L2D

MEDIA LITERACY COMPETENCES
FOR YOUTH WORKERS

MEDIA LITERACY COMPETENCES
FOR YOUTH WORKERS

GÜVENLİ ÇEVRİMİÇİ KULLANIM İÇİN KILAVUZ

ÇEVRİMİÇİ GÜVENLİK MODÜLÜ

GÜVENLİ ÇEVRİMİÇİ KULLANIM İÇİN KILAVUZ

MODÜL ÇEVRİMİÇİ GÜVENLİK

Başlık :	GÜVENLİ ÇEVRİMİÇİ KULLANIM İÇİN KILAVUZ
Anahtar Kelimeler :	Çevrimiçi Güvenlik, İnternet Güvenliği, Dijital Gizlilik, Siber Güvenlik, Güvenli Çevrimiçi Uygulamalar, Kişisel Bilgilerin Korunması, Veri Güvenliği, Parola Yönetimi, Çevrimiçi Tehditler, Kötüye Kullanım Bildirimi, Gizlilik Ayarları
Hazırlayan :	
Dil :	Türkçe
Hedefler :	● Çevrimiçi güvenliği tanımlayın: Çevrimiçi güvenlik kavramını ve günümüz dijital dünyasındaki önemini açıklayın. ● Çevrimiçi tehditleri tanımlayın: Öğrencilerin kimlik avı, kötü amaçlı yazılım, kimlik hırsızlığı, siber zorbalık ve dolandırıcılık gibi çeşitli çevrimiçi tehditleri tanımalarına yardımcı olun. ● Gizlilik endişelerini anlayın: Katılımcıları kişisel bilgileri çevrimiçi ortamda korumanın önemi ve gizlilik ihlallerinin olası sonuçları hakkında eğitin.

Co-funded by the European Union

	• Güçlü parolalar geliştirin: Hesap güvenliğini artırmak için güçlü ve benzersiz şifreler oluşturma tekniklerini öğretin. • Kimlik avı girişimlerine karşı koruma sağlayın: Kimlik avı e-postalarını, mesajlarını ve web sitelerini tespit etmek ve bunların kurbanı olmaktan kaçınmak için stratejiler sağlayın. • Sosyal medya profillerini güvenli hale getirin: Gizlilik ayarlarını düzenlemek, kişisel bilgilerin paylaşımını kontrol etmek ve arkadaşlık isteklerini ele almak için yönergeler sunun. • Güvenli çevrimiçi iletişimi teşvik edin: Sosyal medyada, forumlarda ve mesajlaşma platformlarında güvenli bir şekilde iletişim kurmanın etkili yollarını öğretin ve hassas ayrıntıları paylaşmaktan kaçınmayı vurgulayın. • Eleştirel düşünme becerilerini geliştirin: Özellikle sahte haberler ve çevrimiçi yanlış bilgiler bağlamında bilgi ve kaynakları eleştirel bir şekilde değerlendirme becerisini teşvik edin. • Çevrimiçi taciz ve takip ile başa çıkın: Çevrimiçi taciz veya takip vakalarına nasıl yanıt verileceği ve bunların nasıl rapor edileceği konusunda rehberlik sunun.
Öğrenim Çıktıları:	
İçerik İndeksi :	1. 1. INTERNET GÜVENLIĞI 2. 1.1. İNTERNET GÜVENLİĞİNİN TANIMI 3. 1.2. KAPSAM VE ÖNEMİN ANLAŞILMASI 4. 1.2.1. İnternet Güvenliğinin Kapsamı 5. 1.2.2. İnternet Güvenliğinin Önemi 6. 1.3. İNTERNET GÜVENLİĞİ KAVRAMLARININ EVRİMİ 7. 1.4. Güvenli Bir Çevrimiçi Deneyimin Temel Bileşenleri 8. 9. 2. ÇEVRIMIÇI TEHDITLER 10. 2.1. ÇEVRİMİÇİ TEHDİT TÜRLERİ 11. 2.2. UYARI IŞARETLERININ TANINMASI 12. 2.3. ÇEVRİMİÇİ TEHDİTLERİ GÖRMEZDEN GELMENİN SONUÇLARI 13. 14. 3. KIŞISEL BILGILERIN KORUNMASI 15. 3.1. MAHREMİYETİN KORUNMASININ ÖNEMİ 16. 3.2. GÜVENLI ÇEVRIMIÇI HESAP YÖNETIMI 17. 3.3. SORUMLU SOSYAL MEDYA PAYLAŞIMI

	18. 19. 4. SOSYAL MEDYADA GÜVENLI BIR ŞEKILDE GEZINME 20. 4.1. GİZLİLİK AYARLARININ YAPILMASI 21. 4.2. ARKADAŞLIK İSTEKLERİNİ VE MESAJLARINI İŞLEME 22. 4.3. KÖTÜ NIYETLI HESAPLARIN BILDIRILMESI VE ENGELLENMESI 23. 24. 5. SİBER GÜVENLİK VE MOBİL CİHAZLAR 25. 5.1. AKILLI TELEFON VE TABLETLERIN GÜVENLIĞININ SAĞLANMASI 26. 5.2. UYGULAMA İZİNLERİ VE VERİ ERİŞİMİ 27. 5.3. MOBİL CİHAZLARIN ÇALINMA VE KAYBOLMAYA KARŞI KORUNMASI
İçerik Geliştirme :	1. 1. İNTERNET GÜVENLİĞİ 1.1. İNTERNET GÜVENLİĞİNİN TANIMI Çevrimiçi güvenlik olarak da bilinen internet güvenliği, eyleme geçirilebilir yönergelere uyma, modern teknoloji hakkında kapsamlı bir anlayış kazanma ve çevrimiçi dünyanın çeşitli kötü niyetli yönlerine karşı savunmak için dijital cihazlarınızı proaktif olarak koruma uygulamasıdır. İnternet kullanıcılarının sayısı küresel olarak artmaya devam ettikçe, hükümetler, kuruluşlar ve internet servis sağlayıcıları da dahil olmak üzere çeşitli paydaşlar, çocuklar, gençler ve yaşlılar gibi savunmasız nüfusların geniş sanal alemle etkileşime girerken güvenliği konusunda giderek daha fazla endişe duymaya başladılar. Endişe verici istatistikler, internet kullanıcılarının %45'inden fazlasının bir tür siber tacize maruz kaldığını ortaya koyarak, daha güvenli çevrimiçi uygulamaların teşvik edilmesine ve dijital sorumluluk kültürünün geliştirilmesine duyulan acil ihtiyacın altını çizmektedir. Bu acil kaygıları ele almak ve daha güvenli bir dijital ortamın oluşturulması için her Şubat ayında küresel ölçekte Daha Güvenli İnternet Günü kutlanmaktadır. Bu yıllık etkinlik, internet güvenliği konusunda farkındalığı artırmak için özel bir platform olarak hizmet etmekte, bireyleri ve toplulukları çevrimiçi etkileşimlerinde dikkatli, bilgili ve proaktif olmaya teşvik etmektedir. Dünya çapında hükümetler, kar amacı gütmeyen kuruluşlar ve teknoloji şirketleri, internet kullanıcılarını çevrimiçi dünyada güvenli bir şekilde gezinmek için gerekli bilgi ve becerilerle donatmak amacıyla farkındalık kampanyaları, eğitim

	atölyeleri ve etkileşimli etkinlikler düzenleyerek Güvenli İnternet Günü girişimlerine aktif olarak katılmaktadır. Birleşik Krallık'ta Get Safe Online kampanyası internet güvenliğinin teşvik edilmesinde önemli bir güç olarak ortaya çıkmıştır. Devlet kurumu Serious Organized Crime Agency (Ciddi Organize Suç Ajansı'nın) (SOCA) önemli sponsorluğu ve Microsoft ve eBay gibi büyük internet şirketlerinin işbirliğiyle yürütülen kampanya, internet kullanıcılarını siber tehditlere karşı kendilerini korumaları için pratik rehberlik ve kaynaklarla güçlendirmeyi amaçlıyor. Kolay erişilebilir bilgiler, ipuçları ve araçlar aracılığıyla Get Safe Online, bireylerin dijital dayanıklılığını artırarak Birleşik Krallık internet topluluğunu daha sağlam ve çevrimiçi tehlikelere karşı daha savunmasız hale getirmeye çalışmaktadır. İnternet gelişmeye ve günlük hayatımızda giderek daha ayrılmaz bir rol oynamaya devam ettikçe, internet güvenliğinin sağlanması çok önemli hale gelmektedir. Sorumlu bir çevrimiçi davranış kültürünü teşvik ederek, Daha Güvenli İnternet Günü gibi girişimlerle farkındalığı artırarak ve Get Safe Online kampanyası gibi erişilebilir kaynaklar sağlayarak, herkes için daha güvenli ve daha emniyetli bir dijital ortam yaratmak için hep birlikte çalışabiliriz. Sürekli bağlantı halinde olan dünyamızda internet güvenliğinin önemi yadsınamaz. İnternet öğrenme, iletişim ve eğlence için benzersiz fırsatlar sunarken aynı zamanda kullanıcıları potansiyel risk ve tehlikelere de maruz bırakmaktadır. Teknoloji ilerledikçe ve çevrimiçi tehditler daha sofistike hale geldikçe, internet güvenliği konusunda bilgili ve proaktif olmak her yaştan birey için çok önemlidir. Genellikle dijital yerliler olan çocuklar ve gençler için internet güvenliğini anlamak, sorumlu ve güvenli çevrimiçi etkileşimler için çok önemlidir. Ebeveynler, eğitimciler ve vasiler, genç internet kullanıcılarına rehberlik etmede, onlara kişisel bilgilerini paylaşmanın, yabancılarla iletişim kurmanın ve güvenli olmayan çevrimiçi etkinliklere katılmanın potansiyel risklerini öğretmede hayati bir rol oynamaktadır. İnternet güvenliğini artırmak için, en son siber güvenlik trendleri ve en iyi uygulamalar konusunda güncel kalmak çok önemlidir. Yazılım ve uygulamaların düzenli olarak güncellenmesi, güvenilir antivirüs yazılımlarının kullanılması ve otomatik güncellemelerin etkinleştirilmesi,

