Watchlist Internet

İnternet dolandırıcılığı, tuzaklar ve sahtecilikler

İNTERNET ÜZERİNDEN DOLANDIRICILIK

Kendinizi nasıl korursunuz?

Available on the iPhone App Store

ANDROID APP ON Google play

www.watchlist-internet.at

Broşür basit dil kuralları temellerine dayanmaktadır.

Sahte online mağazalar

İnternet Üzerinden Alışveriş

Tehlikeler

İnternet üzerinden alışveriş yapmak keyiflidir: İstediğiniz zaman kendi evinizin rahatlığında alışveriş yapabilirsiniz.

Ne yazık ki, online alışverişin tehlikeleri de vardır: Dolandırıcılar internette ucuza ürünler sattıklarını düşündürerek sizi kandırır.

Bu tür sahte mağazalar genellikle diğer sıradan mağazalar gibi görünür. Ancak bu gibi yerlerden alışveriş yapmamalısınız. Çünkü paranızı kaybedebilirsiniz. Hiçbir ürün alamazsınız veya sipariş ettiğinizden tamamen farklı bir şey alırsınız.

Kendinizi nasıl korursunuz?

Künyeyi kontrol edin. Bilmediğiniz bir web sitesinden alışveriş yapmadan önce mağaza künyesine bakın. Künyede, web sitesinin hangi şirkete ait olduğu yazmalıdır. Web sitesinde künye yoksa, oradan satın almayın!

Arama motoruna sorun (örneğin Google veya Bing). Arama motoruna mağazanın adını ve „müşteri deneyimi“ veya „dolandırıcılık“ gibi kelimeleri girin. Bu şekilde varsa o mağaza hakkındaki uyarıları bulabilirsiniz. Ne olumlu ne de olumsuz sonuç çıkmıyorsa, o mağazadan alışveriş yapmamak en iyisidir.

Fiyatları karşılaştırın. Geizhals.at veya idealo.at gibi sitelerdeki fiyatları karşılaştırın. Ürünler web sitesindekinden çok daha pahalıysa, bu dolandırıcılık anlamına gelir.

Dolandırıcılık mesajları

Kimlik Avı

Tehlikeler

Kimlik avı mesajları olarak adlandırılan sahte e-postalar ile suçlular veri çalmaya çalışır. Dolandırıcılar tanınmış şirketler veya bankalar adına e-posta gönderir. Örneğin bir bankanın sahte giriş sayfasına yönlendiren bir bağlantıya tıklamanız beklenir. Orada kişisel verilerinizi girmeniz beklenir ve bu veriler suçluların eline geçer.

SMS („smishing“) veya telefon aramaları („vishing“) da bu dolandırıcılık türü için kullanılır.

Kendinizi nasıl korursunuz?

Her zamanki gibi giriş yapın. Müşterisi olduğunuz banka veya şirketlerden gelen e-posta veya SMS mesajlarındaki bağlantılara tıklamayın. Tarayıcınıza geçin ve kullanıcı hesabınıza giriş yapın. Mesajın var olup olmadığını oradan kontrol edin.

Göndereni kontrol edin. Suçlular genellikle bilinen bir şirket gibi davranır. Size kimin mesaj gönderdiğini kontrol edin. Gönderenin adı ve e-posta adresi gerçekten eşleşiyor mu?

Gizli verileri ifşa etmeyin. Sizden bir şifre veya benzeri gizli bir veri vermeniz mi isteniyor? Bunu asla e-posta, SMS veya telefon yoluyla yapmayın.

Tehlikeli programlar

Tehlikeler

Kötü amaçlı yazılımlar suçlular tarafından ağlara, bilgisayarlara, tabletlere veya mobil cihazlara erişim sağlamak için kullanılır.

Burada amaç cihazlarınıza zarar vererek para veya veri elde etmektir.

Kötü amaçlı yazılımlar cihazınıza birçok farklı yolla girebilir: Örneğin, suçlular size e-posta yoluyla tehlikeli dosyalar gönderebilir. Kötü amaçlı yazılımlar genellikle aslında güvenli olduğu düşünülen programların ve uygulamaların içinde gizlenir.

Kendinizi nasıl korursunuz?

Güncellemeleri gerçekleştirin.
Bilgisayarınızdaki ve akıllı telefonunuzdaki işletim sisteminizi ve programlarınızı güncel tutun. Bu şu anlama gelir: Güncellemeleri hemen yapın!

