

Dijital Güvenlik Bilincinin Eğitim Yoluyla Oluşturulması

Aysel Güney¹

Özet

Dijital teknolojilerin yaygınlaşması bireylerin dijital ortamlarda karşılaştığı güvenlik tehditlerini de artırmıştır. Özellikle çocuklar ve gençler, interneti aktif kullanan gruplar arasında yer almakta ve çeşitli siber risklere karşı savunmasız kalabilmektedir. Bu nedenle dijital güvenlik bilincinin erken yaşlarda kazandırılması büyük önem taşımaktadır.

Eğitim, dijital güvenlik konusunda bireylerin farkındalık kazanmasını, riskleri tanımasını ve güvenli internet kullanımı alışkanlıklarını geliştirmesini sağlar. İlkokuldan üniversiteye kadar dijital güvenlik temelli içeriklerin eğitim müfredatlarına entegre edilmesi gerekmektedir. Ayrıca öğretmenlerin ve ailelerin bu konuda bilinçli olması, öğrencilerin dijital dünyada karşılaşılabilecekleri tehditlere karşı korunmasında önem taşımaktadır.

Bu çalışmanın amacı, eğitim yoluyla dijital güvenlik bilincinin nasıl geliştirilebileceğini ortaya koymak ve bu sürecin bireyler üzerindeki etkilerini incelemektir. Bu amaçla da dijital güvenlik eğitimlerinin nasıl tasarlanabileceği, uygulamada karşılaşılan zorluklar ve çözüm önerileri ele alınmıştır. Aynı zamanda, dünyadan ve Türkiye’den örneklerle de yer verilmiştir. Sonuç olarak, dijital güvenlik bilinci kazandırmak, sadece bireyleri değil, toplumu da ilgilendirmektedir ve bu bilinç, etkili bir eğitim süreciyle gerçekleştirilebilir.

GİRİŞ

Dijital teknolojilerin günlük yaşamın her alanına entegre olması, bireylerin dijital ortamda daha fazla vakit geçirmesine neden olmuş, bu durum beraberinde ciddi güvenlik tehditlerini de getirmiştir. Özellikle çocuklar ve gençler gibi dijital araçlara erken yaşta maruz kalan gruplar, bilinçsiz

1 Doç. Dr. Aysel Güney, Bilecik Şeyh Edebali Üniversitesi, Uygulamalı Bilimler Fakültesi, Muhasebe ve Finans Yönetimi Bölümü, aysel.guncu63@gmail.com
ORCID: 0000-0001-7017-8435

kullanım nedeniyle çeşitli risklerle karşı karşıya kalmaktadır ki dijital güvenlik bilincinin oluşturulması, bireylerin hem kendilerini hem de dijital toplumu koruyabilmeleri açısından hayati bir öneme sahiptir (Korucu,2021).

Dijital çağda bireylerin ve kurumların güvenliğini sağlamak, bilgi teknolojilerinin doğru ve bilinçli kullanımına bağlıdır. Dijital güvenlik bilinci oluşturmak, sadece teknik önlemler almakla sınırlı değildir; bu bilinç bireylerin dijital dünyadaki riskleri anlamaları ve bu risklere karşı doğru davranış biçimlerini benimsemeleriyle mümkündür. Günümüzde siber saldırılar, veri hırsızlığı, kimlik dolandırıcılığı gibi tehditler hızla artmaktadır. İnsan hatası veya bilgisizlik, bu tür saldırılara karşı en zayıf halka olabilmektedir. Bu nedenle bireylerin (Solmaz, 2023):

- Kişisel verilerinin korunması,
- Güvenli şifre kullanımı,
- E-posta ve sosyal medya dolandırıcılıklarına karşı dikkatli olmaları,
- Güncel yazılım ve sistemleri kullanmaları gibi temel dijital güvenlik önlemlerini öğrenmeleri

Dijital güvenlik bilincinin oluşturulmasında eğitim önemli bir role sahiptir. Tüm eğitim süreçlerinde dijital dünyaya ilişkin bilinçli bir bakış açısı kazanılması, teknolojiyi etik ve güvenli bir şekilde kullanılması açısından önemlidir. Özellikle dijital okuryazarlık kavramı altında değerlendirilen dijital güvenlik, bireylerin yalnızca bilgiye erişmesini değil, aynı zamanda bu bilgiyi güvenli ve sorumlu bir şekilde kullanmasını da kapsamaktadır (Özaydın.2021).

1. Dijital Güvenlik Nedir?

Dijital güvenlik, bireylerin ve kurumların dijital ortamlarda kişisel verilerini, gizliliğini ve bilgi sistemlerini korumaya yönelik alınan önlem ve stratejilerin bütünüdür (Vikipeia). Gelişen teknolojiyle birlikte bilgiye erişim kolaylaşmış; ancak aynı zamanda kötü niyetli kişilerin bu bilgilere erişme ve kullanma yolları da gelişmiştir. Bu nedenle dijital güvenlik, yalnızca teknik bir konu değil, aynı zamanda bireylerin farkındalığını, davranış biçimlerini ve toplumsal sorumluluklarını da kapsayan çok boyutlu bir alandır. Güvenlik duvarı kullanmak, yazılımları güncel tutmak, önemli verilere erişimlerde şifre kullanmak vb. yöntemler siber saldırılardan korunmak için alınabilecek basit dijital güvenlik önlemleridir (Teymourlouci, 2015). Siber saldırılardan korunmak için, teknolojiyi kullanan kişilere saldırı yöntemleri ve tehditler konusunda eğitimler verilmesi ve dijital veri güvenliği farkındalıklarının arttırmak gerekmektedir (Hart, Margheri, Paci, Sassone, 2020).

