SİBER DOLANDIRICILIK YÖNTEMLERİ HAKKINDA BİLGİLENDİRME

Değerli Tedarikçilerimiz,

Özellikle son dönemlerde sosyal medya, e-posta ve internet ortamında kullanılan dolandırıcılık yöntemleriyle pek çok kişi maddi ve manevi zararlara uğratılarak siber korsanların hedefi haline gelmektedirler.

Bu saldırı yöntemleri ile ilgili olarak, sizlere, bilgi güvenliği farkındalığınızı arttırmaya yönelik açıklamalarla birlikte, bu tip saldırıların hangi yollarla yapıldığını ve bu saldırılardan korunabilmenin ipuçlarını paylaşacağız.

Sosyal Medya Dolandırıcılığı

Artan sosyal medya kullanımına bağlı olarak, sosyal medya dolandırıcılığı siber suçlar arasında artış göstermektedir.
Facebook, YouTube, Twitter, Instagram, WhatsApp, Messenger gibi çeşitli sosyal ağlar aracılığıyla kullanıcı ile iletişime geçilerek, bir kişi ya da kurumu taklit ederek, inandırıcı bir senaryoyla güvenlik açısından kritik olan kişisel ve finansal bilgilerin alınması yoluyla gerçekleştirilen ve insan faktörüne dayanan dolandırıcılık türüdür. Dolandırıcılar, genellikle sosyal medya aracılığıyla arkadaş listenizde bulunan hesabı ele geçirip arkadaşınız gibi davranarak,

- Hediye çekilişi kampanyasına katılım,
- Belirli bir hesaba para gönderimi,
- Kredi puanınızı yetersiz belirterek adınıza kredi çekme için para gönderimi

talebi, vb. çeşitli senaryolarla sizi etkileyip ikna ederek, kişisel ve finansal bilgilerinizi (kart bilgisi, internet bankacılığı şifresi, SMS ile iletilen mobil onay kodu, tek kullanımlık şifre vb.) isteyebilmektedir. Bu tip dolandırıcılık faaliyetleri genellikle, kimlik ve hesap bilgilerini ele geçirmeyi amçalmakla birlikte zaman zaman zararlı yazılımların yayılması için de kullanılabilmektedir.

Nasıl Korunabilirsiniz?

- İnternet ortamında bir kişinin kendisini tanıttığı kişi olduğundan emin olmak son derece zor olduğundan, güvenliğiniz açısından kişisel ve finansal bilgilerinizi bu kişilerle kesinlikle paylaşmayınız.

- Bu tarz girişimlerde çok acil karar vermenizi gerektirecek bir senaryo yaratılıp hedef kişinin duyguları manipüle edilmekte ve mantıklı düşünmeye vaktinin kalmaması amaçlanmaktadır. Gerçekten acil bir durum olma ihtimaline karşı farklı bir kanaldan (örneğin telefon ederek) tanıdığınız kişiyle temas kurmayı deneyiniz.

E-Posta ve Kısa Mesaj Dolandırıcılıkları

E-posta, SMS ya da sosyal medya platformları aracılığıyla güven ortamı oluşturup paylaşılan bağlantının tıklanması sağlandıktan sonra sahte internet sitesine kullanıcıları yönlendirerek güvenlik açısından kritik bilgilerin ele geçirildiği dolandırıcılık türüdür. Bu şekilde gerçekleştirilen dolandırıcılıklar genellikle oltalama (phishing) olarak da bilinmektedir.

Şişecam/Paşabahçe tarafından gönderildiği izlenimi veren;

- "Hediye bonusunuzu alabilmeniz için üyelik bilgilerinizin güncellenmesi gerekmektedir."
- "Mobil uygulamamıza buradan giriş yapabilirsiniz."
- "Kredi kartınızdan/hesabınızdan şüpheli işlemler tespit edilmiştir."
- "Mobil uygulamamıza giriş yap, araba kazanma şansını yakala"

vb. ifadelerle içeriğinde link bulunan e-posta, sms gönderilebilmekte ya da sosyal medya üzerinden link paylaşımı yapılabilmektedir. Bu linklerin tıklanması durumunda sahte internet sitelerine yönlendirilerek kişisel ve finansal bilgilerinizin girişi istenmektedir.

Nasıl Korunabilirsiniz?

- Kurumumuz tarafından kesinlikle hesabınızı doğrulamak amacıyla kişisel ya da finansal bilgi girişi talep edilen e-posta ya da kısa mesaj gönderilmemektedir.

- Kurumumuz tarafından internet mağazasına ya da mobil uygulama giriş sayfasına yönlendirilen bir link paylaşımı yapılmamaktadır. Bu şekilde talep edilen bilgileri paylaşmayınız.

- Şişecam/Paşabahçe tarafından kısa mesaj ya da e-posta yoluyla kesinlikle bilgi güncellemesi yapılmamaktadır.

- Paylaşılan link bilgisinde harf eksikliği ya da hatası olup olmadığını, Şişecam/Paşabahçe internet sitesi adresinin tam yazılıp yazılmadığını kontrol ediniz.

- Girmiş olduğunuz linkteki adres çubuğunun yeşil olduğunu kontrol ediniz.

- Önemle belirtmek isteriz ki, sizin de iş yapmakta olduğunuz bir tedarikçiniz ya da bir müşteriniz tarafından banka hesaplarının değiştirildiğine dair bir bilgilendirme maili alıyorsanız, mutlaka çalıştığınız tedarikçi ya da müşterinize başka bir yoldan (telefon, görüntülü arama gibi) ulaşarak böyle bir taleplerinin olup olmadığından kesin olarak emin olun.

- Dijital dönüşüm çalışmalarımızı tüm hızıyla sürdürdüğümüz ve teknolojinin getirdiği tüm olanaklardan en geniş kapsamda yararlandığımız bu dönemde risklere karşı azami ölçüde dikkatli olmamız gerekmektedir. Bilgi güvenliği farkındalığına vermiş olduğunuz önem için teşekkür ederiz.

Saygılarımızla,
Türkiye Şişe ve Cam Fabrikaları A.Ş.