

Tetikte olun; internette tuzağa düşmeyin

İnternet sadece bilim ve teknoloji, kültür ve ekonomi değil, **suç için** de sayısız imkanlar doğuruyor. **İnsanoğlunun en eski sanatlarından biri** olan dolandırıcılığın, bilgi çağındaki



sürümleri hala insanların **safliğından** istifade ediyor. İnternet dolandırıcılıkları da zaman zaman **komedî filmlerini** gölgede bırakıyor.

Bazı dolandırıcılık metotları gerçekten de en saf kullanıcıları hedef alıyor. Ancak bazı türleri de var ki kolay kolay farkına varmak mümkün olmuyor. İşte bu makalemizde en basitinden, en gelişmişine türlü **internet dolandırıcılığı** metodunu sizler için derledik. Sonuçta hiçbir güvenlik

yazılımı, hiçbir güvenlik teşkilatı insanı bilgi ve bilinç sahibi olmak kadar **koruyamaz**.

1. Sosyal ağ dolandırıcılığı

Facebook'tan para isteyen olursa dikkat edin!

Sahtekârlar; Facebook, Twitter, MySpace gibi bir sosyal ağdaki bir kullanıcı hesabını çalıyorlar. Daha sonra kurbanın eşinden, dostundan başının belada olduğunu, acilen paraya ihtiyacı olduğunu söyleyen mesajlarla, belirli bir adrese para yollamalarını istiyorlar.

Bunun çok farklı çeşitleri mevcut, mesela flört ederek kendisine hediye, para veya kontör yollatanlar var. Sirenlerin cazibesine kapılmayın...

2. Bahis dolandırıcılıkları

Maç sonuçlarını önceden bilen olmaz, olsa da size söylemez! Bu dolandırıcılık metodunda ertesi gün oynanacak olan bir maçın sonuçları, kurbanı e-posta ile atılıyor. Ücretsiz bir hizmet olarak tanıtılan bu maç sonuçları birkaç gün boyunca doğru çıkmaya devam ederek, en şüpheli kurbanı bile postayı atanların maç sonuçlarını bildiğine inandırıyor.

Bir süre sonra ise kurbanı daha sonraki maçların sonuçlarını da öğrenmeye devam etmek istemesi durumunda, belirli bir hesaba yüklü bir miktarda para yatırması gerektiği söyleniyor. Bahislerde büyük paralar kazanma hayalleri kuran kurban da parasından oluyor.

Peki dolandırıcıların maç sonuçlarını nasıl bildiklerini merak ettiniz mi? Elbette bilmiyorlar! Rastgele yolladıkları milyonlarca e-postadan illa ki birkaç tanesi üst üste sonuçları doğru tutturuyor.

3. Kriz vurguncuları

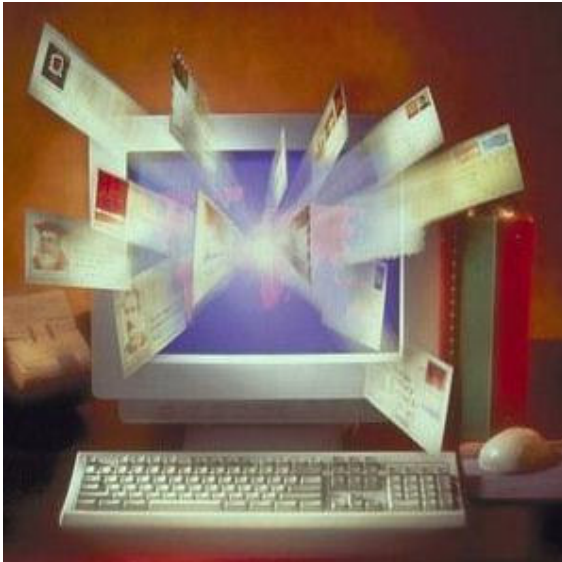
Borç içindeki insanların çaresizliğinden faydalanıyorlar. Ekonomik güçlüğü düşen, borcunu ödeyemeyenlere bir darbe de dolandırıcılardan geliyor. Sıkıntıdaki kurbanın internet, telefon, posta gibi yollarla ulaşan dolandırıcılar, borçlarının ödenmesinde yardımcı olacak ödeme planları sunuyorlar. Gösterilen veya yatırılan teminatları da türlü şekillerde çalarak kayıplara karışıyorlar. Özellikle de kredi kartı borçlarını devralmayı vadeden dolandırıcılara rastlanıyor.

