmiş, mikro öğrenme nesneleri video tabanlı tasarlanmış ve öğrenme nesnelerini daha gerçekçi hale getirmesi ve metinlerin ekranda çiziminin öğrenci ile etkileşimi sağlaması amacı ile el yazısı ile çizim efekti eklenmiştir. İkinci döngü sonucunda elde edilen bulgular video tabanlı mikro öğrenme nesnelerinin başarılı olduğunu, tasarıma eklenen karakterin ve kullanılan efektin odaklanmayı ve motivasyonu artırdığını göstermektedir.

Bölüm 5

Sonuç ve Öneriler

Bu araştırmanın temel amacı, ilköğretim düzeyinde siber güvenlik mikro-öğrenme nesneleri tasarlamak, geliştirmek ve öğrencilerin siber güvenlik farkındalık düzeylerini, siber güvenlik farkındalık ölçütleriyle değerlendirmektir. Bu ölçütler; (a) E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık; (b) E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık, (c) E-postalarda şifre hedefli tehditlere yönelik farkındalık; (d) E-posta güvenlik ayarlarının kullanımına ilişkin farkındalıktır.

Araştırmada, Milli Eğitim Bakanlığı'nın (MEB) yayınlamış olduğu İlköğretim ikinci kademe Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programında; *6. Sınıf seviyesinde,* "Bilişim suçlarına karşı alınabilecek önlemler ve stratejiler geliştirir" hedefi (MEB, 2018) kapsamında geliştirilen *(a) E-postalardaki kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlerin farkına varabilme, (b) E-postalardaki yazım hatası kaynaklı tehditlerin farkına varabilme, (c) E-postalardaki şifre hedefli tehditlerin farkına varabilme, (ç) E-posta güvenlik ayarlarını kullanabilme* kazanımları odağında siber güvenlik mikro-öğrenme nesnelerinin geliştirilmesi amaçlanmıştır.

Bu araştırmada öğrencilerin siber güvenlik farkındalıklarına katkı sağlayabilecek mikro öğrenme stratejisini temel alan siber güvenlik mikro öğrenme nesneleri tasarımı yapılmıştır. Ortaokul düzeyinde 6. sınıf seviyesinde öğrenim görmekte olan 55 öğrenciyle bir birini takip eden iki döngü şeklinde eğitsel tasarım tabanlı araştırma yöntemiyle gerçekleştirilmiştir. Araştırmanın her iki mezo döngüsü "analiz ve inceleme", "tasarım ve geliştirme" ve "değerlendirme ve yansıma" olmak üzere 3 mikro döngüden oluşmaktadır. Süreç, Talim Terbiye Kurulu'nun (MEB, 2018) Bilişim Teknolojileri Dersi 6. sınıflar için genel çerçevesi tanımlanan "Bilişim suçlarına karşı alınabilecek önlemler ve stratejiler geliştirir" hedefi odağında, Siber Güvenlik Farkındalığı kazanımları (a) *E-Postalarda Kaynağı Bilinmeyen Bağlantı ve İçerik Kaynaklı Tehditlerin Farkına Varabilme*: Kaynağı bilinmeyen bağlantıların, dosyaların bulunduğu, e-postalara karşı farkındalığı; (b) *E-Postalarda Yazım*

Hatası İçeren Tehditlerin Farkına Varabilme: Bilinen kaynakları taklit ederek gönderilen e-postalar içerisindeki yazım hatalarına karşı farkındalığı; (c) *E-Postalarda Şifre Hedefli Tehditlerin Farkına Varabilme:* Kullanıcı şifrelerini hedef alan saldırılar, şifre güvenliği ve güçlü şifre oluşturma farkındalığı; (ç) *E-Posta Güvenlik Ayarlarını Kullanabilme:* E-posta servislerinin sunmuş olduğu güvenlik hizmetleri, güvenlik ayarlarının kullanımı ve önemine yönelik farkındalığı; kapsamında yapılandırılmıştır.

Her iki döngüde elde edilen sonuçlar, siber güvenlik farkındalığı ana ölçütleri ve alt ölçütlerinin değerlendirilmelerine göre yorumlanmıştır. Birinci mezo döngüde elde edilen sonuçlar doğrultusunda ikinci mezo döngüdeki süreç yapılandırılmıştır. Her iki döngü sonuçları itibariyle, tasarlanan siber güvenlik mikro öğrenme nesnelerinin, öğrencilerin siber güvenlik farkındalığına katkı sağladığını göstermektedir. Araştırmanın ilk mezo döngüsü sonucunda tasarlan siber güvenlik mikro öğrenme nesnelerinin yeniden düzenlenmesi için eklemeler yapılması gerektiğini gösteren bulgular elde edilmiş, öğrenme nesneleri yeniden düzenlenmiştir.

Siber güvenlik farkındalığına yönelik olarak, her iki döngüdeki SGF-DPA değerlendirme sonuçları incelendiğinde birinci döngüde değerlendirme ortalamaları yetersiz düzeyde olan bütün ölçütlerin ikinci düzeyde kısmen yeterli düzeye yükseldiği görülmektedir. Bu sonuca göre, ikinci döngüde Hug'ın (2005) tanımlamış olduğu mikro öğrenme boyutları çerçevesinde yeniden düzenlenen mikro öğrenme nesnelerinin siber güvenlik farkındalığına katkı sağlamada başarılı olduğunu söylemek mümkündür. Birinci döngüde değerlendirme sonuçlarına göre en düşük ortalamaya sahip *E-posta güvenlik ayarlarının kullanımına ilişkin farkındalık* ölçütünün, ikinci döngüde diğer ölçütlere nazaran daha büyük bir yükseliş göstererek ortalamalara göre en yüksek ikinci ölçüt olması dikkat çekicidir. İkinci döngüde, Gmail ücretsiz e-posta servisinin sunmuş olduğu güvenlik ayarları hizmeti kullanılarak gerçekleştirilen sınıf içi uygulamaların bu etkiye neden olduğu söylenebilir.

E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık boyutu alt ölçütleri için, birinci döngüde *E-postayı açma, E-posta içeriğindeki bağlantıya tıklama*, *E-postada istenen kişisel verileri gönderme* ve *E-posta içeriğindeki eki cihaza indirme* ölçütleri oldukça yetersiz düzeyinde değerlendirilmişken, ikinci döngüde yetersiz düzeyin üzerinde değerlendirildiği görülmektedir. Bu sonuca göre, ikinci döngüde Hug'ın (2005) tanımlamış olduğu mikro öğrenme boyutları çerçevesinde yeniden düzenlenen mikro öğrenme nesnelerinin *E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik* farkındalığa katkı sağlamada başarılı olduğunu söylemek mümkündür. Case ve King (2016) ile Jerrim (2023) siber tehditlere karşı eğitimin, öğrencilerin siber güvenliklerine daha fazla dikkat etme konusunda etkili olabileceğini savunmuşlardır. *E-postalarda kaynağı bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalık* boyutu alt ölçütlerinden, ilk döngüde tüm ölçütler oldukça yetersiz düzeydeyken *Gönderen adresini kontrol etme* ölçütünün yetersiz düzeyde olduğu görülmektedir. Siber güvenlik mikro öğrenme nesnelerinin öğrencilerin siber güvenlik farkındalığının artmasına etkili olduğu ifade edilebilir. Birinci döngüde değerlendirme sonuçlarına göre en düşük ortalamaya sahip *E-postada istenen kişisel verileri gönderme* ölçütünün, ikinci döngüde diğer ölçütlere nazaran daha büyük bir yükseliş göstererek ortalamalara göre en yüksek ikinci ölçüt olması dikkat çekicidir. İkinci döngüde, gerçekleştirilen öğretimi destekleyen ve öğrencilerle etkileşimi artıran etkinliklerin etkili olduğu söylemek mümkündür.

E-postalarda yazım hatası kaynaklı tehditlere yönelik farkındalık boyutu alt ölçütleri için, birinci döngüde tüm ölçütler yetersiz düzeyde değerlendirilmişken, ikinci döngüde kısmen yeterli düzeyde değerlendirildiği görülmektedir. İkinci döngüde kullanılan "https://phishingquiz.withgoogle.com/" çevrim içi e-postaları hedefleyen siber tehdit testinin *E-postalarda yazım hatası kaynaklı tehditlere yönelik* farkındalığa olumlu yönde etki ettiğini söylemek mümkündür. Ayrıca Hug'ın (2005) tanımlamış olduğu mikro öğrenme boyutları çerçevesinde yeniden düzenlenen mikro öğrenme nesnelerinin *E-postalarda kaynağı*

bilinmeyen bağlantı ve içerik kaynaklı tehditlere yönelik farkındalığa katkı sağlamada başarılı olduğu söylenebilir. Bulgular Weaver ve arkadaşlarının (2021) yapmış olduğu araştırmada belirttiği gibi e-postaları hedef alan siber tehditlere yönelik hazırlanan öğrenme nesnelerinin kullanımının saldırıları tespit etme ve sınıflandırma da öğrencilerin siber güvenlik farkındalığına katkı sağlayabileceğini söylemek mümkündür.

E-postalarda şifre hedefli tehditlere yönelik farkındalık boyutu alt ölçütleri için, *E-posta şifresi ile klavye düzeni ilişkisi* alt ölçütünde, ikinci döngüde kısmi bir düşüş olduğu diğer tüm alt ölçütlerde yükseliş olduğu görülmektedir. İkinci döngü sürecinde kullanılan çevrim içi şifre aracının bu yükselişte etkili olduğunu söylemek mümkündür. Muniandy ve arkadaşlarının (2017) yapmış olduğu araştırmada belirtilen öğrencilerin şifre kullanımı konusunda yetersiz olduğu ve bu durumun siber tehditlere karşı savunmasız olmalarının önüne geçebilmek için mikro-öğrenme stratejisini temele alan öğretim materyalleri tasarımı ile başarılı sonuçlar alınabileceği görülmektedir.

