

DİJİTAL ORTAMLARDA GİZLİLİK VE GÜVENLİK

5. SINIF



www.sinanakdemir.com.tr

**"GÜNLÜK HAYATTA İNTERNETİ NE SIKLIKLA
KULLANIYORSUNUZ? (OYUN, ÖDEV, VİDEO VB.)"**

**"Girdiğiniz bu dijital
ortamlar sizce ne kadar
gizli ve güvenli?"**



www.sinanakdemir.com.tr



**GÜNLÜK HAYATTA DİJİTAL ORTAMDA
KARŞILAŞABİLECEĞİMİZ GÜVENLİK
TEHDİTLERİ NELER OLABİLİR?**



www.sinanakdemir.com.tr

DİJİTAL ORTAMLARDAKİ TEMEL TEHDİTLER



1. Zararlı Yazılımlar (Malware)

Bilgisayarımıza, tabletimize veya telefonumuza izinsiz sizden "yaramaz" programlardır.

- Örnek: Oyun indirdiğinizi sanırken arka planda tüm dosyalarınızı şifreleyen veya bilgisayarınızı yavaşlatan bir virüs.

DİJİTAL ORTAMLARDAKİ TEMEL TEHDİTLER



2. Kimlik Hırsızlığı

Bir başkasının sizin kullanıcı adınızı, şifrenizi veya kişisel bilgilerinizi ele geçirerek "sizmiş gibi" davranmasıdır.

- Örnek: Sosyal medya hesabınızın çalınması ve listenizdeki arkadaşlarınızdan sizin adınıza para istenmesi

DİJİTAL ORTAMLARDAKİ TEMEL TEHDİTLER



3. Kişisel Bilgilerin Çalınması

Sadece size özel olması gereken verilerin (T.C. kimlik no, adres, telefon, anne-baba adı) kötü niyetli kişilerin eline geçmesidir.

- Örnek: Bir web sitesine kayıt olurken gereksiz yere istenen "ev adresi" bilgisinin, sitenin veri tabanı saldırıya uğradığında başkalarının eline geçmesi.

DİJİTAL ORTAMLARDAKİ TEMEL TEHDİTLER



4. Sosyal Mühendislik Saldırıları

Teknik bir açıktan ziyade, insanların güvenini, merakını veya korkusunu kullanarak onları kandırma yöntemidir.

- Örnek: "Tebrikler! Ücretsiz oyun kredisi kazandınız. Almak için buraya tıklayın ve şifrenizi girin" mesajı. Aslında orada bir hediye yoktur, sadece sizin şifrenizi öğrenmeye çalışıyorlardır.



BİLGİ GÜVENLİĞİNİN 3 TEMEL TAŞI

Bir sistemin güvenli olup olmadığını anlamak için bu üç bileşene bakarız:

Gizlilik

(Confidentiality):

Bilginin sadece yetkili kişilerce görülmesidir. (Örn: Mesajını sadece arkadaşının okuması).

Bütünlük (Integrity):

Bilginin izinsiz değiştirilmemesi, doğruluğunun korunmasıdır. (Örn: Notlarının e-Okul'da doğru kalması).

Erişilebilirlik

(Availability): İhtiyaç duyulduğunda sisteme ulaşılabilmesidir.

(Örn: EBA'nın her istediğinde açılması).

Dijital Ortam	Karşılaşılabilecek Risk / Tehdit	Bilgi Güvenliği Bileşeni (CIA)	Tür (Security mi, Safety mi?)
Sosyal Medya	Özel fotoğrafların veya mesajların başkaları tarafından görülmesi.	Gizlilik (Confidentiality)	Safety (Çevrim İçi Emniyet)
E-Ticaret	Ödeme yaparken kredi kartı bilgilerinin çalınması.	Gizlilik (Confidentiality)	Security (Dijital Güvenlik)
Bilişim Sistemleri	Bir web sitesinin hacklenerek içeriğinin (fiyatlar, isimler) değiştirilmesi.	Bütünlük (Integrity)	Security (Dijital Güvenlik)
Oyun Platformları	Sunuculara yapılan saldırı sonucu oyunun açılmaması veya çökmesi.	Erişilebilirlik (Availability)	Security (Dijital Güvenlik)
Sosyal Medya	Birinin sizin adınıza sahte hesap açıp yanlış bilgiler paylaşması.	Bütünlük (Integrity)	Safety (Çevrim İçi Emniyet)
Dijital Bankacılık	Hesaba giriş yetkisinin engellenmesi veya sistemin kilitlenmesi.	Erişilebilirlik (Availability)	Security (Dijital Güvenlik)
Oyun / Chat	Tanımadığınız kişilerin sizi rahatsız etmesi veya kötü içerik göndermesi.	Gizlilik (Özel alan ihlali)	Safety (Çevrim İçi Emniyet)

