GİZLİLİK VE GÜVENLİK

Bilgi güvenliği dendiğinde 3 temel özellik belirlenmiştir.

Gizlilik

Önemli bilgilerin yetkisiz kişilerin eline geçmemesi bilgi güvenliğini ifade eder.

Erişilebilirlik

Bilginin ihtiyaç duyulduğu zaman erişilebilir olmasıdır.

Bütünlük

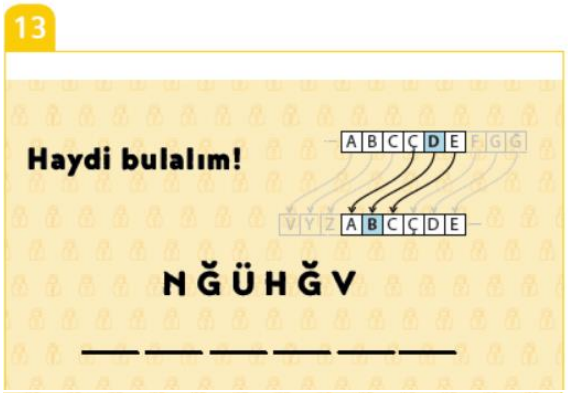
Verinin yetkisiz kişiler tarafından değiştirilememesini kapsayan bir özelliktir. Bunun için bilginin değiştirilmesini engelleyecek güvenlik tedbirleri alınır.

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. (Erişebilirlik)

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

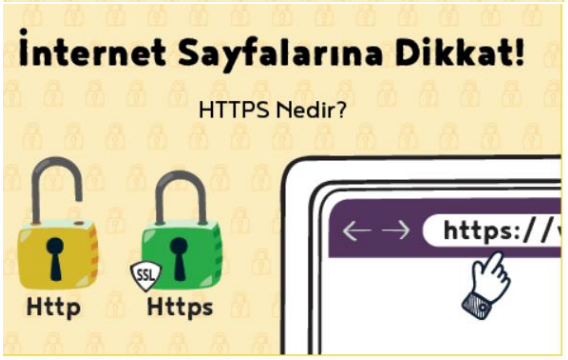
Örnekteki tabloda ilk harf sırası normal alfabenin harf sıralaması, ikinci harf sırası ise üç sıra harf kaydırarak elde edilen harf sıralamasıdır.



13. 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 anlamanın 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 şifrelenip gönderildiğini anlamamızı sağlar.

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.