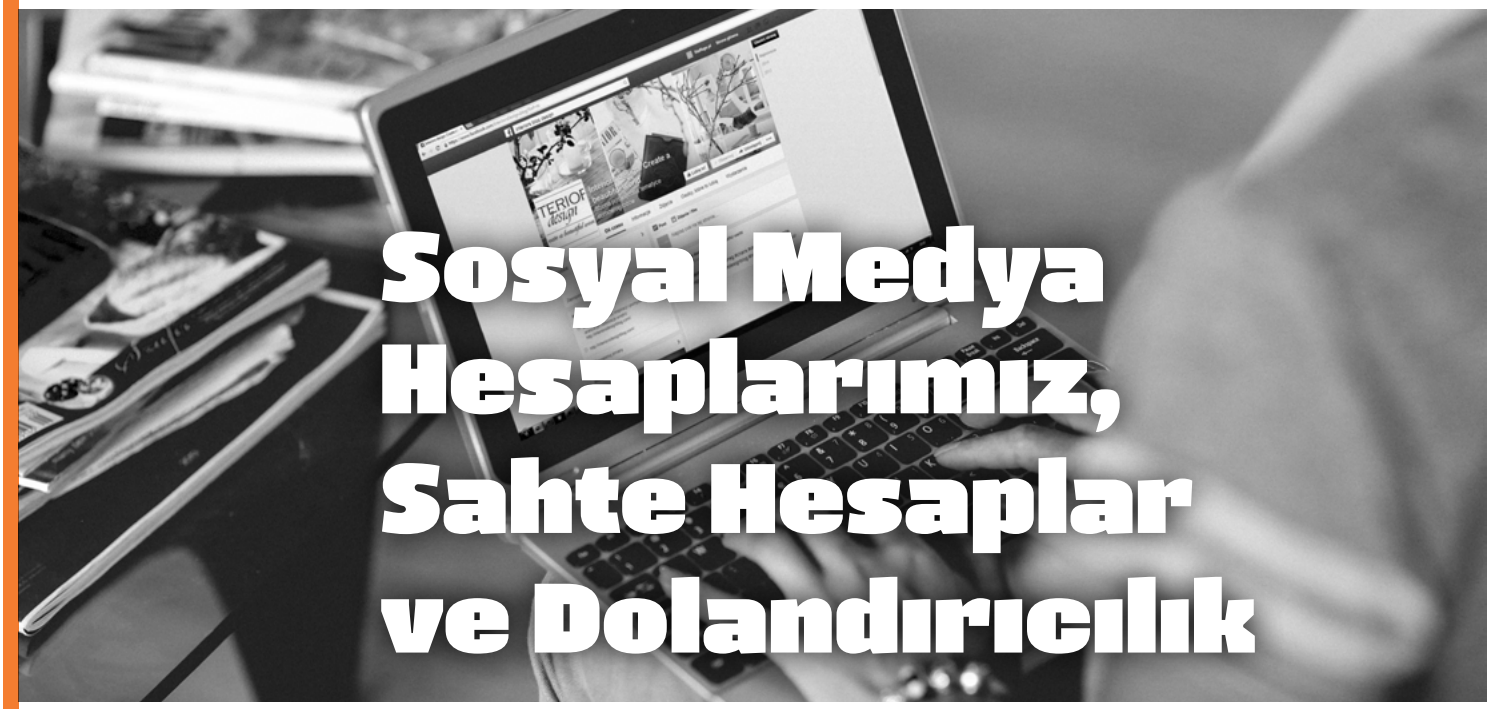
GÜVENLİ GÜNLER BÜLTENİ

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar.
Bültenlerin her ay size ulaşması için üye olunuz: http://eepurl.com/bP-tWn

EYLÜL 2016



Sosyal Medya Hesaplarımız, Sahte Hesaplar ve Dolandırıcılık

Gün geçmiyor ki Facebook ve Linkedin gibi çeşitli sosyal medya platformlarında bir arkadaşımızın güncelleme bilgisinde "hesabım kopyalanmış, benden gelen arkadaşlık isteklerini kabul etmeyin" mesajı görmeyelim.

Ayrıca, dolandırıcılık amacıyla yapılan bu tip hareketlerde dönemsel artışlar yaşanıyor. Her yaştakilerin tercihi olduğu için en sık ve en çok dolandırıcılık girişimine rastlanılan platform Facebook.

Bir yakın arkadaşınız size Facebook'tan yeni bir arkadaşlık isteği gönderiyor.

Arkadaşlık isteğini gönderen kişi aslında arkadaşınız, tanıyorsunuz. Üstelik birçok ortak paylaşımınız var.

Biraz şaşkınlıkla da olsa, "herhalde hesabında problem yaşadı, yeniden açıyor" diye düşünüp bu isteği kabul ediyorsunuz. Hatta arkadaşınızın resmine bakıp yorum da yapıyorsunuz: "aaa zaten burada değil miydi :)".

Biraz sonra arkadaşınızdan size bir mesaj geliyor ve başlıyorsunuz mesajlaşmaya:

Nasılsın?

İyiyim sen nasılsın?

Ne olsun uğraşıyoruz işte... senden ne haber?

Sorma başım dertte biraz :(senden bir destek isteyeceğim.

Elbette, ne istersen.

