Değerli ziyaretçimiz,

INTERCOM-KURZ BİLGİ İŞLEM BİRİMİ olarak;

siz değerli müşterilerimizin ve çalışanlarımızın işlem güvenliğini sağlamak adına, yeni ve gelişmiş güvenlik uygulamalarını sürekli takip ediyor ve üst düzey güvenlik standartlarını kullanmaya gayret ediyoruz. Yine de en zayıf halkamız kadar güçlü olduğumuzun ve bu zayıf halkanın genellikle insan faktörü olduğunun bilinciyle hareket etmeye çalışarak işlem güvenliğinin temini ve devamı için firmamız müşterilerini ve çalışanlarını bilgilendirmeyi ilke edinerek, kişisel güvenlik ve gizlilik seviyenizi en yüksekte tutabilmek adına bu bildirimi yapmaktayız.

Son zamanlarda firmamızın alan adı kullanılmak suretiyle, özellikle de Bilgi İşlem departmanımızdan gönderiliyormuş gibi gönderilen virüslü iletilerin posta kutularımıza ulaşmadan güvenlik sistemimiz tarafından engellenmekte olduğunu görmekteyiz. Bu ve benzeri zararlı iletiler müşterilerimizi de hedef alabileceğinden ve bu iletiler güvenlik önlemlerimizi atlayabileceğinden aşağıda yer alan uyarıları siz değerli müşterilerimizin ve çalışanlarımızın dikkatine sunmak isteriz.

- Mal satın almak için anlaştığınız firma ile e-posta üzerinden mi bağlantı kuruyorsunuz?
- E-postaların kötü niyetli kişilerce ele geçirilmesi konusunda bilgi sahibi misiniz?
- Virüsler gibi zararlı yazılımların tanıdığınız güvendiğiniz kişilerden size virüs ve benzeri zararlı yazılım ve kodları gönderebileceğini biliyor musunuz?
- Her gün gerçekleştirdiğiniz rutin işlerinizde Word, Excel, PowerPoint, zip, rar, pdf dosya türlerini mi kullanmak zorunda kalıyorsunuz?
- İş ortağınız bir anda ödemeyi farklı bir banka ya da hesaba mı yapılmasını istedi?
- Bilgi işlem biriminden hesap kotanızın dolmakta olduğuna dair bildirim mi aldınız?

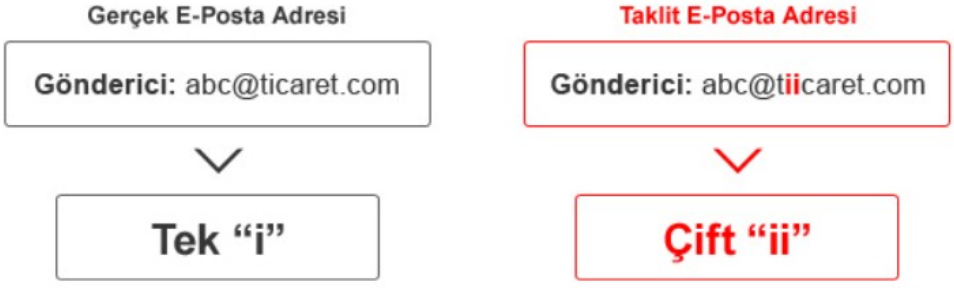
Yukarıda örneği verilmiş tüm durumlar günümüzde sosyal mühendislik yöntemleri ile bizleri hedef alan saldırı yöntemleri/araçlarıdır. Dolandırıcılar bu gibi yöntemlerden faydalanarak her gün yeni yollar deneyerek bizleri, müşterilerimizi, iletişim kurduğumuz kişi ve kurumları hedef alan saldırılar düzenlemekteler/düzenleyebilirler.

Bu gibi yollarla dolandırıcılar;

- İş ilişkisi olduğu tespit edilen kişilerden/kuruluşlardan mal/hizmet sunan tarafın ele geçirilen veya taklit edilen e-postası üzerinden Mal/hizmet alıcısı taraf ile yazışarak çeşitli bahaneler ile transfer bilgilerini değiştirmekte ve yapılacak para transferlerinin dolandırıcılara ait başka bir banka hesabına veya IBAN'a gönderilmesini sağlayabilmektedirler.
- Mal/hizmet alıcısı taraf ile yazışmalarında "hesabınızın süresi doldu, güncellemek için lütfen giriş yapın" gibi isteklerle şifre ve parolaları çalmayı hedeflemekteler.
- Çalışan hesap bilgilerini başkalarına karşı saldırılarda kullanabilmekteler. (En basit olarak bir başkasına spam e-posta göndermek için)

Bu ve benzeri durumlarda nelere dikkat etmelisiniz?