	dijital cihazların ortaya çıkan tehditlere karşı savunmasını güçlendirebilir. Ayrıca, mümkün olan her yerde çok faktörlü kimlik doğrulamanın kullanılması, çevrimiçi hesaplara ekstra bir koruma katmanı ekler. Olumlu ve güvenli bir çevrimiçi topluluğun teşvik edilmesi, dijital empati ve saygının geliştirilmesini de gerektirir. Çevrimiçi etkileşimlerde nezaket ve empatiyi teşvik etmek, siber zorbalık ve zehirli davranışlara karşı koyarak interneti herkes için daha sıcak bir alan haline getirebilir. 1.2. KAPSAM VE ÖNEMİN ANLAŞILMASI 1.2.1. İnternet Güvenliğinin Kapsamı • Virüsler, kötü amaçlı yazılımlar, kimlik avı, fidye yazılımı ve kimlik hırsızlığı gibi siber tehditlere karşı koruma. • Kişisel bilgilerin ve dijital kimliğin yetkisiz erişime ve kötüye kullanıma karşı korunması. • Sosyal medyada sorumlu bir şekilde gezinme ve siber zorbalık veya çevrimiçi tacizle başa çıkma. • Güvenli çevrimiçi işlemlerin sağlanması ve çevrimiçi alışveriş veya bankacılık yaparken finansal bilgilerin korunması. • Veri ihlallerini ve gizlilik ihlallerini önlemek için mobil cihazları güvenli bir şekilde kullanma ve yönetme. • Çevrimiçi dolandırıcılıkları, sahte web sitelerini ve kimlik avı girişimlerini tanıma ve bunlardan kaçınma. • Çocuklara ve gençlere çevrimiçi güvenliği öğretmek ve sorumlu dijital alışkanlıklar geliştirmelerine yardımcı olmak. 1.2.2. İnternet Güvenliğinin Önemi • Kişisel ve Finansal Bilgilerin Korunması: İnternet güvenliği önlemleri hassas verileri korur, kimlik hırsızlığını ve finansal dolandırıcılığı önler. • Gizliliğin ve Dijital İtibarın Korunması: Çevrimiçi faaliyetler konusunda dikkatli olmak, bireylerin gizliliklerini ve dijital itibarlarını korumalarına yardımcı olur. • Siber Tehditlere Karşı Koruma: Çevrimiçi risklerin farkında olmak ve güvenlik uygulamalarını takip etmek, günlük yaşamı, iş operasyonlarını aksatabilecek veya hassas bilgileri tehlikeye atabilecek siber tehditlere karşı koruma sağlar. • Olumlu Dijital Deneyimlerin Güçlendirilmesi: İnternet güvenliği, bireylerin taciz veya mağduriyet korkusu olmadan çevrimiçi ortamda olumlu, zenginleştirici deneyimler yaşamalarını sağlar.

- Dijital Vatandaşlığın Teşvik Edilmesi: Bireyler internet güvenliğini uygulayarak sorumlu ve saygılı bir dijital topluluk oluşturmaya katkıda bulunurlar.
- Ekonomik Etki: Siber güvenlik olaylarının bireyler, işletmeler ve hükümetler için ciddi ekonomik sonuçları olabilir, bu da internet güvenliğini genel güvenliğin önemli bir unsuru haline getirir.
- Savunmasızların Korunması: İnternet güvenliği özellikle çevrimiçi tehlikelere karşı daha hassas olabilecek çocuklar, gençler ve savunmasız nüfuslar için çok önemlidir.

1.1. İNTERNET GÜVENLİĞİ KAVRAMLARININ EVRİMİ

- "İnternet Güvenliği Kavramlarının Evrimi", internet güvenliği anlayışının ve kullanıcıları çevrimiçi tehditlerden korumak için alınan önlemlerin zaman içinde nasıl geliştiğini ifade eder. İnternet büyüdükçe ve değiştikçe, siber tehditlerin yarattığı zorluklar da artmış, bu da çevrimiçi güvenliği sağlamak için yeni kavramların ve stratejilerin geliştirilmesine yol açmıştır. Bu bölümde internet güvenliği uygulamalarını şekillendiren tarihsel bağlam ve önemli dönüm noktaları ele alınmaktadır.

- Erken Dönem İnternet: İnternetin ilk günlerinde, çevrimiçi güvenlik kavramı nispeten basitti. Çoğu kullanıcı, kişisel bilgilerini çevrimiçi paylaşmanın risklerini anlayan teknoloji meraklısı bireyler veya profesyonellerdi. Ancak, potansiyel siber tehditler konusunda halk arasında sınırlı bir farkındalık vardı.

- Çevrimiçi İletişimin Yükselişi: Çevrimiçi iletişim platformları ve sosyal medya ortaya çıktıkça, internet güvenliği yeni boyutlar kazandı. Kullanıcılar daha fazla kişisel bilgi paylaşmaya başladı, bu da gizlilik ve kimlik hırsızlığı ile ilgili endişelerin artmasına yol açtı. Siber suçlular kullanıcıların güvenini istismar etmeye çalıştıkça kimlik avı ve spam e-postalar gibi kavramlar önem kazanmaya başladı.

- Öncü Siber Güvenlik Önlemleri: Artan tehdit ortamıyla birlikte siber güvenlik önlemleri de gelişmeye başladı. Antivirüs yazılımları, güvenlik duvarları ve şifreleme teknolojileri, kötü amaçlı yazılımlara ve yetkisiz erişime karşı korunmak için temel araçlar haline geldi. Bu ilk siber güvenlik

	çözümleri, gelecekte daha gelişmiş koruma mekanizmalarının temelini oluşturdu. • Farkındalık Kampanyaları ve Girişimleri: Siber tehditler daha yaygın hale geldikçe, çeşitli kuruluşlar, hükümetler ve teknoloji şirketleri halkı internet güvenliği konusunda eğitmek için farkındalık kampanyaları ve girişimleri başlatmaya başladı. Bu çabalar, yaygın çevrimiçi riskler hakkında farkındalık yaratmayı ve kullanıcıları daha güvenli çevrimiçi uygulamaları benimsemeye teşvik etmeyi amaçlamıştır. • Siber Zorbalık Hakkında Artan Endişeler: Sosyal medya ve çevrimiçi iletişimin yükselişi siber zorbalık konusuna da dikkat çekmiştir. Çevrimiçi taciz ve siber zorbalık vakaları arttıkça, internet güvenliği çabaları bu tür dijital saldırganlığı ele almak ve etkilenen bireyleri desteklemek için genişledi. • Mobil İnternet ve Yeni Zorluklar: Akıllı telefonların ve mobil internet erişiminin ortaya çıkışı, internet güvenliği için yeni bir dizi zorluğu da beraberinde getirmiştir. Uygulama izinleri ve kötü amaçlı yazılımlar gibi mobil cihazlarla ilişkili benzersiz riskler, özel güvenlik önlemleri gerektirdi. • Kimlik Doğrulamada Gelişmeler: Şifrelerin çevrimiçi hesapları korumada tek başına yetersiz kalması nedeniyle iki faktörlü kimlik doğrulama (2FA) ve çok faktörlü kimlik doğrulama (MFA) popülerlik kazandı. Bu yöntemler ek bir güvenlik katmanı sağlayarak yetkisiz erişim riskini azalttı. • Dijital Okuryazarlık Vurgusu: İnternet güvenliği kavramları sadece teknik güvenlik önlemlerini değil, aynı zamanda dijital okuryazarlık ve eleştirel düşünme becerilerini de kapsamaya başladı. Kullanıcıları yanlış bilgileri, sahte haberleri ve çevrimiçi dolandırıcılıkları tespit etme konusunda eğitmek, çevrimiçi tehditlerle mücadelede hayati önem kazandı. • Siber Güvenlik Sektörünün Yükselişi: Siber tehditlerin artan karmaşıklığı, güçlü bir siber güvenlik endüstrisinin doğmasına neden oldu. Siber güvenlik hizmetleri, tehdit analizi ve olaylara müdahale konularında uzmanlaşmış şirketler ve

profesyoneller, gelişen çevrimiçi risklere karşı savunmada önemli bir rol oynadı.

- İnternet Güvenliğinin Eğitime Entegrasyonu: İnternet güvenliği eğitiminin öneminin farkına varan okullar ve eğitim kurumları bunu müfredatlarına dahil etmeye başladı. Çocuklara ve genç yetişkinlere sorumlu çevrimiçi davranış ve dijital vatandaşlık öğretmek modern eğitimin önemli bir yönü haline geldi.
- Medya okuryazarlığı, insanlara medya tarafından sunulan dinamikleri ve mesajları daha iyi anlamaları ve bunları bağımsız ve eleştirel bir şekilde yeniden işlemeleri için gerekli tüm araçları sağlamak amacıyla doğmuş bir öğretim konusudur. Bugün, insanlara sosyal medya ile ilişkilerini daha iyi yönetmeyi öğretmek, onları "neyi nasıl paylaşacakları" veya "sahte haberleri" nasıl tanıyacakları konusunda eğitmek gerekiyor. Akıllı telefonlar sayesinde internet kullanımı, öğrenme için sonsuz bir potansiyel sunarken, aynı zamanda "bu araçların yüzeysel kullanımı" ile bağlantılı riskler de barındırmaktadır. "Dijital Göçmenler", ait olmadıkları sanal bir dünyanın yazılı olmayan kurallarıyla başa çıkmaya alışık olmadıkları için büyük risk altındadır. Genellikle ana iletişim sistemlerini bilmezler ve topluluğa kendi katkılarını sunmak için yeni mesajları işleme yeteneğine sahip değildirler, pasif unsurlar olarak kalırlar.

Güvenli Bir Çevrimiçi Deneyimin Temel Bileşenleri

"Güvenli Bir Çevrimiçi Deneyimin Temel Bileşenleri", internet kullanırken güvenli ve korumalı bir ortam yaratmaya katkıda bulunan temel unsurlardır. Bu bileşenler, bireylerin çevrimiçi ortamda güvenliklerini ve gizliliklerini sağlamak için kullanabilecekleri çeşitli uygulamaları, davranışları ve araçları kapsamaktadır. Bu temel bileşenlerin anlaşılması ve uygulanması, olumlu ve güvenli bir internet deneyimi için hayati önem taşımaktadır.