**"KİŞİSEL VERİ DENDİĞİNDE
AKLINIZA NE GELİYOR?"**



www.sinanakdemir.com.tr

DİJİTALDE PAYLAŞIM SINIRLARIMIZ



- T.C. Kimlik Numaran
- Ev Adresin ve Konumun
- Anne ve Babanın Telefon Numaraları
- Banka ve Kredi Kartı Bilgileri
- Özel Şifrelerin

Başkalarının Haklarına Saygı
Dijital dünyada sadece kendi verilerimizi değil, başkalarının verilerini de korumalıyız. Bir arkadaşının fotoğrafını veya bir bilgisini, ondan izin almadan paylaşmak bir "Kişisel Sınır" ihlalidir.

Bilgi Türü	Kişisel Veri mi?	Neden?
En sevdiğim renk	✗ Hayır	Birçok kişi aynı rengi sevebilir, seni ele vermez.
Parmak izim	✓ Evet	Dünyada sadece sana özeldir.
Tuttuğum takım	✗ Hayır	Milyonlarca kişiyle paylaştığın genel bir bilgidir.
T.C. Kimlik Numaram	✓ Evet	Devlet katında sadece seni temsil eden, en önemli kimlik bilgindir.

SOSYAL MEDYADA GİZLİLİK

Kişisel bilgilerimizi korumak için sosyal medya araçlarında şu "kilitleri" kullanmalıyız:

1. PROFİLİNİ DÜNYAYA KAPAT (PROFİL GİZLİLİĞİ)

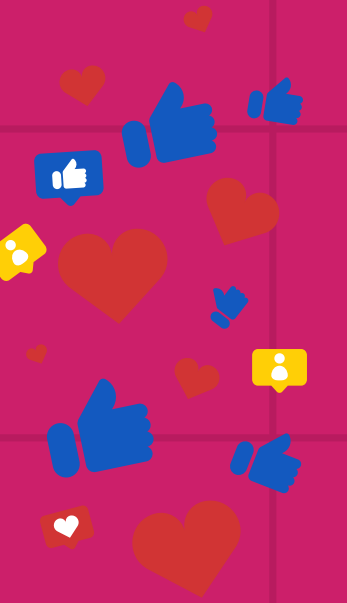
Hesabını "Gizli" moduna al. Böylece paylaşımlarını sadece senin onayladığın, gerçekten tanıdığın kişiler görebilir. Tanımadığın kişilerin hayatına göz atmasına izin verme!

2. GÖRÜNÜRLÜK SINIRINI BELİRLE (ERİŞİLEBİLİRLİK SINIRI)

Paylaştığın her fotoğraf veya belgenin bir "görünürlük ayarı" vardır. Paylaşım yapmadan önce kontrol et: Herkes mi, Arkadaşlar mı, yoksa Sadece Ben mi? En güvenlisi sadece arkadaşlarınla paylaşmaktır.



SOSYAL MEDYADA GİZLİLİK



3. İZİNİ KAYBETTİR (KONUM KAPATMA)

Fotoğraflarına veya hikayelerine yer bildirimi (konum) eklemekten kaçın. Evinin, okulunun veya her gün gittiğin parkın yerini kötü niyetli kişilere kendi elinle gösterme!

4. KONTROL SENDE OLSUN (ETİKETLEME KONTROLÜ)

Başkalarının seni fotoğraflarda etiketlemesini onaya bağla. Senin iznin olmadan kimse senin fotoğrafını kendi profilinde veya senin profilinde gösteremesin.

NEDEN BU KADAR ÖNEMLİ?



Kişisel verilerini paylaşmamanın temel nedenleri:

- **Güvenlik:** Kötü niyetli kişilerin sana veya ailene ulaşmasını engellemek.
- **Gelecek:** İnternette paylaşılan her şey kalıcıdır; ileride silmek istesen de birileri kaydetmiş olabilir.
- **Kontrol:** Seninle ilgili hangi bilginin kimde olacağına sadece sen karar vermelisin.

GÖREVİMİZ GÜVENLİK!

"Melis, çok popüler bir fotoğraf düzenleme uygulaması indirdi. Uygulama Melis'ten şu bilgileri istiyor: Adı, Soyadı, Ev Adresi, Okul Adı ve şifre olarak '12345' girmesini öneriyor. Ayrıca uygulamanın adres çubuğunda 'Güvenli Değil' uyarısı çıkıyor."

Soru: Melis, kişisel bilgilerini korumak için hangi güvenlik önlemlerini almalıdır?



ÇÖZÜM



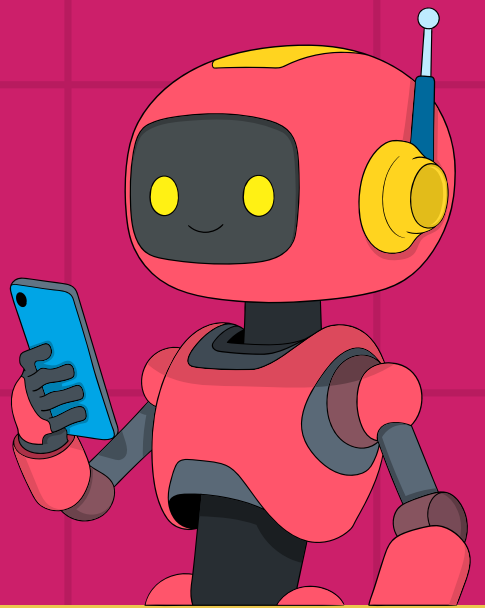
- Güçlü Şifre Oluşturma: Kolay tahmin edilemeyen şifreler seçilmeli.
- Gizlilik Ayarları: Uygulamanın hangi verilere eriştiği kontrol edilmeli.
- İki Faktörlü Doğrulama (2FA): Sadece şifre değil, ikinci bir onay (kod) kullanılmalı.
- Güvenli Bağlantı: Web adresinin başında HTTPS ve Kilit Simgesi olduğu kontrol edilmeli.

YAPAY ZEKÂ VE GÜVENLİĞİMİZ

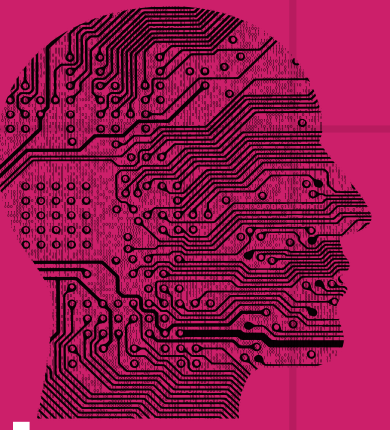
Yapay zekâ (ChatGPT, görsel üreticiler vb.) harika araçlardır ancak dikkatli olmalıyız!

TARTIŞMA SORULARI:

- Yapay zekâ uygulamalarına kişisel bilgilerinizi (adres, telefon, özel sırlar) yazmak güvenli midir?
- Bu araçları kullanırken nelere dikkat etmeliyiz?



YAPAY ZEKA ARKA PLANDA NELER YAPIYOR?



Yapay zeka araçlarını (ChatGPT, Gemini, resim çizme siteleri vb.) kullanırken şu 3 Altın Kuralı asla unutmamalıyız:

1. Yapay Zeka Unutmaz! Yapay zekaya yazdığınız her şey, onun "eğitimi" için sistemde saklanır.
2. Verileriniz Başkalarına Cevap Olabilir!
3. "Ücretsiz" Her Zaman Bedava Değildir! Kişisel bilgileriniz reklam şirketlerine veya üçüncü şahıslara satılabilir..

Özetle: Yapay zekaya, okul bahçesinde hiç tanımadığın birine söylemeyeceğin hiçbir şeyi YAZMA!

GÜVENLİ ŞİFRE



Zayıf bir şifre, hırsıza anahtarı teslim etmektir. İşte güçlü bir şifrenin formülü:

1. Uzunluk: En az 8 karakter olmalı.
2. Büyük ve Küçük Harf: (Örn: A, b)
3. Rakamlar: (Örn: 5, 8)
4. Özel Karakterler: (Örn: !, @, ?, #)
5. Kişisel bilgiler içermemeli (Ad, Soyad, Doğum Tarihi)

Örnek Güvenli Şifre: iRoN-159*

İKİ FAKTÖRLÜ DOĞRULAMA (2FA) NEDİR?

