Australian Banking Association

Güvenliğinize Dikkat Edin:
Dolandırıcılardan sakının

COVID-19 ile ilgili dolandırıcılık ve sahtekârlık olaylarının önümüzdeki aylarda artması beklenmektedir.

Dolandırıcılar sahte e-postalar atarak, sizi telefonla arayarak veya kısa mesaj göndererek kişisel bilgilerinizi almaya çalışırlar. Bankanızdan, Dünya Sağlık Örgütü'nden, hükümetten, hayır kurumlarından veya seyahat acenteleri, elektrik, telefon ve internet sağlayıcıları ya da en yakınınızdaki süpermarket gibi işyerlerinde çalışıyorlarmış gibi yaparlar.

Kendinizi Koruyun

Bankanız size e-posta veya kısa mesaj göndererek hesap bilgilerinizi veya mali bilgilerinizi ASLA sormaz. Aynı şekilde ev telefonu, cep telefonu veya internet bankacılığı oturum açma bilgilerinizi ve adresinizi güncellemenizi de istemez.

Hükümet ve yasal kuruluşlar bir bağlantıya tıklayarak bilgilerinizi güncellemenizi sizden ASLA istemezler. Şüphe duyarsanız, bir arkadaşınızla veya aile bireyiyle konuşun veya ilgili kuruluşla doğrudan iletişime geçip sorun.

Tanımadığınız biri sizi arayıp kişisel bilgilerinizi sorarsa TELEFONU KAPATIN. Şirketi doğrudan arayın ve sizi arayıp aramadıklarını sorun.

Tanımadığınız insanlardan ve bilmediğiniz kuruluşlardan gelen e-posta eklentilerini ASLA açmayın. Bir teklif gerçek olamayacak kadar iyiyse veya sizden çok fazla bilgi istiyorlarsa her zaman uyanık olun.

Bankanız size yardımcı olabilir. Aşağıdaki durumlarla karşılaşırsanız hemen bankanızı arayın:

- asılsız bir telefon görüşmesinde, e-posta veya kısa mesaj iletişiminde banka bilgilerinizi paylaştıysanız
- yanlışlıkla bir bağlantıya tıkladıysanız veya eklentiyi açtıysanız
- hesabınızda sıra dışı işlemler yapıldığını fark ettiyseniz.

Dolandırıcıları nasıl anlarsınız

- Kişisel bilgilerinizi, örneğin adres, doğum tarihi, banka hesabı bilgileri, vergi numarası veya PIN ya da parolanızı güncellemeniz veya onaylamanız istenirse.
- E-posta veya kısa mesajda şüpheli görünen bağlantılar varsa. Emin değilseniz bir arkadaşınızdan veya aile ferdinden yardım isteyin.
- Hemen ödeme yapmanız veya avans yatırmanız istendiyse.
- Teklif gerçek olamayacak kadar iyiyse, muhtemelen gerçek değildir.
- E-posta adresi, şirketin kullandığından farklıysa.
- Sizi arayan kişi bilgisayarınıza uzaktan erişmek istiyorsa.

Australian Banking Association

www.ausbanking.org.au

Mali bilgilerinizi sahtekârlığa ve dolandırıcılığa karşı korumak için tüyolar

- Aramayı şüpheli bulduğunuzda telefonu hemen kapatıp şirketin web sitesine giderek ya da başka bir şekilde telefon numarasını bulun ve şirketi doğrudan arayın.
- Parolanızı ve PIN'inizi asla paylaşmayın. Cihazlarınıza parola koyun. Kullandığınız bilgisayarı başkalarıyla paylaşıyorsanız, parolanızı asla kaydetmeyin ve hesabınızdan her işiniz bittiğinde çıkın, oturumu kapatın.
- Şüpheli işlemleri hızla fark edebilmek için banka hesabınızı sık sık kontrol edin.
- Satın alma işlemlerinde kartınızı kaydırarak (swipe) okutmaktan kaçının. Kartınızı dokunmatik ekranda (tap) okutmak veya yuvaya sokarak (insert) okutmak genellikle daha güvenlidir.
- Kredi kartlarınızdaki nakit avansları engelleyin.
- Bankanızla konuşarak hesabınızı en iyi şekilde korumanın yollarını öğrenin.
- Dolandırıldığınızı düşünüyorsanız derhal bankanıza haber verin.

Sahtekârlar sizden para çalmak için çeşitli yollara başvurur, bunlardan bazıları şöyledir:

E-dolandırıcılık– Banka, hayır kurumu ya da hükümet gibi güvenilir bir kaynaktan gelmiş gibi görünen bir e-posta veya kısa mesaj ile kişisel bilgilerinizi almaya çalışırlar. Bu mesaj gerçek gibi görünür ve genellikle sizden kişisel bilgilerinizi sahte bir web sitesine girmenizi ya da bir bağlantıya tıklamanızı isterler. Böylece sahtekârlar bilgisayarınıza ve kişisel bilgilerinize erişebilir.

İnternet üzerinden alışveriş dolandırıcılığı – sahtekârlar, internet üzerinde gerçek mağazalar gibi görünürler, ancak ya web siteleri sahtedir ya da gerçek bir perakende sitesinde sahte bir reklam verirler. İnternet üzerindeki sahte alışveriş siteleri genellikle havale, uluslararası para transferi veya hediye kartı gibi ödemeyi önden almak için sıra dışı ödeme yöntemlerine başvururlar.

Yatırım dolandırıcılığı – sahtekârlar, mali veya yatırım tavsiyesi veren borsa simsarı ya da portföy yöneticisi kılığına girerler. Sizden, kimi zaman gerçek, kimi zaman gerçek olmayan bir yatırım fırsatı için paranızı alırlar ve geri vermezler.

Uzaktan erişimle dolandırıcılık– sahtekârlar, bilgisayarınız veya internet bağlantınızda sorun olduğunu veya bilgisayarınıza virüs girdiğini iddia ederler. Billgisayarınıza erişmek için sizden bir uygulama indirmenizi ya da onlara bilgisayarınıza erişim izni vermenizi isterler. Bu fırsatı kişisel bilgilerinize ulaşmak için kullanırlar veya sorunu çözmeleri karşılığında "ücret" talep ederler.

Romantik ilişkilerde dolandırıcılık – sahtekârlar sizden para veya hediye almak için sizinle ilişki kurarlar. Bu ilişkiyi uzun zamana yayarlar ve sonunda sizden varlıklarınızı onların adına geçirmenizi veya vasiyetinize onların adını eklemenizi isterler. Genellikle sağlık, seyahat veya aile sorunu nedeniyle para isterler.

İŞİNİZE YARAYABİLECEK BAĞLANTILAR:

www.ausbanking.org.au/safe-savvy-a-guide-to-help-older-people-avoid-abuse-scams-and-fraud

www.esafety.gov.au/seniors/staying-safer-online

www.scamwatch.gov.au/