- Siber Güvenlik Farkındalığı: Güçlü bir siber güvenlik farkındalığı geliştirmek, güvenli bir çevrimiçi deneyim için esastır. Bu, en son siber tehditler hakkında bilgi sahibi olmayı, kimlik avı ve kötü amaçlı yazılım gibi yaygın saldırı yöntemlerini anlamayı ve şüpheli faaliyetlerin uyarı işaretlerini tanımayı içerir. Farkındalık, bireylerin dijital

	dünyada gezinirken bilinçli kararlar vermelerini ve gerekli önlemleri almalarını sağlar. • Gizlilik Koruması: Kişinin gizliliğini korumak, internet güvenliğinin çok önemli bir yönüdür. Bu, çevrimiçi paylaşılan bilgilere dikkat etmeyi ve kişisel bilgileri aşırı paylaşmaktan kaçınmayı içerir. Finansal bilgiler ve kimlik belgeleri gibi hassas verilerin korunması, kimlik hırsızlığı ve dolandırıcılığı önlemek için çok önemlidir. • Güçlü Kimlik Doğrulama: Çevrimiçi hesaplar için sağlam kimlik doğrulama yöntemlerinin kullanılması hayati önem taşır. Bu, her hesap için güçlü, benzersiz parolalar kullanmayı ve mevcut olduğunda iki faktörlü kimlik doğrulama (2FA) veya biyometrik kimlik doğrulama gibi ek güvenlik katmanlarından yararlanmayı içerir. Güçlü kimlik doğrulama önlemleri, hesaplara yetkisiz erişimi önlemeye ve hassas bilgileri korumaya yardımcı olur. • Güvenli Tarama Uygulamaları: Kötü amaçlı web sitelerinden ve potansiyel tehditlerden kaçınmak için güvenli tarama alışkanlıklarını uygulamak gereklidir. Bu, hassas bilgileri girmeden önce web sitesi URL'lerini doğrulamayı, şüpheli bağlantılara veya açılır pencerelere tıklamaktan kaçınmayı ve yerleşik korumalara sahip güvenli tarayıcıları kullanmayı içerir. • Düzenli Yazılım Güncellemeleri: Yazılımları, işletim sistemlerini ve uygulamaları güncel tutmak, güvenli bir çevrimiçi deneyimi sürdürmek için çok önemlidir. Düzenli güncellemeler genellikle bilinen güvenlik açıklarını ele alan güvenlik yamalarını içerir ve siber suçluların bunları istismar etmesini zorlaştırır. • Güvenli Ağlar: Güvenli ve güvenilir ağlara bağlanmak, aktarım halindeki verileri korumak için kritik önem taşır. Uygun güvenlik önlemleri olmayan halka açık Wi-Fi ağlarından kaçınmak, potansiyel veri müdahalesini ve yetkisiz erişimi önlemek için çok önemlidir. • Güvenli Sosyal Medya Uygulamaları: Sosyal medya platformlarını kullanırken dikkatli olmak, kişisel bilgileri korumak ve sosyal saldırıların kurbanı olmaktan kaçınmak için çok önemlidir. Gizlilik

ayarlarını düzenlemek, arkadaşlık istekleri konusunda seçici olmak ve hassas verileri herkese açık bir şekilde paylaşmaktan kaçınmak temel sosyal medya güvenliği uygulamalarıdır.

- Kimlik Avına Karşı Uyanık Olmak: Kimlik avı girişimlerine karşı uyanık olmak hayati önem taşır. Bu, e-posta gönderenlerin kimliklerini doğrulamayı, şüpheli bağlantılara tıklamamayı veya bilinmeyen kaynaklardan gelen ekleri indirmemeyi ve kimlik avı girişimlerini bildirmeyi içerir.

- Ebeveyn Kontrolleri ve Denetimi: Ebeveynler ve veliler için, ebeveyn kontrollerinin uygulanması ve çocukların çevrimiçi faaliyetlerinin izlenmesi, genç kullanıcılar için güvenli bir internet deneyiminin kritik bileşenleridir. Bu, yaşa uygun içerik erişimi sağlar ve çocukları potansiyel olarak zararlı çevrimiçi içerikten korur.

- Dijital Okuryazarlık ve Eleştirel Düşünme: Dijital okuryazarlık ve eleştirel düşünme becerilerini geliştirmek, yanlış bilgileri, sahte haberleri ve çevrimiçi dolandırıcılıkları tespit etmek için temeldir. Bilgi kaynaklarının nasıl değerlendirileceğini anlamak ve içeriğin güvenilirliğini doğrulamak, daha güvenli bir çevrimiçi deneyime katkıda bulunur.

2. ÇEVRİMİÇİ TEHDİTLER

2.1. ÇEVRİMİÇİ TEHDİT TÜRLERİ

Çevrimiçi tehdit türleri, internet kullanıcılarının verilerinin güvenliğini, gizliliğini ve bütünlüğünü tehlikeye atabilecek çeşitli kötü niyetli faaliyetleri ve saldırıları ifade eder. Bu tehditleri anlamak, bireylerin dijital ortamda gezinirken uygun önlemleri almaları ve kendilerini korumaları için çok önemlidir. İşte bazı yaygın çevrimiçi tehdit türleri:

- Kimlik Avı: Kimlik avı, siber suçlular tarafından kullanıcıları kandırarak oturum açma bilgileri, finansal bilgiler veya kişisel veriler gibi hassas bilgileri ifşa etmelerini sağlamak için kullanılan aldatıcı bir tekniktir. Oltalama girişimleri genellikle kurbanları bilgilerini vermeye ikna

	etmek için meşru varlıkları taklit eden sahte e-postalar, web siteleri veya mesajlar içerir. • Kötü Amaçlı Yazılım: Kötü amaçlı yazılım, cihazlara veya ağlara bulaşmak ve zarar vermek için tasarlanmış kötü amaçlı yazılımlardır. Buna virüsler, solucanlar, Truva atları, fidye yazılımları ve casus yazılımlar dahildir. Kötü amaçlı yazılımlar verileri tehlikeye atabilir, bilgi çalabilir, işlemleri aksatabilir ve hatta cihazları kullanılamaz hale getirebilir. • Fidye yazılımı: Fidye yazılımı, kullanıcının verilerini şifreleyerek kendi dosyalarını veya sistemlerini etkin bir şekilde kilitleyen belirli bir kötü amaçlı yazılım türüdür. Siber suçlular şifre çözme anahtarını sağlamak için bir fidye ödemesi talep eder, ancak fidye ödemesinin verilerin iadesi ile sonuçlanacağının garantisi yoktur. • Sosyal Mühendislik: Sosyal mühendislik, hassas bilgilere veya sistemlere yetkisiz erişim elde etmek için bireylerin manipüle edilmesini içerir. Bu, kullanıcıları gizli bilgileri ifşa etmeleri için kandırmak için kimliğe bürünme, manipülasyon veya insan psikolojisinden yararlanma yoluyla yapılabilir. • Veri İhlalleri: Veri ihlali, siber saldırganlar bir kuruluşun veya bireyin verilerine yetkisiz erişim sağladığında meydana gelir. Bu veriler kişisel bilgileri, mali kayıtları veya fikri mülkiyeti içerebilir. Veri ihlalleri bireylerin mahremiyeti açısından ciddi sonuçlar doğurabilir ve kimlik hırsızlığına veya mali kayba yol açabilir. • Kimlik Hırsızlığı: Kimlik hırsızlığı, dolandırıcılık amacıyla başka birinin kimliğine bürünmek için sosyal güvenlik numaraları, kredi kartı bilgileri veya giriş bilgileri gibi kişisel bilgilerin çalınmasını içerir. Siber suçlular bu çalıntı bilgileri mali kazanç elde etmek veya başka suçlar işlemek için kullanabilir. • Siber Zorbalık: Siber zorbalık, genellikle sosyal medya platformlarında veya mesajlaşma uygulamaları aracılığıyla gerçekleşen bir tür çevrimiçi taciz veya zorbalıktır. Mağdura zarar

vermek, gözünü korkutmak veya küçük düşürmek amacıyla incitici mesajlar göndermeyi, söylentiler yaymayı veya utanç verici içerikler paylaşmayı içerir.

- Hizmet Engelleme (Denial of Service)(DoS) ve Dağıtılmış Hizmet Engelleme (Distributed Denial of Service)(DDoS) Saldırıları: DoS ve DDoS saldırıları, bir web sitesini veya çevrimiçi hizmeti trafik seline boğarak meşru kullanıcılar için erişilemez hale getirmeyi amaçlar. Bu saldırılar çevrimiçi hizmetleri kesintiye uğratabilir ve işletmeler için mali kayıplara neden olabilir.

- Ortadaki Adam (Man-in-the-Middle)(MitM) Saldırıları: MitM saldırıları, bir kullanıcı ve bir web sitesi gibi iki taraf arasındaki iletişimi yakalamayı ve gizlice dinlemeyi içerir. Saldırgan daha sonra iletişim kuran tarafların bilgisi olmadan değiş tokuş edilen verileri görüntüleyebilir veya manipüle edebilir.

- Sıfırıncı Gün İstismarları: Sıfırıncı gün açıkları, henüz satıcı veya geliştiriciler tarafından bilinmeyen yazılım açıklarını hedef alır. Siber suçlular bu açıkları, bir yama veya düzeltme mevcut olmadan önce saldırılar başlatmak için kullanır ve bu da onları savunmayı zorlaştırır.

- Nesnelerin İnterneti (Internet of Things)(IoT) Zafiyetleri: Daha fazla cihaz internete bağlandıkça, IoT güvenlik açıkları endişe kaynağı haline gelmiştir. IoT cihazlarındaki zayıf güvenlik önlemleri, ev ağlarına erişim sağlamak veya gizliliği tehlikeye atmak için kullanılabilir.

