
DIGI
WELL

Avrupa Birliği tarafından
ortak finanse edilmektedir

# Dijital Esenlik ve Güvenliği Herkes için Erişilebilir Hale Getirerek Dijital Yılmazlığın İnşası

**DigiWELL**

**2022-2-SK01-KA220-ADU-000096888**

**Dijital Yılmazlığın İnşası – Kılavuz ve Metodoloji**

**Eylül, 2023**

İçindekiler Tablosu

Özet

1. Giriş
    1.1. Kılavuz ve Metodolojinin Amacı
    1.2. AB Dijital Yeterlilik Çerçevesi (DigComp)
    1.3. Kılavuz ve Metodoloji Yetişkinler için Neden İyi bir Kaynaktır?
    1.4. Kılavuz ve Metodoloji Yetişkin Eğitimciler için Neden İyi bir Kaynaktır?
    1.5. DigiWELL Proje Sözlüğü ve Kullanımı

Arka Plan ve Bağlam

2. Dijital Esenlik
    2.1. Esenlik Nedir?
    2.2. Esenlik ve Dijitalleşme
    2.3. Dijital Esenlik Nedir?
    2.3.1. Zihinsel Sağlık, Esenlik ve Dijital Esenlik
    2.3.2. Dijital Esenliğe Neden İhtiyaç Duyarız?
    2.3.3. İyi ve Kötü Dijital Esenlik
    2.3.4. Bireylerin Dijital Esenliğini Geliştirmek: Herkese ve Yetişkin Eğitimine Yönelik Faydalar

3. Dijital Güvenlik
    3.1 Dijital Güvenlik ve Siber Güvenlik
    3.2. Yetişkinlerin Karşılaştığı Siber Güvenlik Tehditleri
    3.3. Yetişkinler için Dijital Güvenlik Pratikleri
    3.4. Yetişkinlere Yönelik Dijital Güvenlik Kaynakları

**4. Yetişkinler İçin Dijital Güvenliği Sağlamanın En İyi Uygulamaları**

**4.1. Dijital Güvenliği Sağlamada Temel Konular**

**4.2. Dünyadan En İyi Örnekler**

**4.2.1. Siber Avrupa**

**4.2.2. Arayüz ve Teknolojinin Uyarlanması**

**4.2.3. Yardım Hatları ve Özel Destek**

**4.2.4. Farkındalık Kampanyaları ve Eğitim**

**4.2.5. Mali Koruma Programları**

**4.2.6. Teknoloji Sektörü ile İş birliği**

**4.2.7. Uluslararası Kaynaklar, Raporlar ve Girişimler**

**4.3. Dijital Güvenlik Konusunda Yetişkin Eğitiminin En İyi Uygulamaları**

**5. Yetişkinlerin Eğitimi: Dijital Yılmazlık Nasıl İnşa Edilir?**

**5.1. Andragojinin Dört İlkesi**

**5.2. Eğitmenler Andragojiyi Nasıl Uygulayabilir?**

**6. Sonuç**

**7. Kaynaklar**

# Özet

COVİD-19 salgını sonrasında yaşamımızda fazlasıyla yer alan dijital teknolojilerin ve internetin kullanımıyla birlikte bazı ihtiyaçlar hayati hale geldi. Bunlardan en önemlisi, dijital dünyada zarar görmeden güvenli bir şekilde işlem yapabilmektir. Özellikle yetişkinler, kendilerini siber tehditlerden koruyabilmek için dijital güvenlik önlemlerine ve bazı yeterliliklere ihtiyaç duymaktadır. İnternet ve dijital teknolojiler yaşamı kolaylaştırsa da aynı zamanda bazı olumsuz psikolojik sorunlar da yaratmaktadır. Örneğin, siber zorbalık başa çıkılması zor bir sorun haline gelmiştir. Buna bağlı olarak dijital dünyada esenliğin sağlanması artık günümüz koşullarında bir zorunluluk haline gelmiştir. Yine bu konuyla ilgili olarak, dijital teknolojinin kullanımının giderek artması ve dijital dönüşümün geldiği nokta, dijital yorgunluk gibi bazı konuları insanların gündemine getirmektedir.

DigiWELL projesi, dijital esenlik ilkelerini yetişkin eğitimine dâhil etmeyi amaçlamaktadır. Bu proje, yetişkin eğitimi kuruluşlarının, ağlarının ve girişimlerinin genel uygulamalarına katkıda bulunmaya yöneliktir. Proje, dijital çağda teknolojinin yetişkinlerin ruh sağlığını, üretkenliğini ve genel esenliğini nasıl etkilediğini ele almanın ne kadar önemli olduğunu vurgulamaktadır. DigiWELL'in ana hedefi, yetişkin öğrenenlere dijital dünyada bilinçli ve etik ilkeler gözeterek gezinmek için gerekli bilgi, yetenek ve kaynakları sağlamaktır. DigiWELL projesi ayrıca yetişkin öğrenenlerin güçlendirilmesine yönelik ek girişimlerin oluşturulmasını ve yürütülmesini de içerir. Bu etkinliklerin amacı, yetişkinlerin dijital esenliği teşvik etme konusundaki deneyimlerini, zorluklarını ve zaferlerini paylaşabilecekleri destekleyici bir ortam sağlamaktır. Bu doğrultuda, DigiWELL projesi, bireylere ve yetişkin örgütlerine, dijital esenliğin önemi ve yetişkinlerin, eğitimcilerin ve yetişkin eğitimcilerin dijital refahının nasıl teşvik edileceği konusunda bilinçlenmesi ve aydınlanması için birçok fırsat sunmaktadır. Dijital refahın bütünsel bir yaklaşımla gerçekleşebilmesi, ilgili tüm paydaşların bireylerin dijital esenlik ihtiyaçlarını destekleyecek şekilde harekete geçmesiyle mümkün olmaktadır. Bu çerçevede bu kılavuzda sunulan bilgiler, ipuçları ve iyi uygulamalar, çoğumuzun daha iyi bir dijital esenliğe ve aynı zamanda daha güçlü dijital yaşamlara sahip olması için bireyleri ve ilgili kuruluşları inisiyatif almaya davet etmektedir.

# 1. Giriş

## 1.1. Kılavuz ve Metodolojinin Amacı

- Yetişkinleri dijital esenlik ve dijital güvenlik konularında ve bunlar için gerekli yeterlilikler konusunda teşvik edip bilgilendirerek, dijital esenlik ve dijital güvenliğin herkes için erişilebilir olmasına katkıda bulunmak.
- Dijital yılmazlığı, dijital esenliği ve dijital güvenliği, terminoloji çerçevesini ve dijital esenlik ve dijital güvenliğin en iyi uygulamalarını tanıtmak.
- Geliştirilen çıktıların ortak ülkelerdeki ilgili kuruluşlara uyarlanmasıyla çok kültürlülüğü sağlamak

## 1.2. AB Dijital Yeterlilik Çerçevesi (DigComp)

DigComp'ta dijital yeterlilik, "öğrenme, iş ve topluma katılım için dijital teknolojilerin kendinden emin, eleştirel ve sorumlu bir şekilde kullanılmasını ve dijital teknolojilerle etkileşim kurulmasını" kapsar. Bilgi, beceri ve tutumların bir bileşeni olarak tanımlanır. Council Recommendation on Key Competences for Life- long Learning, 2018).

DigComp Dijital Yeterlilik çerçevesi, dijital yeterliliğin temel bileşenlerini 5 alanda tanımlamaktadır. Bu alanlar aşağıda özetlenmiştir:

**Bilgi ve veri okuryazarlığı:** Bilgi gereksinimlerini ifade etmek, dijital verileri, bilgileri ve içeriği bulmak ve almak. Kaynağın ve içeriğinin uygunluğunu değerlendirmek. Dijital verileri, bilgileri ve içeriği depolamak, yönetmek ve düzenlemek.

**İletişim ve iş birliği:** Kültürel ve nesilsel çeşitliliğin farkında olarak dijital teknolojiler aracılığıyla etkileşimde bulunmak, iletişim kurmak ve iş birliği yapmak. Kamu ve özel dijital hizmetler ve katılımcı vatandaşlık yoluyla topluma katılmak. Kişinin dijital varlığını, kimliğini ve itibarını yönetmek.

**Dijital içerik oluşturma:** Dijital içerik oluşturmak ve düzenlemek. Telif hakkı ve lisansların nasıl uygulanacağını anlayarak bilgi ve içeriği mevcut bilgi birikimine geliştirerek entegre etmek. Bir bilgisayar sistemi için anlaşılır yönergelerin nasıl verileceğini bilmek.

**Güvenlik:** Dijital ortamlardaki cihazları, içerikleri, kişisel verileri ve gizliliği korumak. Fiziksel ve psikolojik sağlığı korumak, sosyal iyi oluş ve sosyal katılım için dijital teknolojilerden haberdar olmak. Dijital teknolojilerin ve kullanımının çevresel etkilerinin farkında olmak.

**Problem çözme:** İhtiyaçları ve sorunları belirlemek, dijital ortamlarda kavramsal sorunları ve problem durumlarını çözmek. Süreçleri ve ürünleri yenilemek için dijital araçları kullanmak. Dijital evrimi takip etmek.

Güvenlik alanındaki temel yeterliliklerden biri sağlığı ve esenliği korumaktır. Sağlığı ve esenliği korumak şu anlamlara gelmektedir; (a) dijital teknolojileri kullanırken sağlık risklerinden, fiziksel ve psikolojik sağlığa yönelik tehditlerden kaçınabilmek, (b) dijital ortamlardaki olası tehlikelerden (örneğin siber zorbalık) kendini ve başkalarını koruyabilmek ve (c) sosyal iyi oluş ve sosyal kapsayıcılık için dijital teknolojilerden haberdar olmak.

## 1.3. Kılavuz ve Metodoloji Yetişkinler için Neden İyi bir Kaynaktır?

Yukarıda da belirtildiği gibi, COVID-19 salgını sonrası yaşamımızda fazlasıyla yer alan dijital teknolojilerin ve internetin kullanımıyla birlikte bazı ihtiyaçlar hayati hale geldi. Bunlardan en önemlisi, dijital dünyada zarar görmeden güvenli bir şekilde işlem yapabilmektir. Özellikle yetişkinlerin kendilerini siber tehditlerden koruyabilmeleri için dijital güvenlik önlemlerine ve bazı yeterliliklere ihtiyaçları vardır. İnternet ve dijital teknolojiler yaşamı kolaylaştırsa da aynı zamanda bazı olumsuz psikolojik sorunlar da yaratmaktadır. Örneğin,

siber zorbalık başa çıkılması zor bir sorun haline gelmiştir. Buna bağlı olarak dijital dünyada esenliğin sağlanması artık günümüz koşullarında bir zorunluluk haline gelmiştir. Yine bu konuyla ilgili olarak, dijital teknolojinin kullanımının giderek artması ve dijital dönüşümün geldiği nokta, dijital yorgunluk gibi bazı konuları insanların gündemine getirmektedir.

Bu kılavuz, mümkün olduğu kadar çok sayıda gerçek dünya örneğini kullanmaktadır. Knowles'un (1968) çizdiği çerçeve doğrultusunda yetişkin öğrenmesini desteklemek için yetişkin öğrenenlerin bazı kavramları kendilerinin keşfetmelerine olanak tanır.

## 1.4. Kılavuz ve Metodoloji Yetişkin Eğitimciler için Neden İyi bir Kaynaktır?

Eğitim ve öğretim, bireyleri kendilerini ve kuruluşlarını siber tehditlere karşı korumak için gereken bilgi, beceri ve en iyi uygulamalarla güçlendirerek dijital güvenlik konusundaki farkındalığın artırılmasında çok önemli bir rol oynamaktadır. Ayrıca dijital güvenliğe yönelik eğitim ve öğretim, güçlü bir siber güvenlik kültürü oluşturmanın temel bileşenleridir. Belirli ihtiyaçlara ve rollere göre uyarlanmış eğitim programları tasarlamak, yetişkinleri, siber tehditleri etkili bir şekilde tanımlamak ve bunlara yanıt vermek için gereken bilgi ve becerilerle donatır.

Eğitim, bireylerin kimlik avı, kötü amaçlı yazılım, sosyal mühendislik ve fidye yazılımı gibi çeşitli siber tehdit türlerini anlamalarına yardımcı olur. Bireyler bu tehditlerin farkına vararak dijital platformları kullanırken daha dikkatli ve temkinli olabilirler. Eğitim, bireylere kimlik avı e-postalarını, mesajlarını veya web sitelerini nasıl tanımlayacaklarını öğretebilir. Bu yolla, şüpheli unsurları tespit etmeyi ve kötü amaçlı bağlantılara tıklamaktan veya hassas bilgiler vermekten kaçınmayı öğrenirler. Aynı zamanda eğitim, mobil cihazların güvenliğinin sağlanması, şifrelerle korunması, şifreleme kullanılması ve uygulama indirirken dikkatli olunmasına ilişkin yönergeleri de içerirken, bireylerin ilgili siber güvenlik düzenlemeleri ve uyumluluk gerekliliklerinden haberdar olmalarını sağlayarak yasal ve etik uygulamaların sürdürülmesine yardımcı olur. Son olarak, eğitim yoluyla bireyler, siber güvenliğin ortak bir sorumluluk olduğunu ve güvenli bir ortamı sürdürmek için herkesin aktif katılımının gerekli olduğunu anlar; bu da iyi siber güvenlik alışkanlıkları edindirerek; bireyleri hem işte hem de kişisel yaşamlarında güvenlik önlemlerini uygulamaya teşvik eder.

