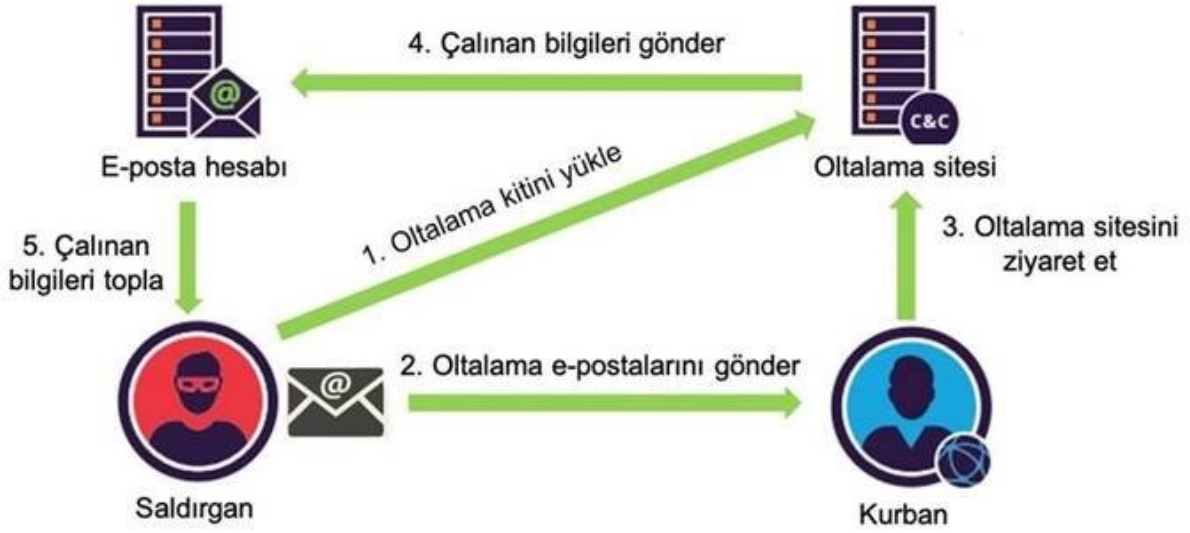

Oltalama(Phishing) Saldırıları

Oltalama (Phishing), genel olarak bir kişinin parolasını, banka hesabını veya kredi kartı bilgilerini öğrenmek amacıyla kullanılır. Saldırgan tarafından özel olarak hazırlanan oltalama (phishing) e-postası resmi bir kurumdan geliyormuş gibi ya da gerçek bir e-posta şeklinde görülür. Hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahte sitelere yönlendirilerek parolalarını vermeleri sağlanır. Diğer bir yandan bu e-postalara eklenen dosyaların çalıştırılması ile kurbanların bilgisayarları ele geçirilerek saldırganın kontrolü altına girebilir.

Kurumlar için büyük riskler oluşturan bu saldırı türüne karşı büyük kayıplar yaşanmaması için kurum çalışanlarının bilgilendirilmesi amacıyla alınması gereken önlemler aşağıda sıralanmıştır.

- Şüpheli görülen e-posta içeriğindeki linkler tıklanmamalıdır. Sözde sistem yöneticisi tarafından gönderilmiş gibi görünen ve e-posta kotasının dolduğu gerekçesi ile şifre bilgileri isteyen e-postalara cevap verilmemelidir.
- E-posta mesajlarındaki şüpheli görülen kısaltılmış linklere (bit.ly, ow.ly, tinyurl.com, goo.gl vb.) tıklanmamalıdır.
- Şüpheli veya bilinmeyen web sitelerine kişisel bilgiler verilmemelidir.
- E-posta hesabı için kullanılan şifre, diğer hesaplardaki şifrelerden farklı olmalıdır.
- Antivirüs ve antispyware programları kullanılmalıdır.
- Yasal olmayan veya kaynağı belirsiz yazılımlar yüklenmemeli ve çalıştırılmamalıdır.
- Kredi kartı numaraları, kişisel bilgiler ve her türlü şifre hiç bir zaman e-posta ile açıkça gönderilmemelidir.

Bu tip saldırılara karşı korunmanın en etkili yolu, bu konuda bilinçli ve bilgili olmaktır.