

GÜVENLİK DİJİTAL DÜNYADA

Siber suç vaka çalışmalarının
analiziyle yaşlılar için pratik
çözümler



İÇİNDEKİLER:

BÖLÜM 1.

SİBER SALDIRILAR VE İNTERNET GÜVENLİĞİ

- WI-FI ağları üzerinden saldırı (özel ve genel)
- E-posta saldırıları
- Zayıf şifre saldırıları
- Kimlik avı
- Kötü amaçlı yazılımlar ve bilgisayar virüsleri

BÖLÜM 2 FİNANSAL VE YATIRIM DOLANDIRICILIĞI

- Finansal ve yatırım manipölasyonları
- Görünür fedakarlık: yardım dolandırıcılığı
- Cazip illüzyonlar: hayali ödüller ve çekilişler
- Dijital para dolandırıcılıkları
- Uluslararası finansal dolandırıcılık

BÖLÜM 3 SOSYAL MANİPÜLASYON VE DUYGUSAL ALDATMA

- Erkek-kadın ilişkilerinde dolandırıcılık
- Smishing - SMS dolandırıcılığı
- Yaşlıları ilgilendiren telefon dolandırıcılıkları
- Duygusal aile bağlarını istismar eden dolandırıcılıklar
- Tıbbi ürünlerle ilgili dolandırıcılıklar

BÖLÜM 4 ÇEVİRİMİÇİ İŞLEM DOLANDIRICILIĞI

- Seyahat ve bilet dolandırıcılıkları
- Abonelik dolandırıcılığı
- Sahte çevrimiçi mağazalar oluşturmada dolandırıcılık
- İnternet reklamları aracılığıyla yapılan sahtekarlık amaçlı satın almalar (satın alma)
- Sınıflı ilan siteleri üzerinden yapılan dolandırıcılık amaçlı satın alımlar (satış)

BÖLÜM 5 KİMLİK MANİPÜLASYONU VE KAMU GÜVENİNİN SÖMÜRÜLMESİ

- Suça karışma iddiaları
- Devlet kurumlarının taklidi şeklinde manipölasyonlar
- Deepfake teknolojisi kullanılarak yapılan manipölasyon
- Devlet kurumlarını taklit eden hizmet dolandırıcılığı
- Sahte hesaplar aracılığıyla dolandırıcılık



Funded by
the European Union



Modern teknoloji giderek daha fazla hayatımıza entegre oluyor ve bu da sanal dünyada güvenliğin hayati önemini vurguluyor. Bu konu, genellikle modern teknolojilerde o kadar da yetenekli olmayan ve siber tehditlere daha fazla maruz kalan yaşlılar için özellikle önemlidir. "Dijital dünyada güvenlik" e-kitabı, yaşlıların kendilerini internetteki tehditlere karşı korumalarına yardımcı olan gerekli bilgi ve araçları sunar.

Bu e-kitap, Avrupa Birliği tarafından finanse edilen 2023-1-PL01-KA220-ADU-000160325 numaralı "Cyber Safe Senior" projesinin bir parçası olarak oluşturulmuştur. Bu proje, yaşlıların İnternet güvenliği kuralları konusunda farkındalıklarını artırmayı ve dijital becerilerini geliştirmeyi amaçlamaktadır. İnternetin güvenli kullanımı konusunda eğitime olan artan talebe yanıt olarak, proje yaşlıların tehlikelerden kaçınmalarına ve acil durumlarda tepki vermelerine yardımcı olmak için pratik ipuçları, vaka çalışmaları ve analizler sunmaktadır.

E-kitap, siber saldırılar, finansal dolandırıcılık, sosyal manipülasyon, çevrimiçi işlem dolandırıcılığı ve kimlik hırsızlığı gibi siber güvenliğin çeşitli yönlerine ilişkin bölümler içerir. Her bölüm, siber suçluların faaliyetlerini gösteren ve onlara karşı etkili bir şekilde nasıl savunma yapılacağını gösteren vaka çalışmaları içerir. Pratik tavsiyeleri sayesinde, bu e-kitap modern teknolojileri güvenli bir şekilde kullanmak isteyen yaşlılar için değerli bir bilgi kaynağıdır.



Funded by
the European Union



Projenin bir parçası olarak, yalnızca değerli bilgiler sağlamakla kalmayıp aynı zamanda kullanıcıları meşgul eden ve onlara ilgi gösteren benzersiz materyaller hazırladık. Temel unsurlardan biri, profesyonelce hazırlanmış video kliplerdir - gerçek durumları, olası tehditleri ve tehlikelere karşı uygun tepkileri erişilebilir bir şekilde gösteren beş dinamik, görsel olarak çekici film. Bu filmler, sağlanan bilgilerin anlaşılmasını ve hatırlanmasını kolaylaştıran pratik örneklerle eğitmeyi amaçlamaktadır.

Ayrıca etkileşimli bir sınav paketi hazırladık. Bu sınavlar yalnızca eğitici değil, aynı zamanda ilgi çekici ve eğlenceli olacak şekilde geliştirildi, böylece katılımcılar eğlenirken bilgilerini test edebilirler. Alıcıları bu şekilde etkilemek yalnızca mesajı daha çekici hale getirmekle kalmaz, aynı zamanda etkinliğini de artırarak edinilen bilginin daha uzun süre akıllarında kalmasını sağlar.

Eğitim ve eğlenceyi bir araya getiren bu unsurlar, projeyi sadece değerli kılmakla kalmıyor, aynı zamanda her alıcı için çekici ve keyifli hale getiriyor.



Funded by
the European Union



VİDEOLAR:

Duygusal manipölasyon - yardım dolandırıcılığı

Finansal manipölasyon

Şifre kırma

Sahtecilik ve deepfake

Çevrimiçi alışverişin tuzakları

QUIZ:

SMS Dolandırıcılıkları: Kendinizi Ne Kadar İyi Koruyabilirsiniz?

E-posta saldırıları, kimlik avı dolandırıcılıkları, zayıf parola kullanmanın riskleri ve kötü amaçlı yazılımlar ve bilgisayar virüsleri.

Sahtecilik ve deepfake teknolojileri.

Çevrimiçi Alım Satım: Tehditleri Fark Edebilir misiniz?

Finansal manipölasyon ve yaşlıların duygularını sömürme.

BÖLÜM 1.

SİBER SALDIRILAR VE İNTERNET GÜVENLİĞİ

Günümüzün dijital dünyasında, yaşlılar çevrimiçi güvenliklerini tehdit eden siber saldırılara karşı giderek daha savunmasız hale geliyor. Bu bölümde, yaşlıların kendilerini tehditlerden korumalarına yardımcı olabilecek saldırı yöntemlerini ve güvenlik önlemlerini tartışacağız.

WI-FI saldırıları, suçluların verileri ele geçirmek için kullanabileceği hem özel hem de genel ağları içerir. Genel erişim noktalarını kullanmanın risklerini anlamak ve güvenli wi-fi ağlarını tanıyabilmek önemlidir.

Kimlik avı gibi e-posta saldırıları, kişisel bilgileri elde etmek için güvenilir kurumlardan geliyormuş gibi görünen sahte mesajlar gönderir. Zayıf parolalar, özel hesaplara erişimi kolaylaştırabilecek başka bir sorundur.

Kötü amaçlı yazılımlar ve virüsler cihazlara sızabilen ve verileri çalabilen ciddi bir risk oluşturur. Düzenli güncellemeler, antivirüs yazılımları ve şüpheli bağlantılardan kaçınma gibi koruma yöntemlerini tartışacağız.

Yaşlıların bu riskleri anlamalarına, bunlardan kaçınmalarına ve çevrimiçi ortamda verilerini ve gizliliklerini korumalarına yardımcı olacak pratik ipuçlarına ve stratejilere odaklanacağız.

WI-FI aęları zerinden saldırı (zel ve genel)

TEHLİKE ZELLİKLERİ:

Genel WI-FI aęları, İnternet'e cretsiz eriřim saęlar ve byk bir kolaylık olarak kabul edilir. Ktphaneler, kafeler, havaalanları, restoranlar ve oteller dahil olmak zere birok genel alanda mevcuttur. Ancak, aık WI-FI- uzun zamandır bilgileriniz iin riskli bir evrimii ortam olarak kabul edilmektedir. Hibir WI-FI tamamen risksiz olmasa da, zel verilerinizin gvenlięi byk lde WI-FI trne baęlıdır. Hem zel hem de genel WI-FI aęlarına ynelik saldırılar birok biimde olabilir.

Bu tr saldırıların beř tr řunlardır:

Bir MitM saldırısında, saldırgan taraflardan birini taklit ederek bir WI-FI aęındaki iki cihaz arasındaki iletiřimi kesintiye uęratır. Bu sayede kullanıcıların bilgisi olmadan oturum ama bilgileri, parolalar veya bankacılık bilgileri gibi verileri ele geirebilir.

Evil Twin saldırısında, saldırgan ilk bakıřta meřru bir aęa benzeyen sahte bir WI-FI aęı oluřturur. Kullanıcılar gerek bir aęa baęlandıklarını dřnerek sahte bir aęa baęlanırlar ve bu da saldırganın iletilen tm verileri engellemesine olanak tanır.

Ortadaki
adam saldırısı
(MitM)

Kt İkiz tipi
saldırı

WI-FI ağıları üzerinden saldırı (özel ve genel)

TEHLİKE ÖZELLİKLERİ:

WI-FI Parolasına Kaba Kuvvet Saldırısı

Saldırgan, farklı karakter kombinasyonlarını sistematik olarak test eden programlar kullanarak WI-FI parolasını tahmin etmeye çalışır. Bir parola zayıf veya çok basit olduğunda, bu saldırı etkili olabilir ve ağa yetkisiz erişime izin verebilir.

Paket Koklama türü bir saldırı

Bu saldırıda saldırgan, bir WI-FI ağı üzerinden gönderilen veri paketlerini yakalamak ve analiz etmek için özel bir yazılım kullanır. Güvenli bir ağda bile, veriler düzgün bir şekilde ŞİFRElenmemişse okunabilir ve kullanılabilir.

Hizmet Reddi (DoS) saldırısı

Bir DoS saldırısında, saldırgan bir WI-FI erişim noktasına çok sayıda geçersiz istek veya yanlış yetkilendirme iptali sinyali göndererek ağ tıkanıklığına neden olur. Bu, ağı geçici olarak devre dışı bırakabilir veya bozabilir ve kullanıcıların bağlantıyı kullanmasını önleyebilir.

WI-FI ağıları üzerinden saldırı (özel ve genel)



SONUÇLAR:

Halka açık ve ücretsiz İnternet erişimini kullanmak, hassas verileri ve çevrimiçi güvenliği tehlikeye atabilecek bir dizi tehlikeyle birlikte gelir. Halka açık WI-FI ağılarını kullanırken risklerin ne olduğunu bilmek önemlidir.

WI-FI ağına yönelik farklı saldırı türlerinin yol açtığı sonuçlar:

01 Aracı Adam (MitM)

Yaşlılar, bir suçlunun banka hesaplarına veya sosyal paylaşım sitelerine giriş bilgilerini ele geçirmesi durumunda kimlik hırsızlığının kurbanı olabilir veya birikimlerini kaybedebilirler.

02 Kötü İkiz

Kullanıcılar, güvenli bir ağ kullandıklarını düşünerek farkında olmadan oturum açma kimlik bilgilerini, kredi kartı numaralarını veya diğer hassas bilgileri verebilirler.

WI-FI ağıları üzerinden saldırı (özel ve genel)



SONUÇLAR:

03 Kaba kuvvet

Yaşlıların basit veya tekrarlanan şifreler kullanması durumunda, suçlular ağlarına erişebilir ve bu da gizlilik ihlallerinin yanı sıra internet faturalarının artmasına da yol açabilir.

04 Paket Koklama

Saldırganlar şifrelenmemiş verileri ele geçirirse, yaşlılar e-posta, parola ve kişisel bilgiler gibi özel bilgilerin sızdırılması riskiyle karşı karşıya kalabilir.

05 Hizmet Reddi (DoS)

DoS saldırıları yaşlıların interneti kullanmasını engelleyebilir; bu durum özellikle sevdikleriyle iletişim kurmak veya günlük işlerini halletmek için teknolojiye güvenen kişiler için sorun teşkil edebilir.

WI-FI ağıları üzerinden saldırı (özel ve genel)



ARKA PLANDA TARİHLE KORUMA YOLLARI



Philip yakındaki bir restoranda akşam yemeği yemeye karar verdi. Restoranın halka açık WI-FI'sini kullanarak son haberleri kontrol etmek için e-postasını açtı. Ne yazık ki, halka açık WI-FI ağılarıyla ilişkili tehlikelerin farkında olmadığı için bağlantısını güvence altına almadı. Bir Aracı Saldırısı sonucunda suçlu, e-posta oturum açma bilgilerini ele geçirdi ve bu da hesabına yetkisiz erişime ve gizli bilgilerin potansiyel olarak sızdırılmasına neden oldu.



Philip'in hikayesi nadir değildir ve sadece yaşlıların başına gelmez. Ancak bu düzeltilebilir. Aşağıdaki ipuçlarıma göz atın.

Tehditleri fark etmemenin sonuçları:

ADIM 1: Kamuya açık bir alanda bulunan bir restoranın WI-FI ağına saldırı

Philip, e-postasını kontrol etmek için restorandaki genel WI-FI ağını kullanıyor. İki faktörlü kimlik doğrulamanın olmaması gibi uygun güvenlik önlemlerinin olmaması, suçlunun oturum açma ayrıntılarını ele geçirmesine izin verdi.

ADIM 2: Yetkisiz e-posta erişimi

Saldırı sonucunda suçlu, Philip'in e-posta hesabına yetkisiz erişim sağlayarak özel yazışmalar, kişiler ve diğer gizli veriler gibi hassas bilgilere ulaştı.

ADIM 3: Gizli bilgilerin sızdırılması

Bir e-posta hesabını ele geçirmek, Philip'in gizliliğini ve güvenliğini tehdit edebilecek gizli bilgilerinin potansiyel olarak sızdırılmasına yol açabilir. Bir suçlu bu verileri dolandırıcılık, kimlik hırsızlığı veya diğer yasa dışı faaliyetler için kullanabilir.

ADIM 4: Duygusal sonuçlar

Philip, halka açık WI-FI ağını kullanırken stres, kaygı ve güven kaybı yaşadı. Ayrıca, parolaları değiştirme, hesapları izleme ve daha fazla saldırıyı önlemek için eylemde bulunma ihtiyacı ek zaman ve çaba gerektirebilir.

WI-FI ağıları üzerinden saldırı (özel ve genel)

— ARKA PLANDA TARİHLE KORUMA YOLLARI

WI-FI üzerinden yapılan saldırılardan korunmak için aşağıdaki yöntemleri izleyerek bu tür sonuçlardan kurtulabilirsiniz.



Güçlü parolalar kullanın:

WI-FI ağınıza güçlü ve benzersiz bir parola ile güvence altına alın. Ad, soyad, doğum tarihi veya diğer kolay tahmin edilebilir karakter kombinasyonları gibi bariz parolalar kullanmamaya dikkat edin.

Yazılımı güncelle:

Bilinen güvenlik açıklarına karşı korunmak için yönlendirici yazılımınızı düzenli olarak güncelleyin.



WI-FI ağıları üzerinden saldırı (özel ve genel)



ARKA PLANDA TARİHLE KORUMA YOLLARI



Şifrelemeyi etkinleştir:

Güvenli WI-FI ağlarında bile, aktarılan tüm verilerin şifrelendiğinden emin olun.

Genel WI-FI ağlarından kaçınin:

Mümkünse, hassas verileri iletmek için halka açık WI-FI ağlarını kullanmaktan kaçınin. Kullanmanız gerekiyorsa, sanal özel ağ (VPN) kullanın.



Ağınızı izleyin:

Yetkisiz cihazları hızla tespit etmek için WI-FI ağınıza hangi cihazların bağlı olduğunu düzenli olarak kontrol edin.

E-posta saldırıları

TEHLİKE ÖZELLİKLERİ:

E-posta tabanlı saldırılar, e-posta hesapları aracılığıyla sistemlere veya bilgilere yetkisiz erişim elde etmek için yapılan kötü amaçlı girişimlerdir. Yaşlıların savunmasız olduğu birçok saldırı türü vardır. En yaygın olanlardan bazılarını tanımaya değer.

E-posta kutularına yönelik başlıca saldırı türleri:

Kimlik avı, dolandırıcıların güvenilir kaynaklardan (örneğin bankalar, devlet daireleri) geliyormuş gibi görünen sahte e-postalar gönderdiği yaygın bir yöntemdir.

Dolandırıcıların eylemi:

- Sahte bağlantılar ve ekler: Dolandırıcılar, şifreler ve kredi kartı numaraları gibi hassas bilgileri elde etmek için tasarlanmış sahte web sitelerine bağlantılar veya ekler içeren mesajlar gönderir.
- Aciliyet duygusu yaratma: E-postalar genellikle hesabınızla ilgili sorunlar, bilgilerinizi derhal güncellenmeniz gerektiği veya şüpheli etkinlikler hakkında uyarılar hakkında bilgiler içerir.

Hedef odaklı kimlik avı, saldırıların kişiselleştirildiği ve belirli kişileri hedef aldığı daha gelişmiş bir kimlik avı biçimidir.

Dolandırıcıların eylemi:

- Kişiselleştirilmiş mesajlar: Dolandırıcılar, meşru e-postalar oluşturmak için sosyal medya gibi herkese açık kaynaklardan mağdur hakkında bilgi toplarlar.
- Arkadaş taklidi: Bu mesajlar çoğu zaman kurbanın tanıdığı biri (örneğin iş yerinden bir meslektaş) tarafından gönderilmiş gibi görünür.

Kimlik avı
saldırıları

Mızraklı Kimlik
Avı saldırıları

E-posta saldırıları

TEHLİKE ÖZELLİKLERİ:

E-posta Sahteciliği saldırıları

E-posta sahteciliği, dolandırıcıların e-posta başlıklarını değiştirerek bunların güvenilir bir kaynaktan gönderilmiş gibi görünmesini sağlayan bir tekniktir.

Dolandırıcıların eylemi:

- Sahte başlıklar: Dolandırıcılar, mesajların başlıklarını değiştirerek gerçek bir adresten, örneğin bir arkadaştan, patrandan veya güvenilen bir kurumdan gönderilmiş gibi görünmesini sağlarlar.
- Kimlik Gizleme: Mesajlar gerçek görünür ve bu da alıcılar ve istenmeyen posta önleme sistemleri tarafından tespit edilmelerini zorlaştırır

Kötü amaçlı yazılım ve fidye yazılımının dağıtımı

Siber suçlular genellikle kötü amaçlı yazılımları dağıtmak için e-posta hesaplarını ele geçirirler.

Dolandırıcıların eylemi:

- Enfekte ekler: E-postalar, açıldığında kurbanın bilgisayarına kötü amaçlı yazılım yükleyen ekler içerir.
- Kötü amaçlı bağlantılar: E-postalar, bilgisayarınıza otomatik olarak kötü amaçlı yazılım indirip yükleyen web sitelerine bağlantılar içerebilir.

E-posta iletişimlerine yönelik aracı saldırılar (MITM)

MITM saldırısı, bir saldırganın iki taraf arasındaki verileri, taraflardan birinin bilgisi olmadan ele geçirip iletmesi durumunda gerçekleşir.

Dolandırıcıların eylemi:

- Veri ele geçirme: bilgisayar korsanları, oturum açma kimlik bilgileri veya şirket sırları gibi hassas bilgileri elde etmek için iletişimlerini ele geçirir.
- Sahtecilik: Ayrıca, bir taraf adına mesaj göndererek iletişimin manipüle edilmesine olanak tanıyabilirler.

E-posta saldırıları

TEHLİKE ÖZELLİKLERİ:

E-posta ele geçirme veya ele geçirme saldırıları

Bilgisayar korsanları, şifrenizi tahmin ederek veya diğer yöntemleri kullanarak e-posta hesabınıza erişmeye çalışırlar.

Dolandırıcıların eylemi:

- şifre tahmini: Bilgisayar korsanları, şifrenizi tahmin etmek için kaba kuvvet gibi teknikler kullanabilirler.
- Kimlik Avı: Ayrıca, oturum açma bilgilerinizi vermeniz için sizi kandırmak amacıyla kimlik avı veya diğer sosyal mühendislik tekniklerini de kullanabilirler.

Kimlik bilgisi toplama saldırıları

Bilgisayar korsanları, kullanıcıları kandırarak giriş bilgilerini vermeleri yoluyla e-posta hesaplarına erişim sağlıyor.

Dolandırıcıların eylemi:

- Kimlik avı: Kullanıcıya, oturum açma bilgilerine yönelik sahte bir istek içeren bir e-posta gönderilir.
- Sosyal etki: Bilgisayar korsanları, başka biriymiş gibi davranarak kullanıcı adı ve şifre isterler; çoğunlukla isteklerini daha inandırıcı kılmak için sosyal medya bilgilerini kullanırlar.

E-posta saldırıları



SONUÇLAR:

E-posta saldırılarının gizli verileri ve çevrimiçi güvenliği tehdit edebilecek bir dizi ciddi sonucu vardır. Kendinizi korumak için bunları tanımak önemlidir.

01 Kimlik avı saldırıları

- Kimlik hırsızlığı: Yaşlılar oturum açma bilgilerini, kredi kartı numaralarını verebilir ve bu da kimlik hırsızlığına yol açabilir.
- Maddi Kayıp: Verilerin iletilmesi yetkisiz işlemlere ve maddi kayıplara yol açabilir.

02 Mızraklı Kimlik Avı saldırıları

- Gizliliğin ihlali: Yaşlılar, güvendikleri biriyle iletişim kurduklarını düşünerek gizli bilgileri paylaşabilirler.
- Maddi ve Manevi Kayıplar: Maddi ve manevi kayıplara yol açacak eylemlerde bulunmaya yönlendirilebilirler.

03 E-posta Sahteciliği saldırıları

- Güvenlik ihlali: Yaşlılar yanlış bilgilerle hareket edebilir ve bu da güvenlik ihlallerine yol açabilir.
- Kötü amaçlı yazılım kurulumu: Bağlantılara veya eklere tıklamak kötü amaçlı yazılımların kurulumuna yol açabilir.

E-posta saldırıları



SONUÇLAR:

04 Kötü amaçlı yazılım ve fidye yazılımının dağıtımı

- Sistem Hasarı: Kötü amaçlı yazılımlar bilgisayarınıza zarar verebilir ve kullanılmaz hale getirebilir.
- Fidye Yazılımı: Kötü amaçlı yazılımlar bilgisayarınızdaki dosyaları şifreleyebilir ve bunların kilidini açmak için fidye talep edebilir.

05 E-posta iletişimlerine yönelik aracı saldırılar (MITM)

- Gizliliğin kaybı: Yaşlılar bilmeden gizli bilgileri ifşa edebilirler.
- Manipülasyon: Saldırganlar iletişimin her iki tarafını da yanıltabilirler.

06 E-posta ele geçirme veya ele geçirme saldırıları

- Kimlik hırsızlığı: bilgisayar korsanları hassas bilgilere erişebilir ve bunları kimliğinizi çalmak için kullanabilirler.
- Spam gönderme: Ele geçirilen hesaplar spam ve kötü amaçlı yazılım göndermek için kullanılabilir.

07 Kimlik bilgisi toplama saldırıları

- Erişim Kaybı: Yaşlılar e-posta hesaplarına erişimlerini kaybedebilirler.
- Gizlilik ihlali: bilgisayar korsanları özel bilgilere ve yazışmalara erişim sağlayabilir.

E-posta saldırıları



ARKA PLANDA TARİHLE KORUMA YOLLARI



Daniel ailesiyle iletişimde kalmak için düzenli olarak e-posta kullanıyor. Yurt dışında yaşayan oğlu ona sık sık e-postayla güncellemeler gönderiyordu. Bir gün Daniel, oğlu tarafından gönderilmiş gibi görünen bir e-posta aldı.

Gönderen: tom@example.com

Konu: Yeni tatil fotoğrafları!

Merhaba Baba, umarım her şey yolundadır. Son gezimizden fotoğrafları sizinle paylaşmak istedim.

Bunları görmek için aşağıdaki bağlantıya tıklayın.
[Fotoğraflara bakın]

Saygılarımla, oğlunuz

Tehditleri fark etmemenin sonuçları:

ADIM 1: Bağlantıya tıklayın

Daniel, oğlundan bir mesaj aldığını düşünerek linke tıkladı.

ADIM 2: bilgisayarınıza bulaştırın

Bağlantıya tıklamak Daniel'in bilgisayarına yüklenen kötü amaçlı yazılımı indirdi. Bu tür yazılımlar çevrimiçi etkinliğinizi izleyebilir, parolalarınızı ve diğer gizli bilgilerinizi çalabilir.

E-posta saldırıları



ARKA PLANDA TARİHLE KORUMA YOLLARI

Daniel'in örneği e-posta kutularına yönelik saldırıların ne kadar tehlikeli olabileceğini gösteriyor.

Mesajdaki bağlantı, bilgisayarına otomatik olarak kötü amaçlı yazılım indirip kuran bir web sitesine yönlendiriyordu.



ADIM 3: Bilgisayarınıza bulaştırın

Kötü amaçlı yazılım, Daniel'in banka hesap numaraları, çeşitli servislerin şifreleri ve özel belgeleri de dahil olmak üzere kişisel verilerine erişim sağlamayı başardı.

ADIM 4: Duygusal stres

Daniel aldatıldığını hissetti ve birinin oğlunu taklit ettiğinden endişelendi. Olay onda büyük stres ve kaygıya neden oldu.

E-posta saldırıları



ARKA PLANDA TARİHLE KORUMA YOLLARI

E-posta saldırılarına karşı kendinizi korumak için aşağıdaki yöntemleri izleyerek bu tür sonuçlardan kaçınabilirsiniz.



E-postaları açarken dikkatli olun:

Daniel e-postaları açarken dikkatli olmalı:

Aksiyon:

- Özellikle mesajda bağlantı veya ekler varsa, gönderenin e-posta adresini mutlaka kontrol edin.
- Mesajları dikkatlice okuyun ve alışılmadık isteklere ve dil bilgisi hatalarına dikkat edin.



Antivirüs yazılımı güncellemeleri:

Daniel, bilgisayarında ve telefonunda düzenli olarak güncellenen antivirüs yazılımlarına sahip olduğundan emin olmalı.

Aksiyon:

- Antivirüs yazılımını düzenli olarak güncelleyin ve sistemi tarayın.
- En son işletim sistemi ve web tarayıcısı güncellemelerini yükleyin.



E-posta saldırıları

— ARKA PLANDA TARİHLE KORUMA YOLLARI

İki Faktörlü Kimlik Doğrulama (2FA):

Daniel, tüm ilgili hesaplarda iki faktörlü kimlik doğrulama (2FA) kullanarak ek bir güvenlik katmanını etkinleştirmeyi düşünmelidir. Bu yaklaşım, parola ortaya çıksa bile güvenlik seviyesini önemli ölçüde artırır.

Aksiyon:

- Ek bir güvenlik katmanı: ŞİFREniz açığa çıksa bile güvenlik seviyenizi artıran tüm önemli hesaplarınızda 2FA kullanın.



2FA aktivasyonunu değerlendirmeye değer:

- Paranıza güvenli bir şekilde erişebilmek için çevrimiçi olarak banka hesabınıza giriş yapın.
- Önemli bilgilerin ve yazışmaların saklandığı e-posta hesabınıza giriş yaptığınızda.
- Özellikle aile ve arkadaşlarla iletişim kurmak, kişisel fotoğraf ve bilgileri paylaşmak için bir sosyal medya platformuna erişildiğinde.

Daniel bu önlemleri alarak e-posta saldırıları ve diğer siber suç türleriyle ilgili pek çok potansiyel tehditten kaçınabilir.

Tavsiyelerimi aklınızda tutun, çünkü bu, interneti kullanırken kendinizi daha güvende hissetmenize ve kişisel ve finansal verilerinizi yetkisiz erişime karşı korumanıza yardımcı olacaktır.



Zayıf ŞİFRE saldırıları



TEHLİKE ÖZELLİKLERİ:

Zayıf parolalar kullanılarak yapılan saldırılar, siber suçluların en sık kullandığı yöntemlerden biridir.

E-posta kutularına yönelik başlıca saldırı türleri:

Sözlük saldırısı, önceden hazırlanmış bir listeden (sözlük) çok sayıda olası parolanın test edilmesini içerir. Bu liste genellikle yaygın sloganlar ve sözcük varyasyonları içerir. Kullanıcı "ŞİFRE", "123456" veya "qwerty" gibi tahmin edilmesi kolay parolalar kullanıyorsa bu etkili bir yöntemdir.

**Sözlük
saldırısı**

Kaba kuvvet saldırısında saldırgan, doğru parola bulunana kadar tüm olası karakter kombinasyonlarını sistematik olarak test eder. Bu tür saldırılar uzun sürebilirken, kısa ve basit parolalar için etkili olabilir.

**Kaba kuvvet
saldırısı**

Bu saldırı, oturum açma bilgileri ve parolalar gibi önceki bilgi sızıntılarından toplanan verileri kullanır. Saldırganlar, kullanıcıların birden fazla web sitesinde aynı oturum açma bilgilerini yeniden kullanma eğiliminde oldukları gerçeğine güvenerek, farklı web sitelerinde aynı oturum açma-parola kombinasyonlarını kullanmaya çalışır.

**Kimlik bilgisi
doldurma
saldırısı**

Doğrudan bir parola saldırısı olmasa da, kimlik avı kullanıcıları oturum açma kimlik bilgilerini gönüllü olarak ifşa etmeye kandırmaya çalışan bir tekniktir. Saldırganlar gerçek web sitelerine benzeyen sahte web siteleri oluşturur (ör. bankacılık, e-posta) ve insanları oturum açmaya teşvik eden e-postalar gönderir.

**Kimlik avı
saldırısı**

Zayıf şifre saldırıları



SONUÇLAR:

Zayıf parolalar kullanan saldırıların yaşlılar için bir dizi ciddi sonucu vardır ve hassas verileri ve çevrimiçi güvenliği tehdit edebilir. Kendinizi korumak için bunları bilmeniz önemlidir.

01 Sözlük saldırısı

"ŞİFRE" veya "123456" gibi kolayca tahmin edilebilir şifreler kullanan yaşlılar bu saldırıya kurban gidebilir. Sonuç olarak, gizlilikleri ihlal edilebilir ve kişisel veya finansal veriler çalınabilir.

02 Kaba kuvvet saldırısı

Kısa ve basit parolalar kullanan yaşlılar kaba kuvvet saldırılarına karşı savunmasızdır. Suçlular WI-FI üzerinden hesaplarına erişebilir ve bu da olası veri sızıntılarına ve kimlik hırsızlığına yol açabilir.

03 Kimlik bilgisi doldurma saldırısı

Birden fazla web sitesinde aynı giriş bilgilerini kullanma eğiliminde olan yaşlılar bu tür saldırılara karşı savunmasızdır. Bu, çeşitli çevrimiçi platformlardaki hesaplarına yetkisiz erişime yol açabilir.

04 Kimlik avı saldırısı

Bu tür tehditlerin daha az farkında olabilecek yaşlı yetişkinler, kimlik avı saldırılarına karşı hassastır. Suçlular, insanları kandırarak hesap giriş bilgilerini elde etmek için sahte web siteleri veya e-postalar kullanabilir ve bu da kimlik hırsızlığı veya mali dolandırıcılıkla sonuçlanabilir.

Zayıf şifre saldırıları



ARKA PLANDA TARİHLE KORUMA YOLLARI



Anna, iş yerindeki meslektaşlarıyla iletişimde kalmak için Facebook hesabını kullanıyor. Günlük olarak orada fotoğraflar yayınlıyor, önemli etkinlikleri paylaşıyor ve profesyonel projeleri koordine ediyor. Ne yazık ki, Facebook şifresinin kırıldığı ve hesabının siber suçlular tarafından ele geçirildiği bir saldırıya kurban gitti.



Bu tür vakalar nadir değildir ve yalnızca yaşlıları değil, aynı zamanda mesleki olarak aktif ve teknoloji konusunda bilinçli kişileri de etkiler. Yaşına bakılmaksızın herkes, uygun çevrimiçi güvenlik önlemlerini almazsa siber suçluların kurbanı olabilir.

ADIM 1: Basit bir parola kullanma

Anna, sözlük saldırısını daha da kolaylaştıran "12345678" gibi basit bir şifre kullandı.

ADIM 2: Benzersiz parolalar yok

Anna birçok web sitesinde aynı şifreyi kullandı. şifreyi başka sitelerde de kullandı ve bu da veri sızıntısına neden oldu.

Zayıf şifre saldırıları

— ARKA PLANDA TARİHLE KORUMA YOLLARI

Zayıf parola saldırılarına karşı korunmak için aşağıdaki yöntemleri izleyerek bu tür sonuçlardan kaçınabilirsiniz.



şifrenizi güçlü ve benzersiz bir şİFREle değiştirin:

Anna Facebook şifresini derhal başka hiçbir web sitesinde kullanılmayan güçlü, uzun ve benzersiz bir şifrele değiştirmelidir. şifre harf, sayı ve özel karakterlerin bir karışımını içermelidir.

İki faktörlü kimlik doğrulamayı (2FA) etkinleştirin:

Facebook hesabınızda iki faktörlü kimlik doğrulamayı etkinleştirmek iyi bir fikirdir, bu ek bir güvenlik katmanı sağlayacaktır. Bu sayede, birisi şifreyi bilse bile, örneğin bir SMS kodu gibi ikinci bir kimlik doğrulama faktörü olmadan giriş yapamayacaktır.



Güvenlik ayarlarınızı kontrol edin:

Bilinmeyen herhangi bir cihaz veya uygulama eklenip eklenmediğini görmek için Facebook güvenlik ayarlarınızı gözden geçirmeli ve tüm cihazlardan çıkış yapmalısınız. Ayrıca, ayarlanmışlarsa güvenlik sorularınızı da değiştirmelisiniz.

Zayıf şifre saldırıları



ARKA PLANDA TARİHLE KORUMA YOLLARI



Facebook'a bir olay bildirin:

Doğru çözüm, Facebook Destek ekibiyle iletişime geçip hesabınızın tehlikeye atıldığını bildirmektir. Facebook, hesabınızı kurtarmanıza ve daha fazla saldırıya karşı korumanıza yardımcı olabilir.

Diğer hesaplara göz atın:

Aynı şifreyi kullanmış olabileceği diğer web sitelerindeki hesaplarınızı kontrol etmeye ve şifreleri benzersiz ve güçlü olanlarla değiştirmeye değer. Bu, daha fazla hesap ele geçirilmesini önleyecektir.



Kimlik avı eğitimi:

Gelecekte bu tür saldırılardan kaçınmak için kimlik avı girişimlerini nasıl tanıyacağınızı öğrenmek de iyi bir uygulamadır. Anna şüpheli e-postalara, bağlantılara dikkat etmeli ve giriş sayfalarının URL adreslerini dikkatlice kontrol etmelidir.

Kimlik avı

TEHLİKE ÖZELLİKLERİ:

Phishing, dolandırıcıların gizli bilgileri elde etmeye çalıştığı bir siber saldırı biçimidir. "Phishing" kelimesi, metaforik olarak kullanıcıların kişisel verilerini "balıklemek" anlamına gelen İngilizce "fishing" kelimesinden gelir.

Phishing'in dayandığı dört temel ilke şunlardır:

- **Yöntem:** Dolandırıcılar, güvenilir kuruluřlardan (örneğin bankalar, teknoloji řirketleri, devlet daireleri) geliyormuş gibi görünen sahte web siteleri, e-postalar veya mesajlar oluřtururlar.
- **Teknik:** Orijinal kaynakları taklit eden logolar, renkler ve iletişim tarzları kullanırlar.
- **Amaç:** Mağdurun güvenini kazanarak oturum açma kimlik bilgilerini veya diğeri gizli bilgileri sağlamasını sağlamak

- **Yöntem:** Mağdurun hızlı hareket etmesini sağlamak için aciliyet veya korku duygusunun kullanılması.
- **Teknik:** İddia edilen bir hesap ihlali, ödenmemiş bir ödeme veya acil yanıt gerektiren özel bir fırsat hakkında bir mesaj gönderme.
- **Amaç:** Mağdurun dikkatli bir şekilde düşünmeden, dürtüsel bir şekilde hareket etme olasılığını artırmak.

**Güvenilir
kaynakları
taklit etme**

**Acil ve duygusal
mesajlar
oluřturma**

Kimlik avı

TEHLİKE ÖZELLİKLERİ:

Sahte bağlantılar ve ekler kullanmak

- Yöntem: Kötü amaçlı yazılım içeren sahte web sitelerine bağlantılar veya ekler içeren mesajlar göndermek.
- Teknik: Bağlantılar meşru görünebilir, ancak bunlar oturum açma bilgilerini toplayan veya kurbanın cihazına kötü amaçlı yazılım yükleyen sahte sitelere yönlendirir.
- Amaç: Giriş bilgilerini ele geçirmek, kurbanın cihazına kötü amaçlı yazılım bulaştırmak veya bilgi toplamak için kimlik avı yapmak.

Sosyal mühendislik

- Yöntem: Psikolojik aldatma tekniklerini kullanarak mağduru manipüle etmek.
- Teknik: Kişiselleştirilmiş mesajlar oluşturmak için sosyal medya verileri gibi herkese açık bilgileri kullanma. Dolandırıcılar ayrıca teknik destek çalışanları gibi davranarak telefon görüşmeleri de yapabilirler.
- Amaç: Sahte bir güvenlik duygusu yaratmak ve mağduru gizli bilgileri ifşa etmeye kandırmak.

Kimlik avı



SONUÇLAR:

Phishing neden tehlikelidir? Başarılı bir phishing saldırısının sonuçları ciddi olabilir - para kaybetmekten kimlik hırsızlığına, bir cihazı kötü amaçlı yazılımla enfekte etmeye kadar. Kendinizi korumak için bunları bilmeniz önemlidir.

01 Güvenilir kaynakları taklit etme

- Kimlik hırsızlığı: Yaşlılar, farkında olmadan kişisel bilgilerini verebilir ve bu bilgiler daha sonra kendi adlarına sahte banka veya kredi hesapları açmak için kullanılabilir.
- Maddi kayıp: Banka hesabınızın giriş bilgilerini paylaşmanız yetkisiz işlemlere ve birikimlerinizin kaybına yol açabilir.

02 Acil ve duygusal mesajlar oluşturma

- Yetkisiz ödemeler: Yaşlılar, banka bilgilerini vererek ve gereksiz transferler yaparak yanlış uyarılara hızla yanıt verebilirler.
- Tasarruf Kaybı: Hızlı karar alma cazibesine kapılmak, özellikle yaşlıların dolandırıcıların eline kredi kartı bilgilerini vermesi durumunda önemli maddi kayıplara yol açabilir.
- Artan savunmasızlık: Tekrarlanan dolandırıcılık girişimleri, stres ve belirsizlik nedeniyle yaşlıları gelecekteki saldırılara karşı daha savunmasız hale getirebilir.

Kimlik avı

— SONUÇLAR:

03 Sahte bağlantılar ve ekler kullanmak

- Cihaz enfeksiyonu: Kötü amaçlı yazılımlar yaşlı bir kişinin bilgisayarına veya akıllı telefonuna bulaşarak cihaz üzerindeki kontrolün kaybedilmesine ve gizli bilgilere erişim sağlanmasına yol açabilir.
- Veri hırsızlığı: Kötü amaçlı yazılımlar oturum açma kimlik bilgilerini ele geçirerek dolandırıcıların banka hesaplarına ve diğer gizli kaynaklara erişmesine olanak tanıyabilir.
- Onarım maliyetleri: Kötü amaçlı yazılımları kaldırmak ve enfekte olmuş bir cihazı onarmak, yaşlıların hazırlıklı olmayabileceği yüksek teknik maliyetler gerektirebilir.

04 Sosyal mühendislik

- Telefon dolandırıcılığı: Yaşlılar telefonla gizli bilgilerini vermeye kandırılabilir, bu da kimlik hırsızlığına ve maddi kayba yol açabilir.
- Güven kaybı: Sık sık yapılan sosyal mühendislik saldırıları, meşru kurum ve kişilere karşı güvenin kaybolmasına yol açarak, günlük yaşamı ve finansal yönetimi zorlaştırabilir.
- Duygusal manipülasyon: Korku, stres ve kaygı gibi psikolojik etkiler yaşlıların ruh sağlığını olumsuz yönde etkileyebilir.

Kimlik avı



ARKA PLANDA TARİHLE KORUMA YOLLARI



Maria ailesiyle iletişim kurmak, banka hesaplarını kontrol etmek ve haberleri okumak için düzenli olarak İnternet'i kullanır. Bir gün bankasından gelmiş gibi görünen bir e-posta alır.

Kimden: Bank XYZ no-reply@bankxyz.com Konu: Önemli: Acil hesap doğrulaması gerekiyor!

Sayın Maria, Hesabınıza yetkisiz erişim girişimleri nedeniyle, lütfen kimliğinizi doğrulamak ve hesabınızı güvence altına almak için hemen hesabınıza giriş yapın. Lütfen aşağıdaki bağlantıya tıklayın ve talimatları izleyin:

Giriş yapmak için buraya tıklayın

İşbirliğiniz için teşekkür ederiz, Bank XYZ

Tehditleri fark etmemenin sonuçları:

ADIM 1: Bağlantıya tıklayın

Maria, e-postanın içeriği konusunda endişelenerek, gerçekliğini dikkatlice kontrol etmeden bağlantıya tıklar. Bağlantı onu, bankasının giriş sayfasına benzeyen bir sayfaya götürür.

ADIM 2: Giriş bilgilerinin sağlanması

Maria, hesabını doğruladığını düşünerek sahte web sitesine giriş bilgilerini giriyor.

Kimlik avı

— ARKA PLANDA TARİHLE KORUMA YOLLARI

Maria'nın örneği, güvenilir kaynakları taklit etme gibi yaygın bir kimlik avı yöntemini göstermektedir. Maria'nın bu tehdidi fark edememesinin yol açabileceği sonuçlara bakalım.



ADIM 3: Ek ek

E-postada bir ek de bulunur. Maria kötü amaçlı yazılım içeren bir ek indirir. Dosyayı açtığında, kötü amaçlı yazılım bilgisayarına yüklenir ve dolandırıcıların cihazına uzaktan erişmesine olanak tanır.

ADIM 4: Veri ele geçirme ve para hırsızlığı

Maria bağlantıya tıkladığında dolandırıcılar hemen giriş bilgilerini ele geçirdiler ve Maria'nın gerçek banka hesabına erişim sağladılar.

ADIM 5: Stres ve kaygı

Maria birikimlerinin kaybından dolayı perişan durumda ve gelecekte internet bankacılığını ve diğer internet hizmetlerini kullanmaktan korkuyor.

ADIM 6: Cihazınızı enfekte edin

Maria'nın bilgisayarındaki kötü amaçlı yazılım, dolandırıcıların Maria'nın çevrimiçi faaliyetlerini izlemesine, daha fazla oturum açma bilgisini ele geçirmesine ve potansiyel olarak diğer dosyalara bulaştırmasına olanak tanıyor.

Kimlik avı



ARKA PLANDA TARİHLE KORUMA YOLLARI

Kendinizi kimlik avı dolandırıcılıklarından korumak için aşağıdaki yöntemleri izleyerek bu tür sonuçlardan kaçınabilirsiniz.



Gönderen e-posta adresini ve bağlantıları kontrol etme:

Maria tıklamadan önce gönderenin e-posta adresini ve mesajdaki bağlantıları dikkatlice kontrol etmelidir.

Aksiyon:

- E-posta adresi kontrolü: E-postanın bankanın gerçek alan adından geldiğinden emin olun.



İki faktörlü kimlik doğrulamanın (2FA) ayarlanması:

Maria, banka hesabında iki faktörlü kimlik doğrulamayı (2FA) etkinleştirmelidir; bu, ek bir güvenlik katmanı ekler. Dolandırıcılar parolanızı ele geçirse bile, SMS kodu gibi ikinci bir kimlik doğrulama ögesine de ihtiyaç duyarlar.

Aksiyon:

- 2FA aktivasyonu: Maria, 2FA'yı etkinleştirmek için bankasıyla iletişime geçmelidir.



Kimlik avı

— ARKA PLANDA TARİHLE KORUMA YOLLARI

Antivirüs yazılımını ve işletim sistemini düzenli olarak güncelleyin:

Maria, en son kötü amaçlı yazılımlara ve kimlik avı tehditlerine karşı koruma sağlamak için antivirüs yazılımının ve işletim sisteminin düzenli olarak güncellenmesini sağlamalıdır.

Aksiyon:

- Antivirüs yazılımı: Maria antivirüs yazılımı yüklemeli ve bunun her zaman güncel olduğundan emin olmalı ve düzenli olarak güncellemeyi unutmamalıdır.



Maria bu önlemleri alarak, kimlik avı kurbanı olma riskini azaltabilir, verilerini ve mali kaynaklarını koruyabilir. Gönderenin e-posta adresini her zaman dikkatlice kontrol edin ve beklenmedik e-postalardaki bağlantılara veya eklere tıklamaktan kaçının.



Kötü amaçlı yazılımlar ve bilgisayar virüsleri

TEHLİKE ÖZELLİKLERİ:

Kötü amaçlı yazılım terimi, bir bilgisayara zarar vermek veya kullanıcı tarafından istenmeyen eylemler gerçekleştirmek için tasarlanmış kötü amaçlı programları tanımlamak için kullanılır. Bilgisayar virüsü, dolandırıcılarının karşı karşıya olduğu en ciddi tehditlerden biridir. Kötü amaçlı yazılımlar, verileri çalmaktan bir sistemi yavaşlatmaya ve dosyaları tamamen yok etmeye kadar muazzam hasarlara yol açabilir.

Yaygın kötü amaçlı yazılım türleri:

Kullanıcı verilerine erişimi şifreleyerek engelleyen bir kötü amaçlı yazılım türü. Siber suçlu, şifre çözme anahtarı karşılığında fidye talep eder ve verilere erişimi geri yüklemeyi vaat eder. Ancak suçlular genellikle anlaşmayı bozar, fidye ödendikten sonra bile gizli verileri satar ve kurbanlar tekrar hedef alınabilir.

Bir kullanıcının cihazına sızmak için meşru yazılım gibi görünen bir kötü amaçlı yazılım türü. Yüklendikten sonra cihaza erişim sağlar, diğer kötü amaçlı yazılım türlerinin yüklenmesine, kullanıcıları gözetlemesine ve gizli bilgileri çalmasına olanak tanır. Truva atları genellikle kimlik avı ve kullanıcıyı kötü amaçlı bir dosyayı indirmeye teşvik eden sahte web siteleri gibi sosyal mühendislik tekniklerini kullanarak yayılır.

Fidye yazılımı

Truva atı

Kötü amaçlı yazılımlar ve bilgisayar virüsleri

TEHLİKE ÖZELLİKLERİ:

Solucanlar

Virüslere benzer ancak yayılmak için kullanıcı etkileşimi gerektirmeyen bir kötü amaçlı yazılım türü. Kurulum ve çoğaltma aygıtlarındaki güvenlik açıklarını kullanır. Bir aygıt enfekte ettiğinde, aynı ağdaki diğer aygıtlara bağlanmaya çalışır ve onlara yayılmak için başka güvenlik açıkları arar.

Casus yazılım

Kimlik bilgileri ve kredi kartı numaraları gibi hassas bilgileri casusluk etmek ve toplamak için kurbanın cihazına yüklenen kötü amaçlı yazılım. Casus yazılım diğer programlarla birlikte gelebilir veya bir reklama tıklayarak veya güvenilir olmayan web sitelerinden ücretsiz yazılım indirerek kendiniz yükleyebilirsiniz. Yüklendikten sonra tuş vuruşlarını, tarama geçmişini izler ve cihazınızın kamerasını ve mikrofonunu kullanır.

Dosyasız kötü amaçlı yazılım

Bir cihazı enfekte etmek için kötü amaçlı kod içeren yürütülebilir dosyalar kullanmayan bir kötü amaçlı yazılım türü. Bunun yerine, cihazınızın meşru sistem araçlarında değişiklikler yaparak, sabit sürücünüze dosya indirmenize gerek kalmadan kötü amaçlı etkinlikler gerçekleştirmenize olanak tanır. Kötü amaçlı dosyasız yazılım kodu, hedeflerine ulaşmak için mevcut sistem araçlarını kullanarak doğrudan bilgisayarın belleğinde çalışır.

Kötü amaçlı yazılımlar ve bilgisayar virüsleri



TEHLİKE ÖZELLİKLERİ:

Akıllı telefonlar ve tabletler gibi mobil cihazlara saldırarak hassas verilere erişmeyi amaçlayan bir kötü amaçlı yazılım türü. Yeterli güvenlik önlemleri olmayan cihazlar, genellikle orijinal işletim sistemine yerleşik varsayılan savunma mekanizmalarından yoksun oldukları için bu tür saldırılara karşı savunmasızdır.

Cihazları enfekte eden ve diğer cihazlara yayılmak için çoğalan bir kötü amaçlı yazılım türüdür. Genellikle kendilerini kurbanların yüklediği kötü amaçlı dosyalar veya uygulamalar olarak gizlerler. Saldırganlar genellikle kullanıcıları bu dosyaları indirmeye ikna etmek için kimlik avı saldırıları kullanırlar. Kurban enfekte dosyayı veya uygulamayı indirdiğinde virüs etkinleşir ve cihazda çoğalmaya başlar. Algılanmamak için sık sık dosyaları değiştirir ve diğer cihazları enfekte eder. Virüs gizli verileri çalabilir, cihazınızı yavaşlatabilir, uygulamaları dondurabilir ve dosyaları değiştirebilir ve yok edebilir.

Mobil kötü amaçlı yazılım

Virüsler

Kötü amaçlı yazılımlar ve BİLGİSAYAR virüsleri



SONUÇLAR:

Kötü amaçlı yazılımla enfekte olmanın sonuçları çok ciddidir. Siber suçlular kar elde etme arzusuyla hareket ederler. Bankacılık hizmetleri için kimlik bilgileri elde etmek, kişisel verileri satış için toplamak, bilgisayar kaynaklarına erişimi satmak veya kurbanlardan ücret almak gibi saldırılar başlatmak için enfekte cihazları kullanırlar.

01 Fidyе yazılımı

Yazılım, mali belgeler veya aile fotoğrafları gibi yaşlı birinin önemli verilerine erişimin kaybolmasına neden olabilir. Ayrıca, fidye ödemek veri kurtarmayı garantilemez ve bu da ek mali kayıplara yol açabilir.

02 Truva atı

Yazılım, banka hesap şifreleri veya kredi kartı numaraları gibi hassas bilgilerin çalınmasına yol açarak yaşlıları kimlik hırsızlığı ve maddi kayıp riskine sokabilir.

03 Casus yazılım

Yazılım, yaşlıların konuşmalarını dinlemek veya çevrimiçi faaliyetlerini izlemek için kullanılabilir; bu da onların mahremiyetini ihlal eder ve toplanan verilerin şantaj veya dolandırıcılık amacıyla kullanılmasına yol açabilir.

Kötü amaçlı yazılımlar ve bilgisayar virüsleri



SONUÇLAR:

04 Solucanlar

Yazılım, yaşlı bir kişinin cihazının işletim sistemine zarar verebilir veya siber suçluların kontrolünü ele geçirebilir; bu da cihazın kullanılmasını imkânsız hale getirebilir veya önemli verilerin kaybolmasına yol açabilir.

05 Dosyasız kötü amaçlı yazılım

Yazılım arka planda çalışarak cihazınızın ayarlarını farkında olmadan değiştirebilir veya kaynaklarını kullanabilir; bu da cihazınızın yavaşlamasına veya performansında sorunlara yol açabilir.

06 Mobil kötü amaçlı yazılım

Yazılım, yaşlıların kişisel bilgilerine erişerek veya konumlarını izleyerek veri kaybına veya mahremiyetlerinin ihlal edilmesine yol açabilir.

07 Virüsler

Virüsler, parolalar, finansal bilgiler veya kişisel veriler gibi gizli verileri çalabilir ve kullanıcıların gizliliğini ihlal edebilir. Ağdaki diğer cihazlara çoğalabilir ve yayılabilir, daha fazla enfeksiyona neden olabilir ve sorunun ölçeğini artırabilir.

Kötü amaçlı yazılımlar ve bilgisayar virüsleri

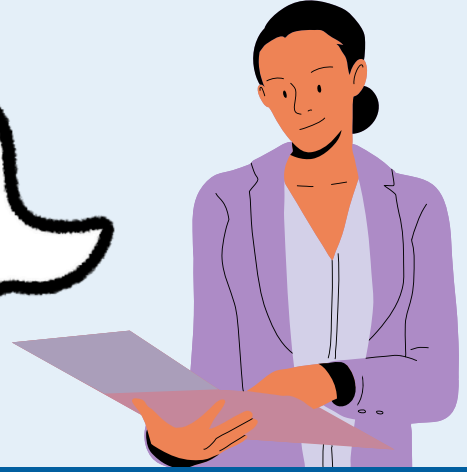


ARKA PLANDA TARİHLE KORUMA YOLLARI



Alexander e-postasına bakıyordu. Beklemediği bir haber gördü ve bu onu meraklandırdı. Bu e-postadaki eke tıkladı. Garip bir şey fark etti. Bir şey bilgisayarındaki dosyaları değiştirmeye başladı ve bu da işinde önemli aksamalara neden oldu. Ne olmuş olabilirdi?

Aleksander'inkine benzer durumlar ne yazık ki oldukça yaygındır. Şüpheli bir e-posta ekine tıklamak, bilgisayarınızın kötü amaçlı yazılımla enfekte olmasına yol açabilir. Sonuç olarak, operasyonlarda ve veri güvenliğinde ciddi kesintiler meydana gelebilir.



ADIM 1: E-posta ekine tıklayın

Aleksander e-postasını tararken, hiç şüphelenmeden e-postadaki eke tıkladı.

ADIM 2: Cihaz enfeksiyonu

Sahte eke tıkladığında cihazına virüs bulaştı.

ADIM 3: Virüsün çoğalması/çoğalması

Kötü amaçlı kod (ekte) Aleksander'ın bilgisayarında hızla çoğalmaya başladı, dosyalarda değişikliklere ve işlerinde aksaklıklara neden oldu.

ADIM 4: Veri hırsızlığı olasılığı

Ayrıca virüsün Alexander'ın cihazından gizli verileri çalma yeteneğine de sahip olabileceği ve bu durumun daha fazla güvenlik ve gizlilik sorununa yol açabileceği belirtiliyor.

Kötü amaçlı yazılımlar ve bilgisayar virüsleri

— ARKA PLANDA TARİHLE KORUMA YOLLARI

Aşağıdaki zararlı yazılımlardan korunma yöntemlerini uygulayarak bu tür sonuçlardan kaçınabilirsiniz.



Yeni şüpheli tehdit mesajları mevcut olduğunda yazılımınızı düzenli olarak güncelleyin; bu, bu güvenlik açıklarını istismar eden kötü amaçlı yazılımlarla bulaşma riskini azaltır.

Özellikle bilinmeyen kişilerden geliyorsa veya şüpheli görünüyorsa, e-posta eklerini açarken ve dosya indirirken dikkatli olun.



Enfeksiyonlara veya veri kaybına yol açabileceğinden şüpheli bağlantılara veya açılır pencerelere tıklamaktan kaçının.

Kötü amaçlı yazılımlar ve bilgisayar virüsleri



ARKA PLANDA TARİHLE KORUMA YOLLARI



Saldırılara karşı savunmasız oldukları için halka açık Wi-Fi ağlarını dikkatli kullanın; İnternet bağlantınızı güvence altına almak için bir VPN hizmeti kullanmayı düşünün. Bir VPN kullanarak, verileriniz halka açık ağlar üzerinden seyahat ederken şifrelenir, yani hiç kimse IP adresinizi göremez veya cihazınızdan gönderdiğiniz veya aldığınız verileri engelleyemez.

Enfeksiyonları önlemeye ve casus yazılım ve reklam yazılımı da dahil olmak üzere kötü amaçlı yazılımları kaldırmaya yardımcı olan antivirüs ve kötü amaçlı yazılım önleme programları kullanın. Antivirüser esas olarak virüsleri tespit etmeye ve ortadan kaldırmaya odaklanırken, kötü amaçlı yazılım önleme, virüs tarayarak sınıflandırılmayan kötü amaçlı uygulamalar da dahil olmak üzere geniş bir kötü amaçlı yazılım yelpazesine ilgilidir.



Bu önerileri izleyerek Alexander ve diğer İnternet kullanıcıları kötü amaçlı yazılımlardan kaynaklanan tehditlerden kaçınabilir. Çok hızlı karar almamaya ve sanal dünyada her zaman dikkatli davranmaya dikkat edin.



Daha Fazla Okuma



WI-FI AĞLARI ÜZERİNDEN SALDIRI (ÖZEL VE GENEL)

- www.keepersecurity.com/pl_PL/threats/man-in-the-middle-attacks-mitm.html
- www.cdv.pl/blog/blog-ekspercki/najpopularniejsze-rodzaje-atakow-hakerskich/
- www.socialwifi.com/pl/baza-wiedzy/bezpieczenstwo-sieci/najpopularniejsze-rodzaje-atakow-na-wifi/



E-POSTA SALDIRILARI

- www.powerdmarc.com/pl/what-are-email-tabanlı-saldırılar/
- <https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y>
- www.keepersecurity.com/blog/pl/2023/08/30/the-most-common-types-of-cyberattacks/



ZAYIF ŞİFRE SALDIRILARI

- www.keepersecurity.com/blog/pl/2024/01/12/types-of-password-attacks/
- www.securivy.com/blog/brute-force/
- www.keepersecurity.com/pl_PL/threats/dictionary-attack.html



KİMLİK AVI

- www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y
- www.orange.pl/poradnik/twoj-internet/co-to-jest-phishing-i-jak-sie-przed-nim-bronic/
- www.kwestiabezpieczenstwa.pl/phishing/



KÖTÜ AMAÇLI YAZILIMLAR VE BİLGİSAYAR VİRÜSLERİ

- www.keepersecurity.com/blog/pl/2024/01/24/twelve-common-types-of-malware/
- www.hackeru.pl/wirus-komputerowy/
- www.powerdmarc.com/pl/types-of-malware/

BÖLÜM 2.

FİNANSAL VE YATIRIM DOLANDIRICILIĞI

Günümüz dünyasında, yaşlılar giderek daha fazla çeşitli biçimlerde ortaya çıkan ve suçlular tarafından sürekli olarak rafine edilen finansal dolandırıcılıkların kurbanı oluyor. Bu bölüm, yaşlıların tehditleri fark etmelerine ve birikimlerini korumalarına yardımcı olmak için en yaygın dolandırıcılık türlerini vurgulamayı amaçlamaktadır.

En yaygın yöntemler arasında, hızlı kar vaatlerine dayanan finansal ve yatırım manipülasyonu ve yaşlıların empatisini sömüren hayırsever dolandırıcılıklar yer alır. Bir diğer tehlike ise, talep etmek için ödeme gerektiren sahte ödüller ve piyangolar aracılığıyla büyük kazançlar vaadidir.

Bitcoin gibi dijital para birimlerini içeren dolandırıcılıklar da daha yaygın hale geliyor ve suç faaliyetleri için yeni bir yol sunuyor. Nijerya dolandırıcılıklarından da bahsetmek önemli – hayali işlemlere dayalı uluslararası dolandırıcılık planları.

Bu tehditleri anlamak, yaşlıların mali durumlarını bilinçli bir şekilde koruyabilmeleri açısından hayati önem taşıyor.

Finansal ve yatırım manipölasyonları

TEHLİKE ÖZELLİKLERİ:

Finansal ve yatırım manipölasyonu, bireyleri paralarını hileli veya uygunsuz planlara yatırmaya ikna etmeyi amaçlayan aldatıcı uygulamalara atıfta bulunur. Bu planlar genellikle yüksek getiriler vaat eder ancak sonunda yatırımcılar için finansal kayba neden olur.

Finansal yatırımlarda manipölasyon türleri:

Dolandırıcılar, yatırımcılara yatırımlarından alışılmadık derecede yüksek getiriler vaat etmek için ikna edici taktikler kullanırlar. Bu vaatler gerçek olamayacak kadar iyi görünebilir ve genellikle emeklilik gelirlerini tamamlamanın yollarını arayan yaşlıları hedef alır.

Dolandırıcılar genellikle bireyleri yatırım ürünlerini iyice araştırmadan veya anlamadan hızlı yatırım kararları almaya zorlamak için yüksek baskı satış taktikleri kullanırlar. Sınırlı süreli teklifler iddia ederek veya kazançlı fırsatları kaçırma korkusunu vurgulayarak aciliyet duygusu yaratabilirler.

Dolandırıcılar, yatırımcıların, özellikle de yaşlıların anlamasının zor olduğu karmaşık veya belirsiz yatırım ürünleri önerebilir. Bu ürünler yüksek ücretler, gizli riskler içerebilir veya yatırılan fonların nasıl kullanılacağı konusunda şeffaflık eksikliği olabilir.

**Yüksek
Getirilerin
Sahte
Vaatleri**

**Hızlı Yatırım
Yapma Baskısı**

**Karmaşık ve
Kafa Karıştırıcı
Yatırım Ürünleri**

Finansal ve yatırım manipölasyonları



SONUÇLAR:

Finansal ve yatırım manipölasyonunun aşğıdaki gibi ciddi olumsuz etkileri olabilir:

01 Mali Sonuçlar

Finansal manipölasyona kurban gitmek, zor kazanılan birikimlerin ve yatırımların kaybına yol açabilir. Beklenenden önemli ölçüde daha az parayla kendinizi bulabilirsiniz, bu da günlük masraflarınızı karşılama ve emekliliğinizin tadını çıkarma yeteneğinizi etkiler.

02 Duygusal Etki

Finansal dolandırıcılar tarafından aldatılmak, ihanete uğramışlık ve hayal kırıklığı hissine yol açabilir. Bir dolandırıcılığa düştüğünüz için utanabilir veya mahcup hissedebilirsiniz, bu da öz saygınızı ve güveninizi etkiler.

03 Kişisel Sonuçlar

Finansal manipölasyona kurban gitmek başkalarına olan güveni aşındırabilir, sizi gelecekteki yatırım fırsatlarına karşı daha temkinli ve şüpheli hale getirebilir. Bu güven kaybı ilişkileri zorlayabilir ve finansal tavsiye veya destek aramanızı zorlaştırabilir.

Finansal ve yatırım manipölasyonları



ARKA PLANDA TARİHLE KORUMA YOLLARI



Sofia, yeni bir teknoloji şirketinde kazançlı bir yatırım fırsatı sunduğunu iddia eden bilinmeyen bir göndericiden bir e-posta alır. E-posta yüksek getiriler vaat eder ve Bayan Jenkins'i yatırımda yerini güvence altına almak için hızlı davranmaya çağırır.

Ancak Sofia, büyük kazançlar vadeden istenmeyen e-postalara karşı dikkatli olunması gerektiği yönündeki okuduğu tavsiyeyi hatırlıyor.

Sofia'nın hikayesi ne yazık ki tek vaka değil, ancak yaşlıları finansal manipölasyondan korumanın önemini gösteriyor. Yaşlılar karşılaşılabilecekleri çeşitli manipölasyon biçimlerinin farkında olmalı ve bunlardan kaçınmak için yöntemler bilmelidir.



ADIM 1: Doğrulama

Sofya herhangi bir işlem yapmadan önce yatırım fırsatının meşruiyetini doğrulamaya karar verir.

ADIM 3: Onay

Hala şüpheli olan Sofia, yatırım fırsatını doğrulamak için doğrudan şirketle iletişime geçmeye karar verir

ADIM 2: Danışma

Sofia, finans alanında deneyimi olan güvendiği aile üyesinden tavsiye istiyor.

ADIM 4: Rapor

Sofia şüpheli e-postayı ilgili makamlara bildirmeye karar verir.

Finansal ve yatırım manipölasyonları

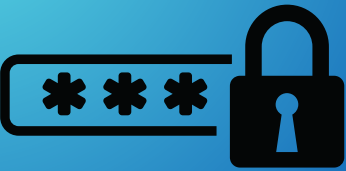


KORUNMA YOLLARI:

Kendinizi finansal ve yatırım manipölasyonlarından korumak, zor kazanılan paranızı korumak için çok önemlidir. İşte atabileceğiniz bazı basit adımlar.

E-postaya dikkat edin:

Büyük karlar veya acil finansal anlaşmalar vaat eden beklenmedik bir e-posta alırsanız, dikkatli olmanızda fayda var. Gönderenin e-posta adresini herhangi bir garip işaret açısından kontrol etmek için bir dakikanızı ayırın. Ve bir şey ters geliyorsa, hiçbir bağlantıya tıklamayın veya hiçbir eki indirmeyin.



şifrelerinizi güçlendirin:

Çevrimiçi hesaplarınız için parolalar ayarlarken güçlü ve benzersiz olduklarından emin olun. Harf, sayı ve sembollerin bir karışımını kullanın ve doğum gününüz veya evcil hayvanınızın adı gibi tahmin edilmesi kolay bilgiler kullanmaktan kaçının.

Finansal ve yatırım manipölasyonları

KORUNMA YOLLARI:

Şüpheli bağlantılara ve web sitelerine dikkat edin:

Şüpheli veya yabancı görünen bir web sitesiyle karşılaşırsanız, kişisel veya finansal bilgilerinizi paylaşmayın. Güvenli web siteleri için adres çubuğunda "https://" ve bir asma kilit sembolü arayın.



Çevrimiçi güvenlik hakkında bilgi sahibi olun:

Yaşlıları hedef alan yaygın dolandırıcılıklar hakkında bilgi edinmenize yardımcı olacak pek çok kaynak ve eğitim materyali mevcuttur.

Son olarak, yardım istemekten korkmayın:

Finansal bir karar konusunda emin değilseniz veya bir dolandırıcılığın hedefi olduğunuzu düşünüyorsanız, tavsiye ve destek için aile üyelerinize, arkadaşlarınıza veya güvendiğiniz profesyonellere ulaşın. Ve finansal manipölasyonun kurbanı olduğunuzu düşünüyorsanız, Federal Ticaret Komisyonu veya eyaletinizin tüketici koruma ajansı gibi ilgili makamlara hemen bildirin.



Görünür fedakarlık: yardım dolandırıcılığı

TEHLİKE ÖZELLİKLERİ:

İnternetteki yardım dolandırıcılıkları genellikle bireylerin cömertliğinden ve iyi niyetinden yararlanır, özellikle 65 yaş ve üzeri yaşlıları hedef alır. Bu dolandırıcılıklar, afet yardımı, tıbbi araştırma veya daha az şanslı olanlara yardım gibi sözde amaçlar için bağış toplayan, meşru kuruluşlar gibi görünen sahte yardım kuruluşlarını içerebilir.

Yardım Kuruluşu Dolandırıcılığında Manipülasyon Türleri:

Dolandırıcılar, kurbanları hızla bağış yapmaya zorlamak için ikna edici bir dil veya duygusal çağrılar kullanabilirler.

Dolandırıcılar, kurbanları aldatmak için tanınmış hayır kurumlarının markalarını taklit eden sahte web siteleri oluşturabilir veya e-postalar gönderebilir.

Dolandırıcılar, sempati uyandırmak ve bağışları teşvik etmek için yürek parçalayıcı hikayeler uydurabilir veya sahte referanslar sağlayabilir

Sahte yardım kuruluşları genellikle misyonları, hedefleri ve bağışlanan fonların nasıl kullanılacağı konusunda belirsiz veya yanıltıcı bilgiler sağlar.

Yüksek baskı taktikleri

Meşru yardım kuruluşlarının taklidi

Sahte hikayeler ve tanıklıklar

Şeffaflığın eksikliği

Görünür fedakarlık: yardım dolandırıcılığı



SONUÇLAR:

Yaşlılar için yardım kuruluşlarına yönelik dolandırıcılıkların kurbanı olmak hem maddi hem de manevi açıdan çok zor olabilir.

01

Mali kayıp

Yardım kuruluşu dolandırıcılığına kurban gitmek, zor kazanılan birikimlerin ve yatırımların kaybına yol açabilir. Beklenenden önemli ölçüde daha az parayla karşılaşabilirsiniz, bu da günlük masraflarınızı karşılama ve emekliliğinizin tadını çıkarma yeteneğinizi etkiler.

02

Duygusal sıkıntı

Yardım amaçlı dolandırıcılığa yönlendirilmek, kendinizi ihanete uğramış, suçlu ve bu dolandırıcılığın kurbanı olmaktan utanmış hissetmenize neden olabilir

03

Güven sorunları

Ayrıca gelecekte gerçek yardım kuruluşlarına güvenmek de zorlaşabilir, çünkü gerçek ve sahte yardım çağrıları arasındaki farkı anlamak zorlaşır.

Görünür fedakarlık: yardım dolandırıcılığı

— ARKA PLANDA TARİHLE KORUMA YOLLARI



Alice, ihtiyaç sahibi çocuklara yardım etmek için bağış talep eden bir yardım kuruluşundan olduğunu iddia eden bir e-posta alır. E-postada, yardım kuruluşunun çalışmalarından faydalandığı iddia edilen çocukların duygusal hikayeleri ve fotoğrafları yer alır. Ancak Alice, hayır kurumlarına bağış yapma vaadinde bulunan e-postalara karşı şüpheli olması gerektiği yönündeki tavsiyeyi hatırlıyor.



Alice'in hikayesi ne yazık ki tek vaka değil, ancak yaşlıları yardım dolandırıcılıklarından korumanın önemini gösteriyor. Yaşlılar karşılaşılabilecekleri çeşitli dolandırıcılık biçimlerinin farkında olmalı ve bunlardan kaçınmak için yöntemler bilmelidir.

ADIM 1: Yardım kuruluşunu araştırın

Alice bağış yapmadan önce yardım kuruluşunun kayıt durumunu kontrol eder ve saygın web sitelerinde incelemelerde bulunur

ADIM 2: İstenmeyen isteklere karşı dikkatli olun

Alice, bağış isteyen bu beklenmedik e-postayı sorguladı.

ADIM 3: Kişisel bilgilerinizi asla paylaşmayın

Alice, Sosyal Güvenlik numarası veya banka bilgileri gibi hassas bilgileri bilinmeyen veya doğrulanmamış hayır kurumlarına vermekten kaçındı.

ADIM 4: Doğrudan bağış yapın

Alice bağış yapmak isterse, e-postalardaki bağlantılara tıklamak veya telefon görüşmelerine yanıt vermek yerine, doğrudan yardım kuruluşunun resmi web sitesi üzerinden bağışta bulundu.

Görünür fedakarlık: yardım dolandırıcılığı



KORUNMA YOLLARI:

Kendinizi hayır kurumu dolandırıcılıklarından ve sonuçlarından korumak çok önemlidir. İşte kendinizi hayır kurumu dolandırıcılığının kurbanı olmaktan korumak için uygulayabileceğiniz bazı basit adımlar

Hayır kurumlarını araştırın ve meşru hayır kurumu web sitelerindeki durumlarını ve yorumlarını kontrol edin.



E-postalar, telefon görüşmeleri veya sosyal medya aracılığıyla gelen beklenmedik bağış taleplerine karşı dikkatli olun; çünkü gerçek hayır kurumları genellikle baskıcı taktikler kullanmazlar.

Sosyal Güvenlik numarası veya banka bilgileri gibi kişisel bilgilerinizi asla tanımadığınız hayır kurumlarıyla paylaşmayın.



Görünür fedakarlık: yardım dolandırıcılığı



KORUNMA YOLLARI:

Doğrudan yardım kuruluşunun resmi web sitesi üzerinden bağışta bulunun veya doğrulanmış adreslerine çek göndererek bağışta bulunun.



Yaygın yardım kuruluşu dolandırıcılıkları hakkında bilgi sahibi olun ve uyarı işaretlerini tanımayı öğrenin.

Yardım kuruluşu taleplerini değerlendirirken veya bir dolandırıcılıktan şüpheleniyorsanız, ailenizden, arkadaşlarınızdan veya mali danışmanlarınızdan yardım istemekten çekinmeyin.



Cazip illüzyonlar: hayali ödüller ve çekilişler

TEHLİKE ÖZELLİKLERİ:

Sahte ödüller, piyangolar ve çekilişlere dayalı dolandırıcılıklar aldatıcıdır ve insanları büyük ödüller kazandıklarına inandırarak kazanma arzularını kasıtlı olarak istismar eder. Dolandırıcılar kurbanlardan sahte kazançlar ödemelerini isterler ancak sonunda kurbanın cüzdanından para çalarlar.

Hayali ödüller ve çekilişlerde manipülasyon türleri:

Dolandırıcılar genellikle hükümetler (özellikle yabancı) tarafından yönetilen tanınmış şirketlerin veya piyangoların temsilcilerini taklit eder ve kurbanlarının güvenini suistimal etmek için manipülatif taktikler kullanırlar; böylece onların finansal güvenlik arzularından faydalanmayı umarlar.

Taklit etme

Dolandırıcılar, kurbanlara benzersiz ve ayrıcalıklı bir fırsat duygusu yaratmak için, kendilerinin tek veya nadir şanslı kazananlar olarak seçildiğine inandırmaya çalışırlar.

Ayrıcalıklılık

Dolandırıcılar, kurbanların hemen ve güvenle tepki vermesini sağlamak için baskı taktikleri kullanarak gerçek olamayacak kadar iyi ödül paraları, lüks ürünler vb. gibi gerçekçi olmayan miktarlarda vaatlerde bulunurlar.

Gerçekçi olmayan
vaatler

Cazip illüzyonlar: hayali ödüller ve çekilişler

— SONUÇLAR:

"Baştan çıkarıcı yanılsama" dolandırıcılıklarının sonuçları çeşitlidir ve genellikle uzun ömürlüdür.

01 Mali Sonuçlar

Bu tür dolandırıcılıkların en kötü sonuçlarından biri, kurbanlar için finansal yıkımdır ve çoğu kurban genellikle önemli finansal kayıplar yaşar. Kurbanlar hayat birikimlerini kaybedebilir, aşırı borçlanabilir veya hatta iflas edebilir. Bu tür finansal durumlardan kurtulmak yıllar alabilir.

02 Duygusal Sonuçlar

Dolandırıcılık mağdurları genellikle derin duygusal sıkıntı yaşar ve ihanet, ihlal, utanç ve suçluluk duygularıyla mücadele eder. Aldatma ve dolandırıcılığın neden olduğu duygusal çalkantı, kaygıya, depresyona ve hatta travma sonrası stres bozukluğuna (TSSB) yol açabilir ve ayrıca fiziksel sağlığı etkileyebilir.

03 Hukuki Sonuçlar

Mağdurların sahte "ödül çekleri" bozdurmaya ikna edildiği dolandırıcılık vakalarında, maddi kayıpların yanı sıra kara para aklama ve sahtecilik suçlamaları da dahil olmak üzere yasal sonuçlarla karşı karşıya kalabiliyorlar.

Cazip illüzyonlar: hayali ödüller ve çekilişler

— ARKA PLANDA TARİHLE KORUMA YOLLARI



Greta, yabancı bir piyangoda büyük ikramiyeyi kazandığını ve ödül parasını talep etmek için hemen bir ön 'yönetim ücreti' ödemesi gerektiğini bildiren beklenmedik bir kısa mesaj aldı. Mesajda ayrıca, ikramiyeyi kazandığına dair bilgileri ve ikramiyeyi alma prosedürlerini kimseyle paylaşmaması gerektiği de açıkça belirtildi.

Dolandırıcı için talihsizlik...

Greta yakın zamanda çevrimiçi dolandırıcılıklarla ilgili oturumların da yer aldığı bir siber güvenlik kursuna katıldı.



ADIM 1: Uyarı işaretlerini tanıma

Greta dolandırıcılığın belirtilerini hemen fark etti: Beklenmedik bir mesaj, (biletini almadığı) bir piyango ikramiyesi ve ön ödeme talebi.

ADIM 3: Katılımdan kaçınma

Greta, gelen kısa mesaja yanıt vermeyerek hem kişisel verilerini korumuş hem de maddi kayıptan kurtulmuş oldu.

ADIM 2: Diğer dolandırıcılık stratejilerini belirleme

Greta, piyango ikramiyesinin ayrıntılarını başkalarıyla paylaşmaması yönündeki talimatın kendisini izole etmek ve dolandırıcılığa düşmesini kolaylaştırmak için bir taktik olduğunu fark etti.

ADIM 4: Raporlama

Greta, dolandırıcılık girişimini hemen ailesine, arkadaşlarına ve ilgili yetkililere bildirdi ve sosyal medyada paylaştı.

Cazip illüzyonlar: hayali ödüller ve çekilişler



KORUNMA YOLLARI:

"Tempting Illusion" türünde bir dolandırıcılık girişimiyle karşılaşırsanız, hatırlamanız gereken ilk şey bedava para olmadığıdır ve şu meşhur sözü aklınızda tutun: "Bir şey gerçek olamayacak kadar iyi görünüyorsa, muhtemelen gerçek değildir." Kendinizi böyle bir durumda bulmanız durumunda kullanabileceğiniz bazı ek ipuçları şunlardır.

Sağduyunuzu kullanın:

E-posta, sosyal medya veya kısa mesaj yoluyla aldığınız beklenmedik ödül bildirimlerine karşı hızlı bir şekilde harekete geçme isteğine direnin!

Herhangi bir eylemde bulunmadan önce herhangi bir çekilişe veya piyangoya katılıp katılmadığınızı düşünün.



Meşruiyeti kontrol edin:

Diğer kanallar üzerinden web sitesini veya bildirim göndericisini kontrol edin.

Güvenilirliği kontrol etmek için internetten araştırma yapın veya ailenize veya arkadaşlarınıza danışın!

Bildirimlerdeki bağlantılara, özellikle şüpheliyse, tıklamayın veya dokunmayın!

Cazip illüzyonlar: hayali ödüller ve çekilişler

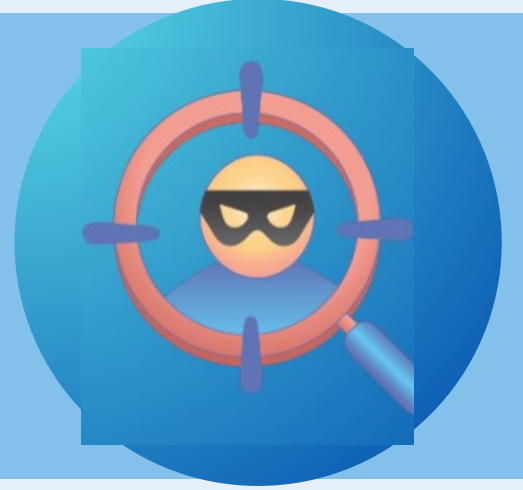


KORUNMA YOLLARI:

Detayları inceleyin:

Aldığınız bildirimdeki tüm bilgileri dikkatlice kontrol edin.

Kişisel bilgiler, finansal bilgiler veya peşin ödeme gibi belirsiz veya alışılmadık taleplere dikkat edin!



Hatırlamak:

Beklenmeyen bir ödül kazanma bildirimi üzerine ödül/parayı almak için asla para göndermeyin veya ücret ödemeyin!

Meşru çekilişlere katılmak veya ödül almak için herhangi bir ödeme yapmanız gerekmez ve çekilişlere katılmak için bir bilet satın almanız gerekir.



Cazip illüzyonlar: hayali ödüller ve çekilişler



KORUNMA YOLLARI:

Kişisel veya finansal bilgilerinizi bir dolandırıcıya ifşa ettiyseniz, e-posta hesabınızın ve diğer tüm hesaplarınızın şifrelerini derhal değiştirmelisiniz. Ayrıca, banka hesaplarındaki PIN kodlarını değiştirin ve çevrimiçi bankacılık kullanıyorsanız, çevrimiçi bankacılık şifrenizi değiştirmeyi unutmayın.

Büyük-küçük harf, rakam ve özel karakter kombinasyonundan oluşan güçlü şifreler kullanın!



Şüpheli bir bağlantıyı açtıysanız ve finansal veya kişisel bilgilerinizi paylaştıysanız veya bir kayıp yaşadıysanız, durumu derhal ülkenizdeki ilgili makamlara bildirin!

Dijital para dolandırıcılıkları

— TEHLİKE ÖZELLİKLERİ:

Kripto para dolandırıcılığı, Bitcoin gibi dijital para birimleriyle ilişkilendirilen her türlü dolandırıcılık faaliyetini ifade eder. Dolandırıcılık ilk coin teklifleri (ICO'lar), Ponzi şemaları ve dolandırıcı yatırım fırsatları dahil olmak üzere birçok form alabilir. Bu dolandırıcılıklar genellikle kurbanları cezbetmek için yüksek getiriler vaat eder ve dolandırıcılar parayla ortadan kaybolduğunda kurbanlar yatırımlarını kaybeder. Yaşlılar, dijital teknolojilere ve internete aşina olmadıkları için bu tür dolandırıcılıklara karşı özellikle savunmasızdır. Dolandırıcılar genellikle yaşlıların güvenini ve finansal güvenliğini istismar eder, bu nedenle farkındalığı artırmak ve onları bu tür dolandırıcılıklardan korumak için eğitim sağlamak önemlidir.

Kripto para dolandırıcılığının türleri:

Bu tür dolandırıcılık, yeni kripto paraların fon toplama aşamasında gerçekleşir. Geliştiriciler, genellikle ayrıntılı bir teknik doküman ve yüksek getiri vaatleriyle umut vadeden yeni bir dijital para sunar. Ne yazık ki, yatırımcılardan yeterli fon topladıklarında, bu geliştiriciler iz bırakmadan ortadan kaybolur ve yatırımcılara değersiz token'lar bırakır.

Bu planlar yüksek, düşük riskli getiriler vaat ediyor. Ancak getiriler karlardan değil, yeni yatırımcılardan gelen fonlar kullanılarak ödeniyor. Plan, yeterli sayıda yeni yatırımcı olmadığında çöküyor ve son yatırımcılar için önemli kayıplara neden oluyor.

Bu tür dolandırıcılık, kripto paraları güvenli bir şekilde sakladığını iddia eden uygulamaları veya yazılımları içerir. Bu cüzdanlar genellikle profesyonel görünümlü arayüzlere sahiptir ve hatta meşru cüzdanları taklit edebilir. Ancak, aslında dijital paraları çalmak için tasarlanmıştır. Bir kullanıcı kripto paralarını bu sahte cüzdanlara yatırdığında, dolandırıcılar bunlara erişim sağlar ve bu da genellikle kullanıcının dijital varlıklarının tamamen kaybolmasıyla sonuçlanır.

**Sahte İlk Para
Arzları
(ICO'lar)**

**Ponzi
Planları**

**Sahte Cüzdan
Dolandırıcılıkları**

Dijital para dolandırıcılıkları

— SONUÇLAR:

Finansal ve yatırım manipölasyonunun aşağıdaki gibi ciddi olumsuz etkileri olabilir:

01 Finansal Kayıp

Kripto para dolandırıcılığının en acil ve belirgin sonucu finansal kayıptır. Mağdurlar genellikle tüm yatırımlarını kaybederler, bu da özellikle birikimlerinin büyük bir kısmını yatırmışlarsa yıkıcı olabilir.

02 Güven Kaybı

Kripto para dolandırıcılığının kurbanları genellikle dijital para birimlerine olan güvenlerini kaybederler ve gelecekte dijital ekonomiye yatırım yapma veya katılma konusunda tereddüt edebilirler. Bu, kripto para birimlerinin büyümesini ve kabulünü engelleyebilir.

03 Hukuki Sonuçlar

Bazı durumlarda, dolandırıcılık planlarına katılanlar, bilmeden bile olsa, yasal sonuçlarla karşı karşıya kalabilir. Bu, düzenleyici otoriteler tarafından soruşturma ve bilmeden dolandırıcılığı kolaylaştırmaya yardımcı oldularsa olası suçlamalar içerebilir.

Dijital para dolandırıcılıkları

— ARKA PLANDA TARİHLE KORUMA YOLLARI



Bir gün Helen bir e-posta aldı. Önemli getiriler vaat eden yeni bir kripto para birimine yatırım yapma davetiydi. Meraklı ve dijital portföyünü büyütmek için istekliydi, araştırmaya karar verdi. E-posta "CryptoGold" adlı bir şirketten geliyordu ve web siteleri etkileyiciydi, memnun yatırımcıların referansları ve yüksek getiri vaatleriyle doluydu. Fırsat kaçırılmayacak kadar iyi görünüyordu, bu yüzden birikimlerinin küçük bir kısmını yatırmaya karar verdi. Günler haftalara dönüştü ve Helen, yatırımının artmasını umarak her gün hevesle çevrimiçi cüzdanını kontrol etti. Ancak, bunun yerine yatırımının azaldığını fark etti. Kafası karışmış ve endişeli bir şekilde "CryptoGold"a ulaşmaya çalıştı. Ancak, tüm e-postaları geri döndü ve bir zamanlar etkileyici olan web sitesi artık erişilemez durumdaydı.

Hellen'in hikayesi, farkındalık yaratarak ve eğitim vererek yaşlıları kripto para dolandırıcılıklarından koruma ihtiyacını vurguluyor. Yaşlılar dijital yabancılık nedeniyle savunmasız olabilir ve bu nedenle riskleri, dolandırıcılık belirtilerini ve yüksek getiri vaatlerine karşı şüphecilikğin önemini anlamaları gerekir. Destekleyici ağlar, güvenli dijital gezinme için de önemlidir.



ADIM 1: Şirketi araştırın

Hellen, yatırım yapmadan önce "CryptoGold"u iyice araştırmalıydı. Web sitesi ve referanslardan etkilenmek yerine, şirketin kayıtlı olup olmadığını kontrol etmeli ve diğer kullanıcıların yorumlarını veya uyarılarını aramalıydı.

ADIM 2: İletişimi doğrulayın

Hellen istenmeyen bir e-posta aldı ve doğrulama yapmadan güvendi. Dikkatli olmalı ve resmi şirket iletişim bilgileri veya bilinen kripto para forumları gibi güvenilir kaynaklarla çapraz kontrol yaparak gönderenin kimliğini doğrulamalıydı.

ADIM 3: Anlık kararlardan kaçın

Hellen, şartları ve riskleri tam olarak anlamak için zaman ayırmadan hızla yatırım yapmaya karar verdi. Aceleci yatırım kararları almaktan kaçınmalı ve bilgili kişilerden veya finansal danışmanlardan tavsiye almalıydı.

ADIM 4: Yatırımları düzenli olarak izleyin

Hellen herhangi bir dolandırıcılık belirtisi fark etmedi ve olumlu getiriler ummaya devam etti. Yatırımlarını düzenli olarak izlemeli ve daha fazla araştırma için olağandışı herhangi bir aktiviteyi veya şeffaflık eksikliğini derhal işaretlemeliydi.

Dijital para dolandırıcılıkları



KORUNMA YOLLARI:

Özellikle yaşlılar için kripto para dolandırıcılığından korunmak çok önemlidir, çünkü dijital teknolojilere aşina olmamaları nedeniyle özellikle savunmasız olabilirler. Dolandırıcılar genellikle yaşlıları yüksek getiri vaatleriyle hedef alır, güvenlerini ve finansal güvenliklerini suistimal eder. Bu dolandırıcılıkların kurbanı olmak önemli finansal kayıplara, dijital yeniliklere olan güvenin kaybolmasına ve olası yasal sonuçlara yol açabilir. Kendini eğitmek, kapsamlı araştırmalar yapmak ve gerçek olamayacak kadar iyi tekliflere karşı sağlıklı bir şüphecilik sürdürmek, kişinin varlıklarını korumak ve finansal refahını sağlamak için önemli adımlardır.

Eğitim:

Kripto paraların nasıl çalıştığını anlamak, dolandırıcılıktan kaçınmanın ilk adımıdır. Bu, arkasındaki teknolojiyi, işlemlerin nasıl çalıştığını ve dijital varlıklarınızı güvenli bir şekilde nasıl depolayıp koruyacağınızı anlamak anlamına gelir.



Araştırma:

Herhangi bir kripto paraya yatırım yapmadan önce, dijital para birimini, arkasındaki ekibi iyice araştırın ve mevcut tüm teknik belgeleri okuyun. Az riskle yüksek getiri vaat eden yeni kripto paralara karşı dikkatli olun.

Dijital para dolandırıcılıkları



KORUNMA YOLLARI:

Cüzdanınızı güvenceye alın:

Dijital varlıklarınızı güvenli bir cüzdan kullanarak koruyun. Bu, para birimini çevrimdışı olarak saklayan bir donanım cüzdanı veya güçlü güvenlik önlemlerine sahip saygın bir çevrimiçi cüzdan olabilir. Mümkünse her zaman iki faktörlü kimlik doğrulamayı etkinleştirin.



Şüpheli olun:

Çok az veya hiç risk olmadan yüksek getiri vaat eden her türlü yatırıma şüpheyile yaklaşın. Bunlar çoğu zaman gerçek olamayacak kadar iyidir. Meşru yatırımların genellikle getiriye garanti etmediğini ve her zaman bir miktar risk içerdiğini unutmayın.

Şüpheli aktiviteyi bildirin:

Potansiyel bir kripto para dolandırıcılığıyla karşılaşırsanız, bunu yerel yetkililere ve ilgili çevrimiçi platformlara bildirin. Bu yalnızca sizi korumakla kalmaz, aynı zamanda başkalarını uyarmaya ve korumaya da yardımcı olur.



Uluslararası finansal dolandırıcılık

— TEHLİKE ÖZELLİKLERİ:

419 dolandırıcılığı, Nijerya dolandırıcılığı olarak da bilinir, Nijerya'da ortaya çıkan, internetin ilk günlerinden beri var olan ve dünya çapında en yaygın dolandırıcılıklardan biri haline gelen kötü şöhretli bir ön ödeme dolandırıcılığıdır.

419 dolandırıcılığındaki manipölasyon türleri:

Konu satırında "Selamlar" kelimesi varsa, zengin bir Nijeryalı prens (hatta bir Nijeryalı astronot), zengin bir avukat veya iş adamı tarafından karşılanırsınız ve kendisine Nijerya'dan parasını transfer etmesi için (veya hesaba erişmesini sağlaması için) yüklü bir miktarda para teklif edilir; karşılığında iddia edilen işlem maliyetlerini karşılamak için küçük bir ön ödeme yapılır.

Konu satırında "Selamlar" kelimesi varsa, çocuklarının kaçırılması gibi zor bir yaşam durumuyla karşı karşıya olan bir kişi tarafından karşılanırsınız; veya siyasi durum nedeniyle kaçak veya masum bir mahkum haline gelen bir kişi vb. Ancak, hepsinin paralarını neden alamadıkları konusunda uzun ve üzücü bir hikayesi vardır, bu yüzden sizden yardım isterler.

Taklit etme
(varyasyon 1)

Taklit etme
(varyasyon 2)

Uluslararası finansal dolandırıcılık

Nijerya dolandırıcılıklarının arkasında, insan duygularını ve zaaflarını manipüle etmek için sistematik bir yaklaşım ve denenmiş ve test edilmiş teknikler kullanan profesyonel dolandırıcılar vardır. Nijerya dolandırıcılığında "senaryo" veya "format" olarak bilinen önceden hazırlanmış bir oyun planı kullanılır. Bu genellikle ayrıntılı hikayeler, sahte kimlikler ve meşru görünen ve dolandırıcıların kurbanlarla iletişimlerinde basitçe kopyalayıp kullandıkları sahte belgeler içerir.

Nijerya dolandırıcılığında iletişim yalnızca e-posta, kısa mesaj veya sosyal ağlar aracılığıyla gerçekleşir. Bu tür dolandırıcılıkta dolandırıcılar kurbanlarla video veya telefon aracılığıyla iletişim kurmaz. Alınan mesajlar dilbilgisi hataları ve kötü metin biçimlendirmesi içerir.

Mağdur artık para veya kişisel bilgi vermeyi bıraktığında veya dolandırıldığını anladığında, dolandırıcılar derhal yazışmalara yanıt vermeyi bırakır ve ortadan kaybolurlar.

**İnsan
duygularıyla
oynamak**

**Yazılı dijital
iletişimin
münhasıran
kullanımı**

Kaybolma

Uluslararası finansal dolandırıcılık



SONUÇLAR:

Bu dolandırıcılık her yaştan insanı, özellikle de hızlı zengin olma planlarına inananları veya finansal olarak saf olanları tehlikeye atabilir. Ancak, yaşlılar daha da savunmasızdır, çünkü genellikle başkalarına daha fazla güvenirler ve çevrimiçi güvenlik hakkında daha az şey bilirler.

01 Mali Sonuçlar

Mağdurlar büyük miktarda para kaybedebilir ve bu da ciddi finansal sorunlara yol açabilir. Mağdurlar olumlu yanıt verdiğinde, dolandırıcılar tarafından daha fazla para istenmesi tuzağına düşerler ve dolandırıcılar her türlü sahte bahaneyi uydurur veya ekstra ödemeler için teklifte bulunur. Bu durumda, Batık Maliyet Yanılgısı da ortaya çıkabilir; burada mağdurlar, vazgeçmek çok daha iyi bir fikir olsa bile, çoktan büyük yatırımlar yaptıkları bir şeyin (ister para, ister zaman, ister emek, ister duygusal enerji, vb. olsun) peşinden gitmeye devam ederler.

02 Duygusal Sonuçlar

Utanç veya mahcubiyet gizli davranışları teşvik ettiğinde, bu durum çoğu zaman mağdurların tekrar tekrar dolandırılmasına yol açabilir.

03 Sosyal Sonuçlar

Dolandırıldıktan sonra kişinin diğer insanlara olan güveni büyük ölçüde azalabilir, bu da yalnızlaşmaya ve ilişkileri sürdürme ve oluşturmada zorluklara yol açabilir.

Uluslararası finansal dolandırıcılık

— ARKA PLANDA TARİHLE KORUMA YOLLARI



Emma internette gezinirken "Selamlar" başlıklı bir e-posta aldı. E-postanın göndereni, Nijerya'dan büyük miktarda para transfer etmek için yardımına ihtiyaç duyan bir Nijeryalı "prens"ti. Karşılığında, işlemi kolaylaştırmak için küçük bir ücret karşılığında yardımı için fonların bir yüzdesini alacaktı.

Emma cazip teklife rağmen şüphelendi!

Dolandırıcı için talihsizlik...

Emma yakın zamanda 419 dolandırıcılığıyla ilgili internette bir makale okudu ve dolandırıcılığın tüm çeşitlerini öğrendi.



ADIM 1: İletişimdeki uyarı işaretlerini tanıma

Emma, e-postanın içeriğinin çok kötü bir İngilizceyle yazıldığını ve hiçbir anlam ifade etmediğini fark etti.

ADIM 3: Kararlı bir eylemde bulunmak

Emma e-postayı hemen spam olarak işaretledi ve sildi. "İddiaya göre" Nijeryalı prenstan gelen diğer takip e-postalarında da aynısını yaptı.

ADIM 2: Bilgiyi kullanma

Emma ayrıca 419 dolandırıcılığıyla ilgili çevrimiçi bir makale okurken Nijerya'da kraliyet ailesinin olmadığını öğrendi.

ADIM 4: Bilgili ve dikkatli bireylerden oluşan bir topluluk oluşturmak

Emma, yaşadıklarını eşi, ailesi ve arkadaşlarıyla paylaştı ve sosyal medyada paylaştı.

Uluslararası finansal dolandırıcılık



KORUNMA YOLLARI:

Eğer 419 tipi bir dolandırıcılık girişimiyle karşılaşırsanız, aklınızda bulundurmanız gereken ilk şey, hiç kimsenin gelen kutusunda beklenmedik bir mesaj yüzünden büyük miktarda para kazanmadığıdır!

Böyle bir durumla karşılaşmanız durumunda uygulayabileceğiniz bazı ek ipuçları:

Eğer 419 dolandırıcılığı teklifi alırsanız ve bunu kabul etmeye karar vererseniz, durun ve kendinize şu iki basit, sağduyulu soruyu sorun:

Neden kişisel ve finansal bilgilerinizi tamamen yabancı biriyle (hiçbir bağlantınızın olmadığı bir ülkeden gelen biriyle) paylaşırsınız ve bu yabancı neden servetinizi paylaşmak için sizi seçer?



“Çocuk kaçırma” hikayesi sizi derinden etkilese bile, sizden maddi yardım isteyen kişinin gerçekliğini kontrol etmeden asla para (veya başka finansal bilgi) göndermeyin!

Ayrıca 419 dolandırıcılıklarının sizi havale hizmetleriyle ödeme yapmaya ikna ettiğini unutmayın! (genellikle Western Union)

Uluslararası finansal dolandırıcılık



KORUNMA YOLLARI:

İçeriğin gerçekliğini inceleyin:

419 dolandırıcıları tekrar tekrar komut dosyaları kullandığından, bir e-postanın gerçekliğini, içeriğin kısa bir bölümünü bir arama motoruna (Google, Bing, vb.) ekleyerek kontrol edebilirsiniz. İçerik bilinen veya ortaya çıkarılmamış dolandırıcılık mesajlarının bir parçasıysa, diğer kurbanlar tarafından daha önce bildirilmiş olan bu dolandırıcılık konusunda uyarıda bulunan web siteleri bulacaksınız.



Dolandırıcılık e-postalarına cevap vermeyin
(şaka bile değil)!

Hemen silin!

Unutmayın, eğer cevap verirsiniz - büyük ihtimalle finansal bir tuzağa yakalanmış olacaksınız!

Uluslararası finansal dolandırıcılık



KORUNMA YOLLARI:

Finansal bilgilerinizi bir dolandırıcıya verdiyseniz, PIN kodunuzu ve giriş şifrenizi değiştirin (eğer internet bankacılığı kullanıyorsanız).

Finansal işlemlerinizi iki faktörlü kimlik doğrulama (2FA) ve işlem uyarısı işlevi gibi ek güvenlik önlemleri alın ve hesap bakiyenizi düzenli olarak takip edin.



REPORT

Maddi bir kayba uğradıysanız, bunu derhal bankanıza ve ülkenizdeki diğer yetkili makamlara bildirin!

Daha fazla okuma



FİNANSAL VE YATIRIM MANİPÜLASYONLARI

- <https://faircanada.ca/investing-basics/protecting-vulnerable-investors-from-financial-abuse/>
- <https://ekonomiktimes.indiatimes.com/wealth/legal/will/how-can-senior-citizens-protect-themselves-from-financial-exploitations-by-their-own-families/articleshow/103877992.cms?from= bay>
- <https://www.morganstanley.com/articles/elder-financial-abuse-protecting-loved-ones>
- <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6044329/>
- <https://www.psychiatrist.com/pcc/financial-abuse-older-adults-screening-prevention-interventions-primary-care-providers/>
- <https://www.youtube.com/watch?v=7G8lil8Yupg>
- <https://www.c-span.org/video/?324176-1/financial-exploitation-senior-citizens>



GÖRÜNÜR FEDAKARLIK: YARDIM DOLANDIRICILIĞI

- <https://www.bbc.com/news/uk-34530586>
- <https://www.youtube.com/watch?app=desktop&v=MTm-fq00UQQ>
- https://www.americansenioralliance.com/episode_5
- <https://www.youtube.com/watch?v=vR53sRLVgpc>
- <https://www.theguardian.com/society/2015/sep/01/charities-face-scrutiny-over-trading-of-elderly-mans-data>

Daha fazla okuma



CAZİP İLLÜZYONLAR: HAYALİ ÖDÜLLER VE ÇEKİLİŞLER

- <https://www.identityguard.com/news/lottery-scams>
- <https://www.pcrisk.com/> [https://www.naperville.il.us/services/naperville-police-department/community-education-and-crime-prevention/frauds-and-scams /](https://www.naperville.il.us/services/naperville-police-department/community-education-and-crime-prevention/frauds-and-scams/)
- <https://www.scamwatch.gov.au/system/files/Little%20Black%20Book%20of%20Scams%20-%20Final.pdf>
- <https://www.gamblingcommission.gov.uk/public-and-players/guide/lottery-scams-and-fraud>
- <https://www.identityguard.com/news/online-safety-tips-for-seniors>
- <https://www.liveabout.com/warning-signs-of-sweepstakes-scams-886996>
- <https://surfshark.com/research/data-breach-impact/crime-lottery-inheritance-scam>
<https://www.aura.com/learn/sweepstakes-scams>



DİJİTAL PARA DOLANDIRICILIKLARI

- <https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams> [https://www.coindesk.com/learn/crypto-scams-types-of-crypto-schemes-and -dolandırılmaktan-nasıl-kaçınılır](https://www.coindesk.com/learn/crypto-scams-types-of-crypto-schemes-and-dolandirilmaktan-nasil-kaçınılır)
- <https://www.fastex.com/en/learn/crypto-scams-explained>
- <https://cointelegraph.com/explained/impersonation-scams-in-crypto-explained>
[https://www.ftc.gov/news-events/news/press-releases/2022/06/new-analytic-finds-consumers -1 milyardan fazla-kripto para birimi-dolandırıcılığının-kaybedildiği-bildirildi-2021](https://www.ftc.gov/news-events/news/press-releases/2022/06/new-analytic-finds-consumers-1-milyardan-fazla-kripto-para-birimi-dolandiriciliginin-kaybedildiği-bildirildi-2021)
- <https://www.mdpi.com/2227-9091/11/3/51>
- <https://www.cybertrace.com.au/cryptocurrency-fraud-explained>
- <https://www.arkoselabs.com/guide-to-cryptocurrency-security>
- <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-new-analiz-reveals-consumers-lost-nearly-500-million-cryptocurrency-scams>
- <https://www.kaspersky.com/resource-center/threats/top-seven-tips-for-preventing-cryptocurrency-scams>

Daha fazla okuma



ULUSLARARASI FİNANSAL DOLANDIRICILIK

- <https://www.altospam.com/en/glossary/scam-nigerian419/>
- <https://www.comparitech.com/identity-theft-protection/nigerian-scam/>
- <https://www.comparitech.com/identity-theft-protection/nigerian-scam/>
- <https://www.britannica.com/topic/cybercrime/Identity-theft-and-invasion-of-privacy#ref829190>
- <https://www.wallstreetmojo.com/nigerian-scam/#nigerian-letter-scam-explained>
- <https://whatismyipaddress.com/nigerian-fraud-combines-scams>
- <https://hackernoon.com/the-nigerian-prince-email-and-the-history-of-social-engineering-techniques>
- <https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html>

BÖLÜM 3.

SOSYAL MANİPÜLASYON VE DUYGUSAL ALDATMA

Modern dolandırıcılıklar giderek daha fazla sosyal ve duygusal manipölasyon biçimini alıyor ve yaşlıları bu tehditlere karşı özellikle savunmasız hale getiriyor. Suçlular hedeflerine ulaşmak için duyguları, güveni ve saflığı istismar ediyor ve sıklıkla kurbanlarının finansal ve duygusal refahını mahvediyor. Bu bölüm, duygusal ve sosyal manipölasyona dayalı en yaygın dolandırıcılıkları ele almayı ve yaşlıların bu tehlikeleri fark etmelerine ve kendilerini korumalarına yardımcı olmayı amaçlıyor.

En tehlikelileri arasında suçluların para koparmak için ilişki kurduğu romantik dolandırıcılıklar yer alır. Smishing ve telefon dolandırıcılıkları da ciddi tehditler oluşturur çünkü dolandırıcılar kişisel bilgileri veya fonları elde etmek için güvenilir kişileri veya kurumları taklit eder.

Dolandırıcıların aile üyeleri gibi davrandığı büyükanne ve büyükbaba dolandırıcılıkları ve tıbbi ürünlerle ilgili dolandırıcılıklar da ek manipölasyon yöntemleridir. Bu tehditleri anlamak, yaşlıların maddi ve manevi refahını korumak açısından hayati önem taşımaktadır.

Erkek-kadın ilişkilerinde dolandırıcılık



TEHLİKE ÖZELLİKLERİ:

Çevrimiçi flört dolandırıcılığı, bir diğer adıyla romantik dolandırıcılık, bir kurbanın çevrimiçi tanıştığı biriyle romantik bir ilişki içinde olduğuna inandırılmasıyla gerçekleşir. Ancak, sözde partneri bir dolandırıcıdır.

Çevrimiçi bir aşkta manipülasyon türleri:

Dolandırıcılar, sahte çevrimiçi profiller oluşturur ve kendilerini kurbandan uzakta, çoğunlukla yurtdışında, görevli (doktor, asker, hayırsever) olarak, bir petrol platformunda çalışan vb. olarak tanıtır.

Dolandırıcının ilgi alanları ve hobileri kurbanlarıinkiyle neredeyse birebir aynı... ve fotoğraflar sadece... VAY! Birkaç "mükemmel fotoğraf" dışında, onun hayatındaki çeşitli durumlarda çekilmiş pek fazla (veya hiç) fotoğrafı yok.

Her şey güllük gülistanlık gibi görünmeye başladığında (aşk ilanı, evlenme teklifi, vb.), dolandırıcı kurbanları özel olarak iletişime geçmeye davet eder (böylece telefon numaralarını, e-posta adreslerini ve diğer bilgileri elde eder) ve onları en kısa sürede şahsen görmeyi vaat eder.

Ve her şey daha da güllük gülistanlıkken, empati uyandıran bir hikâye eşliğinde para talebi gelir ve belirli ödeme yöntemleri (havale, mağdurun adına yeni açılan bir banka hesabı, vb.) talep edilir.

Sahte kimlik

Mükemmellik

Hızlı ilerleme

İstek için...
PARA

Erkek-kadın ilişkilerinde dolandırıcılık



SONUÇLAR:

Romantik dolandırıcılıklar, mağdurlarda ciddi maddi kayıplara ve duygusal sıkıntılara yol açabilir.

01

Mali Sonuçlar

Kurbanlar genellikle ihtiyaç sahibi bir sevdiklerine yardım ettiklerine inandıkları için paralarını kullanmaya ve ilişkiye yatırmaya isteklidirler. Bazı kurbanlar "aşk" uğruna tüm birikimlerini feda eder, ek krediler alır veya hatta varlıklarını satarlar. Dolandırıcıların kurbanlardan elde ettiği veriler (banka hesabı, kredi kartı bilgileri) yetkisiz işlemler veya çekimler yapmak için kullanılabilir ve bu da önemli mali kayıplara yol açabilir.

02

Duygusal Sonuçlar

Çevrimiçi flört dolandırıcılığı, insanların duygularıyla oynadığı için özellikle acımasızdır. Çevrimiçi bir ilişkinin bir dolandırıcılık olduğu gerçeğinin ortaya çıkması, kurbanda fiziksel etkileşime dayalı bir ilişkinin aniden sona ermesiyle benzer duygusal hasara neden olur. Bu, kurbanların dolandırıcıya karşı hissettikleri sevgiyi, dolandırıldıklarını anladıklarında bile, kırmalarını zorlaştırır.

03

Hukuki Sonuçlar

Romantik dolandırıcılık mağdurları utanç, mahcubiyet, stres, kaygı, depresyon ve korku gibi psikolojik acılara eğilimlidir. Mağdurlar majör depresif bozukluk, keder veya travma sonrası stres bozukluğuna (PTSD) benzeyen semptomlar yaşayabilir.

Erkek-kadın ilişkilerinde dolandırıcılık



ARKA PLANDA TARİHLE KORUMA YOLLARI



Kocasının ölümünden iki yıl sonra, Margot'un torunları onu bir çevrimiçi flört sitesine kaydolmaya ikna ettiler. Kısa süre sonra, Afrika'da insani bir görevde olan doktor Tom adında bir adamla sohbet etmeye başladı.

Birkaç haftalık içten sohbetlerin ardından Tom, 'Nakit akışı sorunları' yaşadığını ve masrafları karşılamak için paraya ihtiyacı olduğunu iddia etti. Margot şüphelendi ve alışılmadık isteği torunlarıyla tartıştı. Birlikte, profilini araştırdılar ve Tom'un bir dolandırıcı olduğunu keşfettiler.

Dolandırıcı için talihsizlik...

Margot, dolandırıcılık şüphelerini sevdikleriyle açıkça konuştuğunda doğru kararı verdi.



ADIM 1: Sezgileri takip edin

Margot bir şeylerin ters gittiğini hissetti. İçgüdülerine güvendi ve ona yardım etmek için acele etmedi, ama önce isteğinin tuhaflığını düşündü.

ADIM 2: Güvenilir kişilerden tavsiye almak

Margot, kararı kendisi vermek yerine torunlarına danıştı. Tom'un isteğinin ayrıntılarını onlarla paylaştı ve onların tavsiyesini istedi.

ADIM 3: Araştırma

Birlikte Tom'un profilini araştırdılar ve onun bir dolandırıcı olduğunu öğrendiler. Bu farkındalık, Margot'un ona para göndermesini ve dolandırıcılığın kurbanı olmasını engelledi.

ADIM 4: Raporlama

Margot, tanışma sitesine durumu bildirdi, site yöneticisiyle iletişime geçti ve Tom'u dolandırıcılık şüphesiyle ihbar etti.

Erkek-kadın ilişkilerinde dolandırıcılık



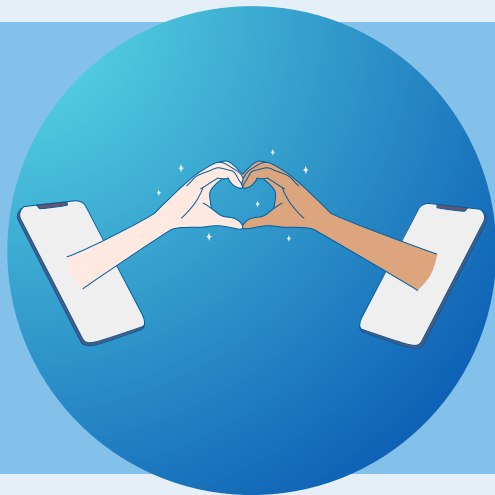
KORUNMA YOLLARI:

Romantik dolandırıcılar, özellikle yakın zamanda dul kalmış veya boşanmış yaşlıların yalnızlığından yararlanarak, onların savunmasızlığından ve maddi kaynaklarından faydalanarak sosyal medya platformları, tanışma siteleri vb. yerlerde sahte çevrimiçi romantik ilişkiler geliştiriyorlar.

Böyle bir durumla karşılaşmanız durumunda uygulayabileceğiniz bazı ek ipuçları:

Çevrimiçi paylaşımlarınıza dikkat edin:

Kamuoyuna açık bir şekilde paylaştığınız bilgiler (ilgi alanlarınız, hobileriniz, yaşam tarzınız vb.) dolandırıcılar tarafından romantik ilginizi çekmek için sahte bir kimlik oluşturmak amacıyla kullanılabilir.



Herhangi bir çevrimiçi ilişkide kişisel/finansal bilgilerinizi kendinize saklayın:

Potansiyel bir çevrimiçi romantik partnerle çok fazla kişisel bilgi paylaşmayın ve kesinlikle finansal bilgilerinizi ifşa etmeyin.

Ama en önemlisi - Hiç tanımadığınız insanlara para göndermeyin veya değerli eşya satın almayın!

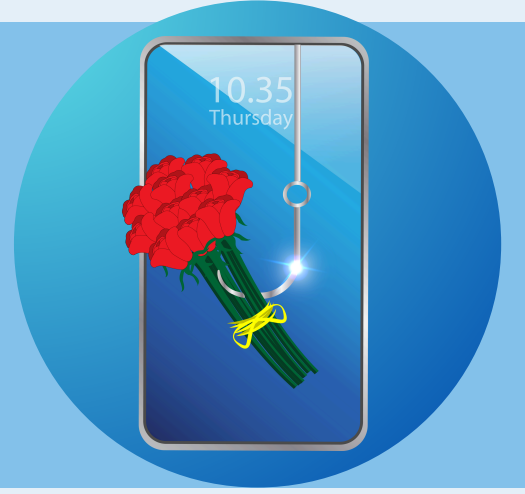
Erkek-kadın ilişkisinde dolandırıcılık



KORUNMA YOLLARI:

Doğrulamak:

Romantik bir çevrimiçi partnerin size söylediği her şeyi doğrulayamasanız da, adını, soyadını, ikamet yerini, sosyal medya profillerini, gönderilen ve paylaşılan fotoğrafların gerçekliğini doğrulamak ve iletişimlerinde tekrarlanan geçmiş hikayeleri veya ifadeleri kullanıp kullanmadıklarını kontrol etmek için internet'i kullanarak belirli somut ayrıntıları kontrol edebilirsiniz. Çünkü dolandırıcılar genellikle aynı geçmiş hikayeleri ve replikleri tekrar tekrar kullanırlar.



Hatırlamak!

Eğer romantik çevrimiçi partneriniz sizinle yüz yüze görüşmeyi reddediyorsa, neden görüşemeyeceğine dair bahaneler uyduruyorsa veya hiçbir zaman görüntülü görüşmeye veya diğer canlı "etkileşimlere" katılmıyorsa, bir dolandırıcıyla işbirliği yapmış olabilirsiniz.

Erkek-kadın ilişkisinde dolandırıcılık

KORUNMA YOLLARI:

Hesaplarınıza ait ŞİFREleri paylaştıysanız ve şüpheli bir etkinlik tespit ettiyseniz, herhangi bir ayarın değiştirilip değiştirilmediğini hemen kontrol edin ve hesaplarınızdaki son oturum açmaları ve etkinlikleri kontrol edin. Bilinmeyen veya şüpheli oturum açmalar fark ederseniz, servis sağlayıcınızı ve kişilerinizi bilgilendirin ve sizden geliyormuş gibi görünen şüpheli mesajlara karşı dikkatli olmaları konusunda uyarın.

En iyi tavsiye, erişim verdiğiniz tüm şifreleri değiştirmenizdir!



REPORT

Çevrimiçi ilişkinizin bir dolandırıcılık olduğundan şüpheleniyorsanız, derhal iletişimi kesin ve dolandırıcıyı sosyal medyada, e-postada, mesajlaşma uygulamalarında, flört sitelerinde vb. engelleyin.

Banka veya kredi hesaplarınız kullanıldıysa bankanızı veya polisi arayın!

Haberi yay!

Smishing SMS dolandırıcılığı



TEHLİKE ÖZELLİKLERİ:

Smishing, "SMS" (kısa mesaj servisi) ve "phishing" kelimelerinin birleşimidir. Bu saldırılarda, siber suçlular hileli kısa mesajlar gönderir ve kurbanları kandırmaya veya manipüle etmeye çalışarak kişisel veya finansal bilgilerini ifşa etmelerini, kötü amaçlı bağlantılara tıklamalarını veya zararlı yazılım veya uygulamaları indirmelerini sağlamaya çalışırlar.

Smishing'de manipülasyon türleri:

Dolandırıcılar, yasal kurumları, işletmeleri veya diğer kuruluşları kısa mesajlar aracılığıyla taklit ederek kurbanları kandırır. Bu mesajlar, kurbanları mesajdaki bir bağlantıya tıklamak, kişisel bilgilerle yanıt vermek veya belirli bir numarayı aramak gibi hemen harekete geçmeye yönlendirir.

Mağdurlar için önemli olabilecek bir durumu kullanmak (bankadan gelen bir mesaj, kredi kartı hizmetleri, müşteri desteği, vb.) dolandırıcıların etkili bir kılık değiştirmesine olanak tanır ve bunun spam olabileceğine dair herhangi bir şüpheyi ortadan kaldırmalarına yardımcı olur.

Bir kurbanın duygularını yoğunlaştırarak mesaj kişiselleştirilmiş hissettirir ve aciliyet, korku veya merak gibi belirli bir duygu tepkisini tetikler. Bu taktikleri kullanarak dolandırıcılar, kurbanları hemen harekete geçmeye teşvik etmek için tasarlanmış mesajlar oluştururlar.

Taklit etme

Mümkün ve makul bağlam

Duygularla oynamak

Smishing-SMS dolandırıcılıkları



SONUÇLAR:

Modern teknolojiler ve siber güvenlik bilgileriyle sınırlı deneyimleri nedeniyle, yaşlılar genellikle sahte eylem çağrıları veya şüpheli bağlantılar gibi smishing mesajlarındaki tehlike işaretlerini tanımakta zorluk çekerler. Daha az şüpheli olma eğilimindedirler ve aldatıcı smishing mesajlarına inanma olasılıkları daha yüksektir.

01 Mali Sonuçlar

Mağdurlar kredi kartı numaraları veya banka hesap numaraları gibi kişisel veya finansal bilgilerini ifşa ederse, dolandırıcılar bu bilgileri yetkisiz işlemler yapmak veya mağdurun hesabından para çekmek için kullandığından finansal olarak daha fazla zarar görebilirler. Bu sonuçlar ciddi finansal sorunlara ve uzun vadeli hasara neden olabilir.

02 Kimlik Hırsızlığı

Kimlik hırsızlığı durumunda, kişisel verileriniz kötüye kullanılır ve bu da kişisel güvenliğinizi ve gizliliğinizi etkiler. Yasadışı faaliyetlerle ilişkilendirilirse, yasal sonuçlarla da karşılaşabilirsiniz. Kimliğinizi geri almak, birçok idari (ve yasal) prosedürü içerdiğinden çok zaman alıcı olabilir.

03 Psikolojik Sonuçlar

Smishing mesajları genellikle korku, panik veya kafa karışıklığı gibi duyguları istismar ederek mağdurların psikolojik iyilik hallerini etkileyebilir.

Smishing SMS dolandırıcılığı



ARKA PLANDA TARİHLE KORUMA YOLLARI



Peter, bankasından akıllı telefonuna hesabının geçici olarak bloke edildiğini bildiren bir kısa mesaj aldı. Mesajda, hesabını etkinleştirmek için HEMEN bir bağlantıya dokunması gerektiği yönünde alışılmadık bir istek vardı. Peter bir an paniğe kapıldıysa da mesajı çok şüpheli bulduğu için bağlantıya tıklamamaya karar verdi.

Dolandırıcı için talihsizlik...

Peter yakın zamanda smishing hakkında çevrimiçi bir eğitim videosu izledi ve bu dolandırıcılık türünün özelliklerini öğrendi.



ADIM 1: Uyarı işaretlerini tanıma

Peter ayrıca mesajda yazım hataları veya garip ifade edilmiş cümleler fark etti; bu da mesajın doğrulanmadığını gösteriyordu.

ADIM 3: Bilgilerin doğrulanması

Peter bağlantıya tıklamak yerine telefon rehberindeki telefon numarasını kullanarak bankayı aradı ve mesajın gerçek olup olmadığını bankayla kontrol etti.

ADIM 2: Kişisel temas eksikliğini fark etmek

Peter ayrıca mesajın anonim olduğunu ve bankanın bilgilerini veya müşterinin daha fazla bilgi için ulaşabileceği bir irtibat kişisini içermediğini fark etti.

ADIM 4: Bilgilendirme/raporlama

Peter'ın bankaya bilgi vermesinin ardından dolandırıcılık girişimi doğrulandı. Banka da tüm müşterilerine bilgi vererek dolandırıcılık girişimini ilgili makamlara bildirdi.

Smishing SMS dolandırıcılığı



KORUNMA YOLLARI:

Kendinizi bu saldırıların potansiyel sonuçlarından korumak kolaydır - sadece onları görmezden gelin. Elbette, tüm mesajları görmezden gelmemelisiniz, çünkü kısa mesajlar birçok perakendeci ve diğer kurumlar için size ulaşmak için meşru bir araçtır.

Böyle bir durumla karşılaşmanız durumunda uygulayabileceğiniz bazı ek ipuçları:

Cevap vermeyin:

Beklenmeyen veya şüpheli bir mesaj alırsanız, hatta "DUR" yazarak aboneliğinizi iptal etmeniz isteniyorsa, bu aktif telefon numaralarını tespit etmek ve dolandırıcılığa yol açmak için kullanılan bir taktik olabilir.



• Örnek 3



Panik yapma:

Acil bir mesaj gibi görünüyorsa, zaman ayırın ve yavaşlayın.

ACİL hesap güncellemelerini veya ACİL sınırlı süreli teklifleri smishing'in potansiyel göstergeleri olarak değerlendirin.

Dikkatli olun!

Smishing SMS dolandırıcılığı

KORUNMA YOLLARI:

Mesajda verilen bağlantıları veya iletişim bilgilerini kullanmayın!

Metinde yer alan bilgiler veya detaylar üzerinden değil, doğrudan resmi iletişim kanalları aracılığıyla doğrulayın, kontrol edin ve iletişime geçin.

Unutmayın!

Meşru kurumlar (örneğin bankalar, devlet daireleri, vb.) asla SMS veya sertifikasız bağlantılar yoluyla hassas verilerinizi talep etmez.



Bir smishing saldırısı girişiminden şüpheleniyorsanız, tüm hesap şifrelerinizi ve PIN kodlarınızı derhal değiştirin.

Ayrıca, alışılmadık oturum açma konumlarına veya şüpheli etkinliklere karşı finanslarınızı ve çevrimiçi hesaplarınızı izleyin.

Smishing kurbanı olduysanız, size hemen yardımcı olabilecek ilgili kurumlarla iletişime geçin. Finansal bir saldırı durumunda, hesabınızı dondurmak veya kredi kartlarınızı iptal etmek için bankanızla iletişime geçin.



Yaşlıları ilgilendiren telefon dolandırıcılıkları



TEHLİKE ÖZELLİKLERİ:

Telefon dolandırıcılıkları, vishing olarak da bilinir, özellikle yaşlılara karşı etkilidir. Tipik taktikler arasında bilinmeyen veya yabancı numaralardan gelen beklenmedik aramalar, sahte numaralar veya Viber ve WhatsApp gibi platformlar bulunur. Vishing aramaları gerçek bir kişiden veya önceden kaydedilmiş bir robot aramadan gelebilir. Dolandırıcılar, kimlik bilgileri, banka hesap numaraları, oturum açma bilgileri ve parolalar gibi gizli kişisel verileri çalmak için ses taktikleri kullanır.

Vishing'de manipülasyon türleri:

Dolandırıcılar genellikle meşru görünmek ve finansal ve kişisel bilgiler elde etmek için banka, devlet kurumu, sigorta veya diğer tanınmış şirketlerin çalışanlarını taklit ederler. Aciliyet duygusu yaratmak için psikolojik taktikler kullanırlar ve kurbanları başlarının dertte olduğuna ikna ederler. Tehdit edebilir ve onları korkutmaya çalışabilirler.

Dolandırıcılar ayrıca kurbanı kendi taraflarında olduklarına ikna etmek için ikna edici bir dil ve ton kullanabilirler. Bu yüzden sıklıkla sohbeti dostça, ulaşılabilir, şefkatli bir şekilde yönlendirirler ve yardımsever görünürler ve sıklıkla muğlak bir dil kullanırlar veya sohbet sırasında kurbanın dikkatini dağıtmak için konuyu değiştirirler.

Dolandırıcılar, aynı numaradan tekrar aramalar da dahil olmak üzere ısrarcılıkla karakterize edilir (hatta kurbanla günde birkaç kez iletişime geçebilirler vb.). Kendi yolunda, yavaş ve istikrarlı bir şekilde, kurbanın güvenini kazanır. Bu taktik, kurbanın güvenini kazanmak ve onları hassas bilgileri ifşa etmeye ikna etmek için kullanılır.

Taklit etme

İnandırıcılık

Azım

Yaşlıları ilgilendiren telefon dolandırıcılıkları



SONUÇLAR:

Yaşlılar genellikle telefon görüşmelerini iletişim kurmanın önemli bir yolu olarak görür ve bir telefon görüşmesinin sağladığı kişisel etkileşime değer verir. Telefon üzerinden kişisel iletişime duyulan bu yüksek güven seviyesi, onları farklı türdeki telefon dolandırıcılıklarına karşı daha savunmasız hale getirir ve dolandırıcılar tarafından yapılan yanıltıcı bilgi taleplerine veya eylemlere daha kolay inanmalarını sağlar.

01 Mali Sonuçlar

Telefon dolandırıcılığı mağdurları genellikle doğrudan finansal kayıplar yaşarlar. Dolandırıcılar, mağdurları ödeme yapmaya veya bankacılık bilgileri vermeye kandırabilir ve bu da yetkisiz işlemlere veya banka hesaplarının boşaltılmasına yol açabilir. Bu, tasarruflarını ve finansal güvenliklerini önemli ölçüde etkileyebilir.

02 Kimlik Hırsızlığı

Telefon dolandırıcılıkları genellikle sosyal güvenlik numaraları, doğum tarihleri ve adresler gibi kişisel bilgilerin çalınmasını içerir. Mağdurlar bu sorunları çözmede ve kimliklerini kurtarmada önemli zorluklarla karşılaşabilirler.

03 İtibar Hasarı

Dolandırıcılığın yetkisiz finansal faaliyetler veya işlemlerden kaynaklandığı durumlarda, mağdurun finansal itibarı da zarar görebilir. İtibarları yeniden inşa etmek zor olabilir ve kapsamlı dokümantasyon ve finansal kuruluşlarla iletişim gerektirir.

Yaşlıları ilgilendiren telefon dolandırıcılıkları



ARKA PLANDA TARİHLE KORUMA YOLLARI



Andrew, sağlık sigortası şirketinden olduğunu iddia eden ve tıbbi kayıtlarını güncellemek için daha fazla bilgiye ihtiyaç duyduğunu söyleyen bir kişiden telefon aldı. Arayan kişi çok arkadaş canlısıydı ancak kendisini adı ve soyadıyla tanıtmadı. Sadece sigorta şirketi adına aradığını ve bunun rutin bir kontrol olduğunu söyledi.

Andrew, sigorta numarası ve doğum tarihi gibi kişisel bilgileri sormaya başlayınca şüphelenmeye başladı.

Dolandırıcı için talihsizlik...

Andrew, güvenlik konularının tartışıldığı ve dolandırıcılık deneyimlerinin paylaşıldığı çevrimiçi forumlarda ve topluluklarda aktif olarak yer almaktadır.



ADIM 1: Arayanın kimliğinin doğrulanması

Andrew, sigorta şirketinin resmi internet sitesinde arayanın kimliğini doğrulayamadı çünkü sigorta şirketinin iddia edilen çalışanı tam adını vermemişti - bu yüzden Andrew şüphelendi.

ADIM 3: Önceki bilgileri kullanma

Andrew, güvenlik konularının tartışıldığı çevrimiçi forumlara aktif olarak katılarak aldatma belirtilerini fark etti ve bu sayede aramanın şüpheli unsurlarını hızla tespit edebildi.

ADIM 2: Şüpheli isteklere karşı dikkatli olun

Arayan kişi sigorta numarası ve doğum tarihi gibi kişisel bilgileri istemeye başlayınca Andrew aramanın gerçekliğini sorguladı ve hemen aramayı sonlandırdı.

ADIM 4: Bilgilendirme/raporlama

Andrew, sağlık sigorta şirketini doğrudan arayarak aramanın bir dolandırıcılık girişimi olup olmadığını kontrol etti ve aktif olduğu forumlarda ve topluluklarda bu konuda bilgi yaymaya çalıştı.

Yaşlıları ilgilendiren telefon dolandırıcılıkları



KORUNMA YOLLARI:

Telekomünikasyon teknolojisinin hızla ilerlemesi nedeniyle dolandırıcılar, dolandırıcılık faaliyetleri yürütmek için anonimlikten ve telefon görüşmelerine kolay erişimden yararlandılar. Bu nedenle, yaşlıların yüksek düzeyde dikkatli olmaları ve telefonla iletişim kurmanın beraberinde getirdiği risklerin farkında olmaları hayati önem taşımaktadır.

Böyle bir durumla karşılaşmanız durumunda uygulayabileceğiniz bazı ek ipuçları:

Bilinmeyen numaralardan gelen beklenmeyen çağrıları görmezden gelin veya onları sesli mesaja yönlendirin ve verilen bilgilere göre geri arayıp aramamaya siz karar verin.

Sağladıkları herhangi bir geri arama numarasını kullanmaktan kaçının, çünkü bu bir dolandırıcılığın parçası olabilir. Bunun yerine resmi telefon numarasını arayın ve talebin meşruiyetini doğrulamak için doğrudan onları arayın.



Telefon üzerinden asla finansal veya kişisel bilgilerinizi paylaşmayın!

Bu tarz bilgilere ulaşmaya çalışan olursa hemen telefonu kapatın!

Yaşlıları ilgilendiren telefon dolandırıcılıkları



KORUNMA YOLLARI:

Şu satırı kontrol edin:

Dolandırıcıların, siz kapattıktan sonra bile telefon hattınızı açık tutabileceğini unutmayın.

Hattın boş olup olmadığını kontrol etmek için farklı bir telefon kullanın veya dolandırıcıların telefonu kapattığından emin olmak için en az 10-15 dakika bekleyin.



Çağrı engellemeyi deneyin:

Olası vishing dolandırıcılıklarını filtrelemek için telefonunuzun çağrı engelleme işlevlerini etkinleştirin. Çoğu akıllı telefon bu işlevleri sunar.

Akıllı telefonunuz yoksa, istenmeyen aramaları engellemek için hangi hizmetleri sunduklarını öğrenmek için telefon servis sağlayıcınızla iletişime geçin.

Vishing mağduruysanız, size yardımcı olabilecek ilgili kurumlarla derhal iletişime geçin.



Duygusal aile bağlarını istismar eden dolandırıcılıklar

TEHLİKE ÖZELLİKLERİ:

Büyükbaba dolandırıcılığı, dolandırıcıların büyükanne ve büyükbabalar ile torunları arasındaki duygusal bağları hedef aldığı bir dolandırıcılık türüdür. Dolandırıcı genellikle sıkıntıda olan ve acil mali yardıma ihtiyaç duyan bir torun gibi davranır.

Büyükbaba dolandırıcılığında manipülasyon türleri:

Dolandırıcı, büyükanne ve büyükbabanın çok fazla düşünmesini veya diğer aile üyeleriyle iletişime geçmesini önlemek için aciliyet duygusu yaratır.

Dolandırıcılar, utandıkları veya daha fazla başlarının derde girmesinden korktukları için büyükanne ve büyükbabalardan durumu gizli tutmalarını isteyebilirler.

Dolandırıcılar, büyükanne ve büyükbabanın torunlarına olan sevgisini ve ilgisini kullanarak hızlı bir yanıt almaya çalışırlar.

Aciliyet

Gizlilik

Duygusal olarak manipülatif

Duygusal aile bağlarını istismar eden dolandırıcılıklar



SONUÇLAR:

Büyükanne ve büyükbaba dolandırıcılığının kurbanı olmak ciddi sonuçlara yol açabilir.

01 Mali kayıp

Finansal olarak, zor kazandığınız parayı kaybedebilirsiniz, çünkü dolandırıcılar genellikle birikimlerinizi tüketebilecek büyük meblağlar isterler. Banka bilgilerinizi verirseniz, daha da fazlasını çalabilirler.

02 Duygusal sıkıntı

Duygusal olarak, sahte acil durumlar önemli stres ve kaygı yaratır ve bunun bir dolandırıcılık olduğunu keşfetmek, sizi derinden ihanete uğramış ve incinmiş hissettirebilir.

03 Güven kaybı

Bu deneyim, güven kaybına yol açabilir, gerçek acil durumlardan şüphe duymanıza ve meşru kaynaklardan bile olsa beklenmedik her türlü temastan şüphe duymanıza neden olabilir.

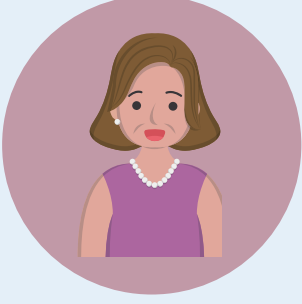
04 İzolasyon

Ayrıca, utanma veya mahcup olma hissi yaşayabilir, bu da aileniz veya arkadaşlarınızla finansal konularda iletişim kurmaktan çekinmenize yol açabilir ve dolandırıcılar sizi kolay bir hedef olarak görüp tekrar hedef alabilirler.

Duygusal aile bağlarını istismar eden dolandırıcılıklar



ARKA PLANDA TARİHLE KORUMA YOLLARI



Mary yalnız yaşıyor ve ailesiyle, özellikle de torunlarıyla yakın bir ilişki yaşıyor. Bir akşam, Mary torunu Jack olduğunu iddia eden birinden acilen büyük miktarda para talep eden bir telefon aldı. Bu çağrı Mary için üzücü ve maliyetli bir deneyime yol açtı.

Ancak Mary, torununun kendisine para isteyen insanlarla telefonda konuşurken dikkatli olması gerektiği yönündeki tavsiyesini hatırlıyor.

Mary'nin deneyimi, yaygın dolandırıcılıklar hakkında bilgi sahibi olmanın ve acil ve duygusal para taleplerini doğrulamanın önemini vurguluyor. Dolandırıcıların aciliyet yaratma, gizlilik talep etme ve duyguları manipüle etme gibi kullandıkları taktikleri anlayarak, yaşlılar kendilerini kurban olmaktan daha iyi koruyabilirler. Şüphemiz varsa, bilgileri her zaman diğer aile üyeleriyle doğrulayın ve asla para göndermek için acele etmeyin.



ADIM 1: Doğrulama

Mary, arayan kişiye yalnızca Jack'in bilebileceği sorular sordu ve dolandırıcılığın önüne geçmek için Jack'i doğrudan aramak için bir an ayırdı.

ADIM 2: Farkındalık

Bu tür dolandırıcılıkları önceden bilmek, Mary'nin uyarı işaretlerini fark etmesine yardımcı oldu.

ADIM 3: İletişim

Mary, olası dolandırıcılıklar konusunda ailesiyle görüştü ve acil durumlar için bir aile şifresi belirlemenin ek koruma sağlayabileceğini söyledi.

Duygusal aile bağlarını istismar eden dolandırıcılıklar



KORUNMA YOLLARI:

Duygusal aile bağlarını istismar eden dolandırıcılıklardan kendinizi korumak, zor kazanılan paranızı korumak için çok önemlidir. İşte atabileceğiniz bazı basit adımlar.

Bilgi sahibi olun:

Yaşlıları hedef alan yaygın dolandırıcılıklar, özellikle de büyükanne ve büyükbaba dolandırıcılıkları hakkında kendinizi ve sevdiklerinizi bilgilendirin. Dolandırıcıların kullanabileceği yeni taktikler hakkında güncel kalmak için güvenilir bilgi kaynaklarını takip edin.



kimlikleri doğrulayın:

Evcil hayvanınızın adı veya ailenizde yaşanan özel bir olay gibi soruları her zaman yalnızca gerçek aile üyesinin bilmesi gerekir. Şüpheleniz varsa, arayanın kimliğini doğrulamak için bilinen bir numarayı kullanarak geri arayın.

Bir aile şifresi oluşturun:

Ailenizle birlikte yalnızca güvendiğiniz kişilerin bilebileceği gizli bir şifre belirleyin. Acil durumlarda aile üyeleriniz olduğunu iddia eden arayanların kimliğini doğrulamak için bu kod sözcüğünü kullanın.



Duygusal aile bağlarını istismar eden dolandırıcılıklar



KORUNMA YOLLARI:

Acelecı kararlardan kaçının:

Beklenmedık veya acıl para talepleri aldığınızda acele etmeyin. Dolandırıcılar, hikayelerini sorgulamanızı veya başkalarından tavsiye almanızı engellemek için aciliyeti kullanırlar.



Arayan kimliği ve çağrı engelleme özelliğini kullanın:

Gelen aramaları taramak ve bilinmeyen veya şüpheli numaraları engellemek için arayan kimliğini kullanın. Dolandırıcılık çağrılarını telefon servis sağlayıcınıza veya ilgili makamlara bildirin.

Kişisel bilgileri koruyun

Telefon veya internet üzerinden kişisel ve finansal bilgilerinizi paylaşırken dikkatli olun. Alıcının kimliğinden emin değilseniz hassas bilgileri vermekten kaçının.



Tıbbi ürünlerle ilgili dolandırıcılıklar

TEHLİKE ÖZELLİKLERİ:

Son yıllarda dolandırıcılar, tıbbi ürünler içeren dolandırıcılık planlarıyla yaşlılar da dahil olmak üzere savunmasız bireyleri giderek daha fazla hedef alıyor. Bu dolandırıcılıklar genellikle sağlık sorunlarıyla ilgili duyguları ve korkuları istismar ederek, gerçek olamayacak kadar iyi mucizevi tedaviler, tedaviler veya çareler vaat ediyor

Tıbbi ürün dolandırıcılığında manipülasyon türleri:

Dolandırıcılar, çok az bilimsel kanıta dayalı olarak mucizevi sonuçlar vaat ederek ürünlerine dair iddialı iddialarda bulunuyorlar.

**Sahte
vaatler**

Sıklıkla, "sınırlı süreli teklif" sona ermeden önce hemen satın almanızı isteyerek, yüksek baskı uygulayan satış taktikleri kullanırlar.

**Yüksek
Baskı
Taktikleri**

Bu dolandırıcılıklar duygularınızla oynuyor, sağlık sorunlarınıza ilişkin korkularınızı istismar ediyor ve hızlı ve kolay bir çözüm için sahte umutlar sunuyor.

**Duygusal
Manipülasyon**

Tıbbi ürünlerle ilgili dolandırıcılıklar



SONUÇLAR:

Tıbbi ürün manipölasyonunun aşağıdaki gibi ciddi olumsuz etkileri olabilir:

01 Mali kayıp

Tıbbi ürün dolandırıcılığının kurbanı olmak, etkisiz veya hatta tehlikeli ürünlere büyük miktarda para harcamanıza ve birikimlerinizi tüketmenize neden olabilir.

02 Sağlık riskleri

Bazı durumlarda dolandırıcılar, ciddi sağlık sorunlarına veya mevcut ilaçlarla etkileşime yol açabilen düzenlenmemiş veya sahte tıbbi ürünler kullanmaktadır.

03 Duygusal Sıkıntı

Dolandırılmak utanç, suçluluk ve mahcubiyet duygularına yol açabilir. İhanete uğramış ve endişeli hissedebilirsiniz, bu da genel ruh sağlığınızı ve refahınızı olumsuz etkileyebilir.

04 Yaşam Kalitesinin Bozulması

Finansal kayıp, sağlık riskleri ve duygusal sıkıntının birleşik etkileri, mağdurların yaşam kalitesinde önemli bir düşüşe yol açabilir. Günlük aktivitelerini yönetmek ve bağımsızlıklarını sürdürmekte zorluk çekebilirler.

Tıbbi ürünlerle ilgili dolandırıcılıklar



ARKA PLANDA TARİHLE KORUMA YOLLARI



Thomas, artrit, diyabet ve yüksek tansiyonu bir gecede iyileştirdiğini iddia eden yeni bir "mucize takviye"nin reklamını yapan bir e-posta alır. E-posta sınırlı süreli bir indirim sunar ve daha iyi bir sağlık fırsatını kaçırmamak için hemen satın alması konusunda onu teşvik eder.

Ancak Thomas, mucizevi tedavilere karşı dikkatli olunması gerektiği yönündeki okuduğu tavsiyeleri hatırlıyor.

Thomas'ın hikayesi ne yazık ki tek vaka değil. Tıbbi ürün dolandırıcılıkları, karmaşık sağlık sorunları için hızlı çözümler vaat ederek yaşlıların zaafalarını ve duygularını hedef alır. Bilgili, şüpheli kalarak ve sağlık uzmanlarına danışarak, kendinizi bu dolandırıcı planların kurbanı olmaktan koruyabilirsiniz. Unutmayın, sağlığınız paha biçilemezdir ve gerçek iyiliğe giden kestirme yollar yoktur.



ADIM 1: Şüpheli kalın

Thomas, meşru tıbbi buluşların uzmanlar tarafından titizlikle test edildiğini ve doğrulandığını hatırlattı.

ADIM 2: Profesyonellere danışın

Thomas kişisel doktorunu arayıp yeni tedaviler veya takviyeler hakkında konuştu.

ADIM 3: Araştırma

Thomas, satın almayı düşünmeden önce ürünün iddialarını destekleyen tarafsız incelemeleri ve bilimsel kanıtları aradı.

Tıbbi ürünlerle ilgili dolandırıcılıklar

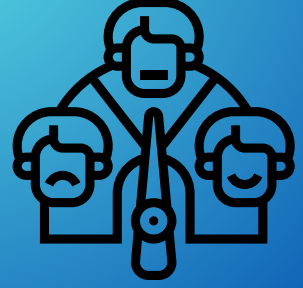


KORUNMA YOLLARI:

Unutmayın, kendinizi tıbbi ürün dolandırıcılığından korumak, zor kazandığınız parayı ve sağlığını korumak için çok önemlidir. En önemli adımlardan biri duygusal destek aramaktır. İşte atabileceğiniz bazı basit adımlar.

Duygusal destek arayın:

Aile, arkadaşlar ve toplum üyelerinden gelen sosyal destek, yaşlılara manipülasyona direnmek için ihtiyaç duydukları duygusal gücü ve güvenceyi sağlayabilir. Yaşlılar desteklendiklerini ve değer gördüklerini hissettiklerinde, duygusal zaafları istismar eden dolandırıcıların kurbanı olma olasılıkları daha düşüktür.



Bilgi sahibi olun:

Sosyal ağlar hayati bir bilgi kaynağı olabilir. Aile üyeleri ve arkadaşlar devam eden dolandırıcılıklar hakkında uyarılarda bulunabilir, dolandırıcılığı nasıl tanıyacağınız konusunda ipuçları verebilir ve tıbbi ürünler ve tedaviler için güvenilir kaynaklar önerebilir. Sosyal destek yoluyla bilgi sahibi olmak, dolandırıcılıklara düşme riskini önemli ölçüde azaltabilir.

Tıbbi ürünlerle ilgili dolandırıcılıklar



KORUNMA YOLLARI:

Sağlık uzmanlarına danışın:

Herhangi bir yeni tıbbi ürünü veya tedaviyi denemeden önce, güvenli ve etkili olduğundan emin olmak için sağlık uzmanınıza danışın.



Mucize iddialarına şüpheyile yaklaşın:

Bir ürün, birbiriyle ilgisi olmayan birden fazla sağlık sorununu tedavi ettiğini veya hızlı ve zahmetsiz sonuçlar sunduğunu iddia ediyorsa, büyük ihtimalle gerçek olamayacak kadar iyidir.

İyice Araştırın:

Ürünü ve arkasındaki şirketi araştırmak için zaman ayırın. Saygın kaynaklardan gelen incelemelere bakın ve ürünün düzenleyici kurumlar tarafından onaylanıp onaylanmadığını kontrol edin.



Daha fazla okuma



ERKEK-KADIN İLİŞKİLERİNDE DOLANDIRICILIK

- <https://www.sciencedirect.com/science/article/pii/S2949791423000441>
- <https://hu.usembassy.gov/be-wary-of-online-romance-scams/>
- <https://consumer.ftc.gov/articles/what-know-about-romance-scams#whatis>
<https://us.norton.com/blog/online-scams/romance-scams>
- <https://www.unit21.ai/fraud-aml-dictionary/romance-fraud>
- <https://www.hsbc.co.uk/help/security-centre/romance-scams-case-study/>
- <https://www.equifax.co.uk/resources/identity-protection/how-to-spot-and-avoid-romance-scams.html>
- <https://dfpi.ca.gov/2024/03/05/romance-scams-what-consumers-need-to-know/>
- <https://complyadvantage.com/insights/what-is-a-romance-scam/>



SMISHING SMS DOLANDIRICILIKLARI

- <https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it>
- <https://www.proofpoint.com/us/threat-reference/smishing>
- <https://www.sinch.com/blog/what-is-smishing/>
- <https://business.bofa.com/en-us/content/what-is-smishing-how-to-prevent-it.html>
- https://www.forbes.com/advisor/business/smishing-nedir/#smishing_karşısında_nasıl_korunulur_bölümü
- <https://www.techtarget.com/searchmobilecomputing/definition/SMiShing>
- <https://cybeready.com/category/the-complete-guide-to-smishing>
- <https://www.rd.com/article/what-is-smishing/>

Daha fazla okuma



YAŞLILARI İÇEREN TELEFON DOLANDIRICILIKLARI

- <https://www.ageuk.org.uk/information-advice/money-legal/scams-fraud/phone-scams/>
- https://www.ageuk.org.uk/globalassets/age-uk/documents/information-guides/ageukig05_avoiding_scams_inf.pdf
- <https://www.helpguide.org/articles/abuse/elder-scams-and-senior-fraud-abuse.htm>
- <https://www.seniorliving.org/research/common-elderly-scams/>
- <https://www.ooma.com/blog/home-phone/protect-seniors-from-elderly-phone-scams>
- https://taking.care/blogs/resources-advice/scams-targeting-the-elderly#How_to_avoid
- <https://www.terranovasecurity.com/solutions/security-awareness-training/what-is-vishing>
- <https://www.kaspersky.com/resource-center/definitions/vishing>
- <https://www.proofpoint.com/us/threat-reference/vishing>



DUYGUSAL AİLE BAĞLARINI İSTİSMAR EDEN DOLANDIRICILIKLAR

- <https://www.homeinstead.com/location/347/news-and-media/the-grandparent-scam/>
- <https://www.europol.europa.eu/media-press/newsroom/news/crime-against-elderly-four-arrests-in-germany-and-poland>
- <https://www.identityguard.com/news/grandparent-scam#:~:text=The%20most%20common%20grandparent%20scam,often%20claim%20to%20be%20yurtdışında.>
- <https://www.cbsnews.com/news/what-being-targeted-by-grandparent-scam-sounds-like-60-minutes/>
- <https://www.youtube.com/watch?v=v2VFy2igHPE>
- <https://globalnews.ca/video/9901367/calgary-senior-falls-victim-to-grandparents-scam-costing-her-thousands>

Daha fazla okuma



TIBBİ ÜRÜNLERLE İLGİLİ DOLANDIRICILIKLAR

- <https://www.forres-gazette.co.uk/news/older-people-targeted-by-medical-scam-116453/>
- <https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products>
- <https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview>
- <https://www.bbc.com/news/business-58029113>
- <https://www.europol.europa.eu/media-press/newsroom/news/544-arrests-and-%E2%82%AC63-million-of-fake-pharmaceuticals-and-illegal-doping-substances-seized>

BÖLÜM 4.

ÇEVİRİMİÇİ İŞLEM DOLANDIRICILIĞI

Çevrimiçi ödemeler ve işlemler çağında, giderek daha fazla çevrimiçi dolandırıcılık bildirimi geliyor. Suçlular, yeni teknolojilerin kullanımında birçok yaşlıya erişebiliyor ve bu da onları dolandırıcılık uygulamalarında daha sofistike hale getiriyor. Bu bölümde, yaşlıların çözmelerine ve kaçınmalarına yardımcı olmak için çevrimiçi işlemlerle ilgili en yaygın dolandırıcılıkları ele alacağız.

Seyahat ve bilet dolandırıcılıkları, asla gerçekleşmeyen hayali teklifler sunmayı içerir. Abonelik dolandırıcılıklarında, yaşlılar otomatik olarak ücret talep eden hizmetleri kabul etmeye kandırılır. Sahte çevrimiçi mağazalar teslim edilmeyen ürünler için ödemeleri gasp eder. Alım-satım dolandırıcılıkları, ürünlerin listelenmediği veya mevcut olmadığı sahte satın alımları ve yaşlıların eşyalarını ilan sitelerinde ücretsiz sattığı durumları içerir.

Bu tehditleri anlamak, yaşlıların internetin sunduğu fırsatlardan güvenli bir şekilde yararlanabilmeleri ve mali durumlarını dolandırıcılıktan koruyabilmeleri açısından büyük önem taşıyor.

Seyahat ve bilet dolandırıcılıkları



TEHLİKE ÖZELLİKLERİ:

Seyahat ve bilet dolandırıcılığı, sahte seyahat, tur ve bilet paketlerinin satışını içeren dolandırıcılık planlarını ifade eder. Bu tür dolandırıcılık genellikle çevrimiçi olarak gerçekleşir; dolandırıcılar profesyonel görünümlü web siteleri kurar veya büyük oranda indirimli fırsatlar sunan e-postalar gönderir. Modern çevrimiçi dolandırıcılık taktiklerine daha az aşina olabilecek yaşlılar, bu dolandırıcılıklara karşı özellikle savunmasızdır. Bilinçsiz müşteriler, özellikle bu tekliflerden etkilenen yaşlılar, bu var olmayan hizmetler için ödeme yaparlar ve dolandırıldıklarını anladıklarında hiçbir başvuru yolu kalmaz. Yaşlıları bu dolandırıcılık planları hakkında eğitmek, önemli mali kayıplardan ve duygusal sıkıntılardan kaçınmalarına yardımcı olmak için çok önemlidir.

Seyahat ve bilet dolandırıcılığı türleri:

Bu, var olmayan uçak biletleri satan dolandırıcıları içerir. Gerçek havayolu siteleri gibi görünen sahte web siteleri kurabilir, müşterileri indirimli bilet fiyatlarıyla cezbedebilir ve ardından ödemeyi aldıktan sonra ortadan kaybolabilirler.

Bu, dolandırıcıların kapsamlı tatil paketlerini büyük oranda indirimli fiyatlarla teklif ettiklerinde gerçekleşir. Müşteri ödemeyi yaptıktan sonra, paketin mevcut olmadığını veya vaat edileni içermediğini keşfeder.

Dolandırıcılar, zaman paylaşımı satıcıları veya satıcıları gibi davranarak zaman paylaşımı mülkleri için harika fırsatlar vaat edebilirler. Önceden ücret talep edebilir ve ödeme yapıldıktan sonra ortadan kaybolabilirler.

**Sahte Uçak
Biletleri**

**Sahte Tatil
Paketleri**

**Zaman Paylaşımı
Dolandırıcılıkları**

Seyahat ve bilet dolandırıcılıkları

— SONUÇLAR:

Seyahat ve Bilet Dolandırıcılığının aşağıdaki gibi ciddi olumsuz etkileri olabilir:

01 Finansal Kayıp

Seyahat ve bilet dolandırıcılığının en doğrudan sonucu maddi kayıptır. Dolandırıcılar var olmayan hizmetler için ödeme alırlar ve kurbanlara paralarını geri almak için başvuracakları hiçbir yer bırakmazlar.

02 Kimlik Hırsızlığı

Bu dolandırıcılıklar sıklıkla kurbanın bir seyahat rezervasyonu bahanesiyle hassas kişisel ve finansal bilgiler vermesini içerir. Bu bilgiler daha sonra kimlik hırsızlığı için kullanılabilir.

03 Duygusal Sıkıntı

Böyle bir dolandırıcılığın kurbanı olmak önemli duygusal sıkıntılara yol açabilir. Planlanmış bir seyahatin heyecanı hayal kırıklığına ve hüsrana dönüşür, dolandırıldıktan sonraki ihlal ve savunmasızlık hislerinden bahsetmiyorum bile.

Seyahat ve bilet dolandırıcılıkları



ARKA PLANDA TARİHLE KORUMA YOLLARI



Bir gün George, bir çevrimiçi seyahat acentesinden Avrupa tatil paketi için harika bir fırsat sunan bir e-posta aldı. Anlaşma, uçuşlar, konaklama ve Roma, Paris ve Londra'da gezi turlarını içeriyordu. Paket büyük ölçüde indirimliydi ve George, hayalindeki seyahat ihtimaliyle heyecanlanarak daha fazla araştırmaya karar verdi.

Seyahat acentesinin web sitesine tıkladı, web sitesi profesyonel görünüyordu, varış noktalarının yüksek kaliteli görüntüleri ve mutlu müşterilerden gelen övgü dolu yorumlar vardı. İkna olan George, tatil paketini ayırtmaya karar verdi. Kredi kartı bilgilerini girdi ve rezervasyonunu onaylayan bir e-posta aldı.

Günler haftalara dönüştü ve George seyahati hakkında daha fazla iletişim alamadı. Endişelenmeye başladı ve seyahat acentesiyle iletişime geçmeye çalıştı ancak telefon numaralarının kapalı olduğunu ve e-postalarının cevapsız kaldığını gördü.

George'un hikayesi, yaşlıları çevrimiçi dolandırıcılıklar konusunda eğitime ihtiyacını vurguluyor. Teknoloji konusunda daha bilgili hale geldikçe, daha yüksek risk altında oluyorlar. Aşırı cazip fırsatlar gibi dolandırıcılık belirtileri ve satın almadan önce bir şirketin gerçekliğini doğrulamanın önemi hakkında onları bilgilendirmek, güvende kalmalarına yardımcı olabilir. Bu tür deneyimleri paylaşmak, yaşlıları çevrimiçi dolandırıcılık konusunda etkili bir şekilde uyabilir.



ADIM 1: Gerçekliği doğrulayın ve anında güvenin

George, seyahat acentesine profesyonel görünümlü web sitesi ve referansları temelinde daha fazla doğrulama yapmadan güvendi. George, müşteri yorumlarını kontrol ederek, kaydını ve fiziksel adresini onaylayarak ve doğrudan onlarla iletişime geçerek yanıt oranlarını değerlendirerek seyahat acentesinin gerçekliğini doğrulamalıydı.

ADIM 2: Kredi kartı bilgilerinizi girmek yerine güvenli ödeme yöntemlerini kullanın

George, ödeme sürecinin güvenliğini sağlamadan doğrudan seyahat acentesinin web sitesine kredi kartı bilgilerini girdi. George, güvenilir bir ödeme platformu aracılığıyla kredi kartları gibi alıcı koruması sunan güvenli ödeme yöntemlerini kullanmalı ve kredi kartı bilgilerini doğrudan tanımadığı web sitelerinde paylaşmaktan kaçınmalıydı.

ADIM 3: Takip iletişimi ve eylemsiz bekleme

George, seyahati hakkında daha fazla iletişim almadan haftalarca bekledi ve ancak endişelenmeye başladığında acenteye iletişime geçmeye çalıştı. George, rezervasyonu yaptıktan kısa bir süre sonra seyahat acentesiyle iletişime geçerek ayrıntıları teyit etmeli ve sürekli iletişimi sağlamalıydı.

ADIM 4: Şüpheli etkinliği bildirin ve gecikmeli yanıt verin

George, bir şeylerin ters gittiğini anlayana kadar kredi kartı şirketine ulaşmayı erteledi. George, işlemi potansiyel olarak durdurmak ve sorunu araştırmak için şüpheli herhangi bir aktiviteyi veya iletişim eksikliğini derhal kredi kartı şirketine bildirmeliydi.

Seyahat ve bilet dolandırıcılıkları



KORUNMA YOLLARI:

Yaşlıların, önemli mali kayıplardan, duygusal sıkıntılardan ve olası Kimlik hırsızlığından kaçınmak için kendilerini Seyahat ve Bilet Dolandırıcılığından korumaları hayati önem taşır. Dolandırıcılar, çevrimiçi dolandırıcılık taktiklerine daha az aşina olabilecek yaşlıları hedef alarak, seyahat fırsatlarına duydukları güven ve heyecandan yararlanırlar. Yaşlılar kendilerini koruyarak, zor kazandıkları paranın çalınmamasını, kişisel bilgilerinin güvende kalmasını ve seyahat planlarının dolandırıcılık planları tarafından mahvedilmemesini sağlayabilirler.

Şirketi İyice Araştırın:

Herhangi bir satın alma işlemi yapmadan önce, her zaman şirket hakkında kapsamlı bir araştırma yaptığınızdan emin olun. Şirketin güvenilirliğini belirlemek ve meşruiyetini sağlamak için müşteri yorumlarını ve derecelendirmelerini aradığınızdan emin olun. Bu, şirketin önceki müşterileri arasındaki itibarı hakkında daha iyi bir anlayış sağlayacaktır.



Sadece Güvenli Ödeme Yöntemlerini Kullanın:

Çevrimiçi satın alım yaparken yalnızca güvenli ödeme yöntemlerini kullanmak çok önemlidir. Doğrudan banka havaleleri yapmaktan kaçının ve güvenli olmayan platformlar üzerinden kredi kartı bilgilerinizi paylaşmaktan kaçının. Alıcı koruması sunan ödeme seçeneklerini kullanmak her zaman daha güvenlidir.

Seyahat ve bilet dolandırıcılıkları



KORUNMA YOLLARI:

Gerçek Olmak İçin Fazla İyi Görünen Fırsatlara Karşı Dikkatli Olun:

Bir fırsat veya indirim gerçek olamayacak kadar iyi görünüyorsa, muhtemelen öyledir. Uçak bileti veya tatil paketleri gibi ürünler için aşırı indirimli fiyatlara karşı özellikle dikkatli olun. Bu tür fırsatlara atlamadan önce biraz piyasa araştırması yapmak her zaman daha iyidir.



• Örnek 3



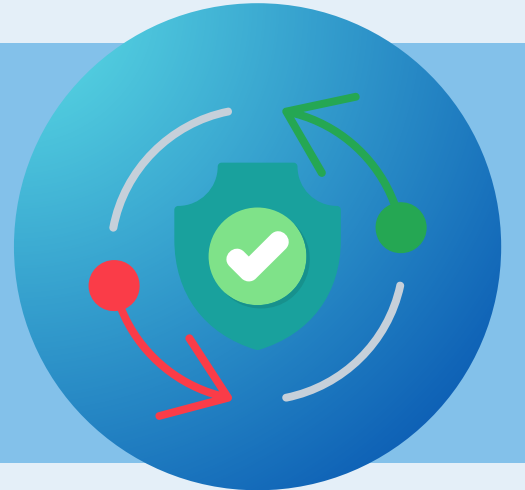
CONTACT US

Havayoluyla veya Otelle Doğrudan İletişime Geçin:

İndirimli uçuş veya otel konaklaması teklif eden bir e-posta alırsanız, teklifi doğrulamak için doğrudan havayoluyla veya otelle iletişime geçmeniz iyi bir fikirdir. Bu, teklifin meşru olduğundan ve dolandırıcılık olmadığından emin olmanızı sağlar.

Kişisel Bilgilerin Güvende Olmasını Sağlayın:

Kişisel bilgileri paylaşırken dikkatli olun. Herhangi bir hassas bilgi girmeden önce platformun güvenli olduğundan her zaman emin olun. Yeterli güvenlik önlemlerinden yoksun platformlarda asla önemli kişisel bilgilerinizi paylaşmayın.



Abonelik dolandırıcılığı



TEHLİKE ÖZELLİKLERİ:

Abonelik dolandırıcılığı, bireylerin bilgileri olmadan pahalı üyeliklere veya hizmetlere kaydolmaya kandırıldığı bir dolandırıcılık türüdür. Bu dolandırıcılıklar genellikle iptali zor olan tekrarlayan ücretlerle sonuçlanır ve yaşlılar da dahil olmak üzere savunmasız bireyleri etkiler.

Abonelik dolandırıcılığında manipölasyon türleri:

Dolandırıcılar, sizi ücretsiz deneme veya düşük maliyetli bir hizmet gibi görünen bir şeye kaydolmaya ikna etmek için yanıltıcı reklamlar veya açılır bağlantılar kullanırlar

Aldatıcı
Reklamlar
ve
Bağlantılar

Aboneliğin maliyeti ve süresi de dahil olmak üzere hüküm ve koşulları çoğu zaman küçük puntolarla gizlenmiştir veya açıkça açıklanmamıştır.

Gizli
Terimler

Kayıt olduktan sonra abonelik otomatik olarak yenilenir ve bu da kredi kartınızdan veya banka hesabınızdan beklenmeyen ücretler alınmasına neden olur.

Otomatik
Yenileme
r

Aboneliğin iptali, karmaşık prosedürler, duyarsız müşteri hizmetleri veya belirsiz iptal politikaları ile kasıtlı olarak zorlaştırılıyor.

İptal Etmede
Zorluk

Abonelik dolandırıcılığı

— SONUÇLAR:

Abonelik dolandırıcılığının aşağıdaki gibi ciddi olumsuz etkileri olabilir:

01 Mali kayıp

Abonelik dolandırıcılığının kurbanı olmak, zor kazanılan birikimlerin kaybına yol açabilir. Öngörmedikleri veya kabul etmedikleri tekrarlayan ücretler nedeniyle önemli miktarda para kaybedebilirsiniz.

02 Kimlik Hırsızlığı

Kişisel bilgilerinizin ve ödeme bilgilerinizin sahte web sitelerine verilmesi kimlik hırsızlığına ve daha fazla mali zarara yol açabilir.

03 Duygusal Stres

Yetkisiz ücretlerle uğraşmanın ve aboneliği iptal etmeye çalışmanın yarattığı hayal kırıklığı ve stres, duygusal sağlığını etkileyebilir.

Abonelik dolandırıcılığı



ARKA PLANDA TARİHLE KORUMA YOLLARI



David, yeni bir vitamin takviyesinin ücretsiz denemesi için çevrimiçi bir reklam gördü. Reklamda, abone olmak için yalnızca küçük bir kargo ücreti ödemesi gerektiği ve ardından yılın geri kalanında sınırsız vitamin alacağı iddia ediliyordu. Takviyeyi denemek konusunda heyecanlı olan David, kargo ücretini karşılamak için kredi kartı bilgilerini girmeye karar verdi. David bunu yaparken bazı internet sitelerinin masum insanların parasını aldığına dair okuduklarını hatırladı. Peki Davut ne yaptı?



Abonelik dolandırıcılığı, özellikle yaşlılar için maliyetli ve sinir bozucu bir deneyim olabilir. Dikkatli olarak, küçük yazıları okuyarak ve kişisel ve finansal bilgilerinizi korumak için adımlar atarak, bu dolandırıcılıkların kurbanı olmaktan kaçınabilirsiniz. Ücretsiz denemelere ve indirimli tekliflere her zaman dikkatli yaklaşın ve ödeme bilgilerinizi vermeden önce tüm şartları anladığınızdan emin olun. Bilgili olun, dikkatli olun ve kendinizi abonelik dolandırıcılığından koruyun.

ADIM 1: Küçük yazıları okuyun

Kayıt yaptırmadan önce devam eden abonelikler veya ek ücretler olup olmadığını kontrol etti.

ADIM 2: Araştırma

Şirketi araştırdı ve başkalarının da benzer sorunlar yaşayıp yaşamadığını görmek için yorumları okudu

ADIM 3: İfadeleri izleyin

Yetkisiz suçlamaları erken yakalamak için ifadelerini düzenli olarak kontrol etti.

Abonelik dolandırıcılığı

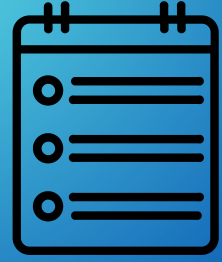


KORUNMA YOLLARI:

Abonelik dolandırıcılıklarından korunmak, zor kazanılan paranızı korumak için çok önemlidir. İşte atabileceğiniz bazı basit adımlar.

Küçük Yazıları Okuyun:

Herhangi bir hizmete kaydolmadan önce, özellikle ücretsiz deneme veya indirimli teklif içeriyorsa, her zaman hüküm ve koşulları okuyun



Ücretsiz Denemelere Karşı Dikkatli Olun:

Kredi kartı bilgilerinizi gerektiren ücretsiz denemelere karşı dikkatli olun. Denemenin ücretli aboneliğe dönüşüp dönüşmediğini ve maliyetlerinin ne olacağını kontrol edin.

Şirketi araştırın:

Aboneliği sunan şirketin yorumlarını ve derecelendirmelerini inceleyin. İyi bir üne ve güvenilir bir müşteri hizmetlerine sahip olduklarından emin olun.



Abonelik dolandırıcılığı

KORUNMA YOLLARI:

Banka Ekstrelerini İzleyin:

Yetkisiz veya şüpheli harcamalar için banka ve kredi kartı ekstrelerinizi düzenli olarak kontrol edin.

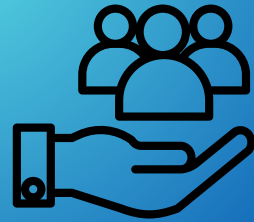


Uyarıları Ayarlayın:

Yeni ücretler veya işlemler hakkında sizi bilgilendirmek için hesap uyarılarını kullanın. Bu şekilde, yetkisiz ücretleri hızla tespit edebilir ve itiraz edebilirsiniz.

Yardım İsteyin:

Abonelik dolandırıcılığının kurbanı olursanız, yetkisiz ücretleri bildirmek için derhal bankanız veya kredi kartı şirketinizle iletişime geçin. Daha fazla ücretlendirmeyi durdurmanıza ve paranızı kurtarmanıza yardımcı olabilirler.



Sahte çevrimiçi mağazalar oluşturmada dolandırıcılık

— TEHLİKE ÖZELLİKLERİ:

Sahte çevrimiçi mağazalar, meşru alışveriş siteleri gibi görünmek için oluşturulmuş dolandırıcı web siteleridir. Bu dolandırıcılar, insanları satın alma yapmaya kandırmak için aldatıcı satış taktikleri kullanırlar. Mağdurlar, sipariş ettikleri ürünleri almak yerine genellikle sahte ürünler, düşük kaliteli ürünler veya hiçbir şey almazlar. Bu tür dolandırıcılık, yaşlılar da dahil olmak üzere savunmasız bireyleri önemli ölçüde etkileyebilir.

Sahte online mağazalardaki manipülasyon türleri:

Dolandırıcılar, popüler ürünlerde inanılmaz düşük fiyatlar veya büyük indirimlerle alıcıları cezbediyorlar.

Sahte sitelerin bazıları oldukça gelişmiş olsa da, birçoğunun tasarımı kötü, bağlantıları bozuk veya görselleri düşük kalitededir.

Meşru işletmeler, fiziksel adresler ve müşteri hizmetleri telefon numaraları da dahil olmak üzere net iletişim bilgileri sağlar.

Gerçek müşteri yorumlarının eksikliği veya yalnızca aşırı olumlu, genel yorumların olması kırmızı alarm olabilir.

Meşru alışveriş siteleri verilerinizi korumak için güvenli bağlantılar kullanır. Tarayıcı adres çubuğunda "https" ve bir asma kilit simgesi arayın.

Gerçek
Olamayacak
Kadar İyi
Fiyatlar

Kötü Web
Sitesi
Tasarımı

Sınırlı
İletişim
Bilgileri

Hiçbir
İnceleme veya
Sahte
İnceleme Yok

Güvenli
Bağlantı Yok

Sahte çevrimiçi mağazalar oluşturmada dolandırıcılık

— SONUÇLAR:

Sahte online mağazalarla ilgili dolandırıcılık, aşağıdaki gibi ciddi olumsuz etkilere yol açabilir:

01 Mali kayıp

Sahte çevrimiçi mağazalarla ilgili dolandırıcılığın kurbanı olmak, tasarruflarınızın kaybına yol açabilir. Beklenenden önemli ölçüde daha az paranız olduğunu görebilir, bu da günlük masraflarınızı karşılama ve emekliliğinizin tadını çıkarma yeteneğinizi etkileyebilir.

02 Duygusal stres

Dolandırıldıklarını fark etmek önemli duygusal sıkıntıya neden olabilir. Yaşlılar dolandırıcılığa kandıkları için utanç, mahcubiyet veya suçluluk hissedebilirler. Bu duygusal etki kaygıya, depresyona ve çevrimiçi alışverişe ve finansal kurumlara duyulan güvenin azalmasına yol açabilir.

03 Persolan bilgi hırsızlığı

Sahte çevrimiçi mağazalar genellikle ödeme işlemi sırasında kişisel ve finansal bilgiler toplar. Bu bilgiler kimlik hırsızlığı için kullanılabilir ve yetkisiz işlemlere, kurbanın adına yeni kredi hesapları açılmasına ve diğer dolandırıcılık biçimlerine yol açabilir.

Sahte çevrimiçi mağazalar oluşturmada dolandırıcılık



ARKA PLANDA TARİHLE KORUMA YOLLARI



Eva, sosyal medyada %75 indirimli üst düzey bir blender için bir reklam gördü. Harika fırsattan heyecanlanan Eva, bağlantıya tıkladı ve profesyonel görünen ancak sınırlı iletişim bilgisi sunan bir web sitesine yönlendirildi. Site, düşük fiyatı güvence altına almak için havale yoluyla ödeme yapılması konusunda ısrarcıydı.

Ödemeyi yaptıktan sonra blender'ı hiç teslim almadı ve müşteri hizmetleriyle iletişime geçme girişimleri de yanıtız kaldı.

Eva dolandırılmamak için ne yapmalıydı?



Sahte çevrimiçi mağazalar aldatıcı olabilir ve özellikle yaşlılar için önemli maddi ve duygusal zararlara yol açabilir. Bilgili kalarak ve aşağıda belirtilen koruyucu önlemleri uygulayarak bu dolandırıcılıkların kurbanı olma riskini azaltabilirsiniz. Güvenli ve emniyetli bir alışveriş deneyimi sağlamak için herhangi bir satın alma işlemi yapmadan önce çevrimiçi mağazaları araştırmak ve doğrulamak için her zaman zaman ayırın.

ADIM 1: Web Sitesini Araştırın

Yorumlara bakmalı ve mağazanın iletişim bilgilerine bakmalıydı.

ADIM 2: Güvenli Bağlantıları Doğrulayın

Web sitesinin "https" ve asma kilit simgesi içerdiğinden emin olun.

ADIM 3: Anlaşmalara Şüpheyle Yaklaşın

Gerçek olamayacak kadar iyi indirimi sorgulayın.

ADIM 4: Güvenli Ödeme Yöntemlerini Kullanın

Havale yapmaktan kaçının; bunun yerine kredi kartı kullanın.

Sahte çevrimiçi mağazalar oluşturmada dolandırıcılık



KORUNMA YOLLARI:

Unutmayın, sevgili yaşlılar, sahte çevrimiçi mağazalardan kendinizi korumak paranızı ve duygularınızı korumak için çok önemlidir. İşte atabileceğiniz bazı basit adımlar.

Web Sitesini Araştırın:

Diğer müşterilerin yorumlarını ve derecelendirmelerini kontrol edin. Mağazanın meşruiyetini doğrulamak için güvenilir yorum sitelerini kullanın. Mağazanın iletişim bilgilerini arayın ve satın alma işlemi yapmadan önce iletişime geçmeyi deneyin.



Güvenli Bağlantıları Doğrulayın:

Web sitesinin güvenli bir bağlantı ("https" ve bir asma kilit simgesi) kullandığından emin olun. Güvenli bir bağlantı olmayan sitelere kişisel veya ödeme bilgileri girmekten kaçının.

Gerçek Olmak İçin Fazla İyi Olan Fırsatlara Şüpheyle Yaklaşın:

Fiyatlar inanılmaz derecede düşük görünüyorsa veya fırsatlar gerçek olamayacak kadar iyiye, muhtemelen öyledir. Fiyatları diğer saygın perakendecilerle karşılaştırın.



Sahte çevrimiçi mağazalar oluşturmada dolandırıcılık



KORUNMA YOLLARI:

Güvenli Ödeme Yöntemlerini Kullanın:

Çevrimiçi alışverişlerinizde daha iyi dolandırıcılık koruması sundukları için kredi kartlarını kullanın. Ödemeler için havale, ön ödemeli kartlar veya kripto para birimi kullanmaktan kaçının.



Web Sitesinin Ayrıntılarını Kontrol Edin:

Net, ayrıntılı ürün açıklamaları ve profesyonel görseller arayın. Telefon numaraları ve fiziksel adresler dahil olmak üzere sitenin iletişim bilgilerini doğrulayın

İade Politikasını Öğrenin:

Meşru mağazaların net iade politikaları vardır. Bu bilgi eksikse veya belirsizse dikkatli olun.



İnternet reklamları aracılığıyla yapılan sahtekarlık amaçlı satın almalar (satın alma)



TEHLİKE ÖZELLİKLERİ:

Çevrimiçi sahtekarlık reklamları, dolandırıcıların sosyal medya platformlarını, popüler web sitelerini ve hatta Google gibi arama motorlarını kullanmasıyla önemli bir tehdittir. Sahte reklamlar, pop-up'lar, afişler, sosyal medya reklamları ve sponsorlu içerikler dahil olmak üzere birçok biçimde olabilir. Bu aldatıcı çevrimiçi reklamlar, şüphesiz kullanıcıları tıklamaya kandırmak için tasarlanmıştır ve potansiyel olarak sahte satın alımlara yol açabilir.

Çevrimiçi reklamlar aracılığıyla yapılan satın alımlarda manipülasyon türleri

Dolandırıcılar genellikle gerçek, tanınmış markaların tanıtım materyallerini (logolar, başlıklar, sloganlar vb.) kullanır. Daha sonra, kurbanları dolandırmak için hedefli reklamlar yayınlamaya başlarlar. Dolandırıcılar ayrıca kullanıcıları bu sahte reklamlara tıklamaya ikna etmek için cazip teklifler gibi sosyal mühendislik taktikleri de kullanabilirler.

Sahte reklamlar çok profesyonel ve ikna edici görünebildiğinden, bunları meşru reklamlardan ayırt etmek zordur. Bir kurban bir reklama tıkladığında, genellikle sahte bir mağazaya (burada kimlik avı gerçekleşebilir) veya sahte ürünler satan bir mağazaya gider. Bu durumlarda (kimlik avına ek olarak), kurbanın ürünü alamaması veya ödediğinden daha düşük kalitede bir ürün alması riski de vardır.

Dolandırıcılar genellikle tıkladığında kullanıcıların cihazlarını etkileyebilecek gömülü kötü amaçlı kod içeren sahte reklamlar kullanır. Kötü amaçlı reklamcılık olarak bilinen bu yöntem, siber suçlular tarafından sahte reklamlar aracılığıyla kötü amaçlı yazılım yaymak için kullanılan yaygın bir taktik haline gelmiştir.

Taklit

"Gerçek" mal
yok

Kötü amaçlı
reklamcılık

İnternet reklamları aracılığıyla yapılan sahtekarlık amaçlı satın almalar (satın alma)

— SONUÇLAR:

Seçilen yöntem ne olursa olsun, sahte reklamların arkasındaki dolandırıcılar her zaman maddi kazanç elde etme amacını taşırlar.

01 Finansal sonuçlar - Doğrudan Finansal Hırsızlık

Tanınmış markaların aşırı indirimli ürünlerini sunan sahte reklamlar, genellikle bir işlemin ödeme aşamasında ödeme ayrıntılarını ve hassas bilgileri ele geçirmeyi amaçlayan mağazaları gizler. Bu bilgiler, hesaplardan para çalmak, ek siber saldırılar başlatmak veya diğer siber suçlulara satış yapmak için kullanılabilir. Çoğu durumda, kurbanlar sahte ürünler alır veya hiçbir şey almaz.

02 Finansal sonuçlar - Fidye Yazılımı Maliyetleri

Sistem ihlali ve kötü amaçlı reklamcılık yöntemiyle veri ihlalleri nedeniyle mali sonuçlar da ortaya çıkabilir. Reklama tıklandığında, kötü amaçlı yazılım dosyalarınızı şifreleyen bir tür kötü amaçlı yazılım olan fidye yazılımını indirmeye ve yüklemeye başlar - dolandırıcılar daha sonra serbest bırakılmaları için ödeme talep eder. Fidyeyi ödeme, sisteminizi onarma ve kötü amaçlı yazılımı kaldırma ile ilişkili maliyetler önemli olabilir.

03 Kimlik hırsızlığı

Dolandırıcılar, kimlik avı yöntemiyle, kurbanları kişisel bilgilerini paylaşmaya kandırmak için meşru markaları taklit eder veya cihazdan oturum açma kimlik bilgileri ve finansal veriler gibi hassas bilgileri gizlice toplayan casus yazılımlar (malvertsigs yöntemiyle) yükleyerek, kurbanların hassas verilerinin kötüye kullanıldığı ciddi kimlik hırsızlığına yol açabilir.

İnternet reklamları aracılığıyla yapılan sahtekarlık amaçlı satın almalar (satın alma)



ARKA PLANDA TARİHLE KORUMA YOLLARI



Çeşitli sosyal medya platformlarını düzenli olarak kullanan Liza, Facebook'ta gezinirken çok güzel bir blender sunan bir çevrimiçi reklamla karşılaştı. Reklamda, son derece düşük bir fiyata, hızlı teslimat vaadiyle birinci sınıf bir blender'ın resmi gösteriliyordu. Reklam gerçek olamayacak kadar iyiydi, ama yanlışlıkla tıkladı ve ilk bakışta meşru görünen bir çevrimiçi mağazaya yönlendirildi... Ancak Liza uyarı işaretlerini fark etti!

Dolandırıcı için talihsizlik...

Liza, sosyal medya dolandırıcılıkları hakkında ileri düzey bir çalışmaya katıldı.



ADIM 1: Kalite kontrolü

Liza, yönlendirmeden sonra web sitesinin kötü tasarlandığını, çok sayıda dil bilgisi hatası içerdiğini ve fotoğrafların reklama kıyasla düşük kalitede olduğunu hemen fark etti.

ADIM 3: Meşruiyet kontrolü

Liza web sitesini kontrol ettiğinde şirket adresi, telefon numarası ve müşteri hizmetleri e-postası gibi önemli iletişim bilgilerinin eksik olduğunu gördü.

ADIM 2: Teknik kontrol

Liza, web sitesinin URL'sinin marka adıyla uyuşmadığını fark etti. Bunun yerine, başlık rastgele harflerden ve sayılardan oluşuyordu.

ADIM 4: Geri bildirim kontrolü

Liza ayrıca web sitesinde müşteri yorumları veya geri bildirimleri olmadığını fark etti. Meşru bir çevrimiçi tüccar genellikle önceki müşterilerin yorumlarını ve görüşlerini sağlar.

İnternet reklamları aracılığıyla yapılan sahtekarlık amaçlı satın almalar (satın alma)



KORUNMA YOLLARI:

Sahte reklamlarla yapılan dolandırıcılıklar, suçluların çekici fiyatlarla sahte veya var olmayan ürünleri pazarladığı ve yaşlıların indirimlere olan ilgisinden faydalandığı dolandırıcılıklar. Dolandırıcılar, teslimat gecikmeleri için bahaneler uydurarak dolandırıcılığı uzatabilir ve bu da kurbanların mali zararını daha da artırabilir.

Böyle bir durumla karşılaşmanız durumunda uygulayabileceğiniz bazı ek ipuçları:

Olası dolandırıcılıklara karşı kendinizi korumak için, özellikle şüpheli bulduğunuz reklamları görmezden gelmeniz en güvenli yoldur!

Ayrıca tıkladığınız veya dokunduğunuz yere dikkat edin! Farenizin veya parmaklarınızın ekranda nerede olduğuna ve sayfanın hangi bölümünde gezindiğinize dikkat etmek, yanlışlıkla tıklama veya dokunmaları önlemenize yardımcı olabilir!



Arama motoru sonuçlarının en üstünde yer alanlar da dahil olmak üzere, herhangi bir bağlantıya tıkladığınızda veya tıkladığınızda dikkatli olun.

Reklamlar ile gerçek arama sonuçları arasındaki farkı dikkatlice ayırt edin. Reklamlar genellikle önce görünür ve "Reklam" veya "Reklam" ile işaretlenir.

Dolandırıcıların arama motorlarında reklam yerleşimi için bilerek ödeme yaptıklarını unutmayın!

İnternet reklamları aracılığıyla yapılan sahtekarlık amaçlı satın almalar (satın alma)



KORUNMA YOLLARI:

Web sitesi URL'sini her zaman doğrudan tarayıcınıza yazın:

Tarayıcınızda güvenli olduğunu doğrulamak için kilit simgesini ve "https"yi arayın, URL'yi doğrulayın (URL üzerinde imleci gezdirin).



Bilgisayarınızı koruyun:

Bilgisayarınıza anti-virüs güvenlik yazılımı yüklemek ve düzenli olarak güncellemek önemlidir. Bu, bilgisayarın virüsle hacker saldırıları ve kötü amaçlı yazılımlar gibi farklı tehdit türlerinden korunmasını sağlayacaktır.

Web tarayıcınızda pop-up engelleme özelliğini aktifleştirin!

İnternet reklamları aracılığıyla yapılan sahtekarlık amaçlı satın almalar (satın alma)

KORUNMA YOLLARI:

Sahte çevrimiçi satıcılar/dolandırıcılar genellikle banka havaleleri (kredi kartları gibi diğer ödeme yöntemlerine kıyasla dolandırıcılık durumunda daha az koruma sağladığı için) veya bilinmeyen ödeme platformları gibi güvenilir olmayan yöntemlerle ödeme talep ederler.

Asla bu şekilde ödeme yapmayın! Ayrıca, asla finansal veya diğer hassas bilgilerinizi ifşa etmeyin!

Dolandırıcılığa uğrarsanız, mümkün olduğunca çok kanıt toplayın ve derhal ilgili makamlara bildirin!



REPORT

Bildirin! Çoğu platformda bu tür sorunları ele almak için raporlama mekanizmaları mevcuttur.

Platformdaki raporlama özelliğini kullanın. Bu özellik genellikle reklamdaki veya kullanıcı profilindeki 'Raporla' düğmesi aracılığıyla erişilebilir.

Platformun destek ekibinden talimatları bekleyin ve bildirimde bulunduktan sonra şüpheli kişiyle tüm etkileşimlerinizi sonlandırın.

Sınıflı ilan siteleri üzerinden yapılan dolandırıcılık amaçlı satın alımlar (satış)



TEHLİKE ÖZELLİKLERİ:

Çevrimiçi pazar yerleri, el yapımı el sanatları, antikalar veya gereksiz ev eşyaları vb. gibi eşyalarını satabilecekleri için yaşlıların biraz ekstra para kazanmaları için harika bir yol olabilir. Bu, yaşam standartlarını iyileştirmek veya özel günler için kullanılabilecek ek para kazanmalarını sağlar. Yaşlıların satış yaparken özellikle dikkatli olmaları gerekir, çünkü bu pazarlar potansiyel alıcılar gibi davranan dolandırıcılara da açıktır.

Sınıflandırılmış alıcı dolandırıcılığındaki manipülasyon türleri:

Dolandırıcılar bir ürünü görmeden "satın almaya" isteklidir ve genellikle hastalık, balayı veya yurtdışı seyahati gibi çeşitli bahaneler kullanırlar. Mağdurlarla yalnızca kısa mesaj veya e-posta yoluyla iletişim kurarlar ve telefon görüşmelerinden veya görüntülü aramalardan kaçınırlar. Genellikle ürünün "nakliye acentesine" gönderilmesini isterler veya bir kuryenin ürünü almasını ayarlarlar. Tüm bu iletişim yöntemleri dolandırıcıların kimliklerini gizlemelerine olanak tanır.

Dolandırıcılar yalnızca çek, havale, banka havalesi, uluslararası fon transferi, mobil ödeme uygulamaları vb. ile ödeme talep eder, sahte ödeme onayları gönderir ve kurbanların dolandırıcılık olduğunu anlamadan önce ürünü göndermelerini umarlar. Gönderdikleri ödemede bir sorun olduğu gibi »bahaneler« kullanabilirler, kurbanlardan nakliye veya gönderim masraflarını önceden ödemelerini isteyebilir ve masrafları geri ödeyeceklerine söz verebilirler, vb.

Dolandırıcılar genellikle kurbanlara istenen fiyattan daha fazla para teklif ederler. Sebepler değişir - kurbanın "sıkıntılarını" telafi etmeyi, varsayılan nakliye masraflarını karşılamayı veya ödeme miktarında hata yaptıklarını iddia edebilirler. Ancak, kurbanlar fazla ödeme aldıklarında, dolandırıcılar fazla parayı geri isterler.

**Kişisel temas
yok**

Nakit yok

Fazla ödeme

Sınıflı ilan siteleri üzerinden yapılan dolandırıcılık amaçlı satın alımlar (satış)



SONUÇLAR:

Sınıflandırılmış alıcı dolandırıcılığının kurbanları aşağıdaki olumsuz etkileri yaşayabilir:

01 Mali Sonuçlar

Mağdurlar, ödeme almadan ürün göndermişlerse ürünlerin değerinin parasal kaybı gibi finansal sonuçlarla karşı karşıya kalabilirler. Fazla ödeme yapılmışsa ve mağdurlar parayı iade etmişse, ilk ödemenin hileli olduğunu görmeleri muhtemeldir - çek düşülecektir veya müşterinin çevrimiçi ödemesi reddedilecektir - bu durumda, mağdurlar 'iade ettikleri' parayı ve ürünlerin parasal değerini kaybetmişlerdir.

02 Duygusal sonuçlar

Mağdur, kendisi hakkında olumsuz düşünceler de dahil olmak üzere bir dizi semptom geliştirebilir. Mağdurlar zeki olmadıklarını veya başkalarını yargılama yeteneklerinde bir sorun olduğunu düşünebilirler. Genellikle suçtan kendilerini sorumlu tutarlar, çok fazla güvendiklerini hissederler ve öfkeli, üzgün, ihanete uğramış, çaresiz ve utanmış hissederler.

03 Hukuki sonuçlar

Mağdur çekle ödemeyi kabul etmiş ve onaylamışsa ancak çek sahteyse, banka sahteciliği tespit ettiğinde şüphelenmeyen mağdur yasa dışı çeki bozdurmaya çalıştığı için yasal olarak sorumlu tutulacaktır. Ayrıca mağdur gelecekteki finansal işlemlerde zorluklarla karşılaşabilir.

Sınıflı ilan siteleri üzerinden yapılan dolandırıcılık amaçlı satın alımlar (satış)



ARKA PLANDA TARİHLE KORUMA YOLLARI



Leon, Facebook Marketplace'te ikinci el bir bisiklet için 200 avroluk bir ilan yayınladığında, hemen "Tim"den bir mesaj aldı. Tim, fiyatta pazarlık yapmadan bisikleti satın almak istiyordu ve hatta posta ücreti için 30 avro daha teklif ediyordu. Leon, aynı kasabada yaşamasına rağmen Tim'in ürünü bizzat görmek istememesini tuhaf buldu. Tim ayrıca ürünü PayPal üzerinden ödemek istedi ve Leon'un sosyal güvenlik numarasını ve ev adresini istedi. İşte o zaman Leon aceleyle geri çekildi!

Dolandırıcı için talihsizlik...

Leon, kullanıcı topluluğu içindeki farkındalık kampanyasını izledi ve bu tür dolandırıcılıkların yaygın girişimleri ve önleyici tedbirler konusunda kendini eğitti.



ADIM 1: Şüpheli davranışların tanınması

Leon, Tim'in aynı kasabada yaşamasına rağmen ürünü bizzat görmek istememesini tuhaf buldu. Bu, meşru alıcıların genellikle satın alma işlemi yapmadan önce ürünleri incelemeyi tercih etmesi nedeniyle ilk uyarı işaretiydi.

ADIM 2: Araştırma

Leon, Tim'in profilini araştırdı ve şüpheli iletişim bilgileri ve tutarsız iletişim buldu. Leon, Tim'i engelledi ve hemen tüm iletişimi kesti, böylece daha fazla riskin önüne geçti.

ADIM 3: Koruma

Tim, kendi başına şüpheli olmayan PayPal üzerinden ödeme yapmak istedi, ancak aynı zamanda Leon'un sosyal güvenlik numarasını ve ev adresini de istedi, ki bu oldukça sıra dışı ve gereksiz. Leon bu bilgileri paylaşmamaya bilinçli olarak karar verdi.

ADIM 4: Bilgilendirme/raporlama

Leon, deneyimini toplulukla paylaştı ve Tim'in profilini platforma bildirdi. Bunu yaparak, farkındalığı artırmaya ve diğer kullanıcıları korumaya da yardımcı oldu.

Sınıflı ilan siteleri üzerinden yapılan dolandırıcılık amaçlı satın alımlar (satış)

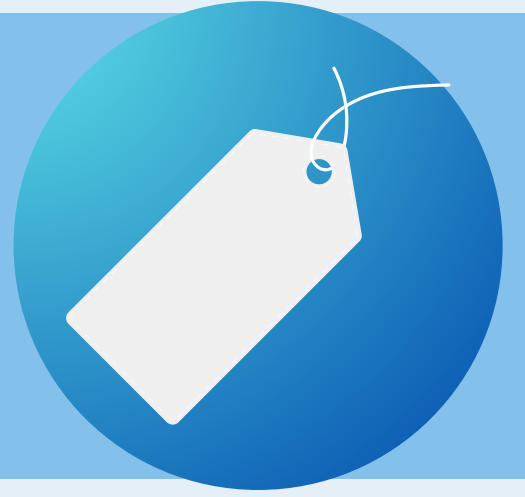


KORUNMA YOLLARI:

Ürünlerinizi çevrimiçi ilan portalları aracılığıyla satışa sunuyorsanız, potansiyel alıcılar gibi davranan dolandırıcılara karşı kendinizi korumak ve onlara karşı güçlenmek için atabileceğiniz bazı basit adımlar şunlardır.

Birisi size istediğiniz fiyattan daha fazlasını teklif ettiğinde dikkatli olun (birden fazla rekabetçi teklifle bir ürün satmıyorsanız). Size daha yüksek bir miktarda ödeme göndermeyi teklif eden ve fazlalığı geri göndermenizi bekleyen biriyle etkileşime girmeyin.

Böyle bir ödemeyi derhal reddedin ve yeni bir işlemle doğru tutarı almanız konusunda ısrarcı olun.



Nakit ödeme talebinde bulunun:

Eğer bu mümkün değilse, ödemeyi almadan önce ürünü göndermeyin ve ödemenin meşru olduğundan emin olun.

Ödeme yapmadan önce gönderirseniz, ürününüzü geri alma şansınız olmaz!



Sınıflı ilan siteleri üzerinden yapılan dolandırıcılık amaçlı satın alımlar (satış)

KORUNMA YOLLARI:

E-posta yoluyla gelen ödeme onaylarına güvenmeyin; sahte olabilirler! Ödemenin alınıp alınmadığını görmek için doğrudan banka hesabınızı kontrol edin

Olası dolandırıcılıklardan kaçınmak için şahsen görüşebileceğiniz yerel alıcılarla anlaşmak ve yalnızca nakit kabul etmek en iyisidir. Görünürdeki herhangi bir nakliye ücreti veya transfer ücreti ödemeyin. Yurt dışındaki alıcılara satış yaparken özellikle dikkatli olunması önerilir.



Gereksiz bilgi sağlama taleplerini görmezden gelin. Sadece işlemi tamamlamak için kesinlikle gerekli olan bilgileri sağlayın.

Bir ürün satıyorsanız, alıcı tarafından size gönderilen hiçbir bağlantıya tıklamayın ve alıcıya banka hesaplarınıza erişmesini sağlayabilecek hiçbir bilgi göndermeyin.

Bildirin! Çoğu platformda bu tür sorunları ele almak için raporlama mekanizmaları mevcuttur. Platformdaki raporlama özelliğini kullanın. Bu özellik genellikle reklamdaki veya kullanıcı profilindeki 'Raporla' düğmesi aracılığıyla erişilebilir. Platformun destek ekibinden talimatları bekleyin ve bildirimde bulunduktan sonra şüpheli kişiyle tüm etkileşimlerinizi sonlandırın.



Daha fazla okuma



SEYAHAT VE BİLET DOLANDIRICILIĞI

- <https://www.comparitech.com/blog/information-security/avoid-common-ticket-and-travel-scams-online/> <https://www.aura.com/learn/airline-scams>
- <https://www.interpol.int/en/Crimes/Financial-crime/Airline-ticket-fraud>
- <https://www.nyccriminallawyer.com/ticket-scams/>
- <https://www.chargebackgurus.com/blog/travel-agency-chargebacks>
- <https://chargebacks911.com/otas-lose-billions-every-year-to-travel-fraud/>
- <https://www.traveldailynews.com/post/how-fraudsters-exploit-travel-agency>
- <https://www.consumerreports.org/travel/avoiding-travel-scams/>
- <https://www.bbb.org/all/travel-scams>
- <https://www.consumer.ftc.gov/articles/travel-scams>



ABONELİK DOLANDIRICILIĞI

- <https://balkaninsight.com/2023/08/22/subscription-scams-the-mobile-users-paying-for-unwanted-services/>
- https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/consumer-frequent-traps-and-scams_en
- <https://www.evz.de/en/shopping-internet/internet-fraud/subscription-traps.html>
- <https://www.europe-consommateurs.eu/en/shopping-internet/internet-fraud-and-scams/subscription-traps.html>
- <https://www.flagright.com/post/understanding-subscription-fraud>
- <https://www.thing.co.uk/news/article/5-subscription-scams-and-traps-to-watch-out-for-aYwJA0u8EFZ9>

Daha fazla okuma



SAHTE ÇEVİRİMİÇİ MAĞAZALAR OLUŞTURMADA DOLANDIRICILIK

- <https://www.statista.com/statistics/1182221/online-shopping-fraud-incidents-uk/>
- <https://www.northyorkshire.police.uk/news/north-yorkshire/news/news/2024/04-april/online-shopping-fraud/>
- <https://us.norton.com/blog/online-scams/fake-e-shops>
- <https://www.youtube.com/watch?v=ltl7DXrNQCA>
- https://www.youtube.com/watch?v=CQYmfcLW_oc



ÇEVİRİMİÇİ REKLAMLAR ARACILIĞIYLA DOLANDIRICI SATIN ALIMLAR (ALİŞVERİŞ)

- <https://www.rd.com/list/fake-ads-on-social-media/>
- <https://www.seniorlifestyle.com/resources/blog/protect-your-parents-from-common-digital-traps/>
- <https://www.takefive-stopfraud.org.uk/advice/general-advice/purchase-fraud/>
örnekler <https://bolster.ai/glossary/fake-ads>
- <https://www.investigatetv.com/2023/11/14/how-determine-if-social-media-ads-are-real-or-fake/>
- https://thegratifiedblog.com/social-media-marketing/how-to-spot-fake-ads-on-facebook/#What_Are_Fake_Ads
- <https://trafficwatchdog.pl/en/articles/85/ad-frauds-in-social-media>
- https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_fraudulentadvertisingonline_execsummary_july2020_final.pdf
- https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

Daha fazla okuma



SINIFLANDIRILMIŞ SİTELER ARACILIĞIYLA DOLANDIRICI SATIN ALIMLAR (SATIŞ)

- <https://www.westpac.com.au/security/types-of-scams/online-shopping-scams/>
- <https://www.ccpc.ie/consumers/money/scams/social-media-scams/>
- <https://www.desjardins.com/qc/en/tips/spot-avoid-scams-online-classifieds.html> <https://www.obvy-app.com/en/magazine/individuals/avoid-scams/scam-siteler-küçük-reklamlar/2341>
- <https://www.interbank.com/fraud-protection/beware-of-online-scams-how-to-spot-fake-listings-on-social-media-sale-groups/>
- <https://www.dropzone.com/help/classifieds/classifieds-buyer-scams-r23/>
- <https://www.nab.com.au/about-us/security/online-safety-tips/buying-selling-scams>
- <https://fastercapital.com/content/Classified-ads-site--Safety-Measures-When-Using-Classified-Ad-Websites.html>
- <https://consumer.ftc.gov/consumer-alerts/2022/07/selling-stuff-online-heres-how-avoid-scam>

BÖLÜM 5.

KİMLİK MANİPÜLASYONU VE KAMU GÜVENİNİN İSTİSMARI

Modern dolandırıcılıklar giderek artan bir şekilde kimlik manipülasyonuna ve kamu kurumlarına duyulan güveni istismar etmeye dayanıyor ve bu da yaşlıları özellikle savunmasız bir konuma sokuyor. Suçlular yalnızca güvenilir kurumları taklit etmekle kalmıyor, aynı zamanda hedeflerine ulaşmak için gelişmiş teknolojileri de kullanıyor. Bu bölümde, yaşlıların bu tehditleri fark etmelerine ve bunlardan kaçınmalarına yardımcı olmak için en yaygın kimlik güven dolandırıcılıklarını ele alacağız.

Yaşlılara yönelik ciddi tehditler arasında, dolandırıcıların yaşlıları para veya bilgi gasp etmek için yalan yere suçlaması yer alır. Hükümet kimliğine bürünme, suçluların kişisel bilgi veya para elde etmek için hükümet gibi davrandığı bir diğer tehlikeli yöntemdir. Deepfake teknolojisi, ciddi sonuçlara yol açabilen sahte ancak ikna edici kayıtların oluşturulmasına olanak tanır. Hükümet kurumlarını taklit eden hizmet dolandırıcılıkları genellikle para gasp etmeyi amaçlayan sahte teklifler içerir. Sahte hesaplar, yaşlıları yanlış bilgi ifşa etmekle tehdit ederek şantaj yapmak için kullanılır.

Bu tehditleri ve mekanizmalarını anlamak, yaşlıların kimliğini, mali kaynaklarını ve kamu kurumlarına olan güvenlerini etkili bir şekilde korumaları için çok önemlidir. Bu bölümde, bu tür dolandırıcılıkları tanımanıza ve bunlardan kaçınmanıza yardımcı olmak için bu konuları ayrıntılı olarak ele alacağız.

Suça karışma iddiaları

TEHLİKE ÖZELLİKLERİ:

Bir kullanıcıyı, kendisini bir yargıç, polis memuru veya savcı olarak tanıtarak ve isminin terörizmle bağlantılı olduğunu iddia ederek dolandırmak. "Suça karışma iddiaları", bir kişinin, kuruluşun veya hatta yaşlıların yasadışı faaliyetlere katıldığı iddialarını veya suçlamalarını ifade eder. Bu iddialar henüz kanıtlanmamıştır ve geçerliliğini belirlemek için soruşturma gerektirir. Suçun niteliği, dolandırıcılık, hırsızlık veya diğer yasadışı eylemler dahil olmak üzere büyük ölçüde değişebilir ve bu tür iddialar, yaşlılar da dahil olmak üzere suçlananlar için ciddi yasal ve sosyal etkilere sahip olabilir. Yaşlılar, dijital teknoloji ve yaygın dolandırıcılık taktikleriyle ilgili potansiyel yetersizlikleri nedeniyle bu tür iddialara karşı özellikle savunmasız olabilir.

Suç katılım iddialarının türleri:

Kurbanın banka hesabının terörist faaliyetleri finanse eden işlemlerle bağlantılı olduğunu iddia etmek, kurbanı korkutmayı ve paniğe yol açmayı amaçlayan bir dolandırıcılık türüdür. Bu senaryoda, dolandırıcı iddianın ciddiyetini vurgular. Dolandırıcı genellikle kurbandan acil bir eylem talep eder, bu da bir "para cezası" veya "ücret" ödemek olabilir. Etkileşim boyunca, dolandırıcı kurbanı paniğe sürüklemek ve kişisel bilgilerini ve/veya parasını paylaşması için onu manipüle etmek için psikolojik manipülasyon taktikleri kullanır. Hatta kurbanı kimseyle iletişime geçmemesi ve bunu gizli tutması konusunda uyarabilir.

Bu senaryoda, dolandırıcı kurbanla iletişime geçebilir ve kendisini yetkili bir kişi olarak tanıtabilir, bir kolluk kuvvetinin veya yargı sisteminin parçası olduğunu iddia edebilir. Kurbanı, adının bilinen bir terör örgütüyle ilişkili kişilerin yer aldığı bir listede bulunduğu konusunda uyarır. Kurbanı korkutmak ve paniğe sürüklemek için uydurma bilgiler verebilir. Kurbandan derhal harekete geçmesini talep ederek, kontrolü sürdürmek için tehditler veya korkutucu konuşmalar kullanabilirler.

Bu senaryoda dolandırıcı kurbanla bir polis memuru, yargıç veya savcı gibi davranarak iletişime geçer. Kurbanı seyahat geçmişinin veya belirli aktivitelerinin şüphe uyandırdığını bildirir. Kurbanın gerçekten ziyaret ettiği belirli yerlerden bahsedebilirler. Daha inandırıcı hale getirmek için seyahat tarihleri veya sizinle iletişime geçtiğine inandıkları şüpheli teröristlerin isimleri gibi ayrıntılar ekleyebilirler. Diğer senaryolarda olduğu gibi dolandırıcı kurbanı hızlı kararlar almaya zorlar ve kurbanın kişisel bilgilerini vermesini sağlamak için manipülasyon taktikleri kullanır.

**Terörist
Finansman
Ağı'na Katılım**

**Bilinen terör
örgütleriyle
ilişki**

**Şüpheli Seyahat
Geçmişi veya
Aktiviteleri**

Sua karışma iddiaları



SONUÇLAR:

Sua karışma yanlışları aşağıdaki gibi ciddi olumsuz etkilere yol açabilir:

01 İtibarın Zarar Görmesi

Sula ilişkilendirilmek, iddialar kanıtlanmasa bile, bir kişinin itibarı üzerinde ciddi etkilere sahip olabilir. Bu, kişisel ilişkileri ve profesyonel fırsatları etkileyebilir.

02 Hukuki Sonuçlar

İddialar cezai soruşturmaya yol açarsa ve kişi suçlu bulunursa, yasal sonuçlarla karşı karşıya kalabilir. Bunlara para cezası, denetimli serbestlik veya hatta hapis cezası dahil olabilir.

03 Duygusal Sıkıntı

Bir sula suçlanmak önemli duygusal sıkıntıya neden olabilir. Kişi korku, utan veya mahcubiyet duyguları yaşayabilir ve bu duyguların psikolojik refahı üzerinde uzun vadeli etkileri olabilir.

Sua Karıřma İddiaları



SONUÇLAR:

04 Kimlik Hırsızlıęı ve Bunu Daha Fazla Su İřlemek İin Kullanma

KİMLİK hırsızlıęı iddiaları, maędur adına daha fazla su faaliyetinin yrtlmesine yol aabilir ve bu da hukuki ve kiřisel sonuları aęırlařtırabilir.

05 Fon Kaybı

zellikle mali dolandırıcılık ieren su iddialarının maędurları, doęrudan hırsızlık yoluyla veya kendilerini savunmakla iliřkili avukatlık cretleri ve dięer maliyetler yoluyla dolaylı olarak nemli mali kayıplara uęrayabilirler.

06 Cihazları Virslerle Bulařtırma

Siber su iddialarının sz konusu olduęu durumlarda, sulanan kiřinin cihazlarının hedef alınması ve virs veya kt amalı yazılımlarla enfekte edilmesi riski vardır; bu da veri ihlallerine ve daha fazla komplikasyona yol aabilir.

Suça Karışma İddiaları

— ARKA PLANDA TARİHLE KORUMA YOLLARI



Bir gün Rita, isminin sahte bir çevrimiçi işlemle ilgili yüksek profilli bir suç soruşturmasında yer aldığına dair bir e-posta aldı. E-posta yerel polis departmanından geliyormuş gibi görünüyordu ve oldukça ayrıntılıydı, aciliyet ve korku hissi yaratıyordu.

E-postada Rita'ya bir bağlantıya tıklaması ve kimliğini doğrulamak ve adını soruşturmadan temizlemek için sosyal güvenlik numarası ve banka hesap bilgileri de dahil olmak üzere kişisel bilgilerini girmesi talimatı verildi. İddialardan korkan ve sorunu hemen çözmek için çaresiz olan Rita talimatları izledi.

Birkaç gün sonra, bankasından hesabında şüpheli aktiviteler olduğunu bildiren bir telefon aldı. Rita, tam bu noktada, suça karışma iddialarını bir hile olarak kullanan bir dolandırıcı tarafından kandırıldığını fark etti.

Bu hikaye, yaşlılara çevrimiçi dolandırıcılıkların riskleri ve taktikleri hakkında eğitim vermenin önemini vurguluyor. Rita'nın vakasında gösterildiği gibi, dolandırıcılar dijital dünyayla ilgili yetersiz bilgilerinden faydalanabilir ve onları hassas kişisel bilgileri ifşa etmeye kandırmak için korkutma taktikleri kullanabilir. Yaşlılara bu tehditler hakkında eğitim vererek ve bu tür taleplerin meşruiyetini nasıl doğrulayacaklarını öğreterek, onları bu tür dolandırıcılıkların kurbanı olmaktan koruyabiliriz.



ADIM 1: Doğrulama

Rita beklenmedik bir e-posta alırsa, özellikle de sözde bir hükümet organından veya kolluk kuvvetlerinden, doğrudan yanıt vermemelidir. Resmi iletişim bilgilerini bağımsız olarak bulmalı ve doğrulamalıdır.

ADIM 3: Hesapları izleyin

Rita, dolandırıcılığı erken yakalamak ve hesaplarını güvence altına almak için şüpheli faaliyetlere karşı finansal ve çevrimiçi hesaplarını düzenli olarak kontrol etmelidir.

ADIM 2: Kişisel bilgileri koruyun

Rita, sosyal güvenlik numarası veya banka bilgileri gibi hassas bilgileri e-posta yoluyla paylaşmamalıdır. Meşru kuruluşlar bunu e-posta yoluyla istemez.

ADIM 4: Güvenlik yazılımı kullanın

Güvenlik yazılımı yüklemek ve güncellemek, Rita'yı virüsler, kötü amaçlı yazılımlar ve Kimlik avı gibi çevrimiçi tehditlerden koruyabilir. Yazılım tehditleri tarayabilir ve şüpheli siteleri engelleyebilir.

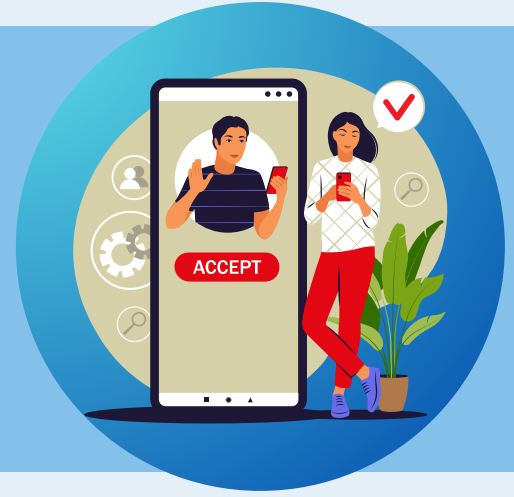
Sua Karışma İddiaları

KORUNMA YOLLARI:

Yaşlılar, itibarlarına zarar verebilecek, yasal sorunlara yol açabilecek ve duygusal sıkıntıya neden olabilecek suç iddialarından kendilerini korumalıdır. Genellikle dijital teknolojiye aşina olmadıkları için hedef alınırlar ve bu da onları dolandırıcılığa karşı savunmasız hale getirir. Önleyici tedbirler, mali durumlarını, kişisel bilgilerini ve refahlarını koruyabilir.

Beklenmeyen İsteklerin Doğrulanması:

Özellikle bir hükümet organı, kolluk kuvvetleri veya kullandığınız bir hizmet olduğunu iddia eden bir kaynaktan gelen beklenmedik e-postalar veya iletişimler aldığınızda her zaman dikkatli olun. E-postaya doğrudan yanıt vermek veya herhangi bir bağlantıya tıklamak yerine, bağımsız olarak kuruluşun resmi iletişim bilgilerini bulun ve doğrulama için onlara ulaşın. Bu şekilde, isteğin meşru mu yoksa potansiyel bir dolandırıcılık mı olduğunu doğrulayabilirsiniz.



Kişisel Bilgileri Paylaşırken Dikkatli Olun:

Kişisel bilgileriniz değerlidir ve her ne pahasına olursa olsun korunmalıdır. Sosyal güvenlik numaranız, banka hesap bilgileriniz veya diğer kişisel olarak tanımlanabilir bilgiler gibi hassas kişisel bilgileri asla bir e-posta isteğine veya doğrulanmamış bir kaynağa yanıt olarak vermeyin. Meşru kuruluşlar genellikle bu tür bilgileri e-posta veya istenmeyen iletişim yoluyla istemezler.

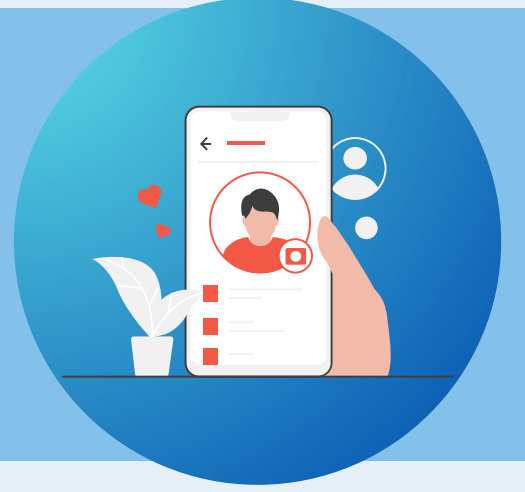


Suça Karışma İddiaları

KORUNMA YOLLARI:

Hesapların Düzenli Takibi:

Finansal ve çevrimiçi hesaplarınızı düzenli olarak izlemek, şüpheli faaliyetleri erkenden tespit etmenize yardımcı olabilir. Bu, daha fazla hasarı önlemek için çok önemlidir, çünkü faaliyeti ilgili yetkililere veya servis sağlayıcıya hemen bildirebilir ve hesabınızı güvence altına almak için adımlar atabilirsiniz.



Güvenli ve Benzersiz Parolaların Kullanımı:

Tüm çevrimiçi hesaplarınız için güçlü ve benzersiz parolalar kullanmak temel bir güvenlik önlemidir. Güçlü bir parola, harflerin, sayıların ve sembollerin bir karışımını içerir ve kolayca tahmin edilemez. Aynı parolayı birden fazla hesapta kullanmayın. Bir hesap tehlikeye girerse, diğerleri güvende kalır.

Güvenlik Yazılımının Kurulumu:

Bilgisayarınıza güvenlik yazılımı yüklemek ve düzenli olarak güