

# OLTALAMA

## Bilgi Notu

### Oltalama Nedir?

Oltalama, kullandığınız her türlü hesap bilgilerinizi veya banka hesabınızla ilgili detayları çalmak için düzenlenen saldırılardır. Aslında bu bir tür sosyal mühendislik saldırısıdır. Bu tip saldırılarda güvenilir bir şirket veya kişi gibi davranarak kurban kandırılır. Oltalama saldırılarında kurbanlara e-posta, anlık mesaj veya kısa mesaj aracılığıyla ulaşılır. Kurban bu mesajda bulunan kötü amaçlı bağlantıya tıkladığı takdirde tuzağa düşer. Tıkladığınız bağlantı bilgisayarınıza kötü amaçlı yazılımların yüklenmesine ya da şifre veya parolanızın ele geçirilmesi için hazırlanmış sahte siteye yönlendirilmenize sebep olabilir. Yüklenen yazılımlar sistemlerinizin kullanım dışı kalmasına veya hassas bilgilerinizin çalınmasına sebep olabilir. Ele geçirilen bilgilerle kurbanlar maddi ve manevi olarak zarara uğratabilir, tehdit veya şantaja maruz kalabilir.

### Oltalama Çeşitleri

#### 1. Oltalama E-postaları

E-posta oltalamada en çok kullanılan yöntemlerden biridir. Bu yöntemle binlerce kullanıcıya aynı sahte iletiyi göndererek birilerinin e-postaya kanmasını beklenir. Kullanıcıların yalnızca küçük bir kısmı tuzağa düşse bile bu yeterlidir. Bunun için taklit ettikleri şirketin veya kişinin e-postalarını detaylı bir şekilde incelerler. Aynı tip söylemleri, aynı yazı tipini ve ifadeleri kullanılır. E-postada şirketin logosuna ve tasarımına yer vermeyi de ihmal etmezler. Buna ek olarak e-postalarında genellikle bir aciliyet duygusu kullanırlar. Yukarıda bahsettiğimiz gibi herhangi bir veri ihlalini bahane ederek acilen şifre değişimi yapmanızı talep edebilirler. Böyle bir durumda kullanıcılar daha az dikkatli olacaktır. Ayrıca mesajlarındaki bağlantıları gerçek bağlantılara oldukça benzer hale getirmeye çalışırlar. Fakat **yazım hatalarına dikkat ederek bağlantının sahte olduğunu anlayabilirsiniz.**

## 2. Hedefli Oltalama

Hedefli oltalamada mesaj veya e-posta tek bir kişiye yöneliktir. Önceden belirlenen hedef kişiye dair tüm detayları toplanır ve kişisel bir mesaj oluşturulur.

Bu tip hedefli oltalama saldırılarında,

- İlk önce mağdurun tanıdığı ve güvendiği kişi veya kurumlar belirlenir.
- Bu kişi veya kurumdan geldiği görüntüsü veren sahte bir e-posta hazırlanır.
- Orijinal e-posta metnine, stiline tıpatıp benzeyen şekilde olmasına, şirket logosunun kullanılmasına özen gösterilir.
- E-postada sizden kişisel bilgileriniz talep edilebilir veya kişisel bilgilerinizle giriş yapmanız gereken bir siteye veya uygulamaya yönlendirilirsiniz.
- Bu bilgileri verdiğinizde veya sisteme şifrenizle girdiğinizde tuzağa düşmüş olursunuz ve bilgileriniz kötü niyetli kişilerin eline geçmiş olur.

### Oltalamadan Korunmanın Yolları

Kullanıcıların oltalamayı önlemek için çeşitli adımlar atması gerekir. Saldırlara karşı sürekli tetikte olmak oldukça önemlidir. Dikkatli olduğunuz takdirde sahte mesajları ve yazım hatalarını fark edebilirsiniz. Sahte linkler de çeşitli yazım hataları veya alan adlarında gariplikler vardır. Ek olarak hem oltalamayı hem de çeşitli siber saldırıları engellemek için bazı siber güvenlik yöntemlerinden yararlanılmalıdır.

**İki faktörlü kimlik doğrulama (2FA):** Saldırıya kurban gidebilecek uygulamalarda iki faktörlü kimlik doğrulama kullanımı çok kritiktir. Şifrenizle oturum açarken fazladan bir doğrulama katmanını kullanmak saldırıların başarıya ulaşma ihtimalin kesinlikle azaltacaktır. Bu şekilde, yalnızca şifre ve kullanıcı adı bilgileriyle hesaplarınıza giriş yapılmasını veya bilgilerinizin değiştirilmesini engelleyebilirsiniz.

**Güçlü parola kullanımı:** Farklı yöntemlerle saldırıya maruz kalındığında güçlü parola kullanımı, parolanızın kolayca ele geçirilmesini engeller ayrıca, sık sık parolaların yenilemeleri ve her uygulamada farklı parola kullanması da çok önemlidir.

**Siber güvenlik farkındalık eğitimleri:** Kalıcı bir siber güvenlik bilinci sağlamak için siber güvenlik farkındalığı eğitimleri şarttır. Bu tip eğitimler size kötü niyetli kişilerin kullandıkları yeni oltalama yöntemlerin ne olduğunun yanı sıra bu yöntemlerden korunma yollarını ve bu yöntemlere karşı daha bilinçli ve daha dikkatli olmanızı sağlar.