Dijital güvenlik, sadece teknolojik bir mesele değil, aynı zamanda sosyal, kültürel ve pedagojik bir konudur. Günümüzde siber zorbalık, kişisel verilerin kötüye kullanımı, kimlik hırsızlığı, ortalama (phishing) saldırıları ve zararlı yazılımlar gibi tehditler, bireylerin güvenli dijital yaşamlarını tehdit etmektedir. Bu tehditlerle baş edebilmenin en etkili yollarından biri ise bireylere bu konularda erken yaşta bilgi ve farkındalık kazandırmaktır (Taha, Dahabiyeh, 2021).

Dijital güvenlik bilincinin oluşturulmasında eğitim önemli bir role sahiptir. Tüm eğitim süreçlerinde öğrencilerin dijital dünyaya ilişkin bilinçli bir bakış açısı kazanması, teknolojiyi etik ve güvenli bir şekilde kullanabilmeleri açısından gereklidir. Özellikle dijital okuryazarlık kavramı altında değerlendirilen dijital güvenlik, bireylerin yalnızca bilgiye erişmesini değil, aynı zamanda bu bilgiyi güvenli ve sorumlu bir şekilde kullanmasını da kapsamaktadır (Mulenga, Marbán, 2020).

Eğitim sürecinin her aşamasında dijital güvenlik konularının yer alması, öğrencilerin eleştirel düşünme becerilerini geliştirmekte, dijital ortamlardaki potansiyel tehlikeleri önceden fark etmelerine yardımcı olmaktadır. Bu aşamada öğretmenlere ve ebeveynlere büyük görevler düşmektedir. Öğretmenlerin dijital güvenlik konusunda yeterli donanımına sahip olmaları, öğrencilere doğru rehberlik edebilmeleri açısından önemlidir. Aynı şekilde, ailelerin de çocuklarını ev ortamında dijital dünyadaki risklere karşı hazırlamaları ve önlemler almaları da gerekmektedir (Korlu, 2019).

Dijital güvenlik bilinci kazandırmasında ayrıca eğitim teknolojileri de önemli yer tutmaktadır. Simülasyonlar, etkileşimli içerikler, dijital oyunlar ve siber güvenlik uygulamaları, öğrencilere hem teorik hem de pratik bilgi kazandırarak onların aktif öğrenmelerini sağlamaktadır. Ayrıca, okullarda düzenlenecek seminerler, atölye çalışmaları ve dijital farkındalık kampanyaları ile bu bilincin pekiştirilmesi de mümkündür (Dönmez, 2019). Dijital güvenlik, sadece teknoloji uzmanlarının değil, toplumun her kesiminin sorumluluğundadır. Bu güvenliği sağlamanın en etkili yolu ise bilinçli bireyler yetiştirmektir. Bireylerin küçük yaşlardan itibaren dijital riskleri tanınması, çevrim içi ortamlarda etik ve güvenli davranışlar geliştirmesi yapılandırılmış ve sürdürülebilir bir eğitim süreciyle mümkündür (Karanfil, Uyar, 2023).

Birçok ülkede dijital güvenlik eğitimi, öğretim programlarına entegre edilmekte, öğrencilere pratik bilgiler ve davranış modelleri kazandırılmaktadır. Örneğin, Avrupa Birliği ülkelerinde “dijital vatandaşlık” kavramı çerçevesinde çocuklara siber güvenlik, kişisel verilerin korunması, dijital ayak izi gibi konular öğretilmektedir. Ülkemizde de son yıllarda bu alanda çeşitli çalışmalar yapılmaktadır; özellikle ortaokul ve lise düzeyinde

bilişim teknolojileri derslerinde güvenli internet kullanımı gibi konulara yer verilmektedir (Canogulları, 2021). Ancak bu eğitimlerin sistematik hale getirilmesi ve uygulama odaklı olması, gerekmektedir.

1.1 Dijital Güvenliğin Temel Unsurları

Dijital güvenlik, genel olarak şu ana başlıklar altında ele alınabilir:

- **Kişisel Veri Güvenliği:** Bireylerin ad, adres, kimlik numarası, banka bilgileri gibi özel verilerinin izinsiz toplanması, saklanması veya paylaşılması ciddi bir güvenlik sorunudur Aynı zamanda e devlet de bulut bilişimde, dijital, akıllı ev ve kent uygulamalarında, sosyal ağlarda kişisel verilerin korunması önem taşımaktadır (Bilir,2021)
- **Kimlik Doğrulama ve Erişim Kontrolü:** Güvenli şifreleme sistemleri, iki aşamalı doğrulama yöntemleri gibi uygulamalar, kişisel hesapların korunmasında önemli rol oynar. Authentication (doğrulama), istemcilerin ağ ile bağlantı kurmadan önce denetimden geçerek kimlik doğruluğunu kanıtlamasıdır. Bu işlem için genellikle kullanıcılara ait veriler ve şifre alınarak veri tabanı kaydı yapılır. Kullanıcının ağa erişmek için veri tabanındaki veriler ile uyumlu olacak kullanıcı adı ve şifre bilgisini sağlaması gerekmektedir. Güvenliğin artırılması amacı ile şifrelerin belirli kurallara bağlı kalınarak oluşturulması ve kullanıcı ve sunucu arasındaki bilgi alışverişinin şifrelenerek üçüncü bir kişinin erişimine kapatılması gerekmektedir (Yıldırım, İnce, 2021)
- **Zararlı Yazılımlar ve Virüsler:** Zararlı yazılımlar sistemsel hatalardan, donanım eksikliklerinden, yazılım donanımındaki eksikliklerden ve bilgisayar ağlarındaki eksikliklerden kaynaklı olarak araçlara zarar verebilir ve bilgilerin çalınması gibi sonuçlar oluşturabilir. Bilgisayarlara ve mobil cihazlara zarar verebilecek, bilgileri çalabilecek kötü amaçlı yazılımların farkında olmak, dijital güvenliğin temelini oluşturmaktadır (Aslan,2020)
- **Sosyal Mühendislik Saldırıları:** Sosyal mühendislik ve oltalama saldırıları, günümüzün dijital ortamında, güvenlik açıklarından yararlanmak ve hassas bilgilere yetkisiz erişim sağlamak için insan psikolojisinden yararlanan zorlu bir tehdidi temsil etmektedir Bireyleri kandırarak bilgi edinmeye çalışan yöntemlerdir Sosyal mühendislik saldırılarının amacı; insanları, şifreleri veya gizli verileri için ya da çeşitli sistemlere veya verilere erişim elde etmek için kullanılacak diğer hassas bilgilerini açığa çıkarmaları için kandırmaktır. E-posta dolandırıcılığı (phishing) bunun en yaygın örneğidir. (Çubukçu, Emül,2023)

