

GİZLİLİK VE GÜVENLİK

BİLGİ GÜVENLİĞİNİ
NELER TEHDİT EDER?



Bilgilerin **yazma, okuma, taşınması** esnasında bozulmalar.

Fiziksel zararlar.

Yok edilme.

İstenmeyen kişilerin, erişebilmesi. (Hack)

Kaybolma.

Silinme.



BİLGİ GÜVENLİĞİ
NASIL SAĞLANIR?

Güvenlik yazılımları.

Yedek alma.

Verileri **şifreleme**.

Oturumu **kapatma**.

Kullanıcı oluşturma.

Parola ile giriş.

Bilgi güvenliđi dendiđinde 3 temel özellik belirlenmiřtir.



Gizlilik



Önemli bilgilerin yetkisiz kişilerin eline geçmemesi bilgi güvenliđini ifade eder.

Eriřilebilirlik



Bilginin ihtiyaç duyulduđu zaman eriřilebilir olmasıdır.

Bütünlük



Verinin yetkisiz kişiler tarafından deđiřtirilememesini kapsayan bir özelliktir. Bunun için bilginin deđiřtirilmesini engelleyecek güvenlik tedbirleri alınır.

ÖRNEKLER

- Okula izinsiz girişlerin engellenmesi.
(Gizlilik)
- Okul notlarınızın öğretmenlerden başkası tarafından değiştirilmemesi. (Bütünlük)
- Özel araç park alanlarına girişler. (Gizlilik)
- Okul kameralarının internetten takibi.
(Erişilebilirlik)
- Okul güvenlik kameralarının başkaları tarafından internetten izlenmesinin engellenmesi. (Gizlilik)
- Defterden sayfa eksilip eksilmediğini anlamak. (Bütünlük)
- İstendiğinde elektronik postalara erişim.
(Erişilebilirlik)

Gizli mesaj nasıl göndeririz?



Sezar şifresi

A	B	C	Ç	D	E	F	G	Ğ	H	I	J	K		
V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	
L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü

En eski bilgi gizleme yöntemlerinden biri 'Sezar şifresi' olarak bilinen harf kaydırma yöntemidir.

Örnekteki tabloda ilk harf sırası normal alfabenin harf sıralaması, ikinci harf sırası ise üç sıra harf kaydırarak elde edilen harf sıralamasıdır.

13

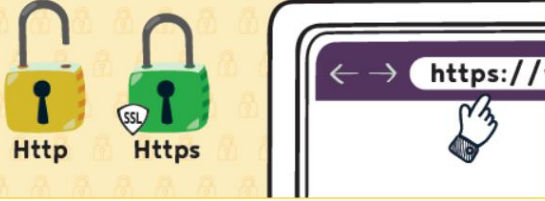
Haydi bulalım!

A B C C D E F G G
V Y Z A B C C D E

N Ğ Ü H Ğ V

İnternet Sayfalarına Dikkat!

HTTPS Nedir?



13. Slayt:

Gördüğünüz şifreli metin sizce ne demek istiyor?

Sezar Şifresi bilgisayar teknolojisi ile çok hızlı çözülebilen bir şifreleme tekniğidir. Artık çok daha karmaşık şekilde de şifreleme yöntemleri kullanılmaktadır.

İnternet'te kullandığımız sitelerde güvenli bir şekilde bağlantı kurduğumuzu anlamamın yollarından biri adres çubuğuna bakmaktır. Eğer HTTPS ile başlayan bir adres ise bu bağlantı güvenlik sertifikası kullanıyor demektir.

Özellikle bankalar internet üzerinden bu şekilde hizmet sunar. Güvenlik sertifikası kullandıklarını ve verilerin şifrenip gönderildiğini anlamamızı sağlar.

ZARARLI YAZILIMLAR



Bilgisayara ve bilgilere zarar vermek amacıyla hazırlanmış yazılımlardır.

Virüsler



Bilgisayara izinsiz girip dosya ve programlara zarar verir. Virüsler işletim sistemini bozabilir, dosyalara zarar verebilir ya da silebilir.

Truva Atı (Trojan)



Zararlı bir yazılım türüdür. Bir uygulama gibi çalışır. Bilgisayarda güvenlik açığı oluşturur. Böylece bilgisayara istenmeyen kişiler izinsiz müdahale edebilir.

Solucan (Worm)



Ağ üzerinden bilgisayarımıza bulaşan ve kendini sürekli kopyalayarak çoğaltan zararlı bir yazılımdır. Kendini sürekli çoğalttığı için bilgisayarı yavaşlatır. Gereksiz yer kaplar.

Reklam Yazılımı (Adware)



Herhangi bir program kullanırken ya da internette gezinirken kendiliğinden reklam açan zararlı bir yazılımdır.

Casus Yazılım (Spyware)



Bilgisayardaki bilgileri toplayıp uzaktaki bir kullanıcıya bilgimiz olmadan gönderen yazılımlardır.

GÜVENLİK YAZILIMLARI

Zararlı yazılımlardan korunmak amacıyla kullanılan yazılımlara **güvenlik yazılımları** denir. Bunlar **Antivirüs Programları** ve **Güvenlik Duvarı** uygulamalarıdır.

ZARARLI YAZILIMLAR BİLGİSAYARIMIZDA NE GİBİ SORUNLARA YOL AÇAR?

- Bilgisayarınızdaki bilgileri çalabilir ve başkalarına gönderebilirler
 - »» E-posta hesaplarınız, parola bilgileriniz gibi.
- İşletim sisteminizin veya diğer programlarınızın
 - »» çalışmamasına,
 - »» hatalı çalışmasına neden olabilirler.
- Bilgisayarınızdaki dosya veya klasörleri
 - »» silebilir,
 - »» kopyalayabilir,
 - »» yerlerini değiştirebilir veya yeni dosyalar ekleyebilirler.
- Yaptığınız her şeyi kaydedebilirler.
 - »» Klavyede yazdığınız her şey veya fare ile yaptığımız tüm hareketler gibi.
- Ekranda can sıkıcı veya kötü amaçlı web sitelerine yönlendiren açılır pencereler oluşturabilirler.
- Tüm verisiyle diski silebilir, hatta biçimlendirebilirler.
- Saldırganların kullanması için güvenlik açıklıkları oluşturabilirler.
- Başka zararlı programların bulaşmasını sağlayabilirler.
- Bilgisayarınız üzerinden başkalarına saldırabilirler.
- Bilgisayarınızın ya da internetin kaynaklarını kullanır, yavaşlamalara neden olabilirler.