2.2. UYARI İŞARETLERİNİ TANIMAK

Uyarı işaretlerini tanımak, internet güvenliği söz konusu olduğunda çok önemli bir beceridir. İnterneti kullanırken bir şeylerin yanlış veya potansiyel olarak zararlı olabileceğine dair göstergelere karşı uyanık olmayı içerir. Uyarı işaretlerini tanıyarak, bireyler kendilerini çevrimiçi tehditlerden korumak için hemen harekete geçebilir ve dolandırıcılık, siber saldırı veya diğer kötü niyetli

	faaliyetlerin kurbanı olmaktan kaçınabilirler. İşte dikkat edilmesi gereken bazı önemli uyarı işaretleri: • İstenmeyen İletişim: Bilinmeyen veya şüpheli kaynaklardan gelen istenmeyen e-postalara, mesajlara veya arkadaşlık isteklerine karşı dikkatli olun. Siber suçlular bu araçları genellikle kimlik avı girişimleri başlatmak veya kötü amaçlı yazılım dağıtmak için kullanırlar. • Kötü Dilbilgisi ve Yazım: Birçok kimlik avı e-postası ve dolandırıcılık mesajı gramer hataları, yazım yanlışları veya garip bir dil içerir. Bu hatalar, iletişimin meşru bir kaynaktan gelmediğinin işareti olabilir. • Kişisel Bilgi Talepleri: Giriş bilgileri, finansal bilgiler veya sosyal güvenlik numaraları gibi hassas bilgilere yönelik taleplere karşı dikkatli olun, özellikle de talep beklenmedik bir şekilde geliyorsa. • Acil veya Tehdit Edici Dil: Sizi hemen harekete geçmeye zorlamak için acil veya tehdit edici bir dil kullanan mesajlar, bir dolandırıcılık veya kimlik avı girişiminin göstergesi olabilir. • Olağandışı Bağlantılar veya URL'ler: Gerçek URL hedefini görmek için farenizi e-postalardaki veya mesajlardaki bağlantıların üzerine getirin. Kısaltılmış URL'lere veya şüpheli web sitelerine yönlendiren bağlantılara karşı dikkatli olun. • Uyumsuz veya Sahte URL'ler: Meşru gibi görünen ancak ince yazım hataları veya varyasyonları olan URL'lere dikkat edin. Dolandırıcılar kullanıcıları kandırmak için iyi bilinen web sitelerine çok benzeyen alan adları kullanabilir. • Tanıdık Olmayan E-posta Göndericileri: Özellikle mesaj beklenmedik ekler veya hassas bilgi talepleri içeriyorsa, e-posta gönderenlerin kimliğini doğrulayın. • Beklenmedik İndirmeler: Kötü amaçlı yazılım içerebileceğinden, başlatmadığınız veya beklemediğiniz indirmelere veya eklere karşı dikkatli olun.

- Olağandışı Hesap Etkinliği: Çevrimiçi hesap etkinliğinizi düzenli olarak gözden geçirin ve yetkisiz girişlere veya işlemlere karşı dikkatli olun.

- Açıklanamayan Sistem Davranışı: Bilgisayarınız veya cihazınız sık sık çökme, yavaşlama veya beklenmedik açılır pencereler gibi alışılmadık davranışlar sergiliyorsa, bu kötü amaçlı yazılım veya diğer güvenlik sorunlarına işaret ediyor olabilir.

- Güvenlik Yazılımından Gelen Uyarılar: Antivirüs veya güvenlik yazılımınızdan gelen uyarılara veya ikazlara dikkat edin, çünkü bunlar potansiyel tehditlere veya şüpheli faaliyetlere işaret edebilir.

- İstenmeyen Teklifler ve Promosyonlar: Gerçek olamayacak kadar iyi görünen istenmeyen tekliflere veya promosyonlara karşı dikkatli olun, çünkü bunlar sizi kişisel bilgilerinizi vermeniz için kandırmaya çalışan dolandırıcılar olabilir.

2.3. ÇEVRİMİÇİ TEHDİTLERİ GÖRMEZDEN GELMENİN SONUÇLARI

Çevrimiçi tehditleri göz ardı etmenin bireyleri, işletmeleri ve hatta toplumu bir bütün olarak olumsuz etkileyebilecek ciddi ve geniş kapsamlı sonuçları olabilir. Çevrimiçi tehditleri ele almamak veya bunlara karşı uygun önlemleri almamak, kişiyi çeşitli siber risklere karşı savunmasız bırakarak mali kayıplara, gizlilik ihlallerine, itibar kaybına ve hatta yasal yansımalara yol açabilir. İşte çevrimiçi tehditleri göz ardı etmenin bazı önemli sonuçları:

- Finansal Kayıp: Dolandırıcılık, kimlik avı saldırıları veya hileli çevrimiçi planların kurbanı olmak önemli mali kayıplara neden olabilir. Siber suçlular bankacılık kimlik bilgilerini, kredi kartı bilgilerini çalabilir veya yetkisiz işlemler gerçekleştirerek banka hesaplarının boşalmasına ve finansal zorluklara yol açabilir.

- Kimlik Hırsızlığı: Kimlik hırsızlığına ilişkin uyarı işaretlerini göz ardı etmek, siber suçluların sosyal

	güvenlik numaraları, doğum tarihleri ve adresler gibi kişisel bilgileri çalmasına olanak tanıyabilir. Çalınan bu bilgileri finansal dolandırıcılık yapmak, mağdurun adına hesap açmak veya diğer suç faaliyetlerinde bulunmak için kullanabilir ve mağdur için uzun vadeli ciddi sonuçlara neden olabilirler. • Veri İhlalleri: Sağlam güvenlik önlemlerinin uygulanmaması veya güvenlik açıklarının giderilmemesi, bireyler ve kuruluşlar için veri ihlallerine yol açabilir. Bir veri ihlali, müşteri verileri, ticari sırlar veya fikri mülkiyet dahil olmak üzere hassas bilgileri açığa çıkararak mali cezalara, yasal yükümlülüklere ve kuruluşun itibarına zarar verebilir. • Fidye Yazılımı Saldırıları: Siber güvenlik uygulamalarının göz ardı edilmesi, bireyleri ve işletmeleri fidye yazılımı saldırılarına açık hale getirebilir. Sistemler fidye yazılımı tarafından tehlikeye atıldığında, değerli veriler şifrelenebilir ve saldırganlar şifre çözme anahtarı için ödeme talep eder. Fidyenin ödenmesi verilerin kurtarılmasını garanti etmez ve mağdurlar veri kaybına veya operasyonel aksaklıklara maruz kalabilir. • İtibari Hasar: Siber zorbalığa veya sosyal medya saldırılarına maruz kalmak, bireyler ve kuruluşlar için önemli itibar hasarlarına neden olabilir. İnternette yayılan yanlış bilgiler, olumsuz yorumlar veya zararlı içerikler kişisel veya marka itibarına zarar vererek sosyal konumu, profesyonel fırsatları ve müşteri güvenini etkileyebilir. • Gizlilik Kaybı: Gizlilik endişelerinin göz ardı edilmesi, kişisel konuşmalar, görüntüler veya videolar dahil olmak üzere özel bilgilerin açığa çıkmasına neden olabilir. Bu mahremiyet kaybının duygusal ve psikolojik sonuçlarının yanı sıra potansiyel şantaj tehditleri de olabilir. • Yasal Sonuçlar: Siber tehditlerin göz ardı edilmesi ve gerekli güvenlik önlemlerinin uygulanmaması yasal sonuçlara yol açabilir. Bireyler veya kuruluşlar veri ihlalleri, gizlilik ihlalleri veya siber güvenlik standartlarına uyulmaması nedeniyle yasal işlemler, para cezaları veya düzenleyici cezalarla karşı karşıya kalabilir.

- Hizmetlerin Kesintiye Uğraması: Çevrimiçi tehditleri göz ardı eden işletmeler faaliyetlerinde aksamalar yaşayabilir. Dağıtılmış hizmet reddi (DDoS) saldırıları gibi siber saldırılar, web sitelerini veya ağları aşırı yükleyerek hizmetleri müşteriler için erişilemez hale getirebilir ve güvenilirlik kaybına neden olabilir.

- Sosyal ve Duygusal Etki: Siber zorbalığı, çevrimiçi tacizi veya yırtıcı davranışları görmezden gelmek, mağdurlar için ciddi sosyal ve duygusal sonuçlar doğurabilir. Kaygı, depresyon, kendini soyutlama ve hatta kendine zarar verme düşüncelerine yol açabilir.

- Ulusal Güvenlik Endişeleri: Çevrimiçi tehditlerin göz ardı edilmesi, bireysel veya kurumsal düzeylerin ötesine geçerek ulusal güvenlik meselesi haline gelebilir. Kritik altyapı veya hükümet sistemlerine yönelik siber saldırılar temel hizmetleri aksatabilir, hassas bilgileri tehlikeye atabilir ve ulusal istikrarı baltalayabilir.

3. SAFEGUARDING PERSONAL INFORMATION

3.1. GİZLİLİĞİN KORUNMASININ ÖNEMİ

Gizliliğin korunması, günümüz dijital çağında teknoloji ve internetin yaygın kullanımı nedeniyle büyük önem taşımaktadır. Bir bireyin kişisel bilgilerinin, verilerinin ve çevrimiçi faaliyetlerinin yetkisiz erişime, kötüye kullanıma ve istismara karşı korunmasını ifade eder. Mahremiyetin korunmasının önemi çeşitli açılardan anlaşılabilir:

- Kişisel Güvenlik ve Emniyet: Gizliliğin korunması, sosyal güvenlik numaraları, finansal veriler veya ev adresleri gibi hassas kişisel bilgilerin gizli ve güvende kalmasını sağlar. Bu bilgilere yetkisiz erişimin engellenmesi, kimlik hırsızlığı, mali dolandırıcılık ve bireyler için ciddi sonuçlar doğurabilecek diğer siber suç türlerinin önlenmesine yardımcı olur.

- Veri Gizliliği ve Kontrolü: Bireyler, verilerinin kuruluşlar tarafından nasıl toplandığını, saklandığını

	ve kullanıldığını kontrol etme hakkına sahiptir. Gizliliğin korunması, bireylerin verilerini paylaşma konusunda bilinçli seçimler yapabilmelerini ve belirli amaçlar için kullanılmasına izin verebilmelerini sağlar. • Güvenin Sürdürülmesi: Gizliliğin korunması, bireyler ve kuruluşlar arasında güvenin oluşturulması ve sürdürülmesi için gereklidir. Kullanıcılar kişisel bilgilerinin sorumlu ve güvenli bir şekilde ele alınacağına güvendiklerinde, çevrimiçi hizmetlere katılma, işlem yapma ve güvenle bilgi paylaşma olasılıkları daha yüksektir. • Kişisel Özgürlüğün Korunması: Mahremiyete saygı duymak, bireylerin çevrimiçi faaliyetleri veya tercihleri temelinde gözetim veya ayrımcılık korkusu olmadan kendilerini özgürce ifade etmelerine izin vermek anlamına gelir. Mahremiyetin korunması, ifade ve düşünce özgürlüğü hakkının korunması için esastır. • Çevrimiçi Taciz ve Takiplerin Önlenmesi: Mahremiyetin korunması bireyleri çevrimiçi taciz ve takipten korur. Gizlilik önlemleri, kişisel bilgilere erişimi kısıtlayarak hedefli saldırı veya siber zorbalık riskini azaltır. • Kişisel İlişkilerin Korunması: Gizlilik koruması, bireylerin güvenilir ilişkiler çerçevesinde iletişim kurmasına ve bilgi paylaşmasına olanak tanıyarak özel konuşmaların ve etkileşimlerin gizli kalmasını sağlar. • Verilerin Kötüye Kullanımını Önleme: Gizlilik koruması, kişisel verilerin bireyin amaçladığı amaçlar dışında kullanılması riskini azaltır. Bu, istenmeyen pazarlama kampanyalarından, spam e-postalardan veya kişisel alanı ihlal edebilecek kişiselleştirilmiş içerikten kaçınmayı içerir. • Ayrımcılık ve Profil Oluşturmanın Önlenmesi: Gizliliğin korunması, bireylerin kişisel bilgileri veya çevrimiçi davranışları temelinde profillerinin çıkarılmasını ve ayrımcılığa uğramalarını önlemeye yardımcı olabilir. Yeterli gizlilik koruması olmadan veri toplanması, adil olmayan ve önyargılı kararların alınmasına yol açabilir.