4. Yaşlıları korkutanlar

İhtiyarları acımadan can evinden vuruyorlar. Bu özellikle de Asya'da çok yaygın bir yöntem. Kurban yaşlı insanlardan seçilerek çeşitli yollardan torunlarının kazada yaralandığı söyleniyor. İnternet üzerinden ziyade telefonda yapılıyor. Yardım çılgınlıkları, ağlamalar gibi oyunculuklarla, ihtiyar kurbanların telaşa kapılarak ellerinin ayaklarının birbirine dolaşmasına sebep olan dolandırıcılar, kurbanın tedavi için acil para yollamasını istiyor.

5. Büyük kazanç vaadi

İnanmayın: "İşimizi gör yüzde 20 senin" Bu dolandırıcılık bir malın satışı karşılığında büyük bir komisyon vaadi şeklinde gerçekleşebiliyor. Alternatif çeşitleri çok olan dolandırıcılıkta kurbanlara iş de teklif edilebiliyor. Bu iş yüzde 20 gibi dev bir komisyon vaat ediyor. Kurbanın çalıntı veya geçersiz bir çek yollanıyor. Kurbandan paranın komisyon hariç kısmının yollanmasını isteyen dolandırıcılar, çekin sahte olduğu anlaşılmeden önce parayı alıp kayboluyor.



6. İzinsiz faturalandırma

Hesabınızdan izinsiz para çeken şirketler ekip çalışması yapıyor

Sahtekâr bir firma müşterinin hesabından mevcut bilgileri kullanmak suretiyle para çekmeye devam edebiliyor.

Ücretsiz denemeler için verilen kredi kartı bilgileri genellikle bu şekilde kullanılıyor. Bu kredi kartı bilgileri sahtekar şirketlerce paylaşılarak kredi kartı her taraftan hortumlanıyor.

7. Banka'dan şifrenizi sorarlarsa

Güvenlik sorularının cevapları sahtekarlara her kapıyı açıyor. Adına aldanmayın, hem telefonda, hem de e-posta'da sık sık yapılan bir dolandırıcılık çeşidi. Bankadan gelmiş gibi duran ciddi bir e-posta veya ciddi bir görevliyle telefon konuşması, kurbanı hesap bilgilerinde güvenlik riski oluşturduğu gerekçesiyle kandırıyor. Doğrulama için bütün özel bilgileri alıp kaydederek kurbanın hesabını boşaltmakta kullanıyor.



Bunun daha gelişmiş bir şeklinde direkt özel bilgileri sormayan dolandırıcı, sadece güvenlik sorularını soruyor ve bu cevaplarla gerçek bankayı arayarak şifre değiştiriyor. Böylece hesabı ele geçiriyor.

8. Virüslü e-postalar

Bedava vaatlerine kanmayın. Bedava vaatleriyle dolup taşan e-postalar, özellikle de anti-virüs reklamları sahtedir. Bunların içerdiği ek dosyalar veya bağlantıların götürdüğü adresler zararlı yazılımlarla dolup taşıyor. Bu yazılımlar bilgisayardan şifreleri çalabiliyor.

9. Sahte aracı kuruluşlar

İsmi, markası bilinir olmayan aracılar güvenmeyin. Süslü, gıcır gıcır, pırıl pırıl hazır fotoğraflar kullanılarak hazırlanmış sitelere ve hesaplara dikkat edin. Özellikle eBay üzerinde yaygınlaşan bir dolandırıcılık metodu bu. Alıcı ve satıcı arasında güven ortamı sağlamak için çalışan bağımsız aracı kuruluş hizmetleri gerçekte olan ve işleyen bir sistem. Ancak sahte aracı kuruluşlar artan sıklıkta alıveriş yapanların belası olmaya başladı.

10. Oltaya gelenler

Phishing yani balıkçılık yönteminde ağa takılanlar soyuluyor. En yaygın internet dolandırıcılığı, yasal bir kurum gibi davranarak hesap bilgilerini çalmak için yapılıyor. Yanlış bir bağlantıya tıklayıp gerçekten bankaya girdiğini sanan kullanıcı, şifresini sahte bir siteye giriş dolandırıcılara vermiş oluyor. İnternet tarayıcılarda bu tür sahte sitelere karşı filtre özelliği gittikçe yaygınlaşıp geliyor. Pek çok dolandırıcılık aslında bu tür altına giriyor.

Kaynak: http://www.chip.com.tr/konu/tetikte-olun-internette-tuzaga-dusmeyin_14736.html