DigiWELL projesi, İnternet Çağında doğmamış yetişkinlerin dijital güvenlik ve dijital esenlik ihtiyaçlarını karşılamayı amaçlamaktadır. Bu amacın, yetişkinlerin özel öğrenme gereksinimlerini karşılayan esnek öğrenme fırsatları yaratıp geliştirerek başarılması hedeflenmektedir. Proje, harmanlanmış bir öğrenme yaklaşımı yoluyla dijital yılmazlığı artırmaya odaklanacaktır. Özellikle bu kılavuz, siber tehditlere karşı etkin bir şekilde savunma yapan ve dijital varlıkları ve hassas bilgileri koruyan, güvenlik bilincine sahip bir kültür oluşturduğu için yukarıdaki amaca katkıda bulunmaktadır.

Başka bir perspektiften, dijital güvenliğe ayrılmış bir bölüm içeren bu kılavuz, yetişkinlerin dijital çağda kendilerini korumaları için gerekli bilgi ve becerilerle donatılmasında hem bireyler hem de topluluklar için daha güvenli ve daha emniyetli bir çevrimiçi deneyimin

desteklenmesinde önemli bir rol oynayabilir. DigiWELL, yetişkinleri potansiyel riskler konusunda eğittiği, siber güvenliğin önemini ve çevrimiçi ortamda kendilerini nasıl koruyacaklarını anlamalarına yardımcı olduğu için yetişkinler için değerli bir kaynaktır. Son olarak, dijital güvenlik önlemlerinin uygulanması konusunda pratik rehberlik sunar ve yetişkinlerin dijital dünyada güvenle gezinmelerini sağlar ve yetişkinlerin yeni dijital güvenlik sorunlarıyla karşılaştıklarında veya belirli konularda bilgi tazelemeye ihtiyaç duyduklarında tekrar başvurabilecekleri bir referans kılavuzu olarak hizmet eder.

## 1.5. DigiWELL Proje Sözlüğü ve Kullanımı

Sözlük, dijital esenlik, dijital güvenlik ve dijital yılmazlık ile ilgili temel terim ve tanımları dijital teknolojilerin yetişkin kullanıcılarına tanıtmayı amaçlamaktadır.

### *Terimlerin Sınıflandırılması*

Sözlükte içerik açısından 3 temel terim kategorisi bulunmaktadır;

1. Bilgi ve iletişim teknolojileri alanına ait terim ve tanımlar (projeye göre dijital teknolojiler).
2. Bilişim, siber ve dijital güvenlik alanına ait terim ve tanımlar (projeye göre dijital güvenlik).
3. Proje hedeflerine göre tanımlanan terimler ve tanımlar: dijital esenlik ve dijital yılmazlık. Bu terimler görece yeni olup proje ekibinin alanyazın araştırmasının bir parçası konumundadır. Bu terimlerin tek tip bir tanımının bulunmadığı vurgulanmalıdır. Bu kategori aynı zamanda zihinsel ve fiziksel sağlık alanındaki terimleri de içermektedir. Örneğin, dijital bağımlılık, dijital yorgunluk/tükenmişlik, dijital detoks vb.

***Uyarı:*** Bir sözlüğün metin veri tabanında bir terimin birçok nedenden dolayı birden fazla tanımı olabilir. Örneğin; Orijinal tanım zaman içinde evrilmiş ve geliştirilmiş olabilir, genel tanım özel bir alana uyarlanmış olabilir, tanımlar benzer olup arada ince farklılıklar olabilir.

### *Terim ve Tanımlar*

***Dijital Yılmazlık:*** 1. Dijital yılmazlık, yeni teknolojileri kullanma ve değişen dijital beceri gereksinimlerine uyum sağlama konusunda farkındalığa, becerilere, çevikliğe ve güvene sahip olmak anlamına gelir. Dijital yılmazlık, sorunları çözme ve beceri geliştirme kapasitesini artırır ve dijital dönüşümlerde yön bulma potansiyelini güçlendirir. 2. Dijital yılmazlık, gençlerin, potansiyel olarak zararlı bilgilere karşı savunmasızlıklarını azaltmak için dijital bilgilere erişirken eleştirel zihniyet geliştirme becerisidir. 3. Dijital yılmazlık, "dijital stres kaynaklarına

iyi uyum sağlama ve sürekli değişen dijital ortamların ve uygulamaların etkisini yönetme becerilerini geliştirme süreci" anlamına gelir.

***Dijital Güvenlik:*** Dijital güvenlik, ağ veya internet hizmetlerindeki fiziksel bir kimliği temsil ettiğinden dijital kimliğin korunmasıdır. Dijital güvenlik, çevrimiçi dünyada kişisel verileri ve çevrimiçi kimliği korumak için kullanılan en iyi uygulamalar ve araçlar kümesidir. Dijital güvenliğe ilişkin araç örnekleri şunlardır: Web hizmetleri, antivirüs yazılımı, akıllı telefon SIM kartları, biyometrik ve güvenli kişisel cihazlar, şifre yöneticileri, ebeveyn kontrolü vb.

***Dijital Esenlik:*** 1. Dijital esenlik, bireyin teknolojinin profesyonel ve kişisel yaşamı üzerindeki olumsuz etkilerini etkili bir şekilde yönetme becerisidir. Dijital esenliğin amacı teknolojik cihazların ve dijital hizmetlerin sağlıklı kullanımını teşvik etmektir. 2. Dijital teknolojinin sağlıklı kullanımıyla yaşanan kişisel esenlik durumu. 3. Dijital esenlik, iletişim ve algılar da dahil olmak üzere, bilgi teknolojisinin insanların uzun ve sağlıklı yaşamlar sürmesine yardımcı olabileceği yolları kapsar.

***Dijital Yeterlilik:*** Öğrenme, iş ve topluma katılım için dijital teknolojilerin kendinden emin, eleştirel ve sorumlu bir şekilde kullanılmasını ve dijital teknolojilerle etkileşim kurulmasıdır. Bilgi, beceri ve tutumların birleşimi olarak tanımlanır.

***Dijital Bağımlılık:*** Dijital bağımlılık, dijital medya, cihazlar ve internetin kullanıcının yaşamını olumsuz etkileyecek şekilde aşırı kullanımıyla ilişkili zararlı bir bağımlılıktır.

***Dijital Beceriler:*** Dijital beceriler, bilgiye erişmek ve onu yönetmek için dijital cihazları, iletişim uygulamalarını ve ağları kullanma becerisidir. İnsanların dijital içerik oluşturmasına ve paylaşmasına, iletişim kurmasına ve iş birliği yapmasına ve yaşamda, öğrenmede, işte ve sosyal etkinliklerde etkili ve yaratıcı bir şekilde kendini gerçekleştirmesine yönelik sorunları çözebilmesine olanak tanımaktadır.

***Siber Tehdit:*** Yetkisiz erişim, bilgilerin imha edilmesi, ifşa edilmesi, bilgilerin değiştirilmesi ve/veya hizmet reddi yoluyla kuruluşları/bireyleri olumsuz etkileme potansiyeli olan her türlü durum veya olay. Amaç, verileri çalmak/zarar vermek veya dijital esenliği bozmaktır.

***Siber Zorbalık:*** Bir veya daha fazla kişinin dijital teknolojiyi kasıtlı olarak ve tekrar tekrar başka bir kişiye zarar vermek için kullandığı, çevrimiçi alanda zorbalığın çeşitli biçimleri için kullanılan bir terimdir (örneğin, e-posta veya anlık mesaj göndermek, sosyal ağlarda veya halka açık forumlarda yorum yayınlamak).

***Siber Güvenlik*:** Siber güvenlik, bilgi güvenliğinin bir alt kümesidir ve amacı siber alanı (yani ağları, intranetleri, sunucuları, bilgileri ve bilgisayar sistemlerini ve altyapısını) yetkisiz erişimden, siber saldırılardan veya hasardan korumaktır. Siber güvenlik, bilgisayarlarda, depolamada ve ağlarda (siber uzayda) bulunan elektronik/dijital formdaki bilgilerin korunmasına odaklanır.

***Dijital Gizlilik:*** Dijital gizlilik, bireyin internete eriştiğinde kişisel bilgilerinin erişimini ve kullanımını kontrol etme ve koruma yeteneğidir. Dijital gizlilik, adlar, adresler, sosyal kimlik numarası, kredi kartı bilgileri vb. gibi kişisel olarak tanımlanabilir bilgileri koruyarak bireylerin çevrimiçi ortamda anonim kalmasına yardımcı olur.

***Dijital Güvenlik - Siber Güvenlik - Bilgi Güvenliği:*** Bilgi güvenliği: önemli verilerin gizliliğini korumak ve güvenliğini sağlamak için bilgileri (herhangi bir formatta ve biçimde) ve bilgi sistemlerini yetkisiz erişime ve kullanıma karşı korur. Siber güvenlik: Tüm ağları ve iletişim sistemlerini, bilgisayar sistemlerini ve diğer dijital bileşenleri ve bunlarda saklanan dijital verileri korur. Dijital güvenlik: Çevrimiçi varlığı (kimlik ve ilgili hassas bilgiler, varlıklar) korur.

***En İyi Uygulama:*** Belirli bir alanda en etkili çözümü sunan, en iyi sonuçlara yol açtığı kanıtlanmış ve yaygın olarak benimsenmek üzere uygun bir standart olarak oluşturulmuş (önerilen) kanıtlanmış bir yöntem veya süreçtir. Dijital güvenlikte bunlar, bir kişinin/kurumun dijital alanda korunmasını sağlamak için tanımlanmış prosedürlerdir (örneğin önerilen teknikler, programlar, talimatlar, kılavuzlar).

# 2. Dijital Esenlik

## 2.1. Esenlik Nedir?

**"Esenlik"** terimi memnun, neşeli ve sağlıklı olma durumunu ifade eder. Bir kişinin fiziksel, zihinsel ve duygusal esenliğini ve varoluşunun diğer alanlarındaki esenliği kapsar. Esenlik, hastalık veya rahatsızlıktan uzak olmanın ötesinde, genel mutluluk ve yaşam kalitesine odaklanır.

***Fiziksel esenlik***, kişinin fiziksel olarak formda olması ve hastalık veya rahatsızlığının olmaması gibi faktörler bağlamında kişinin vücudunun durumudur. Dengeli egzersiz, besleyici gıda, yeterli uyku ve stres yönetimi yoluyla sağlıklı bir yaşam tarzını sürdürmeyi gerektirir.

Bir kişinin bilişsel ve duygusal esenliği, ***zihinsel esenliği*** ile ilişkilidir. Zihinsel esenlik, iyi bir bakış açısına sahip olmayı, doyum yaşamayı ve stresle ve yaşamın zorluklarıyla başa çıkabilmeyi gerektirir. Farkındalık egzersizleri yapmak, hobi edinmek, sevilen kişilerden destek istemek, gerektiğinde profesyonel yardım almak gibi etkinlikler kişinin zihinsel esenliğini beslemeye yardımcı olabilir.

Kişinin duygularını iyi anlaması ve kontrol edebilme kapasitesine sahip olması, ***duygusal esenlik*** olarak adlandırılır. Yılmazlığı geliştirmeyi, iyi ilişkileri sürdürmeyi ve kendine dair olumlu bir algıya sahip olmayı gerektirir. Kişisel farkındalık, duygusal kontrol, etkili iletişim ve destekleyici ilişkilerin geliştirilmesi, bir bütün olarak duygusal esenliğe katkıda bulunur.

Bir kişinin bağlantılarının kalitesi ve bir topluluğa ait olma duygusu, ***sosyal esenliğin*** bileşenleri arasındadır. Sevdiklerinizle, yakın arkadaşlarınızla ve daha geniş bir sosyal ağla kalıcı bağların geliştirilmesini gerektirir. Sosyal faaliyetlere katılmak, topluma katkı sağlamak, bağlılık ve aidiyet duygusunu sürdürmek, sosyal esenliği artırabilir.

Genel olarak **esenlik**, bir kişinin yaşamının farklı yönlerinin birbiriyle nasıl ilişkili olduğunu temele alan kapsamlı bir düşüncedir. Aktif olarak dengeli ve tatmin edici bir varoluş arayışını, kişinin bedensel ve zihinsel sağlığına önem vermesini, sağlıklı ilişkiler geliştirmesini ve kişinin yaşamında anlam bulmasını gerektirir.

## 2.2. Esenlik ve Dijitalleşme

Teknoloji ve dijitalleşme, iletişimi mümkün kılarak, verimliliği artırarak ve bilgiye erişimi geliştirerek esenliği iyileştirme potansiyeline sahiptir. Dijital kullanımı yönetmek, gizlilik ve güvenliği korumak, teknoloji ile yaşamın diğer yönleri arasında iyi bir denge kurmak için olası dezavantajların farkında olmak ve gerekli önlemleri almak çok önemlidir.

Teknoloji ve dijitalleşme, bilgi ve hizmetlere erişimi büyük ölçüde artırmıştır. Bu erişim, genel olarak esenlik üzerinde olumlu bir etkiye sahiptir. İnsanlar artık kişisel gelişime, sağlık bilgilerine, çevrimiçi destek gruplarına ve eğitim kaynaklarına yönelik dijital araçlara kolayca erişebilmektedir. Kesintisiz iletişim ve uzak mesafeler arası bağlantı sayesinde teknoloji, sosyal bağlantıları teşvik etmekte ve yalnızlık duygusunu azaltmaktadır. Toplumsal esenliği artıran dijital platformlar, sosyal medya ve mesajlaşma uygulamaları sayesinde insanlar arkadaşlarıyla, aileleriyle ve topluluklarla iletişim halinde kalabilmektedir. Dijitalleşme aracılığıyla yaşamın birçok yönü daha verimli ve kullanışlı hale gelmiştir. Dijital araç ve hizmetlerin kullanımı sayesinde, bir zamanlar çok fazla zaman ve çaba gerektiren görevler artık hızlı ve zahmetsizce tamamlanabilmektedir. Bu, zamandan tasarruf ederek ve stresi azaltarak genel esenliğe katkı sağlayabilir. Dahası, teknoloji geliştikçe iş piyasasında dijital yetenekler giderek daha önemli hale gelmektedir. Bir kişinin istihdam edilebilirliği ve sosyoekonomik

refahı, bu becerilerin kazanılması ve kullanılmasıyla artırılabilir. Yine de bazı kişilerin veya grupların teknolojiye veya dijital okuryazarlığa erişimi olmadığında ortaya çıkan dijital uçurum, mevcut eşitsizlikleri daha da kötüleştirebilmektedir.

