

Dijital Ortamlarda Gizlilik ve Güvenlik

Dijital ortamlar; internet, bilgisayar, tablet, telefon, oyunlar ve sosyal medya gibi alanlardır. Bu ortamlarda eğlenir, ödev yapar ve arkadaşlarımızla iletişim kurarız. Ancak bu ortamları kullanırken **gizlilik ve güvenliğe dikkat etmezsek** bazı tehlikelerle karşılaşabiliriz.

İnternette karşılaşılabileceğimiz bazı tehlikeleri tanımak, kendimizi korumanın **ilk adımı**dır.





1) Kimlik Hırsızlığı



Kimlik hırsızlığı; bir kişinin **başkasına ait kişisel bilgileri izinsiz kullanmasıdır**.
Bu bilgilerle sahte hesaplar açılabilir veya yasa dışı işler yapılabilir.

Kişisel bilgilere örnekler:

- Ad, soyad
- Doğum tarihi
- Kimlik numarası
- Şifreler

Örnek:

İnternette bir kişinin bilgilerini kullanarak onun adına kredi başvurusu yapmak.

Sonuç:

Bilgilerimizi paylaşmazsak kimlik hırsızlığına karşı kendimizi korumuş oluruz.





2) Sosyal Mühendislik Saldırıları



Sosyal mühendislik, insanları **kandırarak bilgi almaya çalışma yöntemidir**. Genellikle banka, polis veya tanınmış bir kurum gibi davranırlar.

Nasıl yapılır?

- Sahte e-posta gönderilir
- Mesajdaki linke tıklamanız istenir
- Şifre veya kart bilgileri sorulur

Örnek:

Bankadan gelmiş gibi görünen bir e-posta ile sahte siteye yönlendirilmek.

Unutma:

Gerçek kurumlar **asla şifre istemez**.



3) Siber Zorbalık

Siber zorbalık, dijital ortamlarda bir kişiye **bilerek ve sürekli zarar vermektir**.

Örnek davranışlar:

- İzinsiz fotoğraf paylaşmak
- Hakaret etmek
- Tehdit veya şantaj yapmak

Örnek:

Bir arkadaşının fotoğrafını izinsiz alıp alay ederek paylaşmak.

👉 Ne yapmalıyız?

- Cevap vermemeliyiz
- Kanıtları saklamalıyız
- Aileye veya öğretmene söylemeliyiz



4) Virüsler ve Kötü Amaçlı Yazılımlar

Virüsler; bilgisayar, tablet ve telefonlara zarar veren yazılımlardır.

Zararları:

- Dosyaları silebilir
- Bilgileri çalabilir
- Cihazı bozabilir

Örnek:

E-postayla gelen zararlı bir dosyaya tıklayınca virüs bulaşması.



KİŞİSEL BİLGİLERİN GİZLİLİĞİ VE GÜVENLİĞİ

Kişisel bilgiler sadece ad ve soyad değildir.

Kişisel bilgi sayılanlar:

- Kimlik numarası
- Telefon, adres
- E-posta
- Fotoğraf, video
- Konum bilgisi

✎ Bu bilgileri paylaşmak **tehlikeli sonuçlar** doğurabilir.



GİZLİLİK VE GÜVENLİK KİŞİNİN KENDİSİNDEN BAŞLAR

Kişisel verilerin korunmasında yasaların ve uluslararası sözleşmelerin getirmiş olduğu birtakım uygulama ve yaptırımlar olsa da gizlilik ve güvenlik kişinin kendisinde başlamaktadır.

Yasalar ve kurallar olsa bile asıl sorumluluk **bize aittir**.

- Paylaşmadan önce düşünmeliyiz
- Herkese güvenmemeliyiz
- İnternette yaptıklarımızın kalıcı olduğunu unutmamalıyız