1.2 Dijital Güvenlik Tehditleri

Günümüzde bireyleri en çok etkileyen dijital güvenlik tehditleri şunlardır;

- **Siber Zorbalık:** Özellikle gençler arasında yaygın olan, dijital ortamda hakaret, tehdit, iftira gibi davranışlar olarak tanımlanmaktadır. Teknolojik araçlarla yapılan zorbalıklar; şiddet, rahatsızlık verme, iftira, taklit etme, dışa vurma, kandırma, dışlama ve siber taciz gibi şekillerde yapılabilmektedir. Bu zorbalıklarda psikolojik etkilene söz konusudur Özellikle sosyal medya araçlarında yaygın bir şekilde görülen dijital teknik yöntemlerinden biridir (Dinç,2020)
- **Kimlik Hırsızlığı:** Kimlik verileri ele geçirilerek işlenen suçları ifade etmek üzere karşılaştırmalı hukukta “kimlik hırsızlığı” terimi kullanılmaktadır. Bir kişinin bilgilerini ele geçirip onun adına işlem yapılması dijital güvenliğe doğrudan tehdit eden unsurların başında gelmektedir. Mali kimlik hırsızlığı, suçlu kimlik hırsızlığı, kimlik klonlama, tıbbi kimlik hırsızlığı ve ticari kimlik hırsızlığı çeşitleri en yaygın uygulanan dijital güvenlik tehditleridir (Bayzıt,2022)
- **Oltalama (Phishing):** Phishing, kullanıcıyı farklı yöntemlerle kandırarak veya ikna ederek bir linke tıklamaya veya bir uygulamaya girmesini sağlayarak kişisel bilgilerini çalmak ve bu bilgileri kötü amaçla kullanmaktır. Phishing saldırıları farklı yöntem ve tekniklerle düzenlenmektedir. İnternet kullanan kişilerin sosyal medya yoluyla veya epostayla gelen linkleri doğruluğunu kontrol etmesi ve direkt olarak veri girilmesi isteyen web sitelerine karşı farkında ve uyanık olması son derece önemlidir (Kör, Erdoğan,2023)
- **Dijital Ayak İzi:** Dijital ayak izi insanların internet ortamındaki faaliyetlerinde bırakmış oldukları izler ve kayıtlardır. Ayrıca dijital ayak izi kişilerin online platformdaki kimliğini oluşturur. Değiştirilmesi zor olan dijital ayak izi, insanların internetteki hareketlerinin, sanal platformlardaki paylaşımlarının, internet geçmişlerinin ve arama motoru sonuçlarının bir birleşiminden oluşmaktadır. İnsanların dijital ortamdaki varlıkları, kendini ifade etme biçimleri ve paylaşımları dijital ayak izine doğru dönüşmektedir Kişilerin internette bıraktığı bu izlerin kötü niyetli kişilerce kullanılması, uzun vadeli riskler doğurabilir (Taş, Bülbül,2021)
- **Sosyal mühendislik:** Yalan söyleme ve karşı tarafı ikna etme üzerine kurulan bir bilgi toplama sanatıdır. Burada kişilerin güveni kazanılarak kendilerine güvenmelerinin sağlanması amaçlanmaktadır (Memiş,2005)

Güvenli yazılım kullanımı, anti virüs programları ya da teknik şifreleme sistemleri dijital güvenliği sağlamak için gereklidir; ancak bireyin bu araçları doğru kullanamaması durumunda etkisiz kalırlar. İşte bu nedenle **eğitim**, dijital güvenliğin temel dayanağıdır. Bilinçli kullanıcılar yetiştirmek, dijital dünyada sürdürülebilir güvenliğin sağlanmasında en büyük yatırımdır (Önel, Dinçkan, 2007) Günümüzde bazı ülkeler dijital güvenlik eğitimini zorunlu hale getirmiştir. Örneğin Estonya, ilkokul düzeyinden itibaren kodlama ve dijital etik derslerini müfredata eklemiş; dijital vatandaşlık eğitimiyle çocukları küçük yaşta bilinçlendirmeyi başarmıştır. Ülkemizde de de Bilişim Teknolojileri dersi kapsamında dijital güvenliğe yer verilmektedir ancak bu içerik henüz sistematik ve uygulamalı bir yapıya kavuşturulamamıştır. Eğitim politikalarının bu eksiklikleri göz önüne alarak daha bütüncül bir yaklaşımla yeniden yapılandırılması gerekmektedir (Avcı, Oruç, O. 2020).

Son yıllarda dijital güvenlikle ilgili yapılan eğitim programlarına ilişkin dünyadan ve ülkemizden örnekler verebilir;

1.Liselerde Siber Zorbalık Eğitimi Programları (Türkiye, 2024): Millî Eğitim Bakanlığı (MEB), 2024 yılında siber zorbalık ve dijital güvenlik konularında öğrencilere yönelik farkındalık eğitimi başlattı. Ortaokul ve lise düzeyinde, öğretmenlerin de katıldığı bu programda öğrencilere sosyal medyada güvenli davranış, kişisel veri koruma, dijital iz ve çevrimiçi tehditlerle başa çıkma yolları anlatıldı(<https://orgm.meb.gov.tr>).