Teknolojiyi yanlış ve aşırı kullanmanın kişinin ruh sağlığı üzerinde zararlı etkileri olabileceği gibi, teknolojinin kişiler üzerinde iyi etkileri de olabilmektedir. Kaygı, umutsuzluk ve düşük özsaygı; ekranda çok fazla vakit geçirmekten, sosyal medya karşılaştırmalarından ve çevrimiçi tehditlerden etkilenebilir. Ruh sağlığını korumak için sağlıklı bir dengeyi bulmak ve teknolojiyi dikkatli kullanmak çok önemlidir. Ayrıca dijital ortamda bazı gizlilik ve güvenlik sorunları da bulunmaktadır. Siber tehditler, veri ihlalleri ve çevrimiçi dolandırıcılık, insanların finansal güvenliğini ve kişisel bilgilerini tehlikeye atabilir. Dijital çağda genel refahın sürdürülmesi, dijital güvenliğin ve gizliliğin korunmasını gerektirir.

## 2.3. Dijital Esenlik Nedir?

Dijital yılmazlığın geliştirilmesi ve güvenlik prosedürlerinin benimsenmesi, dijital alanda optimal sağlık ve genel esenlik durumuna katkı sağlamaktadır. Bu durum, ***dijital esenlik*** olarak açıklanmaktadır. Dijital esenlik, esenlik kavramından doğar ve bireylerin dijital yaşamlarıyla ilişkilidir. İnsanların hem esenliklerini hem de güvenliklerini başarılı bir şekilde yönetirken dijital dünyaya uyum sağlama, yönetme ve gelişme kapasitesi, dijital esenlik ve dijital güvenliğin bir birleşimi olarak ifade edilen *dijital yılmazlık* olarak adlandırılmaktadır. Dijital yılmazlığın temel taşı, teknolojiyle olumlu ve uygun bir bağlantının kurulmasını ve korunmasını vurgulayan dijital esenliktir. Dijital esenlik, ekran başında geçirilen zamanın sınırlandırılmasını, zihinsel ve duygusal sağlığa yüksek öncelik verilmesini, destekleyici çevrimiçi toplulukların oluşturulmasını ve dijital okuryazarlığın geliştirilmesini gerektirir. Esenlik bağlamında, dijital yılmazlık, insanların genel esenliğini korurken siber zorbalık, çevrimiçi taciz veya tehlikeli içeriğe maruz kalma gibi çevrimiçi zorluklarla başa çıkmalarına yardımcı olur. Bireyler, dijital esenliği dijital güvenlikle bütünleştirerek dijital dünyada güvenle ve sorumlulukla hareket etmelerine olanak tanıyan güçlü bir dijital yılmazlık oluşturabilirler. Bu şekilde dijital dünyanın zorluklarını daha iyi yönetebilir, değişen tehlikelere uyum sağlayabilir, akıllıca kararlar verebilir, kişisel bilgilerini koruyabilir ve interneti kullanırken zihinsel, duygusal ve fiziksel sağlıklarını koruyabilirler. Dijital yılmazlık nihai olarak insanlar için daha güvenli, daha sağlıklı ve daha tatmin edici bir çevrimiçi deneyimi teşvik etmektedir.

### *2.3.1. Zihinsel Sağlık, Esenlik ve Dijital Esenlik*

Yaşam kalitemiz, zihinsel sağlığımız ve genel esenliğimiz arasındaki derin bağlantılardan etkilenir. Düşüncelerimiz, duygularımız ve davranışlarımız gibi yönleri de içeren psikolojik ve duygusal esenliğimiz zihinsel sağlığımız ile ilişkilidir. Bu, sağlığımızın temelini oluşturur ve fiziksel esenliğimiz kadar önemlidir. Bir başka perspektiften ele alındığında, esenlik, yaşamdaki kapsamlı bir denge, doyum ve memnuniyet durumudur. İkisi arasındaki ilişki, kişinin zihinsel sağlığının fiziksel sağlığı üzerinde nasıl önemli bir etkiye sahip olduğuna ve bunun tersinin de

geçerli olmasına dayanmaktadır. Stresi kontrol ederek, engelleri aşarak ve daha tatmin edici ve anlamlı bir yaşamla sonuçlanan sağlıklı ilişkiler kurarak pozitif zihinsel sağlığımızı geliştirdiğimiz zaman bir bütün olarak esenliğimiz de artar. Diğer yandan, iyi olma duygusu, yılmazlığı, duygusal istikrarı ve yaşamdaki zorluklarla daha iyi başa çıkma becerisini geliştirerek zihinsel sağlığı büyük ölçüde iyileştirebilir. Ruh sağlığımız ve esenliğimiz arasındaki ilişkiye odaklanarak mutlu ve müreffeh bir yaşam yaratabiliriz.

Teknolojideki hızlı gelişmeler ve günlük yaşamlarımıza yaygın etkisi nedeniyle, dijital çağda zihinsel sağlık karmaşık ve dinamik bir nitelik kazanmaktadır. Dijital çağ bağlamında kişinin zihinsel ve duygusal esenliği, "dijital zihinsel sağlık" ile nitelendirilebilir. Dijital zihinsel sağlık, sosyal medyayı, çevrimiçi etkileşimleri, dijital teknolojilerin psikolojik etkilerini ve modern yaşamı tanımlayan sürekli bağlılığı içerir. Teknoloji pek çok avantaj ve fırsat yaratmış olmasına rağmen zihinsel sağlık açısından önemli zorluklar da yaratmıştır. Sanal iletişimi devam ettirmesine rağmen, dijital çağ, internet bağımlılığı, siber zorbalık, aşırı bilgi yüklemesi, sosyal karşılaştırma ve izolasyon hissi gibi sorunlara yol açabilmektedir. Bununla birlikte dijital çağ, zihinsel sağlık uygulamaları, çevrimiçi terapi ve sanal destek grupları gibi zihin sağlığı yönetimine yönelik en ileri yaklaşımları da sağlar. Çevrimiçi ve çevrimdışı yaşamlarımız arasında sağlıklı bir denge kurmak, ne kadar dijital medya tükettiğimizin farkında olmak ve potansiyel tuzaklara karşı kendimizi korurken zihinsel sağlığımızı geliştirebilecek dijital araçları aktif olarak aramak, dijital dünyanın karmaşıklıklarını aşabilmek açısından oldukça önemlidir.

Günümüzde zihinsel sağlık ile dijital esenlik arasında derin bir ilişki bulunmaktadır. Bireylerin ruh hali, düşünceleri, duyguları ve davranışları gibi faktörleri kapsayan psikolojik ve duygusal esenlikleri, zihinsel sağlıkları ile ilişkilidir. Öte yandan dijital esenlik, kişinin teknolojiyi kullanırken ve dijital ilişkilere girerken hissettiği denge ve uyumu tanımlamaktadır. Dijital çağın bağlantıları, bilgiye erişimi ve kişisel gelişim fırsatlarını mümkün kılmak gibi birçok faydası bulunmaktadır. Ancak teknolojinin aşırı kullanımı, sürekli bildirimler, sosyal medya baskısı ve aşırı bilgi yüklemesi gerginlik, endişe ve gerçeklikten ayrılma hissine neden olarak bireylerin zihinsel sağlığını olumsuz yönde etkileyebilir. Öte yandan sınırlar koyarak, düzenli olarak ekranlara ara vererek ve dijital tüketime dikkat ederek dijital esenliğe öncelik vermek zihinsel sağlık üzerinde olumlu bir etki uyandırabilir. Hem zihinsel sağlığı hem de dijital esenliği desteklemek ve sanal ve gerçek yaşamlarımız arasında uyumlu bir birlikteliği garanti altına almak amacıyla, dijital katılımlarımız ile çevrimdışı etkinliklerimiz arasında sağlıklı bir denge kurmak oldukça önemlidir. Dijital çağda daha anlamlı ve dengeli bir yaşam, teknolojiyi bilinçli olarak benimseyerek ve zihinsel sağlığı geliştirmek için dijital araçları kullanarak başarılabilir.

### *2.3.2. Dijital Esenliğe Neden İhtiyaç Duyarız?*

Dijital esenliğin temel itici güçleri, yaşam kalitesi, iletişim, üretkenlik ve başarı, zihinsel ve fiziksel sağlıktır. Kişinin sağlıklı, mutlu ve memnun olma durumunu bir bütün olarak kapsadığından dijital esenlik oldukça önemlidir. İnsanların ve toplulukların sosyal, psikolojik ve fiziksel yönleri bağlamında genel sağlıkları ile ilişkilidir. Cep telefonu, sosyal medya ve video

oyunlarının aşırı veya sağlıksız kullanımı zihinsel sağlığa zarar verebilir. Kaygı, umutsuzluk, yalnızlık ve zayıf özsaygı; ekranda aşırı vakit geçirmek, sosyal medyada başkalarıyla sık sık karşılaştırılmak veya siber zorbalık gibi faktörlerin de etkisiyle daha da artabilir. Bu bakımdan dijital esenlik, bireylerin kendi yaşamı üzerinde kontrol sahibi olmalarının yoludur. Zihinsel sağlığı ve dijital esenliği desteklemek ve geliştirmek amacıyla teknolojiyle sağlıklı bir bağlantıya sahip olmak oldukça önemlidir. Cihaz kullanımına sınırlar koymak, dijital detokslara katılmak, çevrimdışı etkinliklere katılmak, kişisel bakım ve yüz yüze etkileşimlere öncelik vermek dijital esenliğin önemli bir parçası olabilir. Dijital teknolojinin zihinsel sağlığımız üzerindeki etkisinin farkında olmalı ve bilinçli kullanımını sağlamak için ileriye dönük önlemler almalıyız.

Dijital esenlik, özellikle COVID-19 salgınının ardından dijital çağda temel bir insan ihtiyacı haline geldi. Teknoloji, iletişim ve eğitimden istihdam ve eğlenceye kadar günlük yaşamımızın her alanını istila etmeye devam ettikçe dijital platformlara olan bağımlılığımız da dolaylı olarak arttı. Salgın, dijitalleşmenin benzeri görülmemiş bir hızla ilerlemesine, uzaktan emeğe, çevrimiçi eğitime ve daha fazla sanal ilişkiye yönelik talebin artmasına neden oldu. Sonuç olarak dijital esenliğimizi korumak, tatmin edici ve sağlıklı bir yaşam sürmek için oldukça önemlidir. Dijital esenliğin temel bir insan ihtiyacı olduğunu kabul ederek, hızla değişen bu dijital ortamda teknolojiyi genel esenliğimize tehdit olarak görmek yerine yaşamlarımızı iyileştirmesini sağlamak için teknolojiyi bilinçli ve sorumlu bir şekilde kullanabiliriz.

### *2.3.3. İyi ve Kötü Dijital Esenlik*

Dijital esenlik, dijital dünyanın çeşitli yönlerini kapsayan kapsamlı bir terimdir. Bir yandan bireylerin fiziksel, psikolojik ve sosyal açıdan sağlıklı olmaları, diğer yandan kendilerini dijital ortamda bilinçli, dengeli, güvende, tatmin olmuş ve sağlıklı hissetmeleri ile ilişkilidir. Görüldüğü gibi "dijital esenlik" terimine yüklenen anlam çoğunlukla dijitalleşmenin olumlu yönüne, yani iyi dijital esenliğe işaret etmektedir. Buna karşın, bireylerin dijital esenliği düşük düzeyde deneyimlemeleri, kötü dijital esenlik anlamına gelir. Bu bakış açısı göz önünde bulundurularak, aşağıdaki hususların iyi dijital esenliğin ana göstergeleri arasında olduğu ileri sürülebilir:

- Dijital güvenlik: Dijital güvenliğin sağlanması kişinin dijital esenliğine kayda değer bir katkı sağlar. Dijital güvenlik, kimliğiniz, verileriniz ve varlıklarınız dahil olmak üzere çevrimiçi varlığınızın korunmasını kapsar.
- Dijital emniyet: Bireylerin dijital dünyadaki potansiyel risklerin farkında olması ve dijital ortamdaki çeşitli tehditleri eleştirel bir şekilde tanımlama ve yönetme becerileri ile ilişkilidir.
- Dijital denge: Teknolojiden ve dijital dünyadan bilinçli olarak faydalanmayı ifade eder. Dijital denge, dijital dünyayı, dijital araç ve gereçleri her şey için değil, belirli yaşam alanları için kullanmakla ilgilidir. Düzenli ve tutarlı bir çevrimiçi/çevrimdışı dengesi ve teknolojiye aşırı bağımlı olmaktan kaçınmak, iyi dijital dengenin işaretleridir.