BİLİŞİM TEKNOLOJİLERİ KULLANILIRKEN DİKKAT EDİLMESİ GEREKENLER

- **Bedava kontör, hediye çeki gibi aldatıcı mesajlar gönderen ve kendini polis, savcı gibi tanıtarak para, kontör, altın vb. isteyen kişilere inanmayın. Bu gibi şüpheli durumları ailenize ve yetkili kişilere bildirin.**
- **Kimlik numarası, adres, iletişim bilgisi ve konum gibi sizi tanıtan ve tarif eden bilgileri paylaşmayın.**
- **Özel resim ve videolarınızı başkaları ile paylaşmayın. Eğlenceli gibi görünen testler, senin hakkında bilgi toplamak için hazırlanmış tuzaklar olabilir. Bir kez daha düşünün.**
- **Bilmediğiniz adreslerden gelen e-postaları açmayın, mesajlardaki bağlantılara tıklamayın. Unutma! Bilinen markalar veya kurumlar sizden asla parola, kimlik bilgileri gibi kişisel bilgiler istemez.**
- **İnternet kafe ve alışveriş merkezleri gibi internetin ortak kullanıldığı alanlarda interneti sadece bilgi alma ve eğlence gibi temel amaçlar için kullanın. Özel işlemlerinizi bu alanlarda yapmayın.**



BİLİŞİM TEKNOLOJİLERİ KULLANILIRKEN DİKKAT EDİLMESİ GEREKENLER

- Olumsuz ve şüpheli durumlarda, durum daha da kötüye gitmeden mutlaka ailenize haber verin.
- İnternetteki bilgilerin tamamının doğru olmadığını unutmayın. Bilginin doğruluğunu ve gerçekliğini farklı kaynaklardan da araştırın.
- Başkalarına karşı saygılı olun; kaba yorumlar ve konuşmalar yapmayın.
- Yasa dışı ve ahlak dışı sitelerden ve uygulamalardan kaçının. Alışveriş, dosya indirme gibi işlemlerinizi bilinen ve güvenli internet sitelerinden yapın.

Etik ilkelere uygun davranmaya özen gösterin. Paylaşımlarınızın sizin haricinizde pek çok kişinin de göreceğini ve geri dönüşünün olmayacağını unutmayın.



BİLİŞİM TEKNOLOJİLERİ KULLANILIRKEN DİKKAT EDİLMESİ GEREKENLER

- Tanımadığınız kişilerle arkadaşlık kurmayın, sohbet etmeyin.
- Gerçek hayatta yapmayacağınız şeyleri dijital ortamlarda da yapmayın.
- İnternette tanıştığınız kişilere gerçek kimliğinizle ilgili bilgi vermeyin.
- Kimsenin özel bilgi ya da belgesini izin almadan saklamayın ve yayınlamayın.
- Güçlü şifreler (parolalar) belirleyin ve bu şifreleri belirli aralıklarla değiştirin.



BİLİŞİM TEKNOLOJİLERİ KULLANILIRKEN DİKKAT EDİLMESİ GEREKENLER

- Dışarıdan (harici bellekler) veya internetten bilgisayarınıza yüklediğiniz dosyaları virüs ve casus yazılım taramasından geçirin.
- Güncel bir antivirüs yazılımı kullanın ve düzenli olarak güncelleyin.
- Bilgisayar, tablet ya da akıllı telefon gibi cihazlarınıza açılış parolası ve ekran kilidi gibi şifreler ekleyin.
- Önemli bilgilerinizi farklı ortamlara belirli aralıklarla yedekleyin.
- Akıllı cep telefonunuza işinize çok yaramayan ve birçok bilginize kolaylıkla erişebilen uygulamaları yüklemeyin.



KİŞİSEL BİLGİLERİN KORUNMASI

1. Güçlü Şifreler Oluşturmak

Çevrimiçi ortamlarda etik değerlere uymalıyız. Sahte kimlik bilgileri kullanmamalıyız. Başkalarının da sizin kimlik bilgilerinizi kullanarak işlemler yapabileceğini düşünün ve **kimlik bilgileriniz ile şifrenizi kimseyle paylaşmayın.**

Güvenli Parola Oluşturma İlkeleri

- Herkesin kolay bulabileceği ve tahmin edebileceği şifreler tercih etmeyin. Doğum tarihiniz, adınız, soyadınız gibi bilgileri şifre olarak kullanmayın.
- Ardışık rakamlar ve harflerden oluşan şifreler belirlemeyin. **123456, abcde** gibi şifreler kullanmayın.
- Çok kısa şifreler kullanmayın, şifrelerin **en az 8 karakter** olmasına özen gösterin. **a1b, 125, aa11** gibi kısa şifreler kullanmayın.

Büyük/küçük harf, rakam ve simgeleri bir arada kullanın. **tekin4025** yerine **TeKiN@4025** gibi kullanımları tercih edin.

- Unutmayacağınız bir şifre oluşturun. Farklı sitelerde uygun eklemeler yaparak şifrenizi farklılaştırın. **bilGe0699** şifresi yerine **bilGe0699+FaCe** şifresini tercih edebilirsiniz.