- Siber Güvenlik ve Dijital Güven: Gizliliğin korunması ve siber güvenlik birbiriyle bağlantılıdır. Gizlilik ihlali siber güvenlik olaylarına yol açabilir ve bunun tersi de geçerlidir. Bireyler ve kuruluşlar gizliliğe öncelik vererek dijital güven ve güvenlik kültürünü teşvik edebilirler.

3.2. GÜVENLİ ÇEVRİMİÇİ HESAP YÖNETİMİ

Güvenli çevrimiçi hesap yönetimi, kişinin çevrimiçi hesaplarını yetkisiz erişim ve veri ihlali riskini en aza indirecek şekilde korumayı ve yönetmeyi amaçlayan bir dizi uygulama ve stratejidir. Doğru çevrimiçi hesap yönetimi, kişisel bilgilerin gizliliğini korumak, kimlik hırsızlığını önlemek ve dijital varlıkları korumak için çok önemlidir. İşte güvenli çevrimiçi hesap yönetimi için bazı temel hususlar ve en iyi uygulamalar:

- Güçlü ve Benzersiz Parolalar: Her bir çevrimiçi hesap için güçlü ve benzersiz parolalar kullanın. "123456" veya " parola" gibi kolayca tahmin edilebilen parolalar kullanmaktan kaçının. Bunun yerine, büyük ve küçük harfler, sayılar ve özel karakterlerden oluşan karmaşık parolalar oluşturun.

- Parola Yöneticileri: Parolaları güvenli bir şekilde oluşturmak, saklamak ve yönetmek için saygın bir parola yöneticisi kullanmayı düşünün. Parola yöneticileri, hepsini hatırlamanıza gerek kalmadan her hesap için güçlü ve benzersiz parolalar tutmanıza yardımcı olur.

- İki Faktörlü Kimlik Doğrulamayı (2FA) Etkinleştirin: Mümkün olduğunda, çevrimiçi hesaplarınız için iki faktörlü kimlik doğrulamayı etkinleştirin. 2FA, şifrenize ek olarak mobil cihazınıza gönderilen tek seferlik bir kod gibi ikinci bir doğrulama biçimi gerektirerek ekstra bir güvenlik katmanı ekler.

- Hesap Etkinliğini İzleyin: Hesap etkinliğinizi düzenli olarak gözden geçirin ve yetkisiz girişler veya şüpheli eylemler için tetikte olun. Olağandışı bir etkinlik fark ederseniz, hesabınızı güvence altına almak için şifrenizi değiştirmek ve hesap sağlayıcınızla iletişime geçmek gibi acil önlemler alın.

	• Halka Açık Bilgisayarlardan ve Wi-Fi'den Kaçının: E-posta veya bankacılık gibi hassas hesaplara halka açık bilgisayarlardan veya güvenli olmayan Wi-Fi ağlarından erişmekten kaçının. Halka açık bilgisayarlar oturum açma kimlik bilgilerini depolayabilir ve güvenli olmayan Wi-Fi verilerinizi potansiyel dinlemelere maruz bırakabilir. • Kimlik Avı Girişimlerine Dikkat Edin: Hassas bilgiler isteyen veya hesaplarınızda oturum açmanızı isteyen istenmeyen e-postalara, mesajlara veya bağlantılara karşı dikkatli olun. Herhangi bir bilgi vermeden önce gönderenin ve web sitesinin gerçekliğini doğrulayın • . • Hesap Kurtarma Bilgilerini Düzenli Olarak Güncelleyin: Alternatif e-posta adresleri veya telefon numaraları gibi hesap kurtarma bilgilerinizi güncel tutun. Bu, şifrenizi unutursanız veya başka giriş sorunlarıyla karşılaşırsanız hesabınıza yeniden erişebilmenizi sağlar. • Gizlilik ve Güvenlik Ayarlarını Gözden Geçirin: Çevrimiçi hesaplarınızın gizlilik ve güvenlik ayarlarını düzenli olarak gözden geçirin. Gizlilik ve işlevsellik arasında doğru dengeyi sağlamak için ayarları tercihlerinize ve ihtiyaçlarınıza göre düzenleyin. • Oturumu Kapatın ve Cihazları Güvenli Hale Getirin: Özellikle paylaşılan veya herkese açık cihazlarda, hesaplarınızı kullanmayı bitirdiğinizde her zaman oturumu kapatın. Ayrıca, kişisel cihazlarınızı güçlü parolalar veya biyometrik kimlik doğrulama ile güvence altına alın. • Parolaları Düzenli Olarak Değiştirin: Özellikle e-posta ve bankacılık gibi kritik hesaplar için şifrelerinizi periyodik olarak değiştirmeyi düşünün. Parolaları düzenli olarak güncellemek ekstra bir güvenlik katmanı ekler. • Hesap Kurtarma Seçeneklerini Etkinleştirin: Kilitlenmeniz durumunda hesabınıza yeniden erişim sağlamak için güvenlik soruları veya yedekleme kodları gibi hesap kurtarma seçeneklerini ayarlayın.

3.3. SORUMLU SOSYAL MEDYA PAYLAŞIMI

Sorumlu sosyal medya paylaşımı, sosyal medya platformlarında mahremiyete saygı duyan, olumlu etkileşimleri teşvik eden ve yanlış bilgi veya zarara katkıda bulunmaktan kaçınan bir şekilde içerik paylaşmanın bilinçli ve dikkatli yaklaşımını ifade eder. Sorumlu sosyal medya paylaşımını uygulamak, dijital görgü kurallarını sürdürmek, olumlu bir çevrimiçi topluluğu teşvik etmek ve hem kişisel hem de kolektif refahı korumak için çok önemlidir. İşte sorumlu sosyal medya paylaşımının bazı temel yönleri:

- Kişisel Bilgilerin Korunması: Ev adresleri, telefon numaraları veya finansal detaylar gibi hassas kişisel bilgileri sosyal medyada paylaşma konusunda dikkatli olun. Kişisel bilgilerin korunması, kimlik hırsızlığı ve gizlilikle ilgili diğer risklere karşı korunmaya yardımcı olur.

- Gizlilik Ayarlarını Ayarlama: Sosyal medya platformlarındaki gizlilik ayarlarınızı düzenli olarak gözden geçirin ve ayarlayın. Her gönderi için hedef kitleyi özelleştirerek yalnızca hedef kitlenin içeriğinizi görüntüleyebilmesini ve etkileşimde bulunabilmesini sağlayın.

- İzne Saygı Göstermek: Fotoğraflarını veya kişisel bilgilerini sosyal medyada paylaşmadan önce kişilerden onay alın. Kişilerin gönderilerde etiketlenme veya içerikte bahsedilme konusundaki tercihlerini dikkate alın.

- Doğruluk Kontrolü ve Yanlış Bilgilendirmeden Kaçınma: Haber makalelerini, bilgileri veya görselleri paylaşmadan önce bunların doğruluğunu güvenilir kaynaklardan teyit edin. Söylentilerin veya yanlış anlatıların yayılmasına katkıda bulunabilecek yanlış bilgileri veya doğrulanmamış içerikleri yaymaktan kaçının.

- Zamanlama ve Sıklık Konusunda Dikkatli Olun: Takipçileriniz için aşırı bilgi yüklemesine yol açabileceğinden aşırı veya uygunsuz paylaşımlardan kaçının. Farklı zaman dilimlerine ve hedef kitlenizin tercihlerine saygı duymak için paylaşımlarınızın zamanlamasına dikkat edin.

	• Pozitif İçeriği Teşvik Etmek: Moral verici, bilgilendirici veya ilham verici içerikler paylaşın. Olumlu paylaşımlar daha sağlıklı bir çevrimiçi ortama katkıda bulunur ve takipçileriniz arasında bir topluluk duygusu yaratır. • Anlaşmazlıkları Saygılı Bir Şekilde Ele Alın: Başkalarıyla aynı fikirde olmasanız bile sosyal medyada saygılı ve yapıcı tartışmalara katılın. Çevrimiçi tartışmalara girmekten veya kişisel saldırılara başvurmaktan kaçının. • Zararlı veya Saldırgan İçerikten Kaçınma: Başkaları için saldırgan, ayrımcı veya zararlı olabilecek içerikleri paylaşmaktan kaçının. Paylaşımlarınızın farklı bireyler ve topluluklar üzerindeki potansiyel etkisinin farkında olun. • Telif Haklarını Koruma: Telif hakkı yasalarına saygı gösterin ve uygun yetkilendirme veya atıf olmadan telif hakkıyla korunan materyalleri paylaşmaktan kaçının. Çalışmalarını paylaşırken orijinal yaratıcılara kredi verin. • Paylaşılan İçeriği Gözden Geçirme: Değerlerinizle ve çevrimiçi ortamda yansıtmak istediğiniz imajla uyumlu olduğundan emin olmak için paylaşılan içeriğinizi düzenli olarak gözden geçirin. Artık mevcut bakış açınızı yansıtmayan gönderileri silin veya güncelleyin. • Dijital Nezaketi Teşvik Etmek: Sosyal medyadaki etkileşimlerinizde nazik ve empatik olun. Siber zorbalık, nefret söylemi veya herhangi bir zararlı davranış biçimine katılmaktan veya bunları yaymaktan kaçının. • Olumlu Bir Çevrimiçi Kültürü Teşvik Etmek: Olumlu bir örnek oluşturarak başkalarını sorumlu sosyal medya paylaşımı yapmaya teşvik edin. Dijital vatandaşlık ve sorumlu dijital vatandaşlar olmanın önemi hakkında tartışmalara katılın. 4. SOSYAL MEDYADA GÜVENLİ BİR ŞEKİLDE GEZİNMEK 4.1. GİZLİLİK AYARLARININ YAPILMASI