- Dijital bağımsızlık: Çevrimiçi olarak geçirilen zamanı kontrol edebilme ve dijital dünyayı kişinin günlük yaşamının odağında tutmama becerisidir. Çevrimiçi olarak çok fazla zaman geçirmek ve aşırı internet kullanımı nedeniyle daha az sosyal etkinlik planlamak dijital bağımlılığın bazı belirtileridir.
- Dijital doyum: Dijital araç ve gereçlerden faydalanarak, teknolojiyle bütünleşerek doyuma ulaşmayı ve haz duymayı ifade eder.
- Dijital fırsat: Dijital teknolojilerin yaygınlaştırılmasıyla ilgili her türlü yeni olasılığın ortaya çıkarılması ve yeni fırsatlar oluşturmak için daha yeni yetkinliklerin kazanılması amacıyla teknolojiden ve dijitalleşmeden yararlanma ile ilişkilidir.
- Teknolojinin eleştirel ve sorumlu kullanımı: Teknoloji, sunduğu fırsatların yanı sıra, kullanıcıların kendi haklarını koruyarak ve başkalarının haklarına saygı göstererek sorumlu davranmasını, hesap verebilir ve dikkatli olmasını, dijital dünyadaki her türlü içeriğe karşı eleştirel düşünmesini gerektirmektedir.

Bu yönler aynı zamanda dijital esenliğin önemli bazı boyutları olarak da düşünülebilir. Bir kişi, dijital araç ve ekipmanları kullanırken görece daha yüksek düzeyde bir dijital güvenliğe, emniyete, dengeye, bağımsızlığa, tatmine, fırsatlara ve/veya teknolojiyi eleştirel ve sorumlu bir şekilde kullanma eğilimine sahipse, iyi bir dijital esenliğe sahip olduğu düşünülebilir. Aksine, eğer kişi yukarıdaki bileşenlerden bazılarına sahip değilse, bu onun kötü bir dijital esenliğe sahip olduğu anlamına gelir. Bir kişinin fiziksel, psikolojik ve sosyal açıdan sağlıklı olmasının aynı zamanda iyi bir dijital refah ile ilişkili olduğunu ve bu tip faktörlerin bireylerin dijital esenliğine ve genel esenliğine potansiyel bir katkıya sahip olduğunu hatırlamak önemlidir.

### *2.3.4. Bireylerin Dijital Esenliğini Geliştirmek: Herkese ve Yetişkin Eğitimine Yönelik Faydalar*

Yetişkin eğitiminde dijital esenliği teşvik etmek veya yetişkinlerin esenliğini ve dijital yılmazlığını güçlendirmek çeşitli faydalar sağlamaktadır. Her şeyden önce, esenlik temel bir insan ihtiyacıdır. Özellikle COVID-19'dan sonra, çoğu insan internette çok daha fazla vakit geçirmekte ve teknolojiyle, riskleri ve tehditleriyle daha fazla karşı karşıya kalmaktadır. İnsanlar kasıtlı olarak isteseler de istemeseler de benliklerini iş yaşamına yansıtmaktadır. Yani, insanların kendi esenliği ile çalışma ortamındaki atmosfer arasında açık bir bağlantı bulunmaktadır. Dolayısıyla bireylerin esenliğini ve dijital esenliğini geliştirmeye yönelik potansiyel eylemler hem onlara hem de çalıştıkları kuruluşlara önemli bir katkıda bulunur. Örgütsel açıdan ele alındığında, çalışanların dijital esenliğini desteklemek ekip performansına, bağlılığa, yenilikçiliğe, memnuniyete ve burada sayılmayan birçok faktöre katkıda bulunur. Dijital esenlik, bireylerin odaklanmalarını kolaylaştırır, katılımcı ve üretken olmalarını sağlar, bu da hem iş ortamının içinde hem de dışında daha sağlıklı yaşamlara katkıda bulunmaktadır. Çalışanların dijital sağlıklı yaşam uygulamalarını benimsemesi, daha az yorulmalarını ve dikkatlerinin daha az dağılmasını sağlamaktadır. Dijital esenliği destekleyen eylemlerin teşvik edilmesi, bireylerin iş-yaşam dengesini güçlendirmektedir. Ayrıca dijitalleşmeye aşırı maruz kalmanın olumsuz etkilerini ortadan kaldırarak kaygı, umutsuzluk, stres vb. duyguların daha az yaşanmasını sağlamaktadır.

Yetişkin eğitimi bağlamında esenlik fikri, geleneksel akademik başarı fikirlerinin ötesinde bir fikirdir ve öğrenenlerin genel sağlığını ve tatminini kapsamaktadır. Dijital çağın ilerlemesi ile birlikte, özellikle mobil bir yaşam tarzı yaşarken büyük ölçüde teknolojiye güvenen dijital göçebeler için "dijital esenlik" kavramının önemi daha da artmıştır. Yetişkin eğitiminde "dijital esenlik" terimi, öğrenenlere interneti duyarlı ve etik bir şekilde kullanmaları için ihtiyaç duydukları bilgi ve becerilerin sağlanmasını kapsar. Dijital göçebeler sıklıkla kişisel ve profesyonel yaşamlarını dengelemek ve yalnızlık duygularının üstesinden gelmek gibi belirli zorluklarla karşılaştıklarından, dijital esenliği teşvik etmek başarılı bir öğrenme ortamı yaratmak için oldukça önemlidir. Dijital esenliği yetişkin eğitimine entegre etmek, öğrencilere ekran başında geçirdikleri süreyi nasıl doğru şekilde kontrol edeceklerini, olumlu çevrimiçi topluluklar oluşturmayı ve dijital kullanımlarına ilişkin farkındalığı nasıl sürdüreceklerini öğretmeyi gerektirir. Ayrıca bu entegrasyon süreci, siber güvenlik, dijital yorgunluk ve veri gizliliği gibi konuları da kapsamaktadır. Günümüzün dijital odaklı dünyasında, eğitimciler, yetişkin eğitiminde dijital esenliğin güçlendirilmesine yönelik açık ihtiyacı gözeterek ve dijital göçebeler ile diğer öğrencilere, dijital etkileşimleri ile genel eğitim arasında sağlıklı bir dengeyi koruyacak araçları sağlayarak olumlu ve zenginleştirici bir öğrenme deneyimi sağlayabilirler.

Dijital esenliği yetişkin eğitimine başarılı bir şekilde entegre etmek dikkatli ve kapsamlı bir strateji gerektirir, çünkü bu karmaşık ve sürekli bir süreçtir. İlk ve en önemli adım, yetişkin öğrenenlere dijital esenliğin değerinin ve dijital esenliğin sağlık ve üretkenliklerini nasıl etkilediğinin farkında olmalarını sağlayacak eğitimler vermektir. Bu eğitim sayesinde dijital dünyada duyarlı ve güvenli bir şekilde gezinmek için gerekli pratik becerileri kazanırlar. İkinci aşama, öğretim materyallerini dijital esenlik kavramının içeriğini yansıtacak şekilde değiştirmektir. Bu süreç, dikkat dağıtıcı dijital unsurların kontrol edilmesi, çevrimiçi gizlilik, dijital görgü kuralları ve dijital okuryazarlık gibi fikirlerin dahil edilmesini gerektirir. Yetişkin öğrenenler teknolojinin avantaj ve dezavantajlarını daha iyi kavrayabilir ve bu özelliklerin eğitim sürecine dahil edilmesi ile teknolojiyi etkili bir şekilde kullanmayı öğrenebilirler. Öğrenenlerin deneyimlerini ve öğrenme tekniklerini paylaşabilecekleri, seminerler ve konuşmalar gibi ek güçlendirme etkinlikleri tasarlayarak dijital esenliğe olan bağlılıklarını yeniden teyit edebilecekleri destekleyici bir ortam yaratılabilir. Dijital çağda esenliği artırmada anlamlı ve etkili olabilmesi ve hızla değişen dijital ortama ayak uydurabilmesi için, yetişkin eğitimi süreçlerinin sürekli olarak geliştirilmesi gerekmektedir.

# 3. Dijital Güvenlik

## 3.1 Dijital Güvenlik ve Siber Güvenlik

Ekonomik İşbirliği ve Kalkınma Örgütü'ne (OECD) göre, **dijital güvenlik**, dijital çağda güven için esastır. OECD, 1990'ların başından bu yana, dijital güvenlik alanında uluslararası işbirliğini kolaylaştırmakta ve politika analizleri ve öneriler geliştirmektedir. Bu alandaki çalışmalar, bilgi ve iletişim teknolojilerinin (BİT) yenilikçiliği, rekabetçiliği ve büyümeyi destekleme potansiyelini engellemeden güveni güçlendiren politikaları geliştirmeyi ve teşvik

etmeyi amaçlamaktadır. Dijital güvenlik, siber güvenliğin teknik yönleri, ceza hukukunun uygulanması veya ulusal ve uluslararası güvenlikle ilgili yönlerinin aksine, daha çok ekonomik ve sosyal yönlerini ifade eder. "Dijital" terimi dijital ekonomi, dijital dönüşüm, dijital teknolojiler gibi ifadelerle tutarlılık göstermektedir. Güveni artırmayı ve BİT fırsatlarını en üst düzeye çıkarmayı amaçlayan paydaşlar arasında yapıcı uluslararası diyalog için bir temel oluşturur[1].

**Dijital güvenlik** ve **siber güvenlik** birbiriyle ilişkili olmakla birlikte aynı anlama gelmemektedir. Her ikisi de dijital varlıkları ve bilgileri yetkisiz erişime, kullanıma veya hasara karşı korumayı içerir, ancak kapsam ve odak açısından farklılık gösterirler.

**Dijital güvenlik**, dijital verileri, bilgileri ve varlıkları yetkisiz erişime, hırsızlığa veya hasara karşı koruma uygulamalarını ifade eder. Bilgisayarlar, akıllı telefonlar, tabletler ve diğer dijital teknolojiler dahil olmak üzere çeşitli dijital platformlar ve cihazlardaki verileri ve bilgileri koruyan daha geniş bir güvenlik önlemleri yelpazesini kapsar.

Dijital güvenlik önlemleri şunları içerebilir:

- Şifre koruması: Çevrimiçi hesaplar ve cihazlar için güçlü ve benzersiz şifreler oluşturma.
- Veri şifreleme: Yetkisiz erişimi veya veri ihlallerini önlemek için verileri kodlamak.
- Güvenli iletişim: Güvenli veri iletimi için şifreleme protokollerinin kullanılması.
- Erişim kontrolleri: Hassas verilere erişimi sınırlamak için izin ve kısıtlamaların uygulanması.
- Cihaz güvenliği: Kaybolan veya çalınan cihazlar için ekran kilitleri ve uzaktan silme gibi özelliklerin kullanılması.

**Siber güvenlik**, dijital güvenliğin bir alt kümesidir ve özellikle dijital varlıkları siber tehditlerden ve saldırılardan korumaya odaklanır. Dijital sistemlere, ağlara ve altyapılara yetkisiz erişime, hasara veya kesintiye karşı savunmayı içerir.

Siber güvenlik önlemleri şunları içerebilir:

- Güvenlik duvarı koruması: Ağa yetkisiz erişimi önlemek için bariyerlerin kurulması.
- İzinsiz giriş tespit sistemleri: Şüpheli faaliyetler ve potansiyel tehditler açısından ağların izlenmesi.
- Kötü amaçlı yazılımdan koruma: Kötü amaçlı yazılımları tespit etmek ve kaldırmak için antivirüs yazılımının kullanılması.
- Olay müdahale planlaması: Siber güvenlik olaylarına etkili bir şekilde müdahale etmek için protokoller geliştirmek.
- Siber tehdit istihbaratı: Siber tehditleri tahmin etmek ve önlemek için bilgi toplamak ve analiz etmek.

[1] https://www.oecd.org/digital/digital-security/

Dijital güvenlik, dijital alandaki verileri ve bilgileri koruyan daha geniş bir uygulama yelpazesini kapsarken, siber güvenlik, dijital sistem ve ağlardaki siber tehditlere ve saldırılara karşı savunmaya odaklanan uzmanlaşmış bir alandır. Her ikisi de dijital varlıkların ve bilgilerin genel güvenliğinin ve korunmasının sağlanmasında önemli bileşenlerdir.

## 3.2. Yetişkinlerin Karşılaştığı Siber Güvenlik Tehditleri

Yetişkinler günümüzün dijital dünyasında çok çeşitli siber güvenlik tehditleriyle karşı karşıyadır. Yetişkinlerin sıklıkla karşılaştığı bazı yaygın siber güvenlik tehditleri şunlardır:

- ***Kimlik Avı Saldırıları:*** Kimlik avı, siber suçlular tarafından bireyleri oturum açma bilgileri, kredi kartı numaraları veya kişisel veriler gibi hassas bilgileri sağlamaları için kandırmak amacıyla kullanılan bir tekniktir. Kimlik avı e-postaları, mesajları veya web siteleri güvenilir kaynaklardan geliyormuş gibi görünebilir ancak kullanıcıları kandırarak bilgilerini ifşa etmeyi amaçlamaktadır.
- ***Kötü Amaçlı Yazılım:*** Kötü amaçlı yazılım, bilgisayar sistemlerine sızmak, zarar vermek veya yetkisiz erişim sağlamak için tasarlanmış yazılımdır. Kötü amaçlı yazılım türleri arasında virüsler, fidye yazılımları, casus yazılımlar ve Truva atları bulunur. Kötü amaçlı yazılım, kötü amaçlı e-posta ekleri, virüslü web siteleri veya güvenliği ihlal edilmiş yazılımlar aracılığıyla yayılabilir.
- ***Kimlik Hırsızlığı:*** Siber suçlular, kimlik hırsızlığı yapmak için Sosyal Güvenlik numaraları, doğum tarihleri veya finansal veriler gibi kişisel bilgileri çalabilir. Bu bilgiler genellikle veri ihlalleri veya kimlik avı girişimleri yoluyla elde edilir.
- ***Çevrimiçi Dolandırıcılıklar:*** Piyango dolandırıcılıkları, aşk dolandırıcılıkları, sahte teknik destek dolandırıcılıkları ve hileli yatırım planları gibi yetişkinleri hedef alan çok sayıda çevrimiçi dolandırıcılık türü vardır. Dolandırıcılar, bireyleri para göndermeye veya kişisel bilgilerini sağlamaya yönlendirmek için çeşitli taktikler kullanır.
- ***Veri İhlalleri:*** Veri ihlalleri, şirketlerin veya kuruluşların elinde bulunan hassas bilgilerin açığa çıkması veya çalınması durumunda ortaya çıkar. Bir yetişkin olarak, kişisel bilgilerinizin etkilenen kuruluşlar tarafından saklanması durumunda veri ihlallerinden etkilenebilirsiniz.
- ***Sosyal Mühendislik:*** Sosyal mühendislik, bireyleri gizli bilgileri ifşa etmeleri veya belirli eylemleri gerçekleştirmeleri için manipüle etmeyi içerir. Siber suçlular, sistemlere veya hesaplara yetkisiz erişim sağlamak için sosyal mühendislik tekniklerini kullanabilir.
- ***Şifre Saldırıları***: Zayıf şifreler veya şifrelerin yeniden kullanılması, siber suçluların yetkisiz erişim elde etmek için şifreleri tahmin etmeye veya kırmaya çalıştığı kaba kuvvet saldırıları veya sözlük saldırıları gibi şifre saldırılarına yol açabilir.