2.”Deepfake” Teknolojileriyle Sahte Video Dolandırıcılıkları (Dünya, 2023–2025): Deepfake, “derin öğrenme” ve “sahte” terimlerinin birleşimidir. Deepfake kullanarak herhangi bir kişi, bir görüntü veya videoda başka bir kişinin yüzünü değiştirebilir veya maskeleyebilir. Deepfake teknolojileri ile oluşturulan sahte videolar, özellikle siyasi figürlerin ve iş insanlarının görüntülerinin manipüle edilmesinde kullanıldı. 2023’te İngiltere’de bir CEO’nun görüntüsü taklit edilerek yapılan sahte bir video üzerinden şirket çalışanları kandırıldı ve büyük miktarda para dolandırıldı (Kırık, Özkoçak,2023).

3. TikTok Üzerinden Kişisel Verilerin Sızdırılması (ABD ve Avrupa, 2024): Avrupa Veri Koruma Kurulu, Tik Tok’un çocuk kullanıcıların verilerini yeterince korumadığı gerekçesiyle 2024’te ciddi yaptırımlar uyguladı. Uygulama, genç kullanıcıların konum bilgisi, tarama geçmişi gibi verileri reklam amaçlı kullanmakla suçlandı (<https://european-union.europa.eu>).

4. Türkiye’de Üniversite Öğrencilerine Yönelik “Siber Farkındalık Yarışmaları” (2023–2024): Türkiye Siber Güvenlik Kümelenmesi,

üniversite öğrencilerine yönelik düzenlediği “CTF – Capture the Flag” yarışmalarıyla gençlerin siber tehditlere karşı savunma becerilerini artırmayı hedeflemektedir(<https://cdn.istanbul.edu.tr.pdf>).

5. Kimlik Avı (Phishing) Saldırılarıyla e-Devlet Bilgilerinin Ele Geçirilmesi (Türkiye, 2024): Phishing kötü niyetli kişilerin güvenilir bir kişi veya kuruluş gibi davranarak mesajlar gönderdiği bir tür siber güvenlik saldırısıdır. 2024’te birçok kullanıcı, e-Devlet benzeri görünen sahte siteler üzerinden kimlik bilgilerini paylaştı. Bu saldırılarda vatandaşlar sahte e-posta ve SMS mesajlarıyla yönlendirildi ve pek çok mağdur yaratıldı (<https://www.microsoft.com>).

2.Eğitimde Dijital Güvenlik Bilinci

Dijital güvenlik alanında bireylerin bilinçlenmesinde ve bu bilinci sürdürülebilir hale getirmede en etkili araçlardan biri eğitimidir. Dijital teknolojilerin yaygınlaşmasıyla birlikte, bireylerin karşılaştığı tehditler daha karmaşık hale gelmiş ve bu tehditlere karşı sadece teknik önlemler yeterli olmamaya başlamıştır. Eğitim yoluyla dijital güvenlik bilincinin oluşturulması, bireylerin hem kendilerini hem de dijital toplumu koruyabilecek becerilerle donatılmasını sağlar (Bozkurt ve diğerleri, 2021).

Dijital güvenliğin sağlanması sadece teknik önlemlerle yapılamaz. Bireylerin bu tehditleri tanıyıp onlara karşı önlem alabilmesi, güvenli davranışları içselleştirmesi gerekir. Özellikle çocuklara ve gençlere bu kavramların basit, anlaşılır ve uygulamalı yöntemlerle öğretilmesi, dijital güvenlik kültürünün temellerini oluşturmaktadır. Dijital güvenlik tehditleri çoğunlukla kullanıcı hatalarıyla başlar: bilinçsizce tıklanan bağlantılar, paylaşılan kişisel bilgiler, şifrelerin güvensiz ortamlarda saklanması gibi. Bu tür durumlar, kullanıcıların bilgi eksikliğinden kaynaklanır. Özellikle çocuklar ve gençler, dijital dünyaya doğuştan adapte olan “dijital yerli” nesil olarak görülse de bu durum onların otomatik olarak dijital güvenlik bilincine sahip olduğu anlamına gelmez. Aksine, bu yaş grubu çoğu zaman deneme-yanılma yoluyla dijital ortamlarda hareket eder ve bu da onları çeşitli tehlikelere karşı savunmasız kılar (Burcu, Tarhan,2024).

Dijital güvenlik eğitimi yalnızca öğrencilerle sınırlı değildir. Eğitimcilerin müfredat içi ve dışı etkinliklerle öğrencilerin güvenli dijital davranışlar geliştirmesinde rehber olması gerekir. Ancak pek çok eğitici dijital güvenlik konusunda yeterli bilgiye ve materyale sahip olmadığından hizmet içi eğitimler ve destekleyici kaynaklarla bu bilgilerin verilmesinin sağlanması önemlidir. Aileler ise çocukların evde dijital araçlarla geçirdiği zamanı denetleyen, örnek olan ve yönlendiren bir konumdadır. Ailelerin bilinçli

olması, çocukların dijital güvenlik konusunda dış dünyadan aldıkları bilgileri pekiştirmelerine katkı sağlar (Çark, 2020).

Verilecek olan dijital güvenlik eğitimi, bireylerin,

- Dijital ortamda nasıl davranmaları gerektiğini öğrenmelerini,
- Karşılaşılabilecekleri riskleri önceden fark etmelerini,
- Dijital hak ve sorumluluklarını kavramalarını öğrenmelerine yardımcı olacaktır.

Ayrıca verilecek dijital güvenlik eğitiminin içeriğinde olması gereken temel konuları ise şöyle sayabilir (Avcı, Aslan,2019):

- Şifre güvenliği ve yönetimi,
- Kişisel verilerin korunması ve gizlilik,
- Phishing (oltalama) ve sosyal mühendislik saldırıları,
- Güvenli internet kullanımı,
- Mobil cihaz ve uygulama güvenliği,
- Güncellemelerin ve anti virüs yazılımlarının önemi,
- Çevrimiçi davranış ve etik kurallar.