	Gizlilik ayarlarının yapılması, kişisel bilgilerin çeşitli platformlar, web siteleri ve uygulamalardaki erişim ve görünürlük düzeyinin özelleştirilmesi sürecini ifade eder. Hangi verilerin paylaşılacağı, kimlerle paylaşılacağı ve üçüncü taraflarca nasıl kullanılacağı konusunda bilinçli seçimler yapmayı içerir. Bireyler, gizlilik ayarlarını düzenleyerek dijital ayak izleri üzerinde daha fazla kontrol sahibi olabilir ve kişisel bilgilerini gereksiz maruziyetten koruyabilirler. İşte gizlilik ayarlarını düzenlemenin önemi ve adımları hakkında ayrıntılı bir açıklama: Gizlilik Ayarlarını Düzenlemenin Önemi: • Kişisel Bilgilerin Korunması: Gizlilik ayarlarının yapılması, bireylerin başkaları tarafından görülebilen kişisel bilgi miktarını sınırlamasına olanak tanıyarak kimlik hırsızlığı, takip veya sosyal mühendislik saldırıları riskini azaltır. • Veri Paylaşımını Kontrol Etme: Gizlilik ayarlarını özelleştirerek, bireyler sosyal medya platformları, web siteleri ve uygulamalarla hangi verileri paylaştıklarını kontrol edebilir, bilgilerinin toplanmasını ve kullanılmasını sınırlandırabilir. • Hedefli Reklamları Önleme: Gizlilik ayarları, bireylerin hedefli reklamlardan ve kişiselleştirilmiş içerikten vazgeçmelerine yardımcı olarak daha özel ve daha az müdahaleci bir çevrimiçi deneyim sağlayabilir. • Verilerin Kötüye Kullanımını Önleme: Gizlilik ayarlarının yapılması, verilerin yetkisiz üçüncü şahıslar tarafından kötüye kullanılması olasılığını azaltarak olası ihlallere ve hassas bilgilere yetkisiz erişime karşı koruma sağlar. • Çevrimiçi Güvenliği Artırmak: Gizlilik ayarları aracılığıyla kişisel bilgilere erişimi kısıtlamak çevrimiçi güvenliği artırabilir ve sosyal mühendislik veya kimlik avı saldırıları riskini en aza indirebilir. Gizlilik Ayarlarını Ayarlama Adımları: • Hesap Ayarlarını Gözden Geçirin: Sosyal medya platformlarında, gizlilik tercihlerini özelleştirme seçeneklerine erişmek için hesap ayarlarını veya gizlilik ayarları bölümünü inceleyin.

	• Gönderiler için Hedef Kitle Seçin: Arkadaşlarınız, arkadaşlarınızın arkadaşları gibi gönderilerinizi kimlerin görüntüleyebileceğini belirleyin. İçeriğinizin görünürlüğünü sınırlamak için daha dar bir kitleyi tercih edin. • Profil Bilgilerini Kontrol Edin: E-posta adresiniz, telefon numaranız veya doğum tarihiniz gibi hangi profil bilgilerinin başkaları tarafından görülebileceğine karar verin. Mümkünse hassas verilerin görünürlüğünü en aza indirin. • Uygulama İzinlerini Yönetin: Mobil uygulamalarda, cihaz ayarlarından uygulama izinlerini gözden geçirin ve yönetin. Her uygulama için yalnızca gerekli izinlere izin verin ve izin gerektirmeyen uygulamaların izinlerini iptal edin. • Veri Toplama İşleminden Çıkın: Bazı platformlar ve web siteleri, reklam amaçlı veri toplama ve paylaşımından vazgeçme seçeneği sunar. Veri takibini azaltmak için bu seçeneklerden yararlanın. • Konum Paylaşımını Özelleştirin: Konumunuzu ne zaman ve kiminle paylaşacağınızı seçin. Gerekmediğinde konum paylaşımını kapatın veya belirli güvenilir uygulamalarla sınırlayın. • Anonim Taramayı Göz Önünde Bulundurun: Tarama geçmişinin ve çerezlerin cihazınızda depolanmasını önlemek için özel veya gizli tarama modlarını kullanın. • Üçüncü Taraf Uygulama Erişimini Kontrol Edin: Hesap bilgilerinize erişimi olan üçüncü taraf uygulamaları gözden geçirin ve yönetin. Artık kullanılmayan veya erişime ihtiyaç duymayan uygulamaların erişimini iptal edin. • Varsayılan Ayarlara Karşı Dikkatli Olun: Birçok platformda varsayılan gizlilik ayarları istenenden daha izin verici olabilir. Bu ayarları tercihlerinize göre düzenlemek için zaman ayırın. • Düzenli Olarak Gözden Geçirin ve Güncelleyin: Platformlar ve uygulamalar gizliliğinizi etkileyen yeni özellikler veya değişiklikler sunabileceğinden

gizlilik ayarlarınızı düzenli olarak gözden geçirin ve güncelleyin.

4.2. ARKADAŞLIK İSTEKLERİNİ VE MESAJLARI İŞLEME

Sosyal medya platformlarında ve mesajlaşma uygulamalarında arkadaşlık isteklerini ve mesajları ele almak, başkalarıyla etkileşimlerinizde dikkatli, anlayışlı ve saygılı olmayı gerektirir. Kişisel sınırları korumak, gizliliğinizi korumak ve olumlu bir çevrimiçi deneyimi teşvik etmek çok önemlidir. İşte arkadaşlık isteklerini ve mesajlarını ele almak için bazı yönergeler:

Arkadaşlık İsteklerini İşleme:

- Kimliği Doğrulayın: Bir arkadaşlık isteğini kabul etmeden önce, kişiyi tanıdığınızdan veya ortak arkadaşlarınız olduğundan emin olun. Tanımadığınız veya şüpheli profillerden gelen istekleri kabul etme konusunda dikkatli olun.

- Gizlilik Ayarlarını Kontrol Edin: Size kimlerin arkadaşlık isteği gönderebileceğini kontrol etmek için gizlilik ayarlarınızı düzenleyin. Yabancılardan istek alma olasılığını azaltmak için arkadaşlık isteklerini arkadaşlarınızın arkadaşlarıyla veya belirli gruplarla sınırlayın.

- Yabancıları Kabul Etmekten Kaçının: Yeni bağlantılar ekleme konusunda seçici olun. Kişisel olarak tanımadığınız kişilerden gelen arkadaşlık isteklerini, özellikle de ortak bağlantıları yoksa, kabul etmekten kaçının.

- Şüpheli Hesapları Engelleyin veya Bildirin: Şüpheli veya sahte hesaplardan arkadaşlık isteği alırsanız, bunları engellemeyi veya platform yöneticilerine bildirmeyi düşünün.

- Profil Bilgilerini İnceleyin: Bir arkadaşlık isteğini kabul etmeden önce, gerçek göründüğünden ve sizin değerleriniz ve ilgi alanlarınızla uyumlu olduğundan emin olmak için istek sahibinin profilini inceleyin.

- Sınırlara Saygı Gösterin: Biriyle bağlantı kurmaktan rahatsız oluyorsanız arkadaşlık isteklerini

	reddetmenizde bir sakınca yoktur. Kendi sınırlarınıza saygı gösterin ve her isteği kabul etmek zorunda hissetmeyin. Mesajları Ele Alma: • Saygılı Olun: Mesajlara kibar ve saygılı bir şekilde yanıt verin. Çevrimiçi bir sohbette size nasıl davranılmasını istiyorsanız siz de başkalarına öyle davranın. • Gönderenleri Doğrulayın: Tanımadığınız bir göndericiden mesaj alırsanız dikkatli olun. Şüpheli bağlantılara tıklamaktan veya bilinmeyen kaynaklardan gelen ekleri indirmekten kaçının. • Hassas Bilgileri Paylaşmaktan Kaçının: Mesajlaşma uygulamaları aracılığıyla hassas kişisel bilgileri, finansal ayrıntıları veya şifreleri paylaşmaktan kaçının. İyi tanımadığınız kişilerle özel bilgilerinizi paylaşma konusunda dikkatli olun. • Taciz veya İstismarı Bildirin: Saldırgan, tehdit edici veya taciz edici mesajlar alırsanız, göndereni platform yöneticilerine veya mesajlaşma uygulamasının destek ekibine bildirin. • Mesaj Gizliliğini Ayarlayın: Size kimlerin mesaj gönderebileceğini kontrol etmek için mesaj gizliliği ayarlarınızı yapın. Mesajlaşma erişimini arkadaşlarınız veya kişilerinizle sınırlayın. • Engelleme Özelliğini Kullanın: Birisi sizi rahatsız ediyorsa veya uygunsuz mesajlar gönderiyorsa, o kişinin daha fazla iletişim kurmasını önlemek için engelleme özelliğini kullanın. • Ton ve Niyete Dikkat Edin: Mesajlar, ton ve yüz ifadelerinin eksikliği nedeniyle kolayca yanlış yorumlanabilir. Kendi iletişiminize dikkat edin ve yanlış anlaşılmaları önlemeye çalışın. • Mesajlaşmaya Ara Verin: Diğer faaliyetlere odaklanmak ve dijital bunalımı azaltmak için mesajlaşmaya ve sosyal medyaya ara vermekte bir sakınca yoktur.

4.3. İSTİSMARCI HESAPLARIN BİLDİRİLMESİ VE ENGELLENMESİ

İstismarcı hesapların bildirilmesi ve engellenmesi, güvenli ve olumlu bir çevrimiçi ortamın sürdürülmesinde çok önemli bir adımdır. İstismarcı hesaplar siber zorbalık, taciz, nefret söylemi ve diğer çevrimiçi istismar biçimleri gibi zararlı davranışlarda bulunabilir. Bu hesapları bildirmek ve engellemek, kendinizi ve başkalarını bu hesapların zararlı eylemlerinden korumaya yardımcı olur. Burada raporlama ve engellemenin nasıl işlediğine ve neden önemli olduğuna dair bir açıklama yer almaktadır:

Taciz İçeren Hesapları Bildirme:

- Zararlı Davranışı Tanımlayın: Taciz, tehdit veya nefret söylemi gibi taciz edici veya zararlı davranışlarda bulunan bir hesapla karşılaşırsanız, bunu fark etmeniz önemlidir.
- Hesabı bildirin: Çoğu sosyal medya platformu ve çevrimiçi hizmetin bir raporlama mekanizması vardır. Yöneticileri veya moderatörleri taciz edici davranış hakkında bilgilendirmek için platformun raporlama özelliğini kullanın.
- Kanıt Sağlayın: Taciz içeren bir hesabı rapor ederken, raporunuzu desteklemek için ekran görüntüleri veya saldırgan içeriğin bağlantıları gibi kanıtlar sağlamak yararlı olabilir.
- Uygun Kategoriyi Seçin: Sosyal medya platformları genellikle farklı raporlama kategorileri sunar. Bildirdiğiniz istismar türüne en uygun kategoriyi seçin.
- Raporlama Yönergelerine Saygı Gösterin: Hesapları geçerli nedenlerle bildirdiğinizden emin olmak için platformun raporlama yönergelerine aşina olun. Raporlama sisteminin etkinliğini engelleyebileceğinden yanlış raporlamadan kaçının.