E-postalarda güvenlik ayarlarını kullanabilme boyutu alt ölçütleri için, ikinci döngüde tüm alt ölçütlerde yükseliş olduğu görülmektedir. İkinci döngü sürecinde Gmail e-posta servis hizmetinin sunmuş olduğu güvenlik ayarları üzerinden yapılan sınıf içi uygulamaların bu yükselişte etkili olduğunu söylemek mümkündür. *Telefonla doğrulama kullanma* alt ölçütünün her iki döngüde diğer alt ölçütlerden belirgin bir şekilde yüksek çıktığı görülmektedir. Bu durumun gerek sosyal ağlarda gerekse e-posta servislerinde kullanıcıların sahip oldukları telefonları giriş ve kimlik doğrulama aracı olarak kullanmalarında hizmeti sunan kuruluşlar tarafından teşvik edilmeleri olduğu düşünülmektedir. Benzer şekilde *Güncellemeleri uygulama* ölçütünün de diğer ölçütlerden belirgin bir şekilde yüksek değerlendirildiği görülmektedir. Mobil cihazlarda ve bilgisayarlarda kullanılan uygulamaların kullanıcıları güncelleme yapmaya teşvik etmelerinin bu sonuçta etkili olduğu düşünülmektedir.

Öğrencilerin ikinci mezo döngü sonucundaki görüşleri incelendiğinde ilk mezo döngü sonucundaki görüşlerinden farklı olarak büyük bir kısmı etkileşimli öğrenme

materyalinin siber tehditleri tespit etmelerini kolaylaştırdıklarını belirtmiştir. Hedef kitlenin seviyesine uygun olarak tasarlanan korsan karakteri eklenmesinin ve video efektlerinde Handwriting tekniği kullanılmasının etkili olduğu söylenebilir. Öğrenci görüşleri ikinci mezo döngüde video tabanlı olarak yeniden düzenlenen mikro öğrenme nesnelerinin siber güvenlik farkındalığına etkisinde Grubbs'un (2022) video tabanlı bir öğrenme nesnesinin daha etkili olduğu bulgusuyla paralellik gösterdiğini söylemek mümkündür.

İkinci mezo döngü sonucunda öğrenciler, birinci mezo döngüye göre daha yüksek oranda E-posta güvenlik ayarlarını yapabilme konusunda zayıf olduklarını, teknik destek kaynaklı sorunların, süre yetersizliği ve mobil cihaz desteği eksikliğinin siber tehditleri tespit etmelerini zorlaştırdığını belirtmiştir. Ayrıca ikinci mezo döngüde birinci mezo döngüye göre nispeten daha düşük oranda öğrenci siber güvenlikle ilgili temel kavramları anlamada güçlü olduğunu ifade etmiştir. Bu durumun öğretim sürecinde sınıf içerisinde kullanılan bilgisayar sayısının yetersizliğinden, özellikle ikinci mezo döngüde sınıf içerisinde Gmail e-posta servisi güvenlik ayarları üzerinde yapılan uygulama ve diğer diğer öğretimi destekleyici uygulamalarda bazı bilgisayarları aynı anda birden fazla öğrencinin kullanmasından kaynaklandığı söylenebilir. Öğrenciler ikinci mezo döngü sonucunda birinci mezo döngü sonucuna göre çok daha yüksek oranlarda gerçek yaşamda karşılaştığı siber tehditlerle öğrendiklerini ilişkilendirme ve gelen e-postalardaki yazım hatasının tehdit içerebileceğini anlama konusunda güçlü olduklarını belirtmişlerdir. İkinci döngüde öğretim tasarımına eklenen "https://phishingquiz.withgoogle.com/" çevrim içi siber tehdit testinin, labirent bulmaca oyunu ve diğer test ve etkinliklerin etkili olduğu düşünülmektedir.

Birinci ve ikinci mezo döngüler sonucunda elde edilen bulgulara göre mikro öğrenme stratejisinin öğrencilerin siber güvenlik farkındalığına yönelik olarak kullanılabilecek etkili bir yöntem olduğu söylenebilir. Birçok araştırmada (Case & King, 2016; Grubbs, 2022; Jerrim, 2023; Mohd Zaharon vd.; 2021; Onashoga vd., 2019; Perrault, 2018; Sun ve Chen, 2016; Sun ve Lee, 2016; Sun ve Lin, 2022; Sun vd., 2017; Weaver vd., 2021) öğrencilerin siber güvenlik farkındalığını artırmak ve siber tehditlere karşı hazır olmalarını sağlamak için siber

güvenlik eğitiminin etkili olabileceği vurgulanmıştır. Her iki döngüde elde edilen bulguların siber güvenlik eğitiminin siber güvenlik farkındalığına katkı sağladığı söylenebilir.

Mikro öğrenme stratejisinin siber güvenlik farkındalığına yönelik olarak etkili olabileceğini söylemek mümkündür. Pascual ve arkadaşları (2020) mikro öğrenmenin öğrencilerin öğrenme performansını artırmada etkili olduğunu göstermiştir. Kasuma ve arkadaşları (2021) mikro öğrenmenin eğitime dahil edilmesinin öğrenciler için daha verimli ve etkili öğrenme deneyimleri sağlayabileceğini öne sürülmüştür. Zarshenas ve arkadaşları (2022) mikro öğrenmenin öğrenciler için etkili bir öğretim yöntemi olabileceği ve öğrenme çıktılarını ve öz yeterliliklerini geliştirebileceği sonucuna varmıştır. Han (2019) mikro öğrenme yönteminin öğrencilerin öğrenme çıktılarını iyileştirmek isteyen eğitimciler için faydalı bir araç olabileceğini öne sürmüştür. Polasek ve Javorcik (2019) mikro öğrenmenin etkili bir öğretim yaklaşımı olabileceği ve öğrencilerin öğrenme çıktılarını ve katılımını artırma potansiyeline sahip olduğu sonucuna varmıştır. Her iki döngü sonucunda elde edilen bulgularla alanyazındaki araştırmalarda elde edilen sonuçlara benzer şekilde mikro öğrenmenin etkili bir strateji olduğu söylenebilir.

Shabadurai ve arkadaşları (2022) araştırmasının video öğesinin mikro öğrenmenin en popüler öğesi olarak kabul edildiğini vurgulamışlardır. Yousef ve arkadaşları (2014) videonun hem öğretim yöntemlerini hem de öğrenme çıktıları açısından mikro öğrenmede etkili bir araç olduğunu savunmuşlardır. Öğrencilerin ikinci mezo döngü sonundaki değerlendirmelerinde görülen yükselişe göre, ikinci döngüde yeninden düzenlenen, video tabanlı mikro öğrenme nesnelerinin başarılı sonuçlar verebileceği sonucuna varılabilir.

Sonuç olarak ikinci döngüdeki siber güvenlik mikro öğrenme nesneleri değerlendirme ortalamaları ve öğrenci görüşleri doğrultusunda siber güvenlik mikro öğrenme nesnelerinin mevcut hâliyle etkili bir öğrenme materyali olarak kullanılabileceği görülmektedir. Ulaşılan sonuçlara göre, tasarım tabanlı araştırmanın, araştırma amacına uygun olarak yürütüldüğü; siber güvenlik mikro öğrenme nesnelerinin amaca uygun özelliklere sahip olduğu ifade edilebilir.

Öneriler

Ulaşılan sonuçlar doğrultusunda aşağıdaki önerilerde bulunulabilir.

1. Siber güvenlik farkındalığını hedefleyen mikro öğrenme stratejisi temelli öğrenme nesneleri başarılı bir şekilde uygulanmıştır. Mikro öğrenme stratejisini temel alan öğrenme nesnelerinin öğretimde uygulanması önerilebilir.

1. Siber güvenlik farkındalığını hedefleyen mikro öğrenme stratejisi temelli eğitimlerin uygulanabilmesi için öğretmenlerin siber güvenlik uzmanları ile işbirliği yapması önerilebilir.

2. İleriki çalışmalarda siber güvenlik kavramı ile ilgili deneyim kazanmış öğretmenler ve öğrencilerle siber güvenlik farkındalığını hedefleyen bu model yeniden düzenlenebilir.

3. Gelecek çalışmalarda öğrenme – öğretme sürecinde mikro öğrenme nesnelerinin kullanımının öğrenenler üzerindeki başarı, motivasyon, iş birliği gibi değişkenlere etkisi incelenebilir.

4. Gelecek çalışmalarda siber güvenlik mikro öğrenme nesnelerinin emniyet hizmetleri gibi güvenlik alanında çalışan meslek grupları ile hizmetiçi eğitim kapsamında katılımcıların siber güvenlik farkındalığına etkisi incelenebilir.

Kaynaklar

Ahmed, N., Islam, M. R., Kulsum, U., Islam, M. R., Haque, M. E., & Rahman, M. S. (2019, September). Demographic factors of cybersecurity awareness in Bangladesh. In *2019 5th International Conference on Advances in Electrical Engineering (ICAEE)* (pp. 685-690). IEEE.

Al-Hamar, Y., & Kolivand, H. (2020, December). A New Email Phishing Training Website. In *2020 13th International Conference on Developments in eSystems Engineering (DeSE)* (pp. 263-268). IEEE. https://doi.org/10.1109/DeSE51703.2020.9450238

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. *Journal of Information & Knowledge Management, 15(01),* 1650007. https://doi.org/10.1142/S0219649216500076

Alqurashi, E. (2017). Microlearning: A pedagogical approach for technology integration. *The Turkish Online Journal of Educational Technology*, *16*, 942-947.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies, 82*, 69-82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Amao, S. (2015). *Active cyber defense to fight cybercrime* (Publication No. 1606336) [Master's thesis, Utica College]. ProQuest Dissertations and Theses Global.

Anderson, R., Böhme, R., Clayton, R., & Moor, T. (2009). Security economics and European policy. In *ISSE 2008 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2008 Conference* (pp. 57-76). Vieweg+ Teubner. https://doi.org/10.1007/978-3-8348-9283-6_6

Anderson, T., & Shattuck, J. (2012). Design-based research: A decade of progress in education research?. *Educational researcher, 41*(1), 16-25. https://doi.org/10.3102/0013189X11428813

Andrade, H. G. (1997). Understanding rubrics. *Educational leadership, 54*(4), 14-17.

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior, 29*(3), 706-714. https://doi.org/10.1016/j.chb.2012.12.018

Barab, S., & Squire, K. (2016). Design-based research: Putting a stake in the ground. In *Design-based Research* (pp. 1-14). Psychology Press.

Baya'a, N., Shehade, H. M. A., & Baya'a, A. R. (2009). A rubric for evaluating web-based learning environments. *British Journal of Educational Technology, 40*(4), 761.

Becker, D., Vennhaus-Bittins, V., Koch, V., & Bornemann, F. (2015). Evidenzbasiert Handeln im Unternehmen. *Digital lernen-evidenzbasiert pflegen: Neue Medien in der Fortbildung von Pflegefachkräften*, 139-146.

Bell, T., Urhahne, D., Schanze, S., & Ploetzner, R. (2010). Collaborative inquiry learning: Models, tools, and challenges. *International journal of science education*, *32*(3), 349-377.

Berkowitz, M. (2017). How to create engaging microlearning content.

Blythe, J. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. *Proceedings of CHItaly 2013 Doctoral Consortium, 1065*, 92-101.

Bogoch, I. I., Frost, D. W., Bridge, S., Lee, T. C., Gold, W. L., Panisko, D. M., & Cavalcanti, R. B. (2012). Morning report blog: a web-based tool to enhance case-based learning. *Teaching and Learning in Medicine*, *24*(3), 238-241.

Boston, C. (2002). *Understanding Scoring Rubrics: A Guide for Teachers*. ERIC Clearinghouse on Assessment and Evaluation, University of Maryland, 1129 Shriver Laboratory, College Park, MD 20742.

Brecht, H. D., & Ogilby, S. M. (2008). Enabling a comprehensive teaching strategy: Video lectures. *Journal of Information Technology Education. Innovations in Practice*, *7*, 71.

Brown, A. L. (1992). Design experiments: Theoretical and methodological challenges in creating complex interventions in classroom settings. *The journal of the learning sciences, 2*(2), 141-178. https://doi.org/10.1207/s15327809jls0202_2

Bruck, P. (2005). Microlearning as strategic research field: An invitation to collaborate(Introductory Note). In *Microlearning: Emerging Concepts, Practices and Techno-logies after eLearning. Proceeding of Microlearning* 2005, Learning & Working in New Media. Book Editors: Theo Hug, Martin Lindber, Peter A. Bruck, Innsbruck uni-versity press, 13–17. Available from: https://www.researchgate.net/publication/239752343_Learning_Organizational_Memory_and_Microlearning_Semantics_for_Microlearning

Bruck, P. A., Motiwalla, L., & Foerster, F. (2012). Mobile learning with micro-content: a framework and evaluation.

Buchem, I., & Hamelmann, H. (2010). Microlearning: a strategy for ongoing professional development. *eLearning Papers, 21*(7), 1-15.

Cain, A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security Applications, 42,* 36-45. https://doi.org/10.1016/j.jisa.2018.08.002

Case, C. J., & King, D. L. (2016). Phishing: Are undergraduates at risk and prepared?. *Issues in Information Systems, 17*(1). https://doi.org/10.48009/1_iis_2016_80-88

Chai-Arayalert, S., & Puttinaovarat, S. (2020). Designing mangrove ecology self-learning application based on a micro-learning approach. *International Journal of Emerging Technologies in Learning*, 15(11), 29 - 41. https://doi.org/10.3991/ijet. v15i11.12585

Chaves, R. O., de Oliveira, P. A. V., Rocha, L. C., David, J. P. F., Ferreira, S. C., Santos, A. D. A. S. D., ... & Brito, M. V. H. (2017). An innovative streaming video system with

a point-of-view head camera transmission of surgeries to smartphones and tablets: an educational utility. *Surgical Innovation*, *24*(5), 462-470.

Choo, C. Y., & Abdul Rahim, A. S. (2021). Pharmacy students' perceptions and performance from a microlearning-based virtual practical on the elucidation of absolute configuration of drugs. *Asian Journal of University Education*, 17(4), 1-10. https://doi.org/10.24191/ajue.v17i4.16187

Chou, T.-S., & Jones, J. (2018). Developing and evaluating an experimental learning environment for cyber security education. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education* (pp. 92-97). https://doi.org/10.1145/3241815.3241855

Cobb, P., Confrey, J., DiSessa, A., Lehrer, R., & Schauble, L. (2003). Design experiments in educational research. *Educational researcher, 32*(1), 9-13. https://doi.org/10.3102/0013189X032001009

Collins, A. (1992). *Toward a design science of education* (pp. 15-22). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-77750-9_2

Corcoran, T. B., Mosher, F. A., & Rogat, A. (2009). Learning progressions in science: An evidence-based approach to reform.

Coronges, K., Dodge, R., Mukina, C., Radwick, Z., Shevchik, J., & Rovira, E. (2012, January). The influences of social networks on phishing vulnerability. In *2012 45th Hawaii International Conference on System Sciences* (pp. 2366-2373). IEEE.

Cosnefroy, L., & Carré, P. (2014). Self-regulated and self-directed learning: why don't some neighbors communicate?. *International journal of self-directed learning, 11*(1-12).

Coventry, L., Briggs, L., Blythe, J. M., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices.

Crawford, C. M. (2001). Rubrics: Models of evaluation within a constructivist learning environment,(ERIC Document Reproduction Service No. ED462910.).

Daro, P., Mosher, F. A., & Corcoran, T. B. (2011). Learning trajectories in mathematics: A foundation for standards, curriculum, assessment, and instruction.

De Gagne, J. C., Park, H. K., Hall, K., Woodward, A., Yamane, S., & Kim, S. S. (2019). Microlearning in health professions education: scoping review. *JMIR medical education, 5*(2), e13997. https://doi.org/10.2196/13997

Decker, J., Hauschild, A. L., Meinecke, N., Redler, M., & Schumann, M. (2017, October). Adoption of micro and mobile learning in German enterprises: A quantitative study. In *European conference on e-Learning* (pp. 132-141). Academic Conferences International Limited.

Delen, E., Liew, J., & Willson, V. (2014). Effects of interactivity and instructional scaffolding on learning: Self-regulation in online video-based environments. *Computers & Education*, *78*, 312-320.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information systems journal, 11*(2), 127-153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007, October). Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 37-44).

Ebbinghaus, H. (1885). Memory: A contribution to experimental psychology. *Teachers College Press.*

Edelson, D. C. (2002). Design research: What we learn when we engage in design. *The Journal of the Learning sciences, 11*(1), 105-121. https://doi.org/10.1207/S15327809JLS1101_4

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – a case study. *Information Security Technical Report, 14,* 223-229. https://doi.org/10.1016/j.istr.2010.05.002

Fernandez, J. (2014). The micro learning trend: Accommodating cultural and cognitive shifts. *Retrieved on* 15-Nisan-2024, from: https://www.learningguild.com/articles/1578/the-microlearning-trend-accommodating-cultural-and-cognitive-shifts/

Fishman, B. J., Penuel, W. R., Allen, A. R., Cheng, B. H., & Sabelli, N. O. R. A. (2013). Design-based implementation research: An emerging model for transforming the relationship of research and practice. *Teachers College Record, 115*(14), 136-156. https://doi.org/10.1177/016146811311501415

Fitria, T. N. (2022). Microlearning in teaching and learning process: A review. *CENDEKIA: Jurnal Ilmu Sosial, Bahasa Dan Pendidikan*, *2*(4), 114-135.

Furnell, S. M., & Vasileiou, I. (2022). A holistic view of cyber security education requirements. In M. Khosrow-Pour (Eds.), *Research anthology on advancements in cybersecurity education* (pp. 289–307). IGI Global. https://doi.org/10.4018/978-1-6684-3554-0.ch013

Gabrielli, S., Kimani, S., & Catarci, T. (2005). The design of microlearning experiences: A research agenda. In T. Hug, M. Lindner & P. Bruck (Eds.), *Microlearning: Emerging concepts, practices and technologies after e-learning. Proceedings of microlearning 2005. Learning & working in new media* (pp. 45-54). Innsbruck, Austria: Innsbruck University Press.

Garba, A., Maheyzah, B., Siti, H., & Dauda, I. (2020). Cyber security awareness among university students: a case study. *Journal of Science Proceedings Series, 2*(1), 82-86. https://doi.org/10.31580/sps.v2i1.1320

Giurgiu, L. (2017). Microlearning an evolving elearning trend. *Scientific Bulletin*, *22*(1), 18-23. https://doi.org/10.1515/bsaft2017-0003

Göschlberger, B. (2017). Social microlearning motivates learners to pursue higher-level cognitive objectives. In *E-Learning, E-Education, and Online Training.* (pp. 201-208). Springer, Cham. doi: 10.1007/978-3-319-49625-2_24

Grubbs, M. J. (2022). Anti-Phishing Game-Based Training: An Experimental Analysis of Demographic Factors. *Available at SSRN Electronic Journal*, 2022. http://dx.doi.org/10.2139/ssrn.4011558

Hadlington, L. & Parsons, K. (2017). Can cyberloafing and internet addiction affect organizational information security? *Cyberpsychology, Behavior, and Social Networking, 20*(9), 567-571. https://doi.org/10.1089/cyber.2017.0239

Halbach, T., & Solheim, I. (2018). Gamified Micro-Learning for Increased Motivation: An Exploratory Study. *International Association for Development of the Information Society*.

Hamdani, K. J., & Mustafa, M. I. E. (2021). Effectiveness of Online Anti-Phishing Delivery methods in raising Awareness among Internet Users.

Han, J. -L. (2019). Micro-lecture teaching for improving the learning effect of non-English majors at North China Electric Power University. *English Language Teaching*, 12(6), 209–216. https://doi.org/10.5539/elt.v12n6p209

Herrington, J. (2012, June). Design-based research: Implementation issues in emerging scholar research. In *EdMedia+ Innovate Learning* (pp. 1-6). Association for the Advancement of Computing in Education (AACE).

Hjalmarson, M. A., Parsons, A. W., Parsons, S. A., & Hutchison, A. C. (2021). Adressing publication challenges in design-based research. *Design-Based Research. Theory and Application*, 23-42.

Hug, T. (2005). Microlearning: A new pedagogical challenge. In T. Hug, M. Lindner, & P. A. Bruck (Eds.), *Microlearning: Emerging concepts, practices and technologies after e-learning* (pp. 7-12). Innsbruck University Press.

Hug, T., Lindner, M., & Bruck, P. A. (2005). Microlearning: Emerging concepts, practices and technologies after e-learning. *Proceedings of Microlearning*, *5*(3), 74.

Hug, T., & Friesen, N. (2007). Outline of a microlearning agenda. Didactics of Microlearning. Concepts, Discourses and Examples, 15-31.

Hug, T. (2012). Mobile Learning as 'Microlearning'.

Internet World Stats (2023), *Internet usage statistics: the internet big Picture. World internet users and 2023 population Stats*. InternetWorldStats. https://www.internetworldstats.com/stats.htm

Jahnke, I., Lee, Y. M., Pham, M., He, H., & Austin, L. (2020). Unpacking the inherent design principles of mobile microlearning. *Technology, Knowledge and Learning*, *25*, 585-619.

Javidi, G., & Sheybani, E. (2018, October). K-12 cybersecurity education, research, and outreach. In *2018 IEEE Frontiers in Education Conference (FIE)* (pp. 1-5). IEEE. https://doi.org/10.1109/FIE.2018.8659021

Jerrim, J. (2023). Who Responds to Phishing Emails? An International Investigation of 15-Year-Olds Using PISA Data. *British Journal of Educational Studies*, *71*(6), 701-724.

Jomah, O., Masoud, A. K., Kishore, X. P., & Aurelia, S. (2016). Micro learning: A modernized education system. *BRAIN. Broad research in artificial intelligence and neuroscience, 7*(1), 103-110.

Kadiev, A. (2021). An evaluation framework for microlearning tools for designing and delivering microlearning content.

Kamruzzaman, M., Islam, M. A., Islam, M. S., Hossain, M. S., & Hakim, M. A. (2016). Plight of youth perception on cyber crime in South Asia. *American Journal of Information Science and Computer Engineering, 2*(4), 22-28.

Karataş, S. (2003). Öğretim amaçlı web sayfası tasarımında renk kullanımı. *Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi*, *23*(2).

Kasuma, S. A. A., Akhiar, A., Haron, H., Fesal, S. N. H. S., & Kadir, N. F. A. (2021). University students' perceptions of motivation, attitude, and self-efficacy in online English language learning. *Pertanika Journal of Social Science & Humanities*, 29(4), 2763-2784. https://doi.org/10.47836/pjssh.29.4.36

Kelly, A. E. (2003). Theme issue: The role of design in educational research. *Educational researcher, 32*(1). https://doi.org/10.3102/0013189X032001003

Khan, B. H. (2019). Microlearning: Quick and meaningful snippets for training solutions. *International Journal of research in Educational Sciences.*, *2*(2), 275-284.

Khong, H. K., & Kabilan, M. K. (2022). A theoretical model of micro-learning for second language instruction. *Computer Assisted Language Learning*, *35*(7), 1483-1506. https://doi.org/10.1080/09588221.2020.1818786

Korstange, R., Hall, J., Holcomb, J., & Jasmeial, J. (2020). The online first-year experience: Defining and illustrating a new reality. *Adult Learning*, 31(3) 95-108. https://doi.org/10.1177/1045159519892680

Kovachev, D., Cao, Y., Klamma, R., & Jarke, M. (2011). Learn-as-you-go: new ways of cloud-based micro-learning for the mobile web. In *Advances in Web-Based Learning-ICWL 2011: 10th International Conference, Hong Kong, China, December 8-10, 2011. Proceedings 10* (pp. 51-61). Springer Berlin Heidelberg.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT), 10*(2), 1-31. https://doi.org/10.1145/1754393.1754396

Lai, J. W., & Bower, M. (2020). Evaluation of technology use in education: Findings from a critical analysis of systematic literature reviews. *Journal of Computer Assisted Learning*, *36*(3), 241-259.

Lane, S. H., Serafica, R., Huffman, C., & Cuddy, A. (2016). Making research delicious: An evaluation of nurses' knowledge, attitudes, and practice using the great American cookie experiment with mobile device gaming. *Journal for Nurses in Professional Development*, *32*(5), 256-261.

Lau, K. W., Lee, P. Y., & Chung, Y. Y. (2019). A collective organizational learning model for organizational development. *Leadership & Organization Development Journal*, 40(1), 107-123. https://doi.org/10.1108/LODJ-06-2018-0228

LeCompte, M. D., & Goetz, J. P. (1982). Problems of reliability and validity in ethnographic research. *Review of educational research*, *52*(1), 31-60.

Leong, K., Sung, A., Au, D., & Blanchard, C. (2021). A review of the trend of microlearning. *Journal of Work-Applied Management*, *13*(1), 88-102. https://doi.org.10.1108/JWAM-10-2020-0044

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems*, *11*(7), 1.

Lindner, M. (2007). What is microlearning. In *Micromedia and Corporate Learning. Proceedings of the 3rd Microlearning 2007 Conference. Presented at the Microlearning* (pp. 52-62).

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28-38. https://doi.org/10.1016/j.cose.2012.12.003

MEB. (2018). *Bilişim Teknolojileri Ve Yazılım Dersi Öğretim Programı (Ortaokul 7 ve 8. Sınıflar)*. http://mufredat.meb.gov.tr/Dosyalar/2018813171426130-2-2018-81Bili%C5%9Fim%20Teknolojileri%20ve%20Yaz%C4%B1l%C4%B1m%20Dersi%20(7%20ve%208.%20S%C4%B1n%C4%B1flar).pdf

McKee, C., & Ntokos, K. (2022). Online microlearning and student engagement in computer games higher education. *Research in Learning Technology*, 30(2680). https://doi.org/10.25304/rlt. v30.2680

McKenney, S. E., & Reeves, T. C. (2012). Toward a generic model for educational design research. *Conducting Educational Design Research*, 61-82.

McKenney, S., & Reeves, T. C. (2014). Educational design research. *Handbook of research on educational communications and technology*, 131-140. https://doi.org/10.1007/978-1-4614-3185-5_11

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. sage.

Mohammed, G. S., Wakil, K., & Nawroly, S. S. (2018). The effectiveness of microlearning to improve students' learning ability. *International Journal of Educational Research Review*, 3(3), 32-38. https://doi.org/10.24331/ijere.415824

Mohd Zaharon, N. F., Mohd Ali, M., & Hasnan, S. (2021). Factors affecting awareness of phishing among generation Y. *Asia-Pacific Management Accounting Journal (APMAJ), 16*(2), 410-444.

Moskal, B. M. (2019). Recommendations for developing classroom performance assessments and scoring rubrics. *Practical Assessment, Research, and Evaluation, 8*(1), 14. https://doi.org/10.7275/jz85-rj16

Moskal, B. M., & Leydens, J. A. (2019). Scoring rubric development: Validity and reliability. *Practical assessment, research, and evaluation, 7*(1), 10. https://doi.org/10.7275/q7rm-gg74

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber security behaviour among higher education students in Malaysia. *J. Inf. Assur. Cyber Secur*, *2017*, 1-13. https://doi.org/10.5171/2017.800299

Neuhold, E. and M. Lindner. 2007. *Quo Vadis, eLearning? Microlearning: Emerging concepts, practices and technologies after e-learning*, 20. Innsbruck: Innsbruck University Press.

Newman, D. (1990). Opportunities for research on the organizational impact of school computers. *Educational researcher, 19*(3), 8-13. https://doi.org/10.3102/0013189X019003008

Nikou, S. (2019, March). A micro-learning based model to enhance student teachers' motivation and engagement in blended learning. In *Society for Information Technology & Teacher Education International Conference* (pp. 509-514). Association for the Advancement of Computing in Education (AACE).

Nikou, S. A., & Economides, A. A. (2018). Mobile-Based micro-Learning and Assessment: Impact on learning performance and motivation of high school students. *Journal of Computer Assisted Learning*, *34*(3), 269-278. https://doi.org/10.1111/jcal.12240

Onashoga, A. S., Ojo, O. E., & Soyombo, O. O. (2019). Securix: A 3D game-based learning approach for phishing attack awareness. *Journal of Cyber Security Technology, 3*(2), 108-124. https://doi.org/10.1080/23742917.2019.1624011

Oxford University Press. (2014). *Oxford Online Dictionary*. Oxford: Oxford University Press. http://www.oxforddictionaries.com/definition/english/Cybersecurity

Özkök, G. A., & Yılmaz, T. (2020). Mesleki eğitime yönelik yeni nesil öğrenme nesnelerinin tasarlanması, geliştirilmesi ve değerlendirilmesi. *Journal of Computer and Education Research*, *8*(16), 757-786.

Park, Y., & Kim, Y. (2018). A design and development of microlearning content in e-learning system. *International Journal on Advanced Science, Engineering and Information Technology*, 8(1). http://dx.doi.org/10.18517/ijaseit.8.1.2698

Pascual, R., Blanco, E., Viveros, P., & Kristjanpoller, F. (2020). Application of microlearning activities to improve engineering students' self-awareness. *International Journal of Engineering Education*, 36(6), 1894-1904.

Paul, A. M. (2016). Microlearning 101. HR Magazine, 61(4), 36-40.

Pawlowski, S.D. & Jung, Y. (2015). Social representations of cybersecurity by university students and implications for instructional design. *Journal of Information Systems Education, 26,* 281-294.

Penuel, W. R., Fishman, B. J., Haugan Cheng, B., & Sabelli, N. (2011). Organizing research and development at the intersection of learning, implementation, and design. *Educational researcher, 40*(7), 331-337. https://doi.org/10.3102/0013189X11421826

Penuel, W. R., Coburn, C. E., & Gallagher, D. J. (2013). Negotiating problems of practice in research–practice design partnerships. *Teachers College Record, 115*(14), 237-255. https://doi.org/10.1177/016146811311501404

Perrault, E. K. (2018). Using an interactive online quiz to recalibrate college students' attitudes and behavioral intentions about phishing. *Journal of Educational Computing Research, 55*(8), 1154-1167. https://doi.org/10.1177/0735633117699232

Plomp, T. (2013). Educational design research: An introduction. *Educational design research*, 11-50.

Poepjes, R., & Lane, M. (2012). An information security awareness capability model (ISACM) [Paper presentation]. *10th Australian Information Security Management Conference*, AISM 2012.

Polasek, R., & Javorcik, T. (2019). Results of pilot study into the application of microlearning in teaching the subject computer architecture and operating system basics.

International Symposium on Educational Technology, 196–201. https://doi.org/10.1109/ISET.2019.00048

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology, 10*(5), 378-382.

Reeves, T. (2006). Design research from a technology perspective. In *Educational design research* (pp. 64-78). Routledge.

Reimann, P. (2013). Design-based research: Designing as research. *R. Luckin, S. Puntambekar, P. Goodyear, B. Grabowski, J. Underwood, J., & N. Winters (Eds.) Handbook of Design in Educational Technology*, 44-52.

Reynolds, J., & Dolasinski, M. J. (2020). Microlearning: A pilot study. *Perspectives in Asian Leisure and Tourism*, *5*(1), 1.

Ricci, J., Breitinger, F., & Baggili, I. (2019). Survey results on adults and cybersecurity education. *Education and Information Technologies*, *24*, 231-249.

Sankaranarayanan, R., Leung, J., Abramenka-Lachheb, V., Seo, G., & Lachheb, A. (2022). Microlearning in diverse contexts: A bibliometric analysis. *TechTrends*, *67*, 260-276. https://doi.org/10.1007/s11528-022-00794-x

Sarıca, H. Ç., & Usluel, Y. K. (2016). Eğitsel bağlamda dijital hikâye anlatımı: Bir rubrik geliştirme çalışması. *Eğitim Teknolojisi Kuram ve Uygulama*, *6*(2), 65-84. https://doi.org/10.17943/etku.12600

Seferoğlu, S. Sadi (2009). Öğretim teknolojileri ve materyal tasarımı. Ankara: Pegem A Yayıncılık.

Şencan, H. (2005). Sosyal ve Davranışsal Ölçümlerde Güvenirlik ve Geçerlik (Reliability and Validity in Social and Behavioral Measurements)(Ankara: Seçkin Yayınları). *PMCid: PMC2361864*.

Shabadurai, Y., Chua, F. F., & Lim, T. Y. (2022). Investigating the employees 'perspectives and experiences of microlearning content design for online training. *International Journal of Information and Education Technology*, *12*(8), 786-793. https://doi.org/10.18178/ijiet.2022.12.8.1685

Shaffer, D., Doube, W., & Tuovinen, J. (2003). Applying Cognitive load theory to computer science education. In *PPIG* (Vol. 1, pp. 333-346).

Shail, M. S. (2019). Using micro-learning on mobile applications to increase knowledge retention and work performance: a review of literature. *Cureus*, *11*(8).

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 373-382). https://doi.org/10.1145/1753326.1753383

Shevchuk, R., Melnyk, A., Opalko, O., & Shevchuk, H. (2020, September). Software for automatic estimating security settings of social media accounts. In *2020 10th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 769-773). IEEE.

Simonet, J., & Teufel, S. (2019). The influence of organizational, social, and personal factors on cybersecurity awareness and behavior of home computer users. In *G. Dhillon (Ed.), SEC 2019, IFIP AICT, 562,* 194–208. https://doi.org/10.1007/978-3-030-22312-0_14

Skalka, J., & Drlík, M. (2018). Conceptual framework of microlearning-based training mobile application for improving programming skills. In *Interactive Mobile Communication Technologies and Learning: Proceedings of the 11th IMCL Conference* (pp. 213-224). Springer International Publishing.

Skalka, J., Drlik, M., Benko, L., Kapusta, J., Rodriguez del Pino, J. C., Smyrnova-Trybulska, E., ... & Turcinek, P. (2021). Conceptual framework for programming skills

development based on microlearning and automated source code evaluation in virtual learning environment. *Sustainability*, *13*(6), 3293.

Skripak, I. A., Aynazarova, S. N., Vladimirovna, E., Tkachenko, A. E., & Erina, L. S. (2020). Digital virtualization technologies in distance learning. *Advanced Trends in Computer Science and Engineering,* *9*(2), 1808–1813. https://doi.org/10.30534/ijatcse/2020/138922020

Souza, M. I. F., & do Amaral, S. F. (2014). Educational microcontent for mobile learning virtual environments.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research*. Sage publications.

Sun, J. C. Y., & Chen, A. Y. Z. (2016). Effects of integrating dynamic concept maps with Interactive Response System on elementary school students' motivation and learning outcome: The case of anti-phishing education. *Computers & Education*, *102*, 117-127.

Sun, J. C. Y., & Lee, K. H. (2016). Which teaching strategy is better for enhancing anti-phishing learning motivation and achievement? The concept maps on tablet PCs or worksheets?. *Journal of Educational Technology & Society*, *19*(4), 87-99.

Sun, J. C.-Y., Kuo, C.-Y., Hou, H.-T., & Lin, Y.-Y. (2017). Exploring learners' sequential behavioral patterns, flow experience, and learning performance in an anti-phishing educational game. *Journal of Educational Technology & Society*, *20*(1), 45-60.

Sun, J. C. Y., & Lin, H. S. (2022). Effects of integrating an interactive response system into flipped classroom instruction on students' anti-phishing self-efficacy, collective efficacy, and sequential behavioral patterns. *Computers & Education*, *180*, 104430.

Tchakounté, F., Wabo, L. K., & Atemkeng, M. (2020). A review of gamification applied to phishing. https://doi.org/10.20944/preprints202003.0139.v1

Tinoca, L., Piedade, J., Santos, S., Pedro, A., & Gomes, S. (2022). Design-based research in the educational field: a systematic literature review. *Education Sciences, 12*(6), 410. https://doi.org/10.3390/educsci12060410

Tinsley, H. E., & Weiss, D. J. (2000). Interrater reliability and agreement. In *Handbook of applied multivariate statistics and mathematical modeling* (pp. 95-124). Academic Press. https://doi.org/10.1016/B978-012691360-6/50005-7

Trowbridge, S., Waterbury, C., & Sudbury, L. (2017, April 10). Learning in bursts: Microlearning with social media. Educause Review. https://er.educause.edu/articles/2017/4/learning-inbursts-microlearning-with-social-media

Türkiye İstatistik Kurumu (2021), *Çocuklarda Bilişim Teknolojileri Kullanım Araştırması*. https://data.tuik.gov.tr/Bulten/Index?p=Cocuklarda-Bilisim-Teknolojileri-Kullanim-Arastirmasi-2021-41132

Türkiye İstatistik Kurumu (2023), *Hane Halkı Bilişim Teknolojileri (BT) Kullanım Araştırması*. https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2023-49407

Uebelacker, S., & Quiel, S. (2014, July). The social engineering personality framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 24-30). IEEE.

Van den Akker, J. (1999). Principles and methods of development research. *Design approaches and tools in education and training*, 1-14. https://doi.org/10.1007/978-94-011-4255-7_1

Van den Akker, J., Gravemeijer, K., McKenney, S., & Nieveen, N. (Eds.). (2006). *Educational design research*. Routledge.

Vayansky, I., & Kumar, S. (2018). Phishing–challenges and solutions. *Computer Fraud & Security*, *2018*(1), 15-20. https://doi.org/10.1016/S1361-3723(18)30007-1

Villanueva, J. A., Lacatan, L. L., Vinluan, A. A. (2020). Information technology security infrastructure malware detector system. *International Journal of Advanced Trends in Computer Science and Engineering, 9*(2), 1583–1587. https://doi.org/10.30534/ijatcse/2020/103922020

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586. https://doi.org/10.1016/j.dss.2011.03.002

Weaver, B. W., Braly, A. M., & Lane, D. M. (2021). Training users to identify phishing emails. *Journal of Educational Computing Research*, *59*(6), 1169-1183.

Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. *Computers & Education*, *186*, 104536.

Wolf, K., & Stevens, E. (2007). The role of rubrics in advancing and assessing student learning. *Journal of Effective Teaching, 7*(1), 3-14.

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences, 5*(4), 297-307.

Yousef, A. M. F., Chatti, M. A., & Schroeder, U. (2014). Video-based learning: A critical analysis of the research published in 2003-2013 and future visions. In *eLmL 2014, The Sixth International Conference on Mobile, Hybrid, and On-line Learning* (pp. 112-119).

Zarshenas, L., Mehrabi, M., Karamdar, L., Keshavarzi, M. H., & Keshtkaran, Z. (2022). The effect of micro-learning on learning and self-efficacy of nursing students: An interventional study. *BMC Medical Education*, 22(664). https://doi.org/10.1186/s12909-022-03726-8

Zhang, X., & Ren, L. (2011). Design for application of micro learning to informal training in enterprise. In *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC)* (pp. 2024-2027). IEEE.

EK-A: Siber Güvenlik Farkındalığı Dereceli Puanlama Anahtarı

…./…./…….

Sevgili Öğrenciler,

Bu siber güvenlik farkındalığı dereceli puanlama anahtarına verdiğiniz cevaplar ile dersinizde kullandığınız siber güvenlik mikro-öğrenme nesnelerinin, siber güvenlik farkındalığınıza etkisinin değerlendirilmesi amaçlanmaktadır. Cevap formunuz isminiz kullanılmadan bilimsel amaçlı kullanılacak olup, üçüncü şahıslar veya kurumlarla paylaşılmayacaktır.

Çalışmaya sunduğunuz katkı için şimdiden teşekkür ederiz.

Sorumlu araştırmacı:

Prof. Dr. G. Alev ÖZKÖK
Eğitim Fakültesi,
Bilgisayar ve Öğretim Teknolojileri
Eğitimi Bölümü

Muhammet Osman ÖZLÜ
H. Ü. Eğitim Bilimleri Enstitüsü

İmza:

İmza:

☐Çalışmanın amacı konusunda bilgilendirildim ve bu çalışmaya katılmayı kabul ediyorum.

E-POSTALARDA KAYNAĞI BİLİNMEYEN BAĞLANTI VE İÇERİK KAYNAKLI TEHDİTLERE YÖNELİK FARKINDALIK

	1 Oldukça Yetersiz	2 Yetersiz	3 Kısmen Yeterli	4 Yeterli	5 Yeterince Güçlü
e-postayı açma	Hesabıma gelen bütün e-postaların gönderenini kontrol etmeden açarım.	Hesabıma gelen e-postaların gönderenini bazen kontrol ederim ve hepsini açarım.	Hesabıma gelen e-postaların gönderenini genellikle kontrol ederim ve tanıdığım kuruluş ve kişilerden gelenleri açarım.	Hesabıma gelen e-postaların gönderenini sık sık kontrol ederim ve ilişkili olduğum kuruluş ve kişilerden gelenleri açarım.	Hesabıma gelen e-postaların gönderenini her zaman kontrol ederim ve sadece tanıdığım adreslerden gelenleri açarım.
Gönderen adresini kontrol etme	Açtığım e-postada gönderenin adresinin doğruluğunu kontrol etmem.	Açtığım e-postada gönderenin adresinin doğruluğunu ara sıra kontrol ederim.	Açtığım e-postada gönderenin adresinin doğruluğunu genellikle kontrol ederim.	Açtığım e-postada gönderenin adresinin doğruluğunu sık sık kontrol ederim.	Açtığım e-postada gönderenin adresinin doğruluğunu her zaman kontrol ederim.
E-posta içeriğindeki bağlantıya tıklama	Açtığım her e-postanın içeriğinde bulunan bağlantıya tıklarım.	Açtığım her e-postanın içeriğinde bulunan bağlantıyı kontrol ederek tıklarım.	Açtığım her e-postanın içeriğinde bulunan bağlantıyı kontrol ederim ve bildiğim bir bağlantı ise tıklarım.	Açtığım her e-postanın içeriğinde bulunan bağlantıyı kontrol ederim ve güvenilir bir bağlantı ise tıklarım.	Açtığım her e-postanın içeriğinde bulunan bağlantıyı kontrol ederim ve tanıdığım kişi ya da kurumlara ait güvenilir bir bağlantı ise tıklarım.
E-postada istenen kişisel verileri gönderme	Kişisel verilerimin talep edildiği bir e-posta alırsam istediği verileri gönderirim / paylaşırım.	Daha önce duyduğum ya da bildiğim bir yerden gelen e-postada kişisel verilerim talep ediliyorsa gönderirim / paylaşırım.	Güvenebileceğim adreslerden gelen e-postalarda kişisel verilerim talep ediliyorsa gönderirim / paylaşırım.	Kullandığım uygulamalardan ya da tanıdığım kişilerden geldiğini düşündüğüm e-postada kişisel verilerim talep ediliyorsa gönderirim / paylaşırım.	Ne sebeple olursa olsun kişisel verilerimi göndermem / paylaşmam.
E-posta içeriğindeki eki cihaza indirme	E-posta içeriğinde bulunan eki cihazıma indirir ve açarım	E-posta içeriğinde bulunan eki önce kontrol eder sonra cihazıma indirir ve açarım.	E-posta içeriğinde bulunan eki kontrol ederim ve “exe” uzantısı dışındaki uzantılara sahip eki cihazıma indirir ve açarım.	E-posta içeriğinde bulunan eki kontrol ederim ve “exe”, “rar” ve benzeri şüpheli uzantılı dosyalar dışındaki uzantılara sahip eki cihazıma indirir ve açarım.	Sadece Güvendiğim kaynaklardan gelen E-posta içeriğinde bulunan eki kontrol ederim ve “exe”, “rar” ve benzeri şüpheli uzantılı dosyalar dışındaki uzantılara sahip eki cihazıma indirir virüs taramasından geçirir ve açarım.

E-POSTALARDA YAZIM HATASI KAYNAKLI TEHDİTLERE YÖNELİK FARKINDALIK

	1 Oldukça Yetersiz	2 Yetersiz	3 Kısmen Yeterli	4 Yeterli	5 Yeterince Güçlü
Yazım kurallarına uygunluğu kontrol etme	E-posta içeriğini okumadan içerikteki bağlantılara tıklarım.	E-posta içeriğine yüzeysel bakarak önemli kısımlarını dikkat eder ve içerikteki bağlantılara tıklarım.	E-posta içeriğini okurum ancak yazım hatalarına kısmen dikkat ederim ve bağlantılara tıklarım.	E-posta içeriğini okurum yazım hatalarına dikkat ederim hatasız olan e-postalara güvenir ve bağlantılara tıklarım.	E-posta içeriğini dikkatle okurum yazım hatalarına dikkat ederim hatasız olan e-postalar güvendiğim kaynaklardan geliyorsa bağlantılara tıklarım.
E-posta eklerinin bağlantılarında adreslerin yazımını kontrol etme	E-posta içeriğindeki eklerin yönlendirdiği adresin yazımını kontrol etmem ve açarım.	E-posta içeriğindeki eklerin yönlendirdiği adresin yazımını kontrol ederim ve açarım.	E-posta içeriğindeki eklerin yönlendirdiği adresin yazımını kontrol ederim ve yazımı doğru ise açarım.	E-posta içeriğindeki eklerin yönlendirdiği adresin yazımını kontrol ederim ve yazımı doğru ise ve güvendiğim adresten gelmişse açarım.	E-posta içeriğindeki eklerin yönlendirdiği adresin yazımını kontrol ederim ve yazımı doğru ise ve güvendiğim adresten gelmişse virüs taramasından geçirerek açarım.
E-postayı gönderenin adresinin yazımını kontrol etme	E-postayı gönderenin adresinin yazımını kontrol etmem.	E-postayı gönderenin adresinin yazımını ara sıra kontrol ederim.	E-postayı gönderenin adresinin yazımını genellikle kontrol ederim.	E-postayı gönderenin adresinin yazımını sık sık kontrol ederim.	E-postayı gönderenin adresinin yazımını her zaman kontrol ederim.
E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etme	E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını kontrol etmem.	E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını ara sıra kontrol ederim.	E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını genellikle kontrol ederim.	E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını sık sık kontrol ederim.	E-postada bulunan reklam bağlantısının yönlendirdiği adresin yazımını her zaman kontrol ederim.
E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etme	E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını kontrol etmem.	E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını ara sıra kontrol ederim.	E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını genellikle kontrol ederim.	E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını sık sık kontrol ederim.	E-postada bulunan ödül bağlantısının yönlendirdiği adresin yazımını her zaman kontrol ederim.

E-POSTALARDA ŞİFRE HEDEFLİ TEHDİTLERE YÖNELİK FARKINDALIK

	1 Oldukça Yetersiz	2 Yetersiz	3 Kısmen Yeterli	4 Yeterli	5 Yeterince Güçlü
E-posta şifre değiştirme sıklığı	Bir kez oluşturduğum şifreyi gerekmediği sürece değiştirmem.	Oluşturduğum şifreyi bir yıldan uzun bir süre kullanırım ve sonrasında değiştiririm.	Oluşturduğum şifreyi en fazla bir yıl kullanırım ve sonrasında değiştiririm.	Oluşturduğum şifreyi en fazla altı ay kullanırım ve sonrasında değiştiririm.	Oluşturduğum şifreyi en fazla üç ay kullanırım ve sonrasında değiştiririm.
E-posta şifre uzunluğu	E-posta şifremin karakter sayısına dikkat etmem.	E-posta şifremi kolay hatırlamak için mümkün olduğunca az karakterle oluştururum.	E-posta şifremi kolay hatırlamak için az karakterden oluştururum ancak güvenlik için en az altı karakterle tanımlarım.	E-posta şifremi güvenlik için sekiz karakterle tanımlarım.	E-posta şifremi güvenlik için sekiz karakterden daha uzun tanımlarım.
E-posta şifresi ile klavye düzeni ilişkisi	E-posta şifremi oluştururken sırasıyla klavye tuş düzenine göre belirlerim.	E-posta şifremi oluştururken klavye tuş düzenine göre çapraz tuşları kullanırım.	E-posta şifremi oluştururken sırasıyla klavye tuş düzenine göre belirlerim ancak harf ve rakamları karışık kullanırım.	E-posta şifremi oluştururken klavye tuş düzenine göre çapraz tuşları kullanırım ancak harf ve rakamları karışık kullanırım.	E-posta şifremi oluştururken klavye tuş düzenindeki karakterleri asla sıralı kullanmam.
Kişisel verilerle şifre belirleme	E-posta şifrem kişisel verilerimden oluşur ve adım, doğum yerim, doğum tarihim gibi verileri açık kullanırım.	E-posta şifrem kişisel verilerimden oluşur ve adım, doğum yerim gibi verilerin sadece sessiz harflerini, doğum tarihim gibi verilerin bir kısmını kullanırım	E-posta şifrem kişisel verilerimden oluşur ancak beraberinde özel karakterlerde kullanırım.	E-posta şifrem kişisel verilerimden oluşur ancak harf ve rakamları karıştırarak oluştururum.	E-posta şifremi oluştururken kişisel verilerimi kesinlikle kullanmam.
Karmaşık ve özel karakterlerle şifre belirleme	E-posta şifrem kolay hatırlanabilir ve özel karakterler içermez.	E-posta şifrem biraz karmaşıktır ve özel karakterler içermez.	E-posta şifrem yeterince karmaşıktır ve özel karakterler içermez.	E-posta şifrem yeterince karmaşıktır ve özel karakterler içerir.	E-posta şifrem çok karmaşıktır ve özel karakterler içerir.

E-POSTA GÜVENLİK AYARLARININ KULLANIMINA İLİŞKİN FARKINDALIK

	1 Oldukça Yetersiz	2 Yetersiz	3 Kısmen Yeterli	4 Yeterli	5 Yeterince Güçlü
Çift faktörlü kimlik doğrulama kullanma	E-posta güvenlik ayarlarından çift faktörlü doğrulama hakkında bir fikrim yok.	E-posta güvenlik ayarlarından çift faktörlü doğrulamayı duydum ancak gerekli görmediğim için kullanmıyorum.	E-posta güvenlik ayarlarından çift faktörlü doğrulamayı biliyorum ancak kullanmıyorum.	E-posta güvenlik ayarlarından çift faktörlü doğrulamayı biliyorum şuan kullanmıyorum ancak ilerde kullanabilirim.	E-posta güvenlik ayarlarından çift faktörlü doğrulamayı biliyorum ve kullanıyorum.
Telefonla doğrulama kullanma	E-posta güvenlik ayarlarından telefonla doğrulama hakkında bir fikrim yok.	E-posta güvenlik ayarlarından telefonla doğrulamayı duydum ancak gerekli görmediğim için kullanmıyorum.	E-posta güvenlik ayarlarından telefonla doğrulamayı biliyorum ancak kullanmıyorum.	E-posta güvenlik ayarlarından telefonla doğrulamayı biliyorum şuan kullanmıyorum ancak ilerde kullanabilirim.	E-posta güvenlik ayarlarından telefonla doğrulamayı biliyorum ve kullanıyorum.
Kurtarma e-postası kullanma	E-posta güvenlik ayarlarından kurtarma e-postası doğrulama hakkında bir fikrim yok.	E-posta güvenlik ayarlarından kurtarma e-postası doğrulamayı duydum ancak gerekli görmediğim için kullanmıyorum.	E-posta güvenlik ayarlarından kurtarma e-postası doğrulamayı biliyorum ancak kullanmıyorum.	E-posta güvenlik ayarlarından kurtarma e-postası doğrulamayı biliyorum şuan kullanmıyorum ancak ilerde kullanabilirim.	E-posta güvenlik ayarlarından kurtarma e-postası doğrulamayı biliyorum ve kullanıyorum.
Güvenlik ayarları hakkında bilgi edinme	E-posta güvenlik ayarları hakkında hiçbir fikre sahip değilim.	E-posta güvenlik ayarlarını duydum ancak önemli olduğunu düşünmüyorum.	E-posta güvenlik ayarlarını duydum ancak yeterli bilgiye sahip değilim.	E-posta güvenlik ayarları hakkında yeterince bilgim var.	E-posta güvenlik ayarlarını biliyorum ve kullanmaya dikkat ediyorum.
Güncellemeleri uygulama	Güncellemeler hakkında hiçbir fikrim yok.	Güncellemeleri duydum ancak uygulamıyorum.	Güncellemeleri duydum ancak nadiren uygularım.	Güncellemeleri biliyorum ara sıra uygularım.	Güncellemeleri biliyorum ve her zaman uygularım.

EK-B: Siber Güvenlik Farkındalığı Öğrenci Görüşme Formu

Sevgili Öğrenciler,

Bu yansıma formuna verdiğiniz cevaplar ile dersinizde uygulanan siber güvenlik farkındalık eğitiminin siber güvenlik farkındalığınızda güçlü, eksik yönlerinizi; öğrenmenize katkılarını veya öğrenmenize engel olarak yarattığı durumları tespit etmek amaçlanmaktadır. Görüşleriniz doğrultusunda oluşturulan mikro-öğrenme nesnelerinin, öğrenmenize daha fazla katkı sağlaması için eksiklikleri giderilecektir.

Cevap kağıdınız isminiz kullanılmadan bilimsel amaçlı kullanılacak olup, üçüncü şahıslar veya kurumlarla paylaşılmayacaktır.

Çalışmaya sunduğunuz katkı için şimdiden teşekkür ederim. Görüşleriniz bizim için değerlidir.

Sorumlu araştırmacı:

Prof. Dr. G. Alev ÖZKÖK
Eğitim Fakültesi,
Bilgisayar ve Öğretim Teknolojileri
Eğitimi Bölümü

İmza:

Muhammet Osman ÖZLÜ
HÜ Eğitim Bilimleri Enstitüsü

İmza:

Siber Güvenlik Farkındalığı Öğrenci Görüşme Formu

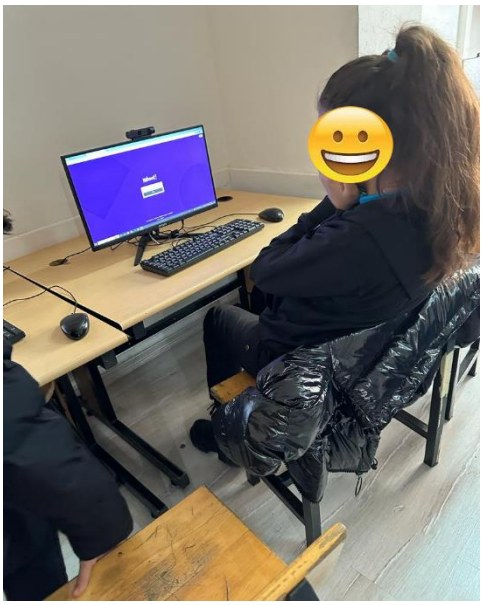
1.Siber Güvenlik mikro-öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmede kazandığım güçlü yönler nelerdir?

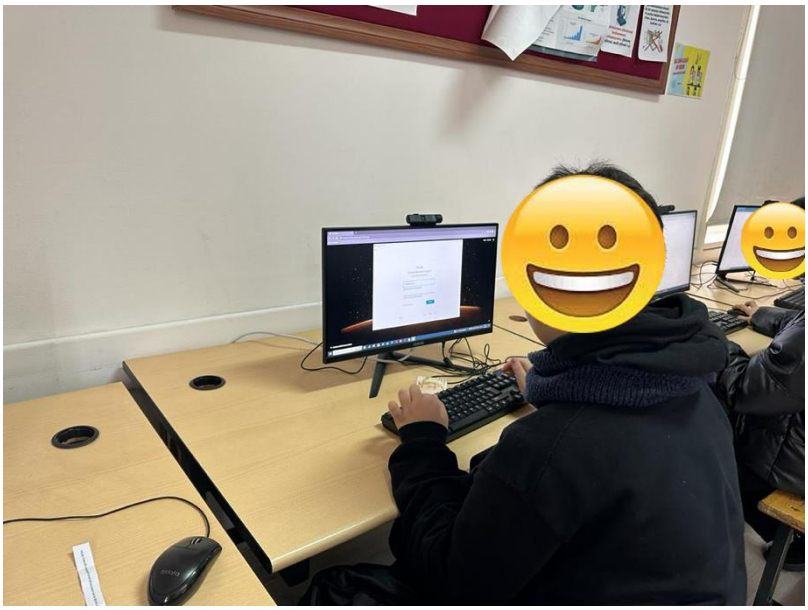
2.Siber Güvenlik mikro-öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmede zayıf yönler nelerdir?

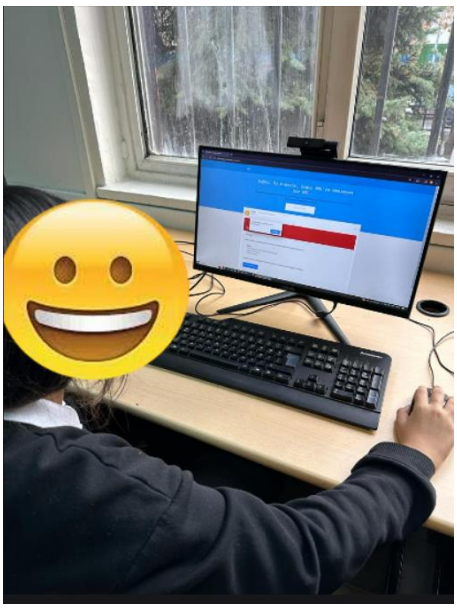
3. Siber Güvenlik mikro-öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmemi kolaylaştıran yönler nelerdir?

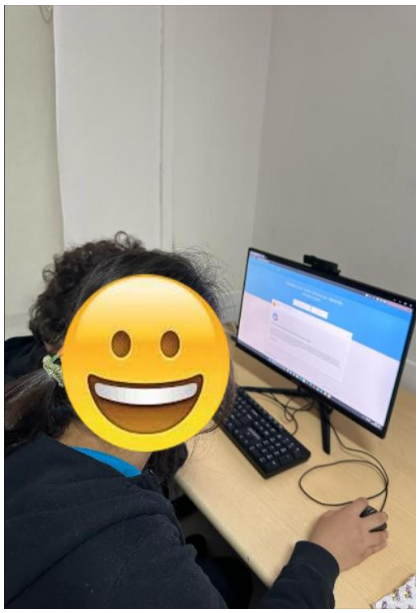
4. Siber Güvenlik mikro-öğrenme nesneleri ile, e-posta hedefli siber tehditleri tespit etmemi zorlaştıran/engelleyen yönler nelerdir?

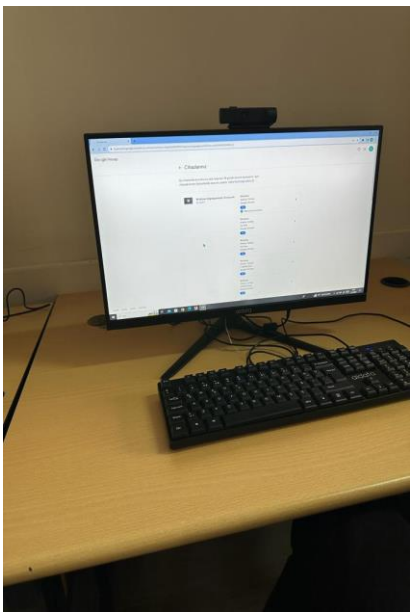
EK-C: Sınıftan Resimler

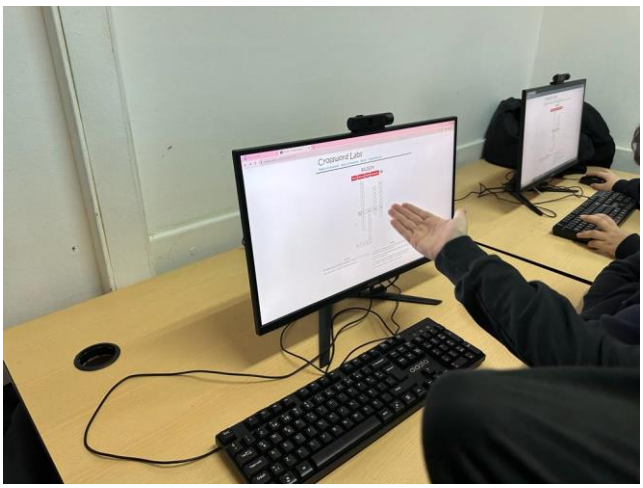


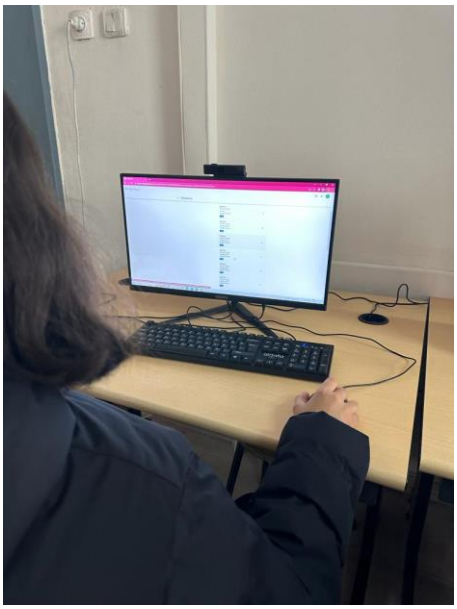


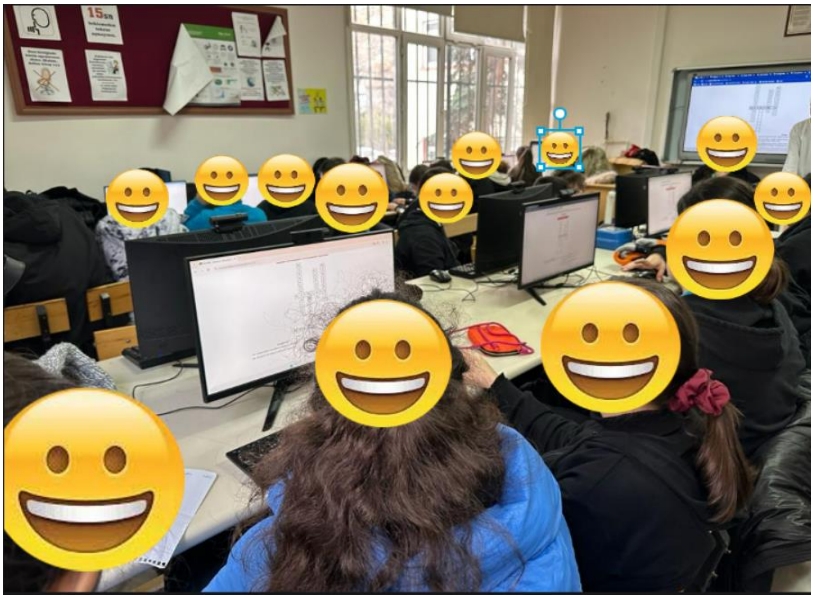


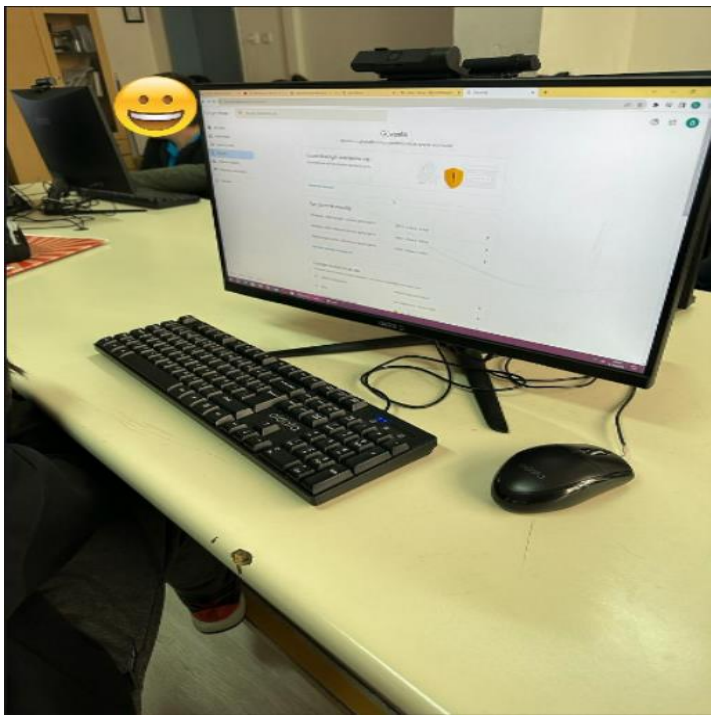




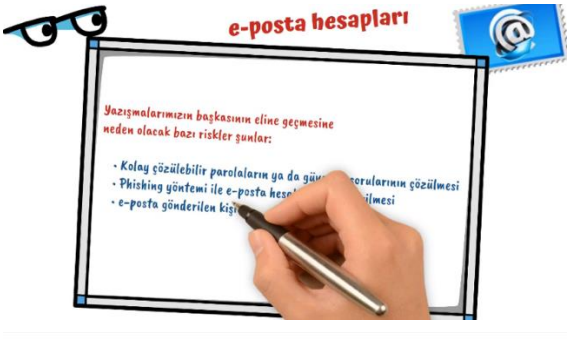








EK-Ç: Mikro-öğrenme Nesnelerinden Görüntüler



EK-D: Araştırma Etik Komisyon İzin Muafiyeti Formu/ Araştırma Etik Komisyonu Onay Bildirimi

T.C.
HACETTEPE ÜNİVERSİTESİ REKTÖRLÜĞÜ
Rektörlük

Sayı : E-35853172-399-00002609748 5.01.2023
Konu : Muhammet Osman ÖZLÜ Hk. (Etik Komisyon İzni)

EĞİTİM BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 09.12.2022 tarihli ve E-51944218-399-00002562301 sayılı yazınız.

Enstitünüz Bilgisayar ve Öğretim Teknolojileri Eğititmi yüksek lisans programı öğrencisi **Muhammet Osman ÖZLÜ**'nün **Prof. Dr. G. Alev ÖZKÖK** sorumluluğunda yürüttüğü **"Ortaöğretimde Siber Güvenlik Odaklı Mikro-Öğrenme Nesnelerinin Tasarım Tabanlı Araştırma Yönetemiyle Modellenmesi"** başlıklı tez çalışması, Üniversitemiz Senatosu Etik Komisyonunun **27 Aralık 2022** tarihinde yapmış olduğu toplantıda incelenmiş olup, etik açıdan uygun bulunmuştur.

Bilgilerinizi ve gereğini rica ederim.

Prof. Dr. Vural GÖKMEN
Rektör Yardımcısı

Bu belge güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu: D48DB467-6FE2-48B3-8371-E1706072854F Belge Doğrulama Adresi: https://www.turkiye.gov.tr/hu-ebys

Adres: Hacettepe Üniversitesi Rektörlük 06100 Sıhhiye-Ankara
E-posta:yazimd@hacettepe.edu.tr İnternet Adresi: www.hacettepe.edu.tr Elektronik Ağ: www.hacettepe.edu.tr
Telefon: 0 (312) 305 3001-3002 Faks:0 (312) 311 9992
Kep: hacettepeuniversitesi@hs01.kep.tr

Bilgi için: Duygu Didem İLERİ
Bilgisayar İşletmeni
Telefon: .

EK-E: Etik Beyanı

Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

* tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
* görsel, işitsel ve yazılı bütün bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
* başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
* atıfta bulunduğum eserlerin bütününü kaynak olarak gösterdiğimi,
* kullanılan verilerde herhangi bir tahrifat yapmadığımı,
* bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

28/05/2024

Muhammet Osman ÖZLÜ

EK-F: Yüksek Lisans/Doktora Tez Çalışması Orijinallik Raporu

28/05/2024

HACETTEPE ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü
Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı Başkanlığına,

Tez Başlığı :Mikro-öğrenme Nesnelerinin Tasarım Tabanlı Araştırma Yöntemiyle Tasarlanması ve Değerlendirilmesi: İlköğretimde Siber Güvenlik Örneği

Yukarıda başlığı verilen tez çalışmamın tamamı (kapak sayfası, özetler, ana bölümler, kaynakça) aşağıdaki filtreler kullanılarak **Turnitin** adlı intihal programı aracılığı ile kontrol edilmiştir. Kontrol sonucunda aşağıdaki veriler elde edilmiştir:

Rapor Tarihi	Sayfa Sayısı	Karakter Sayısı	Savunma Tarihi	Benzerlik Oranı	Gönderim Numarası
07/12/2023	115	169289	30/04/2024.	%14	2251596196

Uygulanan filtreler:
1. Kaynaklar hariç
2. Alıntılar dâhil
3. 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esaslarını inceledim ve çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan eder, gereğini saygılarımla arz ederim.

Ad Soyadı: Muhammet Osman ÖZLÜ

Öğrenci No.: N20132319

Ana Bilim Dalı: Bilgisayar ve Öğretim Teknolojileri Eğitimi

Programı: Bilgisayar ve Öğretim Teknolojileri Eğitimi

Statüsü: ☒ Y.Lisans ☐ Doktora ☐ Bütünleşik Dr.

DANIŞMAN ONAYI

UYGUNDUR.

(Prof. Dr. G. Alev ÖZKÖK)

EK-G: Thesis/Dissertation Originality Report

28/05/2024

HACETTEPE UNIVERSITY
Graduate School of Educational Sciences
To The Department of Computer Education and Instructional Technology

Thesis Title:Design and Evaluation of Micro-learning Objects Using Design Based Research Method: An Example of Cyber Security in Primary Education

The whole thesis that includes the *title page, introduction, main chapters, conclusions and bibliography section* is checked by using **Turnitin** plagiarism detection software take into the consideration requested filtering options. According to the originality report obtained data are as below.

Time Submitted	Page Count	Character Count	Date of Thesis Defense	Similarity Index	Submission ID
07/12/2023	115	169289	30/04/2024	%14	2251596196

Filtering options applied:
1. Bibliography excluded
2. Quotes included
3. Match size up to 5 words excluded

I declare that I have carefully read Hacettepe University Graduate School of Educational Sciences Guidelines for Obtaining and Using Thesis Originality Reports; that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

I respectfully submit this for approval.

Name Lastname:	Muhammet Osman ÖZLÜ
Student No.:	N20132319
Department:	Computer Education and Instructional Technology
Program:	Computer Education and Instructional Technology
Status:	☒ Masters ☐ Ph.D. ☐ Integrated Ph.D.

ADVISOR APPROVAL

APPROVED
(Prof. Dr. G. Alev ÖZKÖK)

EK-H: Yayımlama ve Fikrî Mülkiyet Hakları Beyanı

Enstitü tarafından onaylanan lisansüstü tezimin/raporumun tamamını veya herhangi bir kısmını, basılı (kâğıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım haklan bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinlerin yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan "**Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına ilişkin Yönerge**" kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H.Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- Enstitü/ Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihinden itibaren 2 yıl ertelenmiştir. (1)
- Enstitü/Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren … ay ertelenmiştir. (2)
- Tezimle ilgili gizlilik kararı verilmiştir. (3)

28/05/2024

(imza)

Muhammet Osman ÖZLÜ

"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"

(1) Madde 6. 1. Lisansüstü tezle ilgili patent başvurusu yapılması veya patent alma *sürecinin devam etmesi durumunda, tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü Üzerine enstitü veya fakülte yönetim kurulu iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.*

(2) Madde 6. 2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç; imkânı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez danışmanın önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulunun gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.

(3) Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, tezin yapıldığı kurum tarafından verilir. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, ilgili kurum ve kuruluşun önerisi ile enstitü veya fakültenin uygun görüşü Üzerine üniversite yönetim kurulu tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.*

Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir

**Tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulu tarafından karar verilir.*