Dijital güvenlik konusundaki uygulanmalarında farkındalık yaratmak ve bireyleri bilinçlendirmek amacıyla geliştirilen eğitim stratejilerini aşağıdaki gibi sayabiliriz (Karaaslan, 2021);

1. **Okullarda Dijital Güvenlik Eğitimi:** İlköğretimden başlayarak yükseköğretimde dahil olmak üzere müfredata dijital güvenlik konularının entegre edilmesi, öğrencilerin teknoloji kullanımında sorumluluk sahibi bireyler olarak yetişmesini sağlar ((Taha ve Dehbiyeh, 2021)
2. **Kamu ve Kurumsal Eğitim Programları:** Kamu ve kurumsal eğitim kurumlarında görev alan çalışanlara yönelik düzenli siber güvenlik eğitimleri ile şirket içi veri güvenliğini artırılabilir. Ayrıca kamu kurumlarında da dijital farkındalık eğitim ve seminerlerinin yaygınlaştırılması kurumlar açısından bilinçli dijital araç kullanan çalışan sayısını da arttıracaktır (Yaşar, Çakır, 2015)
3. **Online Eğitim ve Kaynaklar:** İnternet üzerinden erişilebilen ücretsiz veya ücretli siber güvenlik eğitimleri her yaş ve meslek grubundan insanın bu eğitimlere erişimini kolaylaştırmakta ve kişilerin bilinçli olmasını sağlamaktadır. (Yıldırım, Demirer, 2021)

4. **Simülasyon ve Tatbikatlar:** Siber saldırı simülasyonları ve farkındalık uygulamaları, bireylerin gerçek durumlarda nasıl hareket etmeleri gerektiğini deneyimlemelerini sağlamak ve siber saldırılara hazırlıklı olmalarında önemli rol oynamaktadır (Şeker, 2017)
5. **Farkındalık Kampanyaları:** Kamu ve özel sektör tarafından medya, sosyal medya, internet ve diğer iletişim kanalları aracılığıyla sürekli ve güncel içeriklerle, sunum ve tanıtımlarla toplumda siber güvenlik konularında bilinçlendirme yapılmalıdır (Kiraz, 2021).

3.Eğitim Yoluyla Dijital Güvenlik Bilincinin Oluşturulmasında Ortaya Çıkan Sorunlar ve Çözüm Önerileri

Dijitalleşmenin hızla artmasıyla birlikte, bilgi güvenliği ve siber tehditler de aynı oranda karmaşık ve çeşitlenmiş durumdadır. Bu bağlamda dijital güvenlik bilincinin eğitim yoluyla artırılması kritik önem taşımaktadır. Ancak, bu alanda çeşitli engellerle karşılaşmakta ve bu engellerin aşılması için etkili çözümler geliştirilmelidir (Akbiyık, Kestel, 2016)

3.1. Ortaya Çıkan Sorunlar

Dijital güvenlik günümüzde dijitalleşen dünyada ve eğitimde en önemli problemlerden biridir. Dijital güvenlik bilincinin oluşturulmasında karşılaşılan başlıca sorunlar aşağıdaki gibi açıklanabilir:

a) Farkındalık Eksikliği ve Algı Sorunları

Bireyler dijital dünyadaki riskleri küçümsemekte veya yeterince fark etmemektedir. Özellikle yaşlı kesimler, kırsal bölgelerde yaşayanlar ve eğitim seviyesi düşük bireyler arasında dijital güvenlik bilinci düşüktür. Bunun yanı sıra “Bana zarar gelmez” veya “Siber saldırılar sadece büyük şirketlere olur” gibi yanlış algılar yaygın olması da siber saldırılar konusundaki algı eksikliğine neden olmaktadır (Kesici, Mert, Gezgin,2024)

b) Eğitim İçeriklerinin Güncelliğinin Yetersizliği

Siber güvenlik alanında tehditler hızla artarken, eğitim programları çoğu zaman bu değişikliklere aynı hızla uyum sağlayamamaktadır. Bu durum, eğitim alan bireylerin güncel tehditler karşısında hazırlıksız kalmasına yol açmaktadır (Paziuk, Vsevolod 2019)

c) Eğitim Erişimi ve Fırsat Eşitsizliği

Dijital güvenlik eğitimlerine erişimin, özellikle düşük gelirli, kırsal ve dezavantajlı bölgelerde sınırlı olması dijital uçurumun derinleşmesine ve toplumsal güvenlik açığının büyümesine neden olmaktadır. Ayrıca, bazı

meslek grupları veya sektörler de bu eğitimlere yeterince ulaşamamaktadır. Bu durum dijital güvenlikte farkındalığın oluşmasında fırsat eşitsizliklerine neden olmaktadır (Yılmaz,2013)

d) Teknik Dili Anlayamama ve Karmaşık Eğitim Metotları

Dijital güvenlik kavramları ve uygulamaları teknik bir dil içerdiğinden, bu alanda verilen eğitimler çoğu zaman katılımcılar için anlaşılması zor olabilmektedir. Eğitimlerin karmaşık ve teorik olması, bilginin benimsenmesini ve uygulanmasını zorlaştırmakta dijital güvenliğin öneminin anlaşılmasına neden olmaktadır (Yalçın, 2019) Dijital güvenlik eğitimlerine katılımın düşük olması, bireylerin zaman ayırmak istememeleri veya verilen eğitimlerin kendilerine bir fayda sağlamayacağını düşünmeleri motivasyon eksikliğine ve eğitimlerin etkinliğinin azalması sonucunu yaratmaktadır.

e) Standartların ve Yasal Düzenlemelerin Yetersizliği

Siber tehditlere karşı etkili savunma politikalarının geliştirilmesi, teknik, hukuki ve diplomatik stratejileri bir araya getiren çok yönlü bir yaklaşım gerektirmektedir. Uluslararası iş birliği ve bilgi paylaşımı da önem taşımaktadır. Genel olarak dijital güvenlik eğitimine ilişkin standartlar ve yasal düzenlemeler yeterince güçlü olmaması eğitim kalitesinin düşmesine ve uygulamada tutarsızlıklara yol açmaktadır (Taddeo, Floridi, 2018).