Taciz İçeren Hesapları Engelleme:

- Kendinizi Koruyun: Taciz içeren bir hesabı engellemek, o hesabın sizinle etkileşime geçmesini engeller. Ruhsal sağlığınızı korumaya ve sizin için

güvenli bir çevrimiçi alan yaratmaya yardımcı olabilir.

- İstenmeyen Temasları Önleyin: Bir hesabı engellediğinizde, o hesabın arkasındaki kullanıcı sizi takip edemez, size mesaj gönderemez veya gönderilerinize yorum yapamaz.

- Anonimlik: Engelleme genellikle özel bir eylemdir. Engellediğiniz kullanıcı engellendiğine dair herhangi bir bildirim almayacaktır.

- Daha Fazla Etkileşim Olmayacak: Bir hesabı engelledikten sonra, artık onun hiçbir içeriğini veya etkinliğini göremezsiniz ve o da sizinkini göremez.

Raporlama ve Engelleme Neden Önemlidir?

- Zararın Önlenmesi: Taciz içeren hesapların bildirilmesi, hesaba karşı işlem yapılmasını sağlayarak size veya başkalarına daha fazla zarar verilmesini önleyebilir.

- Platform Kurallarının Uygulanması: Taciz içeren davranışların bildirilmesi, platformun hizmet şartlarının ve topluluk kurallarının uygulanmasına yardımcı olarak tüm kullanıcılar için daha güvenli bir ortam yaratır.

- Topluluk Sağlığını Desteklemek: Taciz içeren hesapları bildirerek ve engelleyerek, sağlıklı ve saygılı bir çevrimiçi topluluğun geliştirilmesine katkıda bulunursunuz.

- Kullanıcıları Güçlendirmek: Raporlama ve engelleme, bireylerin çevrimiçi deneyimlerini kontrol altına almalarını ve kendilerini taciz edici veya zararlı etkileşimlerden korumalarını sağlar.

5. SİBER GÜVENLİK VE MOBİL CİHAZLAR

5.1. AKILLI TELEFON VE TABLETLERDE GÜVENLİĞİN SAĞLANMASI

Akıllı telefonların ve tabletlerin güvenliğini sağlamak, bu cihazların çok sayıda kişisel bilgi ve hassas veri depoladığı

	günümüzün mobil odaklı dünyasında çok önemlidir. Bu cihazların güvenliğini sağlamak yetkisiz erişime, veri ihlallerine ve kötü amaçlı yazılım saldırılarına karşı korunmaya yardımcı olur. İşte akıllı telefon ve tabletlerin güvenliğini sağlamak için bazı temel önlemler: • Kilit Ekranı Güvenliğini Etkinleştirin: PIN, desen, şifre veya biyometrik (parmak izi veya yüz tanıma) gibi güvenli bir kilit ekranı yöntemi ayarlayın. Bu, kaybolması veya çalınması durumunda cihazınıza yetkisiz erişimi önler. • Yazılımı Güncel Tutun: Cihazınızdaki işletim sistemini ve uygulamaları düzenli olarak güncelleyin. Üreticiler güvenlik açıklarını gidermek için güncellemeler yayınlar, bu nedenle cihazınızı güncel tutmak olası istismarlara karşı korunmak için çok önemlidir. • Yalnızca Güvenilir Uygulamaları Yükleyin: Uygulamaları resmi uygulama mağazalarından (ör. Google Play Store, Apple App Store) indirin ve bilinmeyen kaynaklardan uygulama yüklemekten kaçının. Resmi olmayan kaynaklardan gelen kötü amaçlı uygulamalar cihazınızın güvenliğini ve gizliliğini tehlikeye atabilir. • Uygulama İzinlerini Gözden Geçirin: Uygulamalara izin verirken dikkatli olun. Her uygulama tarafından talep edilen izinleri gözden geçirin ve uygulamanın işlevselliği için gerekli olup olmadıklarını değerlendirin. Gizliliğinizi tehlikeye atabilecek gereksiz izinleri vermekten kaçının. • Halka Açık Wi-Fi'de VPN Kullanın: Halka açık Wi-Fi ağlarını kullanırken, internet trafiğinizi şifrelemek ve verilerinizi olası gizli dinleme veya gözetlemelere karşı korumak için bir sanal özel ağ (VPN) kullanmayı düşünün. • Güvenli Mobil Tarama: Web siteleri için şifrelenmiş bağlantılar (HTTPS) sunan güvenli tarayıcılar kullanın. Çevrimiçi bankacılık gibi hassas bilgilere güvenli olmayan veya halka açık ağlardan erişmekten kaçının. • Verileri Düzenli Olarak Yedekleyin: Cihazınızın verilerini düzenli olarak güvenli bir bulut hizmetine

	veya harici bir cihaza yedekleyin. Bu, cihazınız kaybolsa, hasar görse veya sıfırlansa bile önemli bilgilerinizin güvende olmasını sağlar. • Şüpheli Bağlantılara Tıklamaktan Kaçının: Bilinmeyen kaynaklardan gelen e-postalardaki, mesajlardaki veya açılır pencerelerdeki bağlantılara tıklama konusunda dikkatli olun. Kötü amaçlı bağlantılara tıklamak kimlik avı girişimlerine veya kötü amaçlı yazılımların yüklenmesine yol açabilir. • Hassas Uygulamalar için Uygulama Kilitlerini Kullanın: Cihazınızdaki hassas uygulamalara veya içeriğe erişimi kısıtlamak için uygulama kilitlerini veya misafir modu özelliğini kullanmayı düşünün. Bu, özellikle cihazınızı başkalarıyla paylaşırken ek bir güvenlik katmanı sağlar. • Cihaz Verilerini Şifreleyin: Cihazınız destekliyorsa, cihaza başka biri tarafından fiziksel olarak erişilse bile verilerinizi yetkisiz erişime karşı korumak için şifrelemeyi etkinleştirin. 5.2. UYGULAMA İZİNLERİ VE VERİ ERİŞİMİ Uygulama izinleri ve veri erişimi, bir kullanıcının cihazındaki çeşitli özelliklere ve verilere erişmek için mobil uygulamalar (uygulamalar) tarafından talep edilen izinleri ifade eder. Kullanıcılar akıllı telefonlarına veya tabletlerine uygulama yükleyip kullandıklarında, uygulamaların düzgün çalışması için belirli cihaz kaynaklarına ve kişisel bilgilere erişmesi gerekebilir. Bu izinler, uygulamaların belirli işlevler sunmasını ve kullanıcı deneyimini geliştirmesini sağlar. Ancak, kullanıcıların gizliliklerini ve güvenliklerini korumak için bu izinleri anlamaları ve yönetmeleri çok önemlidir. İşte uygulama izinlerine ve veri erişimine daha yakından bir bakış: • Uygulama İzinleri Türleri: Uygulama izinleri, uygulamanın işlevselliğine ve platforma (Android veya iOS) bağlı olarak değişebilir. Yaygın uygulama izni türleri arasında cihazın kamerasına, mikrofonuna, konumuna, kişilerine, takvimine, depolama alanına, SMS'lerine, arama kayıtlarına ve daha fazlasına erişim yer alır. Bazı uygulamalar Bluetooth çevre birimleri gibi diğer bağlı cihazları kullanmak için de izin isteyebilir.

	• İzin Talepleri: Kullanıcılar bir uygulamayı yüklediğinde, uygulama çalışması için gereken belirli izinleri talep edebilir. İzin talepleri genellikle uygulama yükleme işlemi sırasında veya uygulama belirli bir özelliğe ilk kez erişmeye çalıştığında sunulur. Kullanıcılar bu izinleri verebilir veya reddedebilir. • Uygulama İzinlerinin Amacı: Uygulama izinleri, belirli uygulama özelliklerini etkinleştirmek için gereklidir. Örneğin, bir fotoğraf düzenleme uygulamasının fotoğraf çekmek ve kaydetmek için cihazın kamerasına ve depolama alanına erişmesi gerekir. Bir navigasyon uygulaması, doğru yol tarifleri sağlamak için konum erişimi gerektirir. • Gizliliğin Korunması: Uygulama izinleri genellikle uygulama işlevselliği için gerekli olsa da, kullanıcılar uygulamanın amacını ve talep edilen izinlerin makul olup olmadığını düşünmeden izin verme konusunda dikkatli olmalıdır. Aşırı izinler vermek gizliliği tehlikeye atabilir veya uygulamaların yasal bir ihtiyaç olmadan hassas verilere erişmesine izin verebilir. • Uygulama İzinlerini Yönetme: Çoğu modern işletim sistemi, kullanıcıların uygulama izinlerini yönetmesine olanak tanır. Kullanıcılar cihaz ayarlarından uygulama izinlerini gözden geçirebilir ve değiştirebilir, böylece istedikleri zaman tek tek uygulamalar için belirli izinleri verebilir veya iptal edebilirler. • İzinleri Dikkatlice Okuyun: İzinleri vermeden önce, kullanıcılar bir uygulama tarafından talep edilen izinleri dikkatlice okumalıdır. Bir uygulama, işlevselliği ile ilgisiz görünen izinler talep ediyorsa, bu bir tehlike işareti olabilir ve kullanıcılar dikkatli olmalı veya alternatif uygulamalar kullanmayı düşünmelidir. • Uygulama İzinleri ve Güncellemeleri: Uygulamaları güncellerken, yeni veya değiştirilmiş izinleri gözden geçirmek çok önemlidir. Bazen uygulama güncellemeleri ek izinler getirebilir ve kullanıcılar bu izinlerin kendi tercihleri ve ihtiyaçlarıyla uyumlu olduğundan emin olmalıdır.