- ***Genel Wi-Fi Riskleri:*** Halka açık Wi-Fi ağlarının kullanılması, yetişkinleri güvenlik risklerine maruz bırakabilir; çünkü bu ağlar uygun şifrelemeye sahip olmayabilir ve saldırganların gizlice dinlenmesine açık olabilir.
- ***İçeriden Gelen Tehditler:*** İçeriden gelen tehditler, kasıtlı veya kasıtsız olarak zarara neden olan veya hassas bilgilerin sızdırılmasına neden olan, sistemlere veya verilere yetkili erişime sahip çalışanları veya kişileri içerir.
- ***IoT Güvenlik Açıkları:*** Nesnelerin İnterneti (Internet of Things - IoT) cihazlarının giderek daha fazla benimsenmesi, bu cihazların birçoğunun yetersiz güvenlik önlemlerine sahip olabileceği ve siber suçlular tarafından istismar edilebileceği için siber güvenlik riskleri oluşturabilir.

Bu tehditlere karşı korunmak için yetişkinlerin güçlü ve benzersiz şifreler kullanmak, çok faktörlü kimlik doğrulamayı etkinleştirmek, yazılım ve cihazları güncel tutmak, şüpheli e-posta ve bağlantılara karşı dikkatli olmak ve internette paylaşılan bilgiler konusunda dikkatli olmak dahil olmak üzere iyi siber güvenlik hijyeni uygulamaları gerekir. Düzenli siber güvenlik farkındalığı eğitimi, bireylerin ortaya çıkan tehditler ve çevrimiçi ortamda güvende kalmaya yönelik en iyi uygulamalar hakkında bilgi sahibi olmalarına da yardımcı olabilir. Bir sonraki bölümde yetişkinlerin siber güvenlik tehditlerine kurban gitme riskini azaltmak ve dijital kimliklerini ve varlıklarını korumak için en temel dijital güvenlik uygulamalarından bazıları ayrıntılı olarak sunulmaktadır.

## 3.3. Yetişkinler için Dijital Güvenlik Pratikleri

Yetişkinlerin kişisel bilgilerini, verilerini ve çevrimiçi hesaplarını siber güvenlik tehditlerinden korumaları için dijital güvenlik uygulamaları gereklidir. Yetişkinlerin izlemesi gereken bazı önemli dijital güvenlik uygulamaları şunlardır:

- ***Güçlü ve Benzersiz Şifreler Kullanın:*** Yetişkinler çevrimiçi hesapları için güçlü ve benzersiz şifreler oluşturmalıdır. "123456" veya "şifre" gibi kolayca tahmin edilebilecek şifreler kullanmaktan kaçının. Karmaşık şifreleri güvenli bir şekilde oluşturmak ve saklamak için bir şifre yöneticisi kullanmayı düşünün.
- ***Çok Faktörlü Kimlik Doğrulamayı (MFA) Etkinleştirin:*** Mümkün olduğunda çevrimiçi hesaplarınızda çok faktörlü kimlik doğrulamayı etkinleştirin. MFA, şifrenize ek olarak mobil cihazınıza tek seferlik kod gönderilmesi gibi ikinci bir doğrulama biçimini zorunlu kılarak ekstra bir güvenlik katmanı ekler.
- ***Yazılım ve Cihazları Güncel Tutun:*** İşletim sisteminizi, web tarayıcılarınızı ve yazılım uygulamalarınızı düzenli olarak güncelleyin. Güncellemeler genellikle bilinen güvenlik açıklarını gideren güvenlik yamalarını içerir.
- ***E-postalar ve Bağlantılar Konusunda Dikkatli Olun:*** Bilinmeyen gönderenlerden gelen e-postaları açarken veya şüpheli bağlantılara tıklarken dikkatli olun. Hassas

bilgiler isteyen veya sizi sahte bir web sitesinde oturum açmaya yönlendiren e-postalara karşı özellikle dikkatli olun.

- ***Ev Ağınızı Güvenli Hale Getirin:*** Ev Wi-Fi yönlendiricinizdeki varsayılan şifreyi değiştirin ve kablosuz ağınızı korumak için WPA2 veya WPA3 şifrelemesini etkinleştirin. Sanal özel ağ (VPN) kullanmadığınız sürece, hassas etkinlikler için genel Wi-Fi ağlarını kullanmaktan kaçının.
- ***Verileri Düzenli Olarak Yedekleyin:*** Önemli dosyalarınızı ve verilerinizi düzenli olarak harici bir sabit sürücüye, bulut depolama alanına veya güvenli bir yedekleme hizmetine yedekleyin. Veri kaybı veya fidye yazılımı saldırıları durumunda, yedek almak dosyalarınızı kurtarabilmenizi sağlar.
- ***Güvenli Wi-Fi ve HTTPS Kullanın:*** Hassas web sitelerine erişirken HTTPS şifrelemesi kullandıklarından emin olun. Web sitesinin güvenliğini doğrulamak için tarayıcının adres çubuğundaki asma kilit simgesini arayın.
- ***Sosyal Medyaya Dikkat Edin:*** Sosyal medya platformlarında paylaştığınız bilgilere dikkat edin. Adresiniz, telefon numaranız veya seyahat planlarınız gibi kişisel ayrıntıları paylaşmaktan kaçının çünkü bu bilgiler sosyal mühendislik saldırıları için kullanılabilir.
- ***Antivirüs ve Güvenlik Yazılımını Kurun:*** Kötü amaçlı yazılımlara ve diğer tehditlere karşı koruma sağlamak için cihazlarınızda saygın antivirüs ve güvenlik yazılımı kullanın. Optimum korumayı sağlamak için yazılımı güncel tutun.
- ***Kendinizi Siber Güvenlik Konusunda Eğitin:*** Saygın kaynakları okuyarak, web seminerlerine katılarak veya siber güvenlik farkındalık programlarına katılarak en son siber güvenlik tehditleri ve en iyi uygulamalar hakkında bilgi sahibi olun (Lütfen yetişkinlere yönelik dijital güvenlik kaynaklarına bakın).

Yetişkinler, bu dijital güvenlik uygulamalarını günlük rutinlerine dahil ederek siber güvenlik tehditlerinin kurbanı olma riskini önemli ölçüde azaltabilir ve dijital kimliklerini ve varlıklarını koruyabilirler.

## 3.4. Yetişkinlere Yönelik Dijital Güvenlik Kaynakları

Kaliforniya Eyalet Üniversitesi'nin San Marcos'taki Siber Güvenlik Eğitim Merkezi[2] (CEH), dijital güvenlik eğitimi ve farkındalığını artırmaya yönelik kaynaklar ve yönlendirmeler sunar. CEH, Kampüs Bilgi Güvenliği Ofisi, Fen ve Matematik Yüksekokulları ve İşletme Yönetiminin ortak bir çabasıdır.

CEH, kampüs dijital güvenlik eğitim programlarının dijital güvenlik alanındaki güncel olaylarla ilgili geniş konuları ele almasını sağlamak için çalışır ve dijital güvenlik konularının üniversite genelinde öğretilen derslere dahil edilmesi için fırsatlar sunar. CEH ayrıca

[2] https://www.csusm.edu/cybersec-hub/index.html

öğrencilere, öğrenci örgütlerine ve genel halka kaynaklar sunmaktadır. Topluluk genelinde dijital güvenlik eğitimi ile iletişimi ve işbirliğini teşvik eder ve kolaylaştırır. Gizlilik ve sosyal medya, öğrenciler için siber güvenlik, günümüz siber güvenliği ve siber güvenlik kavramları gibi konularda öğrenme materyalleri sağlamaktadır.

Ayrıca, 2008 yılında, ENISA[3] Siber Güvenlik Eğitim materyalleri tanıtılmıştır. O zamandan beri Siber Güvenlik alanında başarı için önemli bilgileri içeren yeni bölümlerle genişletilmiştir. ENISA, uygulamalı eğitim oturumlarını desteklemek için öğretmen el kitapları, öğrenci araç setleri ve sanal görüntüler gibi eğitim materyalleri içerir.

# 4. Yetişkinler İçin Dijital Güvenliği Sağlamanın En İyi Uygulamaları

Bağlantı halindeki (çevrimiçi) toplumumuzda dijital güvenlik giderek daha önemli hale gelmektedir ve görece yaşlılar çevrimiçi ortamda en savunmasız gruplardan biridir. Teknoloji ilerledikçe siber tehditler de artmaktadır. Bu nedenle yaşlı yetişkinleri dijital ortamda korumaya yönelik önlemler ve yönergeler oluşturmak önemlidir. Aşağıda, çeşitli ülkelerde uygulanan ve diğerlerine referans olabilecek bazı iyi uygulamalar ve başarılı eylemler yer almaktadır.

Avrupa Birliği'nin Siber Güvenlik Stratejisi, tamamı Avrupa Komisyonu'nun resmî web sitesinde bulunan ve Avrupa'da dijital güvenliği iyileştirmeye yönelik en iyi uygulamalara ilişkin değerli bilgiler sağlayan raporlarda temsil edilmektedir.

## 4.1. Dijital Güvenliği Sağlamada Temel Konular

Bu bölüm, Bölüm 3.3'ün (Yetişkinler için Dijital Güvenlik Pratikleri) tekrarı gibi görünebilir, ancak daha fazla gerçek dünya senaryosu ve örneği içermektedir.

***Güçlü Şifreler:*** Her hesap için güçlü ve benzersiz şifreler oluşturmalarına yardımcı olun. Şifreler uzun olmalı ve büyük-küçük harfler, rakamlar ve özel karakterler içermelidir. Şifreler uzun olmalı (en az 8 karakter), büyük ve küçük harfler, sayılar ve özel karakterler içermelidir. İsimler veya doğum tarihleri gibi öngörülebilir kişisel bilgileri kullanmaktan kaçının. Şifrelerini kimseyle paylaşmamalarını ve düzenli olarak değiştirmelerini hatırlatın.

Örneğin güçlü bir şifre, büyük harflerin, küçük harflerin, sayıların ve özel karakterlerin birleşiminden oluşan “P@ssw0rd2023!” olabilir. İsimler veya doğum tarihleri gibi "John1980" veya "MarySmith123" gibi öngörülebilir kişisel bilgileri kullanmaktan kaçının.

[3] https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material

***Eğitim ve Farkındalık:*** Kimlik avı, kötü amaçlı yazılım ve kimlik hırsızlığı gibi çevrimiçi riskler ve tehditler hakkında onları bilgilendirin. Bu durumları nasıl tanıyıp önleyeceklerini anlamalarına yardımcı olun. Kimlik avı (gizli bilgileri hileli yollarla elde etme girişimleri), kötü amaçlı yazılım (kötü amaçlı yazılım) ve kimlik hırsızlığı gibi çevrimiçi riskler konusunda onları eğitmek önemlidir. Bu uyarı işaretlerini tanımayı öğrenin ve bu tuzaklara düşmekten kaçının. Olası olumsuz etkileri ve kendinizi nasıl koruyacağınızı açıklayın.

Örneğin, kimlik avı e-postalarının yasal kaynaklardan geliyormuş gibi görünebileceğini açıklayın ve bu kaynakların onlardan bağlantılara tıklamalarını ve hassas bilgileri girmelerini isteyebileceklerini bildirin. Onlara şüpheli e-posta örneklerini ve bunları nasıl tanıyabileceklerini gösterin. Sahte antivirüs yazılımı veya pop-up'lar gibi yaygın kötü amaçlı yazılım türleri ve bunlardan nasıl kaçınılacağı hakkında bilgi verin.

***İki Faktörlü Kimlik Doğrulama (2FA):*** Mümkünse iki faktörlü kimlik doğrulamayı uygulamalarına yardımcı olun. Bu, hesaplarınıza ekstra bir güvenlik katmanı ekler. İki faktörlü kimlik doğrulama ekstra bir güvenlik katmanıdır. Mümkünse bu özelliği hesaplarında etkinleştirmelerine yardımcı olun. 2FA, standart bir şifreye ek olarak kısa mesaj kodu, kimlik doğrulayıcı veya parmak izi gibi başka bir kimlik doğrulama yöntemi gerektirir.

Örneğin, şifrelerini girdikten sonra, hesaplarına erişmek için girmeleri gereken doğrulama kodunu içeren bir kısa mesaj alacaklar. Bu, ekstra bir güvenlik katmanı ekler ve yetkisiz kullanıcıların hesaplarına erişmesini zorlaştırır.