3.2. Çözüm Önerileri

Siber güvenlik; yönetsel, teknik ve sosyolojik olarak bütün paydaşların içinde olduğu bir yapıyı gerektirir. Dijital güvenlik bilincinin eğitim yoluyla artırılmasında alınması gereken önlem ve çözümleri aşağıdaki gibi açıklayabilir (Karataş, 2025)

a) Kapsamlı ve Sürekli Farkındalık Kampanyaları Düzenlenmeli

Eğitim kurumlarında öğrenciler için ilk yıl bilgi güvenliği ile ilgili bir dersin müfredata alınması iş hayatına hazırlama ve siber güvenlik farkındalığı oluşturma açısından yararlı olacaktır. Hiyerarşik yapı göz önünde tutularak eğitimler ve farkındalık programları ile zincire dahil bütün kullanıcılar bilinçlendirilmelidir. Dijital güvenlik bilinci geniş halk kitlelerine ulaştırılmalıdır. Medya, sosyal medya, halk eğitim merkezleri, sivil toplum kuruluşları aracılığıyla basit ve etkili mesajlar yaygınlaştırılmalıdır. “Siber güvenlik herkesin sorumluluğudur” bilinci aşılanmalıdır. Siber farkındalık eğitimleri bilgi teknoloji kullanıcıları tarafından mutlaka alınması gereken eğitimlerdendir (Tugal, Almaz, Sevi ,2021)

b) Eğitim İçerikleri Güncel ve Pratik Hale Getirilmeli

Dijital güvenlikle ilgili eğitim konuları riskleri anlamaya ve önlem almaya yardımcı olmalıdır. Saldırı türleri ve yoğunluğu konularının belirlenmesi önemlidir. Tehditler ve teknolojik gelişmeler düzenli olarak takip edilmeli, eğitim materyalleri güncellenmelidir. Ayrıca eğitimlerde sadece teori değil, gerçek hayattan örnekler ve uygulamalı çalışmalar yer almalıdır. Bütün kullanıcılara verilmesi gereken eğitimler şöyle sayılabilir (Yüksel, Öztürk 2017):

- 1.Şifre Güvenliği Eğitimi
- 2.Güvenli İnternet Kullanma Eğitimi
- 3.E-Posta Güvenliği Eğitimi
- 4.Sosyal Mühendislik Eğitimi
- 5.Mobil Cihaz Güvenliği Eğitimi
- 6.Siber Tehdit Türleri Eğitimi
- 7.Kişisel Veri Gizliliği Eğitimi
- 8.Eğitim kurumlarında Uygulamalı Tanıtım Eğitimleri
- 9.Sorumluluklar ve Hukuki Süreçler Eğitimleri

c) Eğitimlere Erişim Kolaylaştırılmalı ve Fırsat Eşitliği Sağlanmalı

Kırsal bölgeler ve dezavantajlı gruplar için ücretsiz, erişimi kolay eğitim platformları oluşturulmalıdır. Mobil cihazlar ve internet erişimi sınırlı olanlar için yüz yüze eğitimler veya basılı materyaller kullanılarak eğitimde fırsat eşitliği yaratılabilir. Eğitim içerikleri sade ve anlaşılır bir dille hazırlanmalıdır. Ayrıca oyunlar, simülasyonlar, interaktif videolar gibi yenilikçi yöntemlerle öğrenme desteklenmelidir.

d) Yasal Düzenlemeler ve Standartlar Güçlendirilmeli

Ülkemizde de son yıllarda ulusal bir sorun haline gelen siber güvenlik saldırıları sonucunda, siber suçlar konusunda hukuksal olarak düzenleme yapılması ihtiyacı ortaya çıkmıştır. Türk Ticaret kanununda ve Türk Ceza Kanunu'nda siber güvenlik faaliyetlerinin yasal düzenlemeleri kapsamında birçok madde bulunmaktadır. (Türk Ceza Kanunu, 2004). 2012/3842 sayılı Bakanlar Kurulu Kararı ile “siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla” Siber Güvenlik Kurulu kurulmuştur (Resmî Gazete, 2012). Ayrıca 2013 yılında Ulusal Siber Güvenlik Stratejisi ve Eylem Planı kabul edilmiştir.

Devlet tarafından dijital güvenlik eğitimi için standartlar belirlenmeli, bu standartlara uygun eğitim programlarının geliştirilmesi ve uygulanması zorunlu kılınmalıdır. Denetim ve yaptırım mekanizmaları oluşturulmalıdır. Yapılan çalışmalardan biriside Cumhurbaşkanlığı dijital dönüşüm ofisine sorumluluklar verilmesidir; ofis, kritik altyapıların belirlenmesine ilişkin çalışmaları gerçekleştirmek, bilgi güvenliği yönetim sistemleri kurmak, işletmek ve teknik standartlara ilgili usul esasları konusunda yetkilendirilmiştir. Bilgisayar Olaylarına Müdahale Ekibi (TR-BOME) ile TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) de hizmete sunulmuştur (Bıçakcı, ve Diğerleri ,2015)

SONUÇ

Eğitim yoluyla dijital güvenlik bilincinin oluşturulması, dijital ortamda karşılaşılan tehditlerin azaltılmasına ve bilgi varlıklarının korunmasına katkı sağlayacak sürdürülebilir bir stratejidir. Devlet, özel sektör, eğitim kurumları ve sivil toplumun iş birliği ile geliştirilecek kapsamlı eğitim politikaları, dijital güvenlik alanındaki farkındalığın artırılması ve risklerin minimize edilmesi açısından temel unsur olacaktır., dijital güvenlik eğitiminin yaygınlaştırılması, sadece bireysel güvenliğin değil, aynı zamanda ulusal güvenlik ve ekonomik istikrarın sağlanmasında da stratejik bir rol oynamaktadır.