- iOS ve Android için Uygulama İzin Talepleri: iOS ve Android uygulama izinlerini farklı şekilde ele alsa da, her iki platform da kullanıcılara kendi ayarlarında izinleri yönetme olanağı sunar. iOS'ta kullanıcılar uygulama ayarlarında "Gizlilik" altında izinleri inceleyebilir ve yönetebilir. Android'de kullanıcılar cihaz ayarlarında "Uygulamalar ve bildirimler" veya "Uygulama yöneticisi" bölümüne giderek izinleri yönetebilirler.

5.3. MOBİL CİHAZLARIN ÇALINMA VE KAYBOLMAYA KARŞI KORUNMASI

Mobil cihazların çalınmaya ve kaybolmaya karşı korunması, kişisel bilgilerin korunması, kimlik hırsızlığının önlenmesi ve hassas verilerin gizliliğinin korunması için çok önemlidir. Akıllı telefonlar ve tabletler gibi mobil cihazlar, taşınabilirlikleri ve depoladıkları değerli bilgiler nedeniyle hırsızlar için genellikle hedeftir. Güvenlik önlemlerinin uygulanması, hırsızlık veya kayıpla ilişkili riskleri önemli ölçüde azaltabilir. İşte mobil cihazları korumak için bazı önemli adımlar:

- Kilit Ekranı Güvenliğini Kurun: PIN, desen, şifre veya biyometrik (parmak izi veya yüz tanıma) gibi güvenli bir kilit ekranı yöntemini etkinleştirin. Bu, yanlış ellere geçmesi durumunda cihazınıza yetkisiz erişimi önler.

- Cihazımı Bul Hizmetlerini kullanın: Aygıtınızda "Aygıtımı Bul" veya "iPhone'umu Bul" özelliğini etkinleştirin. Bu hizmetler, kaybolması veya çalınması durumunda aygıtınızın yerini belirlemenize, kilitlemenize veya uzaktan silmenize olanak tanır.

- Yazılım ve Uygulamaları Güncel Tutun: En son güvenlik yamalarına ve hata düzeltmelerine sahip olduğunuzdan emin olmak için aygıtınızın işletim sistemini ve uygulamalarını düzenli olarak güncelleyin. Üreticiler güvenlik açıklarını gidermek ve cihaz güvenliğini artırmak için güncellemeler yayınlar.

- Cihazları Gözetimsiz Bırakmaktan Kaçının: Mobil cihazınızı restoranlar, toplu taşıma araçları veya spor salonları gibi halka açık yerlerde gözetimsiz bırakma

	konusunda dikkatli olun. Hırsızlık riskini azaltmak için cihazınızı yanınızda bulundurun veya güvenli bir şekilde saklayın. • Kalabalık Alanlarda Dikkatli Olun: Kalabalık alanlarda, özellikle de yankesicilik ve hırsızlığın daha olası olduğu yerlerde çevrenize dikkat edin. Cihazınızı kalabalık alanlarda kullanırken dikkatli olun. • Cihazınızı Evde Güvenli Bir Şekilde Saklayın: Mobil cihazınızı kullanmadığınız zamanlarda, özellikle de evde, güvenli bir yerde saklayın. Tezgahların üzerinde, açık pencerelerin yakınında veya kolay erişilebilir alanlarda bırakmaktan kaçının. • Hassas Uygulamalar için Uygulama Kilitleri Kullanın: Cihazınızdaki hassas uygulamalara veya içeriğe erişimi kısıtlamak için uygulama kilitlerini veya misafir modu özelliklerini kullanmayı düşünün. Bu, özellikle cihazınızı başkalarıyla paylaşırken ekstra bir güvenlik katmanı ekler. • Cihaz Verilerini Şifreleyin: Cihazınız destekliyorsa, cihazınıza başka biri tarafından fiziksel olarak erişilse bile verilerinizi yetkisiz erişime karşı korumak için şifrelemeyi etkinleştirin. • Halka Açık Şarj İstasyonlarından Kaçının: Güvenliği ihlal edilmiş olabileceğinden ve veri hırsızlığı veya kötü amaçlı yazılım yükleme riski oluşturabileceğinden, halka açık şarj istasyonlarını veya USB bağlantı noktalarını kullanmaktan kaçının. • Verileri Düzenli Olarak Yedekleyin: Cihazınızın verilerini düzenli olarak güvenli bir bulut hizmetine veya harici bir cihaza yedekleyin. Bu, cihazınız kaybolsa, hasar görse veya sıfırlansa bile önemli bilgilerinizin güvende olmasını sağlar. • Gizlilik Ekran Koruyucuları Kullanın: Meraklı gözlerin kamusal alanlarda ekranınızı görüntülemesini önlemek için gizlilik ekran koruyucuları kullanmayı düşünün. • Cihazları Yetkililere Kaydettirin: Mobil cihazlarınızı yerel makamlara veya ilgili veri tabanlarına

	kaydettirin. Bu, cihazınızın çalınması durumunda kurtarma sürecine yardımcı olabilir.
Sözlük :	1. Çevrimiçi Güvenlik Çevrimiçi dünyanın kötü niyetli kısımlarına karşı savunmak için eyleme geçirilebilir yönergeleri takip etme, modern teknolojiyi anlama ve dijital cihazları koruma uygulaması. 2. İnternet Güvenliği Bilgisayarları, ağları ve verileri kötü amaçlı yazılımlar, virüsler ve yetkisiz erişim gibi siber tehditlerden korumak için alınan önlemler ve uygulamalar. 3. Dijital Gizlilik Kişinin kişisel bilgi ve verilerine izinsiz olarak erişilmesini, kullanılmasını veya paylaşılmasını kontrol etme ve koruma hakkı. 4. Siber Güvenlik Dijital cihazların, ağların ve bilgi sistemlerinin bilgisayar korsanlığı, veri ihlalleri ve siber saldırılar dahil olmak üzere siber tehditlerden korunması. 5. Güvenli Çevrimiçi Uygulamalar Bireylerin çevrimiçi faaliyetlerinin güvenli olmasını sağlamak ve gizliliklerini korumak için izlemeleri gereken kurallar ve davranışlar bütünü. 6. Kişisel Bilgilerin Korunması Hassas ve kişisel verilerin yetkisiz erişim veya kötüye kullanıma karşı korunması, kimlik hırsızlığı ve dolandırıcılığın önlenmesi. 7. Sosyal Medya Görgü Kuralları Sosyal medya platformlarını kullanırken bireylerin uyması gereken doğru ve saygılı davranışlar. 8. Veri Güvenliği Dijital verileri yetkisiz erişim, değişiklik veya tahribattan korumak için alınan önlemler ve protokoller. 9. Kimlik Hırsızlığını Önleme Kişisel bilgilerin korunmasına ve suçluların bu bilgileri bireylerin kimliğine bürünmek için kullanmasının önlenmesine yönelik teknikler ve uygulamalar. 10. Şifre Yönetimi Çevrimiçi hesapları korumak için güçlü, benzersiz parolalar oluşturmanın ve bunları güvenli bir şekilde yönetmenin sorumlu uygulaması.

	11. Çevrimiçi Tehditler İnterneti kullanırken karşılaşılan kimlik avı, kötü amaçlı yazılım, dolandırıcılık ve siber zorbalık gibi çeşitli riskler ve tehlikeler. 12. Oltalama Farkındalığı Saldırganların genellikle sahte e-postalar veya web siteleri aracılığıyla hassas bilgileri elde etmek için bireyleri kandırdığı kimlik avı girişimlerini tanıma ve bunlardan kaçınma becerisi. 13. Gizlilik Ayarları Kullanıcıların kişisel bilgilerinin görünürlüğünü ve içeriklerinin hedef kitlesini kontrol etmelerine olanak tanıyan çevrimiçi platformlardaki özelleştirilebilir seçenekler. 14. Kötüye Kullanım Bildirimi Platform yöneticilerini veya moderatörleri platformdaki taciz veya nefret söylemi gibi kötü niyetli veya zararlı davranışlar hakkında bilgilendirme süreci. 15. Hesapları Engelleme İstismarcı veya istenmeyen bir hesabın sizinle etkileşime geçmesini veya sosyal medya platformlarında içeriğinizi görüntülemesini engelleme eylemi. 16. Güvenli Çevrimiçi İşlemler Dolandırıcılığı önlemek için satın alma veya finansal işlemler gibi çevrimiçi işlemlerin güvenli ve emniyetli bir şekilde yapılmasını sağlamak. 17. Dijital Ayak İzi Sosyal medya paylaşımları, arama geçmişi ve çevrimiçi etkileşimler de dahil olmak üzere bir bireyin çevrimiçi faaliyetlerinin geride bıraktığı veri ve bilgi izi. 18. Siber Zorbalığı Önleme Çevrimiçi taciz, yıldırma veya zorbalığı durdurmak ve önlemek için alınan önlemler. 19. İki Faktörlü Kimlik Doğrulama (2FA) Kullanıcıların bir hesaba erişmek için iki kimlik biçimi (örneğin, şifre ve telefonlarına gönderilen benzersiz bir kod) sağlamasını gerektiren ek bir güvenlik katmanı. 20. Güvenli Tarama Alışkanlıkları

	Riskli web sitelerinden ve içeriklerden kaçınarak güvenli ve emniyetli internet gezintisi sağlamak için uygulamalar ve yönergeler.
Kaynakça :	Internet Safety Tips & Internet Safety Rules (kaspersky.com) Online Safety (for Teens) - Nemours KidsHealth What is Online Safety? | SWGfL Online safety conversation | LearnEnglish Teens (britishcouncil.org) Internet safety - Wikipedia Online safety issues - Advice to support children | Internet Matters Internet Safety: Introduction to Internet Safety (gcfglobal.org) indianjournals.com/ijor.aspx?target=ijor:ijie&volume=8&issue=2&article=001 "Internet Safety" in: The International Encyclopedia of Media Literacy Online (researchgate.net) İnternette Güvenlik İpuçları - Google Güvenlik Merkezi (safety.google) Being safe online | eSafety Commissioner How to Stay Safe Online: Internet Safety Tips and Resources (reviews.org)
Kaynaklar (videolar, referans bağlantıları)	https://www.youtube.com/watch?v=qZE45J-MIUg&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=aO858HyFbKI&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=HxySrSbSY7o&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=EyQeUwqCDWg&pp=ygULc2FmZSBvbmxpbmU%3D