STOP | THINK | CONNECT™

# Fidye Saldırıları

## Genel Bilgiler & Öneriler

Teknoloji geliştikçe, fidye saldırılarının (ransomware attacks) sıklığı işletmeler ve tüketiciler arasında artmaktadır. Dijital vatandaşların giderek birbirine bağlanan küresel dünyada temel olan dijital hijyen konusunda tetikte olmaları önem arz etmektedir.

### Ransomware ne demektir?

Ransomware kötü amaçlı bir yazılım olup, kurbanının dosyalarına erişerek bunları kilitlemekte, şifrelemekte ve aynı dosyaları geri iade etmek için fidye talep etmektedir. Siber suçlular, kullanıcıların ekleri açmasını veya yasal görünen ama aslında kötü niyetli kod içeren linkleri tıklamasını sağlamak suretiyle bu saldırıları kullanır. Ransomware, kişisel fotoğraf ve anılardan, müşteri bilgileri, mali kayıtlar ve fikri mülkiyet gibi değerli verilerin "dijital kaçırılması" olarak adlandırılabilir. Herhangi bir kişi ya da kuruluş fidye saldırılarının potansiyel bir hedefi olabilir.

### Ne Yapabiliriz?

Aşağıdaki öneriler ışığında hem kendimizi hem de kurumlarımızı ransomware ve diğer kötü niyetli yazılımlara karşı koruyabiliriz.

- **Tüm makinelerinizi temiz tutun:** Tüm internet ile bağlantılı cihazlarınızın yazılımları güncel tutulmalıdır. Bilgisayar ve mobil işletim sistemleri de dahil, bütün önemli yazılımlar, güvenlik yazılımları ve diğer sık kullanılan programlar ve uygulamaların en güncel sürümleri çalıştırılıyor olmalıdır.
- **İki adım önde olun:** Mevcut hesaplarda iki adımlı kimlik onaylaması açılmalıdır. (iki adımlı doğrulama ya da çok faktörlü kimlik onaylama diye de bilinmektedir) . Iki faktörlü kimlik doğrulama, gelişmiş hesap güvenliğinin sağlanması için telefona gelen kısa bir mesajdan parmak izi gibi biyometrik bir simgeye kadar herşeyi kullanabilmektedir.
- **Yedekleme:** Değerli çalışmaların, müziklerin, fotoğrafların ve diğer dijital bilgilerin düzenli bir şekilde elektronik kopyası oluşturulmalı ve güvenli bir şekilde saklanarak korunmalıdır.
- **Daha iyi şifreler oluşturun:** Güçlü bir parola bir cümleden oluşup en azından 12 karakter içermelidir. Parola oluşturmak için akılda kalıcı, beğenilen olumlu cümlelere, deyimlere, atasözlerine odaklanılarak modifikasyonlarla bireye özel oluşturulmalıdır
- **Şüpheye düştüğünüzde silin:** Siber suçlular genellikle e-postadaki bağlantılar, sosyal medya mesajları ve online reklamlar üzerinden kişisel bilgileri çalmaktadırlar. Kaynak biliniyor olsa bile, bir şey şüpheli göründüğünde derhal silinmelidir.
- **Tak & Tara:** USB'ler ve diğer harici cihazlar virüsler veya farklı kötü amaçlı yazılımlarca enfekte olabilirler. Bu cihazları taramak için güvenlik yazılımları kullanılmalıdır.