Bana 1000 TL gönderebilir misin? En kısa sürede ödeyeceğim. Çok kötü durumdayım :(:(:(

Yakın bir arkadaşa sıkıştığı bir zamanda destek vermemek olur mu? Gönderiyorsunuz tabii...

Bir başka senaryo da şu:

Çalıştığınız bankada sizinle ilgilenen hoş, güleryüzlü bir genç müşteri temsilciniz var. Ne zaman ihtiyacınız olsa hemen yardımınıza koşuyor, size yol gösteriyor, işlerinizi hızlandırıyor. Memnuniyetiniz zirvede.

Müşteri temsilciniz sizinle Facebook'tan da arkadaşlık kurmak istiyor ya da zaten arkadaşsınız ama "bir sorun oldu herhalde tekrar gönderdi" diyorsunuz ve gelen teklifi kabul ediyorsunuz.

Ardından yine bir mesajlaşma başlıyor:

Merhaba nasılsınız Harika Hanım?

Teşekkür ederim, siz nasılsınız?

Bir kampanyamız vardı, ama bugün sona eriyor. Çok kısa süre için yapılıyor bu kampanya ve sizin gibi çok iyi müşterilerimle paylaşıyorum sadece bunu.

Çok teşekkürler. Nedir?

Çok şanslısınız, çok az başvuru var ve yapılacak çekilişle sizi bir hafta Bali'de hiçbir ödeme yapmadan ağırlayacağız.

Ooo süpermiş! Ne yapmam lâzım katılmak için?

Bankaya hiç gelmeyin bu kadar kısa süre için. Bana 250 TL göndermeniz yeterli, ben sizin adınıza katılımı gerçekleştireceğim. Bir geldiğinizde de size gerekli imzaları attırırım.

Çok yardımseversiniz, çok teşekkürler.

Birebir aynı olmasa da yukarıda anlatılan senaryolar gerçekte yaşanmış olaylardan alınmıştır. Söz konusu diyalogların benzerini çok sayıda kişi yaşamıştır ve böylece ortaya çıkan para kaybı da azımsanmayacak miktardadır.

Siz bu görüşmeleri yaptığınızı zannettiğiniz kişiden yanıt beklerken, aslına arkadaşınızın/tanıdığınızın konudan, kendisi için açılmış sahte hesaptan haberi bile yoktur.

Senaryolar genellikle ülke gündemi ile de çok ilişkilidir; gündemdeki sıcak konuların istismar edilmesi en sık rastlanılan yöntemlerdendir. Hatırlarsanız geçen yıl birçok kişi, hatta profesörler bile, telefonla yaşadığı dolandırıcılık olaylarında "terör" başlığı altında "koruma yöntemi" öneren girişimlere maruz kalmıştı. Günümüzde de değişik terör kapsamı ve ülkenin siyasi gündemi başlığı altında oluşturulan farklı diyaloglarla para istenmesi yüksek olasılık dahilindedir.

Bu tip dolandırıcılıklardan kendimizi korumak için aşağıdaki önlemleri almamız yerinde olur

- Öncelikle kullandığımız sosyal platformlarda kendi ismimizi sıklıkla aratıp sahte hesap açılıp açılmadığını kontrol etmeliyiz.
- Özellikle arkadaşlarımızda gördüğümüz "hesabım kopyalanmış" bilgisine rastlanılan durumlarda sahte hesap aramasını sıklaştırmalıyız.
- Benzer adlarla açılmış hesapların içeriklerini incelemeliyiz.
- Kendi hesabımızda güvenlik ayarlarını sıkılaştırmalı ve fotoğraf ile diğer paylaşımlarımızı yalnızca arkadaşlarla paylaşıp, herkese açık yapmamalıyız.
- Yukarıda sözü edilen tipte mesajlaşmalarda gelebilecek linklere tıklamamalı, isteyerek ya da istemeden tıklama durumunda da kesinlikle kişisel bilgilerimizi oralarda açılan alanlara girmemeliyiz.
- Banka, hesap, kredi kartı, şifre (internet bankacılığı girişi, Facebook, Gmail, Yahoo gibi girişlerde kullanılan tüm şifreler) gibi bilgileri bu alanlarda kesinlikle paylaşmamalıyız.
- Bu ortamlardan gönderilen tehdit içerikli mesajları kolluk kuvvetleri ile paylaşmalıyız.
- Şüphelendiğimiz durumlarda ilgili kişiyi direk telefonla arayıp yazışmayı gerçekten kendisinin yapıp yapmadığını doğrulamalıyız.
- Bizi acele ettiren, hızlı, düşünmeden harekete geçmemizi isteyen tüm iletişimleri şüphe ile karşılamalıyız.
- Çok yakın tanıdığımız, sevdiğimiz bir kişi olsa bile, kredi kartı gibi hassas bilgileri ve para paylaşmadan önce mutlaka duraklayıp, bu durumun dolandırıcılık olup olmadığını düşünmeliyiz. Şüphelendiğimiz en küçük durumlarda bile, işlemi gerçekleştirmeden önce doğrulamalıyız.

YAZAR HAKKINDA

Harika Yalaza, Intertech A.Ş.'de BT Güvenlik ve Risk Yönetimi'nden Sorumlu Genel Müdür Yardımcısı olarak görev yapmaktadır. İTÜ Matematik Mühendisliği'nden mezun olan Yalaza, ISACA İstanbul Chapter Kurucu Üyesidir.