Şifreniz çalinsa bile hesabınızı koruyan ikinci bir kilittir.

- 1. Aşama: Kullanıcı adın ve şifren.
- 2. Aşama: Telefonuna gelen SMS kodu veya onay bildirimi.

Unutma: Evin anahtarı (şifre) çalinsa bile, içerdeki sürgü (2FA) hırsızı durdurur!



Gizlilik Bütünlük Erişebilirlik **HANGİ BİLEŞEN İHLAL EDİLDİ?**



Aşağıdaki durumları analiz edelim:

- Senaryo A: Bir şirketin tüm müşteri telefon numaralarını yanlışlıkla internette yayınlaması.

İhlal: ?

- Senaryo B: Bir hacker'ın okulun web sitesine girip duyuru metnini değiştirmesi.

İhlal: ?

- Senaryo C: Bir oyun sitesinin saldırı olarak saatlerce kapalı kalması.

İhlal: ?

ÇÖZÜM YOLLARIMIZ NELER?



Güvenlik ihlallerini durdurmak için şu önlemleri almalıyız:

- Gizlilik ve Erişilebilirlik İçin: Güçlü şifreleme yöntemleri ve kişisel verilerin korunması kanunlarına uyum.
- Bütünlük İçin: Veri değişikliklerini izleyen sistemler ve sadece yetkili kişilere "düzenleme" izni verilmesi.
- Genel Önlem: Yedekleme yapmak (Erişilebilirlik için) ve güvenlik yazılımları kullanmak

DİJİTAL KALKANLARIMIZ



Güvenli bir internet deneyimi için 3 temel kural:

1. Güçlü Parola İlkeleri

Uzun Olsun: En az 8 karakter.

Karışık Olsun: Büyük harf, küçük harf, rakam ve sembol (**?, !, ***) içermeli.

Zayıf Parola: 123456, batman2012, qwerty

Güçlü Parola: Ank@ra_06!, Elis.2022*

2. İki Faktörlü Doğrulama (2FA)

Sadece şifre yetmez! Şifreni girdikten sonra telefonuna gelen SMS kodu veya onay bildirimi, hesabının ikinci kilididir.

3. HTTPS ve Kilit Simgesi

Adres çubuğundaki Kilit Simgesi, o siteyle arandaki verilerin şifreli aktığını (HTTPS) gösterir. Kilit yoksa, o sitede bilgi paylaşma!

www.sinanakdemir.com.tr

DİKKAT! ÜCRETSİZ Wİ-Fİ TUZAKLARI

Parklarda, kafelerde veya havaalanlarında bulunan "Umuma Açık (Şifresiz) Kablosuz Ağlar" büyük risk taşır.

- Bu ağlar üzerinden kişisel bilgilerinizi, şifrelerinizi veya banka bilgilerinizi paylaşmayın.
- Kötü niyetli kişiler bu ağlara sizaraak paylaştığınız her şeyi "havada yakalayabilir."



CREATIVE COMMONS (CC)



Tüm hakları saklı olan eserlerin aksine, bazı içerik üreticileri eserlerinin belirli şartlarla paylaşılmasına izin verir. Buna Creative Commons denir. CC Lisans Türleri Nelerdir?

Atıf: Eser sahibinin adını belirtmelisin.

Ticari Olmayan: Bu eseri kullanarak para kazanamazsın.

Türetilemez: Eseri değiştiremezsin, olduğu gibi kullanmalısın.

Aynı Lisansla Paylaş: Yeni eserini de aynı lisansla paylaşmalısın.

Sunum veya projelerinizde telif hakkı sorunu yaşamamak için şu yolları izleyebilirsiniz

- Kendi fotoğraflarınızı çekin veya kendi çizimlerinizi yapın.
- "Açık Kaynak" veya "Public Domain" (Kamu Malı) görselleri tercih edin.
- Kullandığınız materyalin lisans türüne uygun hareket edin ve gerekirse kaynak belirtin.

www.sinanakdemir.com.tr

SON

www.sinanakdemir.com.tr