Bilinmeyen taraflardan gelen ekleri açmayın.
Yalnızca güvendiğiniz göndericilerden gelen e-posta eklerini açmalısınız. Göndereni tanıyor musunuz? Yine de, e-posta içeriğinin mantıklı olup olmadığını kısaca değerlendirin! Bu aynı zamanda bağlantılara tıklarken de geçerlidir.

Programları resmi mağazalardan yükleyin.
Uygulamaları ve programları yalnızca „Google Play Store“ veya „App Store“ gibi mağazalardan yükleyin.

Peşin ücret ödeme dolandırıcılığı

Dolandırıcılık

Tehlikeler

Peşin ücret ödeme dolandırıcılığında, kâr, miras veya uygun kredi teklifleriyle kandırılırsınız. Şantaj e-postaları, sahte aşk ilişkileri ve sözde acil durum yardım çağrıları da yaygın dolandırıcılık türlerindendir. Amaç size para ödetmektir.

Suçlular bunun için çeşitli nedenler uydururlar: Örneğin, vaat edilen kazançları almadan önce ücret ödemeniz gerekir. Bu şekilde saf kurbanlardan para alınır. Suçlular daha sonra parayı alıp kaçarlar.

Kendinizi nasıl korursunuz?

Tanımadığınız kişilere avans ödemesi yapmayın. Para almanız gerekiyordu, ancak aniden sizden ödemeler veya kişisel belgeler mi talep edildi? Bu bir uyarı sinyalidir.

Mesajın içeriğini sorgulayın. E-postayla veya bir sohbet mesajıyla size alışılmadık miktarda para mı vaat ediliyor? Bunun doğru olup olamayacağını değerlendirin. Suçlular bu tür mesajları birçok kişiye rastgele gönderirler.

Mesajları arayın. Mesajların metnini veya yeni internet tanıdıklarının isimlerini „dolandırıcılık“ veya „sahtekârlık“ kelimeleriyle birlikte bir arama motoruna girin. Bu şekilde uyarılarla karşılaşabilirsiniz.

Ticaret dolandırıcılığı

Şüpheli yatırım platformları

Tehlikeler

Paranızı kârlı bir yatırıma yönlendirmek mi istiyorsunuz? Bunu dikkatli bir şekilde yapmalısınız. İnternette yatırım fırsatları ararsanız, dolandırıcı yatırım platformlarıyla karşılaşabilirsiniz.

Suçlular risk almadan yüksek kârlar vaat eder.
Önceden herhangi bir bilgiye ihtiyacınız yoktur, bunun yerine suçlular size kişisel olarak tavsiyelerde bulunur. Kulağa hoş geliyor, ama bu bir aldatmaca!

Kendinizi nasıl korursunuz?

Vaatleri sorgulayın. Dolandırıcı platformlar sizi gerçekçi olmayan tekliflerle cezbeder. Küçük yatırımlar için yüksek kârlar vaat ediliyorsa yatırım yapmayın.

Web sitesini kontrol edin. Künyeyi arayın. Eğer yoksa, uzak durun! Künye var mı? Web sitesi adresini ve „sorun“ veya „dolandırıcılık“ gibi kelimeleri bir arama motoruna girin.

Reklâmlara aldanmayın. Platformu bir reklâmdan veya çevrimiçi bir gazete makalesinden mi öğrendiniz? Dolandırıcı platformlar çok sayıda reklâm yayınlar. „Kısa sürede yüksek kâr“ veya „risksiz kâr“ vaat ediliyorsa, bu bir aldatmacadır.

İnternet birçok avantaj sunar ve hayatı kolaylaştırır. Ancak bilmeniz gereken tehlikeler de vardır. Bu kitapçıkla interneti güvenli bir şekilde kullanmanıza yardımcı oluyoruz:

- İnternette hangi dolandırıcılık yöntemleri yaygındır?
- Bu tehlikeleri nasıl tanıyabilirsiniz?
- Kendinizi internet dolandırıcılığından nasıl korursunuz?

Bu broşür BAWAG Grubu'nun sağladığı fonlarla finanse edilmiştir.

Künye
ÖIAT | Ungargasse 64, 1030 Wien
www.watchlist-internet.at
kontakt@watchlist-internet.at