***Mobil Cihazların Güvenli Kullanımı:*** Mobil cihazlarını korumak için ekran kilitleri, yüz tanıma veya parmak izi ayarlamalarına yardımcı olun. Cihazlarını tanımadıkları kişilerle paylaşmamalarını ve güvenilir olmayan kaynaklardan uygulama indirirken dikkatli olmaları gerektiğini hatırlatın.

Örneğin, onlara bir PIN'i nasıl etkinleştireceklerini veya akıllı telefonlarının kilidini açmak için parmak izlerini nasıl kullanacaklarını gösterin. Cihazlarını tanımadıkları kişilerle paylaşmamalarını ve güvenilir olmayan kaynaklardan uygulama indirirken dikkatli olmaları gerektiğini hatırlatın.

***Yazılım Güncellemeleri:*** Cihazlarınızın (bilgisayarlar, tabletler, akıllı telefonlar) en son güvenlik yamalarının ve güncellemelerinin yüklü olduğundan emin olun. Güncellemeler genellikle bilinen güvenlik açıklarına yönelik düzeltmeler içerir; dolayısıyla cihazlarınızı güncel tutmak, onların korunmasına yardımcı olur.

***Online Alışveriş:*** Onlara yalnızca güvenilir ve güvenli sitelerden alışveriş yapmalarını ve güvenli ödeme yöntemlerini kullanmalarını hatırlatın. Onlara adres çubuğunda kilit aramayı ve ekstra güvenlik önlemleri olan kredi kartı gibi güvenli ödeme yöntemlerini kullanmayı öğretin.

***E-postanın Güvenli Kullanımı:*** Kimlik avı konusunda onları uyarın ve bilinmeyen gönderenlerden gelen bağlantılara tıklamaktan veya ekleri indirmekten kaçınmalarını önerin. Dolandırıcıların meşru gönderenler gibi görünerek hassas bilgiler elde etmeye çalıştığı e-posta kimlik avı konusunda onları uyarın. Bu, şüpheli e-postalardan veya bilinmeyen gönderenlerden gelen bağlantılara tıklamamanın veya ekleri indirmemenin önemini vurgulamaktadır. Gizli bilgileri göndermeden önce e-postaların meşruiyetini gönderenle doğrulamanızı ister.

***Sosyal Medya:*** Gönderilerini kimlerin göreceğini kontrol etmek ve hassas kişisel bilgileri paylaşmaktan kaçınmak için sosyal medyalarındaki gizlilik ayarlarını düzenlemelerine yardımcı olun. Onlara telefon numaraları, adresler veya finansal bilgiler gibi hassas bilgileri sosyal medyada halka açık olarak paylaşmaktan kaçınmalarını öğretin.

Örneğin, gönderilerini yalnızca arkadaşlarıyla görebilecek kişileri kısıtlamak için onlara Facebook'taki gizlilik ayarları konusunda rehberlik edin. Telefon numaraları, adresler veya finansal ayrıntılar gibi bilgilerin sosyal medya platformlarında paylaşılması konusunda dikkatli olmanın önemini vurgulayın.

***Güvenli Dolaşım:*** Güvenli web sitelerini ("https" ve "kilit") tanımayı öğrenin ve şüpheli bağlantılara tıklamaktan veya bilinmeyen dosyaları indirmekten kaçının. Adres çubuklarında kilit olup olmadığını ve başlatılıp başlatılmadıklarını kontrol ederek onlara güvenli web siteleri arasında ayrım yapmayı öğretin. "https" yerine "http". Kötü amaçlı yazılım içerebileceği veya sizi sahte web sitelerine yönlendirebileceği için şüpheli bağlantılara tıklamaktan veya bilinmeyen kaynaklardan dosya indirmekten kaçınmanın önemini açıklayın.

***Wi-Fi Güvenliği:*** Evlerindeki Wi-Fi ağlarında güçlü şifreler kullandıklarından emin olun ve halka açık veya bilinmeyen Wi-Fi ağlarına bağlanmaktan kaçının. Evinizin Wi-Fi ağında güçlü şifreler kullanmanın önemini açıklayın ve halka açık veya bilinmeyen Wi-Fi ağlarına bağlanmaktan kaçının. Güvenli olmayan Wi-Fi ağları, potansiyel olarak saldırıya uğrayabilir veya veri casusluğu amacıyla ele geçirilebilir.

***Etkin Olmayan Hesaplar:*** Güvenlik riskini azaltmak için artık kullanmadıkları çevrimiçi hesapları kapatmalarına veya silmelerine yardımcı olun. Etkin olmayan hesaplar, özellikle kişisel bilgiler içeriyorsa saldırılara karşı savunmasız olabilir.

***Şüpheli Arama ve Mesajlara Dikkat Edin:*** Onlara kişisel veya mali bilgilerini beklenmedik arama veya mesajlara açıklamamalarını öğretin. Beklenmedik aramalara veya kısa mesajlara kişisel veya finansal bilgileri verirken dikkatli olmalarını öğretin. Hassas bilgileri paylaşmadan önce göndereni kimliğini doğrulamaya teşvik edin. Örneğin, sahte teknik destek çağrıları veya piyango kazanma bildirimleri gibi yaygın dolandırıcılıklara örnekler verin.

***Denetim ve Destek:*** Çevrimiçi hesaplarınızın düzenli olarak kontrol edilmesine yardımcı olmayı ve şüpheli faaliyetlerden şüphelenmeleri veya güvenlik sorunları yaşamaları durumunda onlara yardım etmeyi teklif edin. En son çevrimiçi tehditlerle güncel kalın ve sürekli rehberlik ve destek sağlayın. Örneğin onlara çeşitli platformlarda son hesap etkinliklerini ve oturum açma bilgilerini nasıl inceleyeceklerini gösterin.

***Kişisel Bilgiler:*** Onlara kişisel bilgileri çevrimiçi olarak paylaşırken dikkatli olmalarını ve yayınladıkları bilgi miktarını sınırlamalarını öğretin. Adresler, telefon numaraları veya okul bilgileri gibi yayınladıkları bilgilerin miktarını sınırlayın. Bu, gizliliğinizi ve çevrimiçi kimliğinizi korumanın önemini destekler.

***Önemli Verileri Yedekleyin:*** Bir güvenlik ihlali veya cihaz arızası durumunda kaybı önlemek için önemli verileri düzenli olarak yedekleyin.

## 4.2. Dünyadan En İyi Örnekler

### *4.2.1. Siber Avrupa*

ENISA, 2010 yılından bu yana, gerçek yaşamdaki olaylardan ilham alan ve Avrupalı siber güvenlik uzmanları tarafından geliştirilen, heyecan verici senaryolar içeren bir dizi siber olay ve kriz yönetimi tatbikatından oluşan Siber Avrupa'yı (Cyber Europe)[4] düzenlemektedir. Her iki yılda bir, AB ve AEA ülkelerinin kamu ve özel sektörlerinin yanı sıra Avrupa Kurumları, Organları ve Ajansları, mevcut teknik ve operasyonel yeteneklerini güçlendirmek için iş birliği yapmaktadır.

Siber Avrupa tatbikatı iki gün sürmekte ve tüm AB'yi etkileyen siber krizlere dönüşen büyük ölçekli siber güvenlik olaylarını simüle etmektedir. Bu tatbikata katılanlar, gelişmiş teknik siber güvenlik olaylarını analiz edebilecek, yerel düzeyden AB düzeyine kadar koordinasyon ve iş birliği gerektiren karmaşık iş sürekliliği ve kriz yönetimi durumlarıyla baş edebilecektir.

[4] https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme

Siber Avrupa tatbikat serisi, katılımcıların AB çapında hazırlıklı olma durumlarını test etmelerine ve geliştirmelerine, AB siber güvenlik ekosistemi içinde güven oluşturmalarına ve eğitim fırsatları sunmalarına olanak tanıyarak Avrupa'nın büyük ölçekli siber güvenlik olayları ve krizleriyle başa çıkma hazırlıklarını geliştirmeyi amaçlıyor.

Siber Avrupa'ya katılmak aşağıdakiler için mükemmel bir fırsat sağlar:

- Siber farkındalığı artırma
- Siber kriz yönetimi prosedürlerini oluşturma ve/veya teste tabi tutma
- Siber yanıt zinciri içindeki iletişimi iyileştirme
- Ortak bir dil oluşturmak ve birbirinizi daha iyi anlama
- Çeşitli bireysel ve kolektif dayanıklılık becerileri geliştirme
- Karmaşık teknik siber güvenlik olaylarını analiz etme; Karmaşık iş sürekliliği ve kriz yönetimi durumlarını ele alma.

### *4.2.2. Arayüz ve Teknolojinin Uyarlanması*

Japonya, teknoloji ve cihazları görece yaşlı yetişkinler için daha erişilebilir hale getirecek şekilde uyarlamada öncü olmuştur. Örneğin, bazı Japon akıllı telefonları ve tabletleri daha basit kullanıcı arayüzlerine ve geliştirilmiş erişilebilirlik özelliklerine sahiptir; bu da bu aygıtların sınırlı dijital becerilere sahip kişiler için kullanımını kolaylaştırmaktadır. Diğer ülkeler ve teknoloji üreticileri, yaşlı yetişkinlerin dijital cihazları güvenli ve etkili bir şekilde kullanabilmelerini sağlamak için bu tür politikaları benimseyebilir. Bu uygulamaların diğer ülkeler ve teknoloji üreticileri tarafından benimsenmesi, yaşlı yetişkinlerin daha kullanıcı dostu dijital cihazlara erişmesini sağlayarak çevrimiçi güvenliklerini ve katılımlarını artırmaya yardımcı olabilir.

Avrupa topraklarında bu araçların yaşlı yetişkinler tarafından kullanımına ilişkin farkındalığı artırmayı amaçlayan çeşitli kurslar bulunmaktadır. Örneğin, Paris'teki ACDA derneği yaşlıları teknoloji dünyasıyla tanıştırmak için düşük maliyetli kurslar sunuyor. Bu derneğin kursları, bilgisayarın nasıl çalıştırılacağından, yani temel bilgilerden öğrenme fırsatı sunuyor. Bilgisayar birimlerinin, uygulamaların ve dosya formatlarının keşfi öğretiliyor. Bu kursun sonunda katılımcılar, posta kutusunu yönetmek ve düzenlemek ve yazılı bir belgenin nasıl işleneceği konusunda MS Word kullanımını öğrenmek gibi daha ileri beceriler kazanabilmektedir[5].

### *4.2.3. Yardım Hatları ve Özel Destek*

Singapur, dijital güvenlik sorunlarıyla karşı karşıya kalan yaşlılar için kendi yardım hattını kurdu. Bu yardım hattı, siber güvenlik sorunlarını çözmek için tavsiye ve teknik yardım

[5] http://www.aucoursdesages.fr/cours.php

sunmaktadır. Diğer ülkeler, çevrimiçi yardıma ihtiyaç duyan yaşlılara doğrudan ve güvenli bir iletişim kanalı sağlamak amacıyla benzer hizmetleri sunmayı düşünebilir. Bu hizmetler, yaşlı insanlara çevrimiçi dolandırıcılık veya kötü amaçlı yazılım gibi siber güvenlik sorunları konusunda yardım almaları için doğrudan ve güvenli bir iletişim kanalı sağlar. Benzer hizmetlerin diğer ülkelerde de uygulamaya konması, yaşlıların dijital dünyada korunmasında önemli bir destek ağı olabilir.

Örneğin, Avrupa bölgesinde AGE UK derneği[6], dijital dışlanmaya karşı en savunmasız olan yaşlı insanların desteklenmesine öncelik vermektedir.

Yaşlı nüfusa hizmet sağlamanın yanı sıra, kurslar özellikle yüksek risk altındaki bu grubun dijital dünyaya erişmesine yardımcı olmaya odaklanacaktır. Bu yüksek riskli gruplarla çalışırken programın temel bileşenleri büyük ölçüde değişmeden kalacak olsa da programın en çok ihtiyaç duyanlar için erişilebilir ve etkili kalmasını sağlamak amacıyla muhtemelen bazı adaptasyonlar gerekli olacaktır.

Dijital Şampiyon Programındaki yüksek riskli hizmetler aşağıdaki yaşlı yetişkinleri hedef almaktadır:

- Unutkanlık ve/veya hafıza kaybı olanlar
- Düşük gelire sahip olanlar
- Yalnız yaşayanlar
- Hareketlilik sorunları olanlar
- Evden dışarıya çıkamayanlar

### *4.2.4. Farkındalık Kampanyaları ve Eğitim*

Avustralya ve Kanada gibi ülkeler yaşlı yetişkinlere yönelik siber güvenlik kampanyaları ve dijital güvenlik eğitim programları uygulamaya koymuştur. Bu kampanyalar, yaygın siber tehditler hakkında bilgiler, çevrimiçi dolandırıcılıktan kendinizi nasıl koruyacağınızla ilgili ipuçları ve cihazlarınızı güncel tutmanın önemi hakkında bilgi sağlamaktadır. Hükümetler, yaşlı nüfusa ulaşmak ve dijital beceriler konusunda eğitim sağlamak için yerel kuruluşlarla, toplum merkezleriyle ve gönüllü gruplarla ortaklık kurabilmektedir. Bu bilgilendirme ve eğitim kampanyaları, yaşlıları dijital güvenlik eğitimi yoluyla güçlendirmeyi amaçlamaktadır. Çevrimiçi dolandırıcılığı nasıl belirleyip önleyecekleri, kişisel bilgilerini nasıl koruyacakları ve antivirüs ve güçlü parolalar gibi güvenlik araçlarını nasıl kullanacakları öğretilmektedir. Ayrıca sosyal medya kullanımının riskleri ve uygun çevrimiçi gizlilik ayarlarının önemi hakkında da bilgilendirilirler. Yukarıda listelenen Paris'teki ACDA derneği, Dijital Güvenlik alanında da kurslar sunmaktadır.