- E-postaların **gönderici bilgisinin taklit edilebilmesine karşın** bu alanda bir değişiklik olup olmadığını kontrol edin.



- "Acil", "Önemli" gibi ibareler ile gelen para transfer isteği, kullanıcı girişi içeren e-postalara dikkat edin.

- Sizden şifrenizi doğrulamanız için giriş yapmanızı isteyen bağlantılara dikkat edin. Bu bağlantıları tıklamak yerine her zaman kullandığınız giriş yöntemini kullanarak söz konusu hesabınızın aktif olup olmadığını kontrol edebilirsiniz. Veya bu konuda size hizmet verne firma veya birimi arayarak durumu sorabilirsiniz.
- Düzenli olarak ödeme yaptığınız firmanın hesap bilgilerinin değişmesi durumunda talebi bir kez daha inceleyin.
- E-postanın dilini inceleyin, normalde kullanılmayan bir dil ile yazılmış, normalde kullanılmayan ifadeler içeriyorsa şüphelenin ve ilgili birimi bilgilendirin.
- Zamanından önce istenen ödeme taleplerine dikkat edin.
- Ayrıca, ödeme/bilgi talep eden kişi ve ilişkili olduğunuz kuruluşu her durumda mutlaka telefon ile arayarak istenen bilgi hakkında, özellikle de tutar ve IBAN/Hesap No için teyit alın.

Ek uyarı ve hatırlatmalar:

- Bilgisayarlarınızda mutlaka lisanslı ve güncel antivirüs çalıştığından emin olun ve bilgisayarınızı zararlı yazılım ve virüslere karşı taramak için zaman ayırın.
- Ortak kablosuz ağlarda (kafeler, resotranlar, oteller vb. Gibi ortamlarda) zorunlu değilseniz işlem gerçekleştirmeyin, şirket hesaplarınızı kullanmayın.
- İş bilgisayarlarınızda kişisel sosyal medya hesapları kullanmayın. (Bugün özellikle iş amaçlı kullanılan linkedin gibi sosyal medya ortamlarının kötü niyetli kişiler tarafından en yaygın bilgi toplama ortamları olduğunu unutmayın).
- Günümüzde “önemsiz bilgi yoktur” gerçeğiyle hareket ederek sizin için önemsiz görünen bilgileri başkaları ile paylaşmayın. Örnek olarak “tatil planınızı” gerekmedikçe paylaşmayın. Kişilerin tatilde olduğu dönemlerin saldırılara en açık dönemler olduğunu unutmayın.
- Şifre girmeniz gereken uygulamalarda aynı şifreleri kullanmayın. Özellikle bankacılık gibi şifrelerinizi mutlaka diğer hesap şifrelerinizden farklı yapın ve iki adımlı doğrulama yöntemlerini kullanın.
- Şifrelerinizi mutlaka karma (rakam, Büyük harf, küçük harf ve semboller içeren min 8 karakterli) olarak kullanın.
- Bilgisayarlarınızda ve cihazlarınızda gereksiz yazılım bulundurmayın.
- Bazı zararlı iletilerde hizmet veren/alan tarafın gönderen adı, adresi, imzaları birebir taklit edilebildiğinden ayırd edilmesi güçleşir. Bu gibi iletilere karşı son derece dikkatli olmak gerekir.

Ayrıca konuyla ilgili aşağıdaki bağlantıları inceleyebilirsiniz.

- Türkiye Bankalar Birliği’nin virüsler hakkındaki kamuoyu duyurusu
- İstanbul Valiliği’nin bilgi hırsızlığı hakkındaki basın bülteni
- TCMB’den gönderilmiş gibi görünen e-posta hakkında TCMB’nin basın duyurusu
- Sahte E-postalara dikkat! Şirketleri hedef alan dolandırıcılık türündeki e-postalar hakkında uyarı

Saygılarımızla...

INTERCOM-KURZ
BİLGİ İŞLEM