Uzaktan Eğitimde Kişisel Siber Güvenliğin Önemi ve Çözüm Önerileri

Fırat YILMAZ 1, 0000-0002-8751-7234, firat.yilmaz@meb.gov.tr

Dr. Aslıhan İSTANBULLU 2, 0000-0002-1778-859X, aslihan.babur@amasya.edu.tr

1  Amasya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı, 2 Amasya Üniversitesi

Her gün gelişen teknoloji sayesinde toplumumuz eskisinden çok daha bağlantılı hale gelmektedir. Bu gelişmeler günlük hayatımızı kolaylaştırırken kişisel bilgilerimiz açısından risklerde oluşturmaktadır. Çoğu kişi çevrimiçi alışveriş yaparken, e-postalarını kontrol ederken veya sosyal medyayı kullanırken kimliklerinin çalındığını düşünmez. Ancak, kişisel bilgiler internet üzerinden her paylaşıldığında bu bilgilerin çalınma durumu söz konusudur. Bu durum özellikle okul etkinlikleri için çok fazla çevrimiçi vakit geçiren öğrenciler için de geçerlidir. Eğitim amacıyla internete her bağlandıklarında kendilerini riske atarlar. Bu risklerin azaltılmasını sağlamanın en temel yolu kişisel siber güvenliğe önem vermektir. Uzaktan eğitimde öğrencileri bilinçlendirmek ve siber dünyada verilerin nasıl güvende tutulması gerektiği konusunda eğitimcilere büyük rol düşmektedir.

Pandemi, tüm dünyada önemli derecede bir kriz yaratmış, örgün eğitim kurumlarının kapatılması sonucu açık ve uzaktan eğitim uygulamaları eğitimin sürdürülebilirliği için vazgeçilmez bir öğrenme kaynağı olarak gündeme gelmiştir. Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü (UNESCO) (2020) verilerine göre, 07 Nisan 2020 itibariyle, Coronavirüs (Covid-19) pandemisi nedeniyle 188 ülkede okullar kapanmıştır. Bu durum, dünya çapında öğrenci nüfusunun yaklaşık olarak %92’sini (1,576,021,818 öğrenci) etkilemiştir. Bu süreç ülkemiz özelinde değerlendirilecek olursa, bütün öğretim kurumlarında sürdürülen eğitim faaliyetleri askıya alınmış, eğitim öğretim faaliyetleri K-12 seviyesinde Eğitim Bilişim Ağı (EBA) ve TRT’nin 3 TV kanalı üzerinden yürütülmeye, yükseköğretim seviyesinde uzaktan eğitim olanakları ile sürdürülmüştür (Ertuğ, C., 2020). 2019-2020 eğitim öğretim döneminde K-12 düzeyinde 18 milyon, yükseköğretim düzeyinde 8 milyona yakın olmak üzere toplam 26 milyon öğrenciye ait kişisel bilgilerin yanı sıra biyometrik verilerinde elektronik ortamlarda saklandığı, işlendiği ve kullanıldığı devasa boyutta bilgi yığınının ortaya çıkmasına sebep olmuştur.

Pandemi nedeniyle temel eğitimden lisansüstü öğrenim düzeyine kadar öğrencilerin internet kullanım oranlarındaki artış, öğrencilerin kişisel siber güvenliklerini tehdit edecek olumsuz etkilere maruz kalma olasılıklarını da artırmıştır. Siber güvenlik tehditlerine daha fazla ilgi gösterildiği bu dönemde, okullar bilgisayar korsanları tarafından hedef alınması en muhtemel kurumlar arasındadır. Siber suçlular, video konferans için Zoom gibi tele-çalışma için kullanılan araçların popülaritesinden de yararlanarak, saldırılarına devam etmişlerdir. [FBI'ın İnternet Suçları Şikayet Merkezi](https://www.ic3.gov/Media/Y2020/PSA200401) (IC3), tehdit aktörlerinin öğrencilerin çevrimiçi güvenliğini ve gizliliğini baltalamak için dünyanın uzaktan öğrenmeye hızlı geçişinden yararlanabileceği konusunda uyarmıştır. Nitekim 2020 yaz raporunda, okul başına haftalık dijital saldırı sayısının Mayıs ve Haziran'da 368'den Temmuz ve Ağustos'ta 608'e yükseldiği ortaya koyulmuştur. Uzmanlar, dosya adında yakınlaştırma içeren kötü niyetli ekleri olan kimlik avı yazılımı tespit etmişlerdir. Pandeminin başlangıcından bu yana, muhtemelen kötü amaçlı kullanım için 1700'den fazla yeni Zoom alan adı kaydedilmiştir. Diğer örnekler, meşru Google Classroom sitesi gibi görünen yeni alan adlarını içermektedir. Uzaktan eğitim alanında da kullanılan bu sistemler üzerinden kullanıcılar başta Kötü Amaçlı Yazılım (Malware), E-Dolandırıcılık / Kimlik Avı (Phishing), Fidye Yazılımı (Ransomware), Parola Saldırıları (Password Attacks) gibi siber tehditlere maruz bırakılmaktadır. Dolayısıyla uzaktan eğitimde kurum, öğretmen ve öğrencileri suç faaliyetlerinin kurbanı olmadan önce kişisel siber güvenlik konusunda eğitilmesi maddi manevi kayıpların azaltılması ve siber suçun başarı oranını azaltama (Interpol, 2020) açısından önem arz etmektedir.

Siber uzaydaki davranışın doğrudan ulusun ve insanların güvenliği ve güvenliğiyle bağlantılı bir faktör olduğu düşünüldüğünde, kişisel siber güvenlik eğitimi, yolu geçmeden önce her iki tarafa bakmak veya bir arabaya emniyet kemeri takmak gibi çok doğal hale gelmektedir. Öğrenenlere, çevrimiçi olduklarında var olan risklerden ve tehditlerden kendilerini korumalarını sağlamak için teknoloji ve internet ile ilk etkileşime girmeye başladıklarında uygun siber güvenlik alışkanlıklarının öğretilmesi gereklidir. Bu riskler ve tehditler öğrencinin fiziksel, duygusal ve sosyal sağlığını etkileyebilir ve siber zorbalık, kimlik hırsızlığı, istenmeyen cinsel istek ve akıl hastalıklarını içerebilir (Ross,2020). Siber güvenlik teknolojileri, politikaları ve düzenlemeleri geliştirilmesine rağmen birçok kullanıcının bilgi ve iletişim teknolojilerini kullanırken kurallara ve düzenlemelere uymadığı veya beklenen davranışı göstermediği yapılan çalışmalarla belirlenmiştir. Çoğu sistem teknik olarak güvenli olsa da, siber suçların büyük bir kısmı "insan hatası" nedeniyle ortaya çıkmaktadır (Cooke, 2020). Son kullanıcıdan kaynaklanan güvenlik açıkları, toplam güvenlik açıklarının %80' ini oluşturmasına rağmen, siber güvenliğin odak noktası sistem araçları ve teknolojisi olmuştur. Ülkeler en iyi siber savunma teknolojisine sahip olsa dahi, son kullanıcı hatası, kişisel siber güvenlik bilgisi ve farkındalık eksikliği nedeniyle birçok kayıp yaşanmasına neden olur. Dolayısıyla kullanıcıların gizlilik ve güvenlik risklerini ve kendilerini siber saldırılardan nasıl koruyacaklarını anlamaları modern yaşamda temel bir ihtiyaçtır. Eğitim kurumlarının mevcut yönetim yapılarının bir parçası olarak kişisel bilgi güvenliği risklerini yönetmek için kurumsal yaklaşımlar uygulaması gerekmektedir.

**Anahtar Kelimeler:** *Uzaktan Eğitim, Siber Güvenlik, Kişisel Siber Güvenlik*

**KAYNAKÇA**

Cooke, A. (2020). A unique year for cyber security. *Network Security*, *2020*(9), 20.

Ertuğ, C. (2020). Coronavirüs (Covid-19) pandemisi ve pedagojik yansımaları: Türkiye’de açık ve uzaktan eğitim uygulamaları. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, *6*(2), 11-53.

Interpol. (2020). Cybercrime: COVID-19 İmpact <https://www.interpol.int/content/download/15526/file/COVID19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf>. Erişim Tarihi 21/09/2021

Ross, T. (2020). *Technology in the K-12 Education System* (Doctoral dissertation, Utica College).

UNESCO.(2020). COVID-*19 educational disruption and response*, https://en.unesco.org/covid19/educationresponse, web adresinden 26 Aralık 2020 tarihinde erişilmiştir.