[6] https://www.ageuk.org.uk/our-impact/programmes/digital-skills/digital-champions/

Dijital farkındalığa odaklanan bir diğer dernek ise kırılgan grupları teknolojideki son gelişmeler hakkında bilgilendiren ve onları daha güvenli dijital kullanıma yönlendiren Orange Vakfı'dır[7].

Ayrıca Orange vakfı, Fransa genelinde gençlere ve genellikle işsiz, nitelik eksikliği olanlar ve bazen de güvencesiz durumda olan kadınlara yönelik bir dizi ücretsiz dijital eğitim kursu düzenlemektedir. Bu insanları dijital beceriler konusunda eğiterek yeniden sosyalleşmelerine, iş aramalarına, dijital teknolojinin profesyonel kullanımlarını benimsemelerine, iş geliştirmelerine ve hatta dijitali meslek haline getirmelerine yardımcı olmaktadır.

### *4.2.5. Mali Koruma Programları*

Birleşik Krallık ve ABD gibi ülkeler[8], emeklileri çevrimiçi mali dolandırıcılıklardan korumaya yönelik politikalar uygulamaya koydu. Bu politikalar, dolandırıcılık mağdurlarına yönelik sorumluluk sınırlarını ve çalınan fonların geri alınmasına yönelik çözümleri içerir. Diğer ülkeler bu girişimleri araştırabilir ve yaşlıları potansiyel mali kayıplara karşı korumak için bunları kendi mali sistemlerine uyarlayabilir. Yaşlı yetişkinlere yönelik mali koruma, dijital güvenliğin önemli bir parçasıdır. Çevrimiçi mali dolandırıcılığı önlemek ve azaltmak için özel olarak tasarlanmış programlar, bu nüfusa daha yüksek düzeyde güvenlik sağlayabilir. Dolandırıcılık mağdurlarının sorumluluklarına sınırlama getirilmesi ve çalınan paranın geri alınmasına yönelik mekanizmalar oluşturulması atılabilecek adımlardır. Bu politikalar yalnızca yaşlı yetişkinlerin mali refahını korumakla kalmıyor, aynı zamanda onların refahının ve mali güvenliğinin ciddiye alındığına dair açık bir mesaj da veriyor.

Avrupa'da Dolandırıcılık mağdurlarının sorumluluklarına sınırlar koymak, yaşlı yetişkinlerin mali refahını korumanın hayati bir yönüdür. Dolandırıcılık mağdurları uğradıkları mali kayıplardan sorumlu tutulduğunda, mali yıkım ve duygusal sıkıntı gibi ciddi sonuçlara yol açabilmektedir. Toplum, sorumluluğa makul sınırlar koyan politikaları uygulayarak, yaşlı yetişkinlerin karşılaştığı benzersiz hassasiyetlerin farkına varır ve üzerlerine yüklenen yükü hafifletmeye çalışır. Bu önlem bir güvenlik ağı oluşturarak yaşlı yetişkinlerin haksız yere dolandırıcılık faaliyetlerinin sonuçlarıyla karşı karşıya kalmamalarını sağlar. Dolandırıcılık mağdurlarının sorumluluklarına sınırlar koymak, yaşlıların mali refahını korumanın önemli bir unsurudur. Avrupa topraklarında birçok dernek, çoğunlukla çevrimiçi dolandırıcılığın kurbanı olan, farkındalığı olmayan ve mali kayıplara maruz kalabilecek yaşlıları korumaya adanmıştır. Bu dernek / birliklerden biri, İspanya ve Fransa'da sertifikalı bir ajans olan Pazarlama Yönetimi IO'dur (MMIO).[9]

Dolandırıcılık mağdurlarının mali kayıplarından sorumlu tutulması ciddi sonuçlara yol açabilir. Bu nedenle bu konuda farkındalık yaratmak oldukça önemlidir. Toplum, sorumluluğa makul sınırlar koyan politikaları uygulayarak, yaşlıların kendilerine özgü hassasiyetlerini tanır

[7] https://fondationorange.com/en/digital-solidarity
[8] https://www.bankofamerica.com/signature-services/elder-financial-services/
[9] https://www.marketing-management.io/blog/formation-digital-marketing

ve onların üzerindeki yükü hafifletmeye çalışır. Bu önlem bir güvenlik ağı sağlayarak yaşlıların dolandırıcılık faaliyetlerinin sonuçları nedeniyle haksız yere yük altına girmemesini sağlar.

Pazarlama Yönetimi IO (MMIO), internet fırsatları, doğal referanslama, çevrimiçi görünürlük, içerik pazarlaması ve satışların artırılması gibi konuları içerir. Kavramlar basitleştirilmiştir ve eylemler ücretsizdir. Bonus kaynakları da bulunmaktadır.

Kurs videolu 5 ders içermektedir. Facebook, 70'in üzerinde çevrimiçi kursa ücretsiz erişim sağlayan bir platform sunmaktadır. Bu kurslar, özellikle çevrimiçi varlığınızı ve ticari satışlarınızı, güvenliğinizi ve farkındalığınızı geliştirmek için Facebook'u kullanmaya odaklanmaktadır.

### *4.2.6. Teknoloji Sektörü ile İş birliği*

Amerika Birleşik Devletleri gibi bazı ülkeler, yaşlanan nüfusla bağlantılı dijital güvenlik sorunlarını çözmek için teknoloji şirketleriyle ortaklık kurmaktadır. Bu iş birliği, güvenlik yazılımının geliştirilmesini, sahtekarlık tespitinin iyileştirilmesini ve dijital ürün ve hizmetlerde güvenlik özelliklerinin uygulanmasını içermektedir. Teknoloji sektörüyle iş birliği, gelişmiş güvenlik teknolojilerinin uygulanması, sahtekarlık tespitinin iyileştirilmesi ve yaşlılara yönelik dijital ürün ve hizmetlere yönelik güvenlik uygulamalarının teşvik edilmesi gibi en son güvenlik tehditleri ve çözümlerinden haberdar olmanın etkili bir yolu olabilir. Teknoloji sektörüyle iş birliği, dijital tehditlere daha hızlı ve güncel yanıt verilmesini sağlar.

Fransa ve İngiltere gibi diğer ülkelerde, yaşlıların savunma teknolojilerini anlamalarına yardımcı olacak dijital güvenlik kursları bulunmaktadır. Sunulan kurslar, yaşlıların dijitalleşme konusunda bir temel oluşturmalarına ve internette güvenli bir şekilde nasıl gezineceklerini anlamalarına olanak tanımaktadır.

Örneğin, Konexio[10], sosyal ve profesyonel entegrasyonu teşvik etmek için en temelden en ileri düzeye kadar dijital beceriler konusunda eğitim sunmaktadır. Yenilikçi, pratik vaka çalışmalarına dayanan ve çapraz ve ilişkisel becerilere veya sosyal becerilere güçlü bir vurgu yapan eğitim kursları, herkesin toplumun dijitalleşmesine dahil olmasını sağlamayı amaçlamaktadır. Bu kurslar şu konularda çeşitli formasyonlar sunarlar: Dijital beceriler, web tasarımcısı, sistem ve ağ teknisyeni, dijital yardımcılar vb. Program, atölye çalışmaları aracılığıyla profesyonel dünyanın sosyal becerilerini ve sosyal kodlarını öğrenmeye odaklanmaktadır. Aynı zamanda ağları aracılığıyla profesyonel dünyayla doğrudan bağlantı kurma fırsatları da sunmaktadır. Öğrenenlerin ilerleme kaydetmesine ve karşılaşabilecekleri zorlukları çözmelerine yardımcı olmak için düzenli takip ve kişiselleştirilmiş destek sunmaktadır.

[10] https://www.konexio.eu/formations.html

### *4.2.7. Uluslararası Kaynaklar, Raporlar ve Girişimler*

Bu kaynaklar, AB'de yetişkin eğitiminde dijital güvenliğin iyileştirilmesine yönelik rehberlik ve en iyi uygulama örneklerini ele almaktadır.

**Açık, Emniyetli ve Güvenli Bir Siber Alan:** Bu rapor [An Open, Safe and Secure Cyberspace], Avrupa'da açık, emniyetli ve güvenli bir siber alanı teşvik etmeyi amaçlayan AB'nin siber güvenlik stratejisine genel bir bakış sunmaktadır. Raporda risk yönetimi, olaylara müdahale ve kamu-özel sektör ortaklıkları da dahil olmak üzere siber güvenliği iyileştirmeye yönelik en iyi uygulamalar yer almaktadır.

**ENISA Tehdit Ortamı Raporu:** Bu rapor [ENISA Threat Landscape Report], Avrupa Birliği Siber Güvenlik Ajansı (ENISA) tarafından hazırlanmıştır ve en yaygın siber saldırı türleri ve en fazla risk altındaki sektörler dahil olmak üzere Avrupa'daki mevcut siber güvenlik tehdit ortamına genel bir bakış sunmaktadır. Raporda, güvenlik farkındalığı eğitimi, güvenlik açığı yönetimi ve olay müdahale planlaması dahil olmak üzere siber saldırıları önlemeye ve azaltmaya yönelik en iyi uygulamalar yer almaktadır.

**NIS Direktifi ve AB Siber Güvenlik Yasası:** Bu rapor [NIS Directive and EU Cybersecurity Act], Ağ ve Bilgi Sistemleri (NIS) Direktifi ve AB Siber Güvenlik Yasası dahil olmak üzere AB'nin siber güvenliğe ilişkin yasal çerçevesine genel bir bakış sunmaktadır. Rapor, olay raporlama ve risk yönetimi gibi yasal gerekliliklere uymaya yönelik en iyi uygulamaları içermektedir.

**AB Siber Güvenlik Sertifikasyon Çerçevesi:** Bu rapor [EU Cybersecurity Certification Framework], dijital ürün ve hizmetlerin güvenliğini ve güvenilirliğini artırmayı amaçlayan AB'nin siber güvenlik sertifikasyon çerçevesine genel bir bakış sunmaktadır. Raporda, tasarım yoluyla güvenlik, test etme ve değerlendirme ile sürekli izleme ve değerlendirme de dahil olmak üzere siber güvenlik sertifikalarının alınması ve sürdürülmesine yönelik en iyi uygulamalar yer almaktadır.

**KOBİ'ler için Siber Güvenlik:** Bu rapor [Cybersecurity for SMEs], küçük ve orta ölçekli işletmelere (KOBİ'ler) siber güvenlik duruşlarını nasıl geliştirebilecekleri konusunda rehberlik ve en iyi uygulamaları sunmaktadır. Raporda risk yönetimi, güvenlik farkındalığı eğitimi, güvenli yazılım geliştirme ve olay müdahale planlaması konularında tavsiyeler yer almaktadır.

**Yetişkin Nüfusta Dijital Beceriler**: Avrupa Komisyonu tarafından hazırlanan bu rapor [Digital Skills in the Adult Population], AB'deki yetişkin nüfusun dijital becerilerine genel bir bakış sunmaktadır. Yetişkinlerin kendilerini siber tehditlerden korumak için temel bilgi ve becerilere sahip olmaları gerektiğini vurgulayan dijital güvenlikle ilgili bir bölüm içermektedir.

**Yaşam Boyu Öğrenme için Dijital Beceriler**: Avrupa Komisyonu tarafından hazırlanan bu rapor [Digital Skills for Lifelong Learning], yetişkinler arasında dijital becerilerin geliştirilmesine yönelik rehberlik ve en iyi uygulamaları sunmaktadır. Risk yönetimi, güvenli gezinme, şifre yönetimi ve veri koruma konularında tavsiyeler sağlayan dijital güvenlikle ilgili bir bölüm içermektedir.

**Dijital Eğitim için Siber Güvenlik Projesi:** European Schoolnet tarafından hazırlanan bu proje [The Cybersecurity for Digital Education Project], Avrupa'daki öğretmenlere ve öğrencilere siber güvenlik konusunda kaynaklar ve eğitim sağlamaktadır. Proje, eğitimde dijital güvenliği artırmaya odaklanan çevrimiçi kurslar, ders planları ve değerlendirme araçları da dahil olmak üzere bir dizi materyal içermektedir.

**Yaşlılar için Dijital Güvenlik Projesi:** Avrupa Birliği Siber Güvenlik Ajansı'nın (ENISA) hazırladığı bu proje [The Digital Security for Senior Citizens Project], yaşlı vatandaşlara siber güvenlik konusunda kaynak ve eğitim sağlamaktadır. Proje, yaşlı yetişkinler arasında dijital güvenliği artırmaya odaklanan çevrimiçi kurslar, kılavuzlar ve videolar da dahil olmak üzere bir dizi materyal içermektedir.

**Dijital Beceriler ve İş Koalisyonu:** Avrupa Komisyonu'nun bu girişimi [Digital Skills and Jobs Coalition], Avrupalıların dijital ekonomiye tam olarak katılmalarını sağlamak için dijital becerilerini geliştirmeyi amaçlamaktadır. Dijital güvenlik de dahil olmak üzere çeşitli kaynaklar ve eğitim fırsatları içermektedir.

## 4.3. Dijital Güvenlik Konusunda Yetişkin Eğitiminin En İyi Uygulamaları

***ENISA Eğitmenin Eğitimi Programı***

'Siber Güvenlik Uzmanlarına Yönelik Eğitimler' bölümünde yer alan çevrimiçi eğitim materyallerinin ve eğitim kurslarının tamamı 'Eğiticinin Eğitimi' felsefesine dayanmaktadır. 'Eğiticiyi Eğitin' programı ve felsefesi, eğitmen ağını genişletmeyi ve daha iyi bilgi alışverişini teşvik etmeyi amaçlamaktadır. Bu, aşağıdakiler de dahil olmak üzere çeşitli amaçlara hizmet edecektir:

- Eğitimde zamandan ve paradan tasarruf etmek için eğitim materyallerinin paylaşılması,
- Bölgesel eğitim çalışmaları oluşturulması,
- Farklı eğitim sağlayıcılar arasında iş birliğinin geliştirilmesi,
- İyi eğitim uygulamalarının teşvik edilmesi,
- Rekabetin ve duplikasyonların (kopyalamaların) azaltılması.

ENISA'nın çevrimiçi eğitim materyalleri arasında Eğitmen El Kitabı, Öğrenci Araç Seti ve indirilebilecek Sanal Araçlar yer alacaktır. Bu, potansiyel eğitmenlerin kursa hazırlanmalarına olanak tanır ve El Kitabı kurs boyunca öğrenenlere rehberlik etmelerine yardımcı olur. Materyaller; kısa notlar, öğrenenlerin derslerdeki önemli mesajları kavrayıp kavramadıklarını görmek için küçük testler ve eğitmenin dersi daha ilgi çekici veya zorlayıcı hale getirmek için kullanabileceği ekstra bilgi veya alıştırmalar içermektedir.

Birbirlerinin başarılarından ve başarısızlıklarından öğrenmek hem yeni hem de deneyimli eğitmenlerin eğitimleri daha iyi tasarlamalarına ve sunmalarına olanak tanıyarak eğitimleri

daha başarılı, daha "eğlenceli", daha iyi ve daha uzun süreli sonuçlarla yapmalarına olanak tanımaktadır.

***TiK – Kısaca Teknoloji***

Yüksek teknoloji projesi, özel bir tablet eğitimi müfredatına göre eğitilen ve "Tablet Eğitmenleri" olarak adlandırılan genç gönüllülerin (16-30 yaş arası) sunduğu eğitimlerle nesiller arası bir yaklaşımı izlemektedir. Kurslar, çok sayıda yöntemin, esnek yönlendirici soruların ve genç eğitmenlerin özel çabasının ayrıcalığını taşımaktadır. Eğitmenler yalnızca küçük bir gider ödeneği karşılığında gönüllü olarak düşük eşikli kurslar sunarlar. Kursların daha da geliştirilmesi, katılımcıların ve eğitmenlerin geri bildirimleriyle, ayrıca yaşlılara yönelik özel materyaller ve engelsiz broşürlerle de sağlanmaktadır. Kurslar ilgilenenlerin kolayca ulaşabileceği bir yerdedir ve "TiKmodules"in geniş coğrafi dağılımına ve www.digitaleseniorinnen.at adresindeki bilgilere büyük önem verilmektedir. Kursların katılımcıları, özellikle ekonomik açıdan dezavantajlı ve eğitim düzeyi görece düşük kadınlardır. 2018 yılı sonuna kadar 2000'den fazla kişi modüllerden yararlanmış ve 1000 kişi daha kurs programına katılmıştır. Kursa katılan en yaşlı katılımcı 97 yaşında, eğitimini çocuk yuvasındaki genç bir eğitmenden almaktadır. Proje federal ve eyalet düzeyinde birçok kez ödüllendirilmiştir.

## 5. Yetişkinlerin Eğitimi: Dijital Yılmazlık Nasıl İnşa Edilir?

Yetişkin öğrenimine ilişkin bir çalışma alanı olarak Andragoji, 1950'lerde Avrupa'da ortaya çıkmış, ancak andragojinin yetişkin öğrenmesinin bir kuramı ve modeli olarak ele alınması, 1970'li yıllarda andragojiyi "Yetişkinlerin öğrenmesine yardım etme sanatı ve bilimi" olarak tanımlayan Amerikalı uygulayıcı ve yetişkin eğitimi kuramcısı Malcolm Knowles'un öncülüğü ile gerçekleşmiştir (Fidishun 2000). Fidishun (2000), çevrimiçi sınıfların tasarımında andragojik ilkelerin "öğrenenlerin derslerde istedikleri zaman, istedikleri yerde ve kendi hızlarında ilerlemelerini ve esnekliğini" kolaylaştırmak için kullanılmasını önermiştir.

### 5.1. Andragojinin Dört İlkesi

Yetişkinlerin kendilerine özgü öğrenme yöntemleri olduğu göz önüne alındığında, onlara yönelik eğitimin en iyi nasıl düzenlenebileceğini açıklayan 4 temel ilke bulunmaktadır.

- Öğrenme sürecinde yetişkinler, eğitimlerinin nasıl planlandığına, verildiğine ve yürütüldüğüne dâhil olmak ister veya buna gereksinim duyarlar. Neyi, ne zaman ve nasıl öğreneceklerini kontrol etmek isterler.
- Yetişkinler geçmiş deneyimlerini öğrenme sürecine dâhil edebildiklerinde daha fazla kazanım elde ederler. Öğrenimlerine daha fazla bağlam eklemek için daha önce bildiklerinden faydalanabilirler.

- Gerçekleri ve bilgileri ezberlemek yetişkinler için öğrenmenin doğru yolu değildir. Kendilerine sunulan bilgiyi en iyi şekilde alabilmek için sorunları çözmeleri ve akıl yürütmeleri gerekir.
- Yetişkinler "Bu bilgiyi şimdi nasıl kullanabilirim?" sorusunun yanıtını bilmek isterler. Öğrendiklerinin yaşamlarına uygulanabilir olması ve hemen uygulanması gereklidir.

## 5.2. Eğitmenler Andragojiyi Nasıl Uygulayabilir?

### *Öz Yönetimli Öğrenme Yaklaşımını Kullanmak*

Geçmişte, öğrenme genellikle belirli bir zamanda yapılan zorunlu bir etkinlik olarak ele alınmaktaydı. Artık öğrenme yönetim sistemi gibi teknolojilerle, yetişkin öğrenenler için kendi kendini yönlendirebilen, yönetebilen, bağımsız bir öğrenme ortamı yaratılabilmektedir. İstedikleri zaman ve yerde eğitim almalarına olanak tanıyabilir, kaydolmayı seçebilecekleri kurs seçenekleri sunabilir ve kendilerine özgü öğrenme hedeflerine sahip olmalarını sağlayabiliriz.

### *Gerçek Yaşamdan Öğrenme Örneklerini Kullanmak*

Kuramın belirttiği gibi, yetişkinler eğitimin nasıl anında uygulanacağını ve kendilerine nasıl fayda sağlayacağını bilmek isterler. Bu nedenle ders içeriği oluştururken onlara mümkün olduğunca çok sayıda gerçek dünyadan örnek eklemeliyiz.

Yetişkin öğrenenlere dijital esenlik ve/veya dijital güvenlik konusunda eğitim verirken, onlara gerçekte kullanacakları iş akışını adım adım anlatın ve bunu nasıl ve neden kullanacaklarını açıkça belirtin. Eğitimin onlara nasıl katkı sağlayacağını belirtin ve ardından eğitim için gerçek örnekler kullanın.

### *Yetişkin Öğrenenlerin Kendi Çözümlerini Bulmalarına İzin Vermek*

Yetişkinler problem çözmeyi yalnızca gerçeklerin sunulmasına tercih ettiğinden, içerik oluştururken tüm yanıtları hemen ortaya koymak iyi bir fikir değildir. Bunun yerine neden yaratıcı olmayalım ve öğrenenlerin beyinlerini harekete geçirecek kurslar oluşturmayalım?

Bunu, bir öğrenenin gerçekte karşılaşabileceği belirli sorunların ana hatlarını çizen değerlendirmeler ve simülasyonlar eklemek ve ardından yetişkin öğrenenlerin bu sorunların üstesinden gelmek için becerilerini kullanmalarını sağlamak da dahil olmak üzere birkaç basit yolla yapabiliriz.

# 6. Sonuç

Yetişkinlerin ve yaşlıların dijital güvenliği, hükümetlerin ve genel olarak toplumun dikkatini ve eylemini gerektiren önemli bir konudur. Yukarıda belirtilen iyi uygulamaları uygulayarak ülkeler, yaşlanan nüfuslarının dijital olarak korumasını ve esenliğini iyileştirebilirler. Farkındalık yaratma, eğitim, özel destek, teknolojik uyum ve sektör iş birliği, yetişkinler ve yaşlı yetişkinler için güvenli ve olumlu bir çevrimiçi deneyim sağlamanın temel unsurlarıdır.

DigiWELL projesi, dijital esenlik ilkelerini yetişkin eğitimine entegre etmeyi amaçlamaktadır. DigiWELL projesinin girişimleri, yetişkin eğitimi kuruluşlarının, ağlarının ve girişimlerinin genel uygulamalarına katkıda bulunmaya yöneliktir. Proje, dijital çağda teknolojinin yetişkinlerin zihinsel sağlığını, üretkenliğini ve genel esenliğini nasıl etkilediğini ele almanın ne kadar önemli olduğunu göz önünde bulundurmaktadır. DigiWELL'in ana hedefi, yetişkin öğrenenlere dijital dünyada etik yollarla ve bilinçli bir şekilde gezinmek için gerekli bilgi, beceri ve kaynakları sağlamaktır. DigiWELL projesi, ayrıca, yetişkin öğrenenlerin güçlendirilmesine yönelik ek girişimlerin oluşturulmasını ve yürütülmesini de kapsamaktadır. Bu etkinliklerin amacı, yetişkinlerin dijital esenliklerine ilişkin karşılaştıkları zorlukları, deneyimlerini ve dijital esenliği teşvik etmeye yönelik zaferlerini paylaşabilecekleri destekleyici bir ortam sağlamaktır. Bu doğrultuda, DigiWELL projesi, bireylere ve yetişkin örgütlerine, dijital esenliğin önemi ve yetişkinlerin, eğitimcilerin ve yetişkin eğitimcilerin dijital refahının nasıl teşvik edileceği konusunda bilinçlenmesi ve aydınlanması için birçok fırsat sunmaktadır. Dijital refahın bütünsel bir yaklaşımla gerçekleşebilmesi, ilgili tüm paydaşların bireylerin dijital esenlik ihtiyaçlarını destekleyecek şekilde harekete geçmesiyle mümkün olmaktadır. Bu çerçevede bu kılavuzda sunulan bilgiler, ipuçları ve iyi uygulamalar, çoğumuzun daha iyi bir dijital esenliğe ve aynı zamanda daha güçlü dijital yaşamlara sahip olması için bireyleri ve ilgili kuruluşları inisiyatif almaya davet etmektedir.

# 7. Kaynaklar

Sözlüğün hazırlanmasında ücretsiz olarak erişilebilen çevrimiçi kaynaklar kullanılmıştır: Çevrimiçi sözlükler, bilgi güvenliği, dijital teknolojiler ve hizmetler, dijital refah ve dijital dayanıklılık alanındaki bilimsel makaleler ve literatürün yanı sıra alandaki terimler ve tanımlar. Tüm kaynaklar sözlüğün çalışma sürümünün metin veritabanında listelenmiştir.

1 BAI. Committee on National Security Systems (CNSS) Glossary (2015). In *BAI Information Security Consulting & Training [online]*. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

2 *Capterra Glossary*. Capterra. (n.d.). https://www.capterra.com/glossary/

3 CSRC. (n.d.). *Glossary*. Computer Security Resource Center. https://csrc.nist.gov/glossary/

4 *Cybersecurity glossary of terms*. Global Knowledge. (n.d.). https://www.globalknowledge.com/ca-en/topics/cybersecurity/glossary-of-terms/

5 *Glossary*. DigitalHealthEurope. (n.d.). https://digitalhealtheurope.eu/glossary/

6 *Glossary*. The Digital Wellness Lab. (2022). https://digitalwellnesslab.org/parents/glossary/

7 ISO. (n.d.). *ISO/IEC 27032:2023(en) Cybersecurity — Guidelines for Internet security*. Online browsing platform (OBP) - ISO. https://www.iso.org/obp/ui/iso

8 Jirásek, P., Novák, L., Požár, J., & Vavruška, K. (2022). *Výkladový Slovník kybernetické bezpečnosti = Cyber security glossary*. *Fifth edition.* Praha: Česká pobočka AFCEA, 2022. p. 352, ISBN 978-80-908388-4-0

9 Kissel, R. L. (2019, July 16). *Glossary of key information security terms*. NIST. https://www.nist.gov/publications/glossary-key-information-security-terms-1

10 MF SR. (n.d.). *Metodický pokyn na použitie odborných výrazov pre oblasť informatizácie spoločnosti - CSIRT.SK*. CSIRT.SK. http://www.csirt.gov.sk/wp-content/uploads/2021/08/Metodicky_pokyn_glosar_pojmov.pdf

11 Paulsen, C., & Byers, R. D. (2021). *Glossary of key information security terms*. NIST. https://www.nist.gov/publications/glossary-key-information-security-terms-2

12 Stallings, W., & Brown, L. V. (2015). *Computer security: Principles and practice*. *Third edition.* Boston, MA: Pearson, 2015. p.838. ISBN 978-0-13-377392-7. Pearson.

13 *TVETipedia Glossary*. UNSECO-UNEVOC. (n.d.) https://unevoc.unesco.org/home/TVETipedia+Glossary

14 Fidishun, D. (2000). Teaching adult students to use computerized resources: Utilizing Lawler's keys to adult learning to make instruction more effective. *Information Technology and Libraries*, *19*(3), 157-157.

15 European Commission, Directorate-General for Education, Youth, Sport and Culture, Key competences for lifelong learning, Publications Office, 2019, https://data.europa.eu/doi/10.2766/569540