Dijital güvenlik konularının eğitim sistemine bütüncül bir yaklaşımla entegre edilmesi, eğitimcilerin bu konuda desteklenmesi ve öğrencilere yönelik pratik beceriler kazandırılması gerekmektedir. Ayrıca aileler ve toplumun diğer bileşenleri de bu sürece dahil edilmelidir. Dijital güvenlik bilincinin eğitim yoluyla geliştirilmesi, sadece bireylerin değil, aynı zamanda toplumun gelişimi açısından da önemlidir. Eğitim yoluyla oluşturulan bu bilinç, dijital dünyada daha etik ve sorumlu bir toplumun temelini atacaktır.

Dijital güvenlik bilincinin yaygınlaştırılması sürecinde karşılaşılan temel sorunlar ve getirilen çözüm önerileri ile bu engellerin aşılabileceği yönünde somut stratejiler sunulmaya çalışılmıştır. Sürekli güncellenen ve herkes için erişilebilir hale getirilen eğitim programları, sade anlatım ve interaktif eğitim yöntemleri; öğrenme etkinliğini artırmakta ve bireylerin dijital güvenlik farkındalığını yükseltmektedir. Bunun yanı sıra, kurumlarda güvenlik kültürünün geliştirilmesi, çalışanların düzenli ve zorunlu eğitimlere tabi tutulması, devlet tarafından belirlenen standartların ve yasal düzenlemelerin güçlendirilmesi; dijital güvenlik alanında bütüncül bir yaklaşımın tesis edilmesi açısından önem arz etmektedir.

Kaynaklar

- Avcı, Ü. ve Oruç, O. (2020). Üniversite öğrencilerinin kişisel siber güvenlik davranışları ve bilgi güvenliği farkındalıklarının incelenmesi. İnönü Üniversitesi Eğitim Fakültesi Dergisi, 21(1), 284-303
- Akbıyık, C., & Kestel, M. (2016). Siber zorbalığın öğrencilerin akademik, sosyal ve duygusal durumları üzerindeki etkisinin incelenmesi. Mersin Üniversitesi Eğitim Fakültesi Dergisi, 12(3), 844-859.
- Aslan (2020), Zararlı Yazılımların Göstermiş Oldukları Davranışlara Göre Analiz ve Tespit Edilmesi, Ankara üniversitesi, Tez <https://www.proquest.com>
- Avcı, Aslan, (2019), Dijital Veri Güvenliği Farkındalığı ve Bilgi Okuryazarlığı ile Alınan Hizmetçi Eğitimin Etkisi, Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi, 891-914
- Bayzıt, (2022), Kimlik Hırsızlığının Türk Ceza Hukuku Ve Karşılaştırmalı Hukuk Bakımından Değerlendirilmesi, Yedi Tepe Üniversitesi Hukuk Dergisi, 635-658
- Bıçakcı, Ergun, Çelikpala, (2015), Türkiye de Siber Güvenlik, Siber Politika Kağıtları Serisi, 28-52
- Bilir (2021), Kişisel Verilerin Korunması Kişinin Kendisinin Korunmasıdır, TRT Akademi, 172-181
- Bozkurt., Hamutoğlu, Kaban, Taşcı, Aykut, (2021) Dijital Bilgi Çağı ; Dijital toplum, Dijital dönüşüm, Dijital Yeterlilikler; Açık Öğretim Uygulamaları ve Araştırmaları Dergisi, 35-63
- Burcu, Tarhan, (2024), Türkiye de Eğitimde Dijital Dönüşüm, Dokuz Eylül Sosyal Bilimler Enstitüsü Dergisi, Özel Sayı, 322-336
- Canogulları, (2021). Öğretmenlerin bilgi güvenliği konusundaki farkındalıklarının incelenmesi. Kalem Eğitim ve İnsan Bilimleri Dergisi, 11(2), 651-679. doi: 10.23863/kalem.2021.219
- Çark, (2020). “Dijital Dönüşümün İşgücü ve Meslekler Üzerindeki Etkileri”, International Journal of Entrepreneurship and Management Inquiries, 4 (1), 27.
- Çubukçu, Emül, (2023), Sosyal Mühendislik ve Oltalama Saldırılarını Anlamak: Derinlemesine Bir Analiz, researchgate.net, Yönetim Bilişim Sistemleri: İşletmelerde Dijital Dönüşüm Yönetimi. Özgür Yayınları. DOI: <https://doi.org/10.58830/ozgur.pub137.c1385>
- Dinç, (2020), Sosyal Medya Ortamlarında Siber Zorbalık: Lise Öğrencilerinin Siber Zorbalık Deneyimlerinin İncelenmesi, e-Journal of New Media / Yeni Medya Elektronik Dergi, 23-27
- Dönmez, (2019). Lise öğrencilerinin bilgi güvenliği farkındalığı ile dijital okuryazarlığı arasındaki ilişkinin incelenmesi (Yüksek Lisans Tezi).