KİŞİSEL BİLGİLERİN KORUNMASI

Parola Güvenlik Düzeyleri

- **tekin** → Çok Zayıf
- **tekin4025** → Zayıf
- **TeKiN4025** → Orta
- **TeKiN_4025** → Güçlü
- **@TeKiN_4025*** → Çok Güçlü

Parola oluşturma ilkelerini kullanarak güçlü bir parola oluşturunuz.

KİŞİSEL BİLGİLERİN KORUNMASI

2. Gizlilik Ayarlarını Kontrol Etme

- Sosyal medya hesaplarındaki ve diğer uygulamalardaki gizlilik ayarlarını düzenli olarak kontrol etmelisiniz. Bu ayarlar, paylaştığınız içerikleri kimlerin görebileceğini belirler.
- Örneğin, sosyal medya gönderilerinizi sadece arkadaşlarınızın görebileceği şekilde ayarlayabilirsiniz. Bu sayede kişisel bilgilerinizin herkesin erişimine açık olmasını engellemiş olursunuz.



KİŞİSEL BİLGİLERİN KORUNMASI

3. İki Faktörlü Doğrulama

- İki faktörlü doğrulama, hesabınıza ekstra bir güvenlik katmanı ekler. Bu özellik etkinleştirildiğinde, şifrenizi girdikten sonra telefonunuza, e-posta adresinize gönderilen bir kod veya bir uygulama üzerinden oluşturulan bir kod ile kimliğinizi doğrulamanız istenir.
- Şifreniz çalınsa bile, bu ikinci adımı geçemeyen kötü niyetli kişiler hesabınıza erişemez.



KİŞİSEL BİLGİLERİN KORUNMASI

4. Güvenli Bağlantılar Kullanma

- İnternete bağlandığınız ağın güvenli olduğundan emin olun. Özellikle halka açık, şifresiz Wi-Fi ağları güvenli değildir. Bu ağları kullanırken bankacılık işlemleri gibi hassas bilgilerinizi girmemelisiniz.
- Güvenli web siteleri genellikle **https://** ile başlar ve adres çubuğunda bir kilit simgesi bulunur. Bu simge, siteyle aranızdaki bağlantının şifrelendiğini gösterir.



BİLGİ GÜVENLİĞİ VE BİLGİ KORUMA YÖNTEMLERİ

Günümüz koşullarında kişilerin ve kurumların en önemli değerlerinden birisi “**Bilgi**”dir. Önceden basılı ortamlarda veya hafızada saklanan bilgi, bilişim teknolojilerinin gelişmesiyle birlikte artık dijital ortamlarda saklanmaktadır.

Bilgi güvenliği demek, sadece bilginin gizli tutulması anlamına gelmemektedir. Bilgi güvenliği **Gizlilik, Bütünlük ve Erişilebilirlik** olmak üzere üç temel unsurdan oluşur.

Bilgi Güvenliği

Gizlilik

- Bilginin yetkisiz kişilerin eline geçmemesi durumudur.

Bütünlük

- Bilginin yetkisiz kişiler tarafından değiştirilmesi veya silinmesine karşı korunmasıdır.

Erişilebilirlik

- Bilginin ihtiyaç halinde yetkili kişilerce ulaşılabilecek ve kullanılabilecek şekilde korunmasıdır.



BİLGİ GÜVENLİĞİ VE BİLGİ KORUMA YÖNTEMLERİ

Örnek

Bir iş yerinde kullanılan programda, yönetici ve personel olmak üzere farklı yetkilere sahip iki tür kullanıcı vardır.

Yönetici: Kendine ait parola ile giriş yaptığında tüm işlemleri yapabilmektedir.

Personel: Sadece programda yapılan işlemleri görme yetkisine sahip; hiçbir değişiklik ve düzenleme yapamamaktadır.

Yukarıdaki örnek bilgi güvenliği açısından incelendiğinde;

01. Gizlilik

- Yöneticinin programda şifre kullanması ve başkalarıyla bu şifreyi paylaşmaması, bilginin gizliliğidir.

02. Bütünlük

- Personelin bilgiyi değiştirememesi veya silememesi bilginin bütünlüğünün korunmasıdır.

03. Erişilebilirlik

- Yönetici ve personelin ayrı ayrı şifrelerle farklı ihtiyaçlar için programı kullanabilmeleri, bilginin erişilebilirliğidir.