- Hart, , Magheri, , Paci, Sassone, (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95-97, 101827. doi: 10.1016/j.cose.2020.101827
- Karanfi, Uyar (2023), Expoloring tha relationship between digital addiction and online learning readines levels of universty students, *Journal of Educatinal Technology Online learning*,647-664
- Karaaslan, (2022), Siber Güvenlik Felsefesine Giriş, <http://ssrn.com>. (Abstract)
- Karataş, (2025), Uzaktan Eğitimde Kalite Güvence Sistemleri ve Siber Güvenlik, Eğitim ve Bilim Books,95-98
- Kesici, Mert, Gezgin, (2024), Siber Dünyanın Karanlık Yüzü: Güvenlikten Zorbalığa Modern Problemler, Balkan 10th International Conference On Applied Sciences January, 229-238
- Kiraz, (2021), Siber Güvenlik Bağlamında Yeni Tehdit Algılamalarının Türkiye'nin Güvenlik Politikalarına Etkileri, *Journal of Management Theory and Practices Research*, 69-86
- Kırık, Özkoçak, (2023), Medya ve İletişim Bağlamında Yapay Zekâ Tarihi Ve Teknolojisi: Chatgpt ve Deepfake İle Gelen Dijital Dönüşüm, *Karadeniz Uluslararası Bilimsel Dergi*,58-73
- Korlu, (2019). Bir bakışta eğitim 2019'a göre Türkiye'de eğitimin durumu, <https://www.egitimreformugirisimi.org>. Erişim Tarihi: 18.03.2025
- Kör, Erdoğan (2023), Oltalama Saldırılarına Yönelik Bir Araştırma, *İnternational İnformatic Congress 2023 Bildiri Kitabı*, 228-235
- Memiş, (2001), Hukuki Açından Kitlelere E-posta Gönderilmesi. *Erzincan Bin Ali Yıldırım Üniv. Hukuk Fak. Dergisi* ,445-454
- Mulenga, Marbán, (2020). Is COVID-19 the gateway for digital learning in mathematics education? *Contemporary educational technology*, 12(2). doi: <https://doi.org/10.30935/cedtech/7949>. Erişim Tarihi: 18.2.2025.
- Korucu, (2021), Yeni Normal Dünya Düzeninin Siber Güvenlik ve Bilgi Güvenliğine Etkileri, *Yönetim Bilişim Sistemleri Dergisi*,44-59
- Önel, Dinçkan, 2007). Bilgi Güvenliği Yönetim Sistemi Kurulumu, TU-BİTAK-UEKAE Bilgi Güvenliği Yönetim Sistemi Kurulumu Eğitim Dokumanı.
- Özaydın, Kumral (2021), Dijital Yerlilerin Gözünden Dijital Okuryazarlık, *Journal of Research in Education and Society*,363-378
- Paziuk Mitsik (2019). "Global Cybersecurity Culture in the International Discourse Values and Principles", s. 104, <http://journals.uran.ua>, Erişim tarihi:20.04.2025

- Solmaz (2023), Siber Güvenlik Tarihindeki Dönüm Noktaları: Tehditlerin Evrimi ve Savunma Stratejileri, Orta Doğu ve Orta Asya-Kafkaslar Araştırma ve uygulama merkezi Dergisi,1-9
- Şeker E., (2017), Siber Savunma Tatbikatları: Planlama, Uygulama Ve Değerlendirme, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:3, No:2, 33-41
- Taş, Bülbül, (2021) Sosyal Medya Kullanıcılarının Dijital Ayak İzi Farkındalığı, Sosyal, Beşeri ve İdari Bilimler Dergisi, 206-216
- Taha, Dahabiyeh, (2021). College students information security awareness: A comparison between smartphones and computers. Education and Information Technologies, 26, 1721-1736. doi: 10.1007/s10639-020-10330-0
- Taddeo, Floridi, (2018). Regulate artificial intelligence to avert cyber arms race. Nature, 556, 296-298.
- Teymourlouci, (2015). Quick reference: Cyber attacks awareness and prevention method for home users. International Scholarly and Scientific Research & Innovation, 9(3), 678-684. Erişim adresi: <http://waset.org/Publication/10000665>
- Tugal, Almaz, Sevi, (2021), Üniversitelerdeki Siber Güvenlik Sorunları ve Farkındalık Eğitimleri, Bilişim Teknolojileri Dergisi, Cilt: 14, Sayı: 3, 229-237
- Ulusal Siber Yürütülmesi, Güvenlik Çalışmalarının Yönetilmesi ve Koordinasyonuna İlişkin Karar. (2012, 20 Ekim). Resmî Gazete (Sayı:2012/3842). Erişim adresi: <https://www.resmi-gazete.gov.tr>
- Yalçın, (2019) “Soğuk Savaş Sonrası NATO ve Türkiye’de Siber Güvenlik” (Tez No: 545623) [Yayımlanmamış Yüksek Lisans Tezi], Eskişehir Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü.
- Yaşar, Çakır, (2015), Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri, Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 488-507
- Yıldırım, İnce (2021), Kampüs Ağlarında İnternet Erişimi İçin Bağlantı Katmanını Kimlik Doğrulama Uygulaması, Journal of Computer Science, 82-92
- Yıldırım, Demirer, (2021). Eğitim alanında bilgi güvenliği üzerine sistematik bir alanyazın incelemesi: Türkiye örneği. Erzincan Üniversitesi Eğitim Fakültesi Dergisi, 23(3), 835-856. doi: 10.17556/erziefd.862623
- Yılmaz, (2013) “E-dönüşüm Sistemlerinin Bilgi Güvenliği Açısından İncelenmesi E-devlet Kullanıcıları Üzerine Bir Araştırma (Tez No: 327359) [Yayımlanmamış Yüksek Lisans Tezi], Marmara Üniversitesi. Sosyal Bilimler Enstitüsü.
- Yüksel, Öztürk, (2017) “SIP Saldırıları ve Güvenlik Yöntemleri”, Bilişim Teknolojileri Dergisi, 10(3), 301-310,
<https://european-union.europa.eu>.Erişim tarihi:22.05.2025

<https://cdn.istanbul.edu.tr/FileHandler2.ashx?f=ctf-yarismasi.pdf>,
tarihi:24.05.2025

erişim

<https://www.microsoft.com> , erişim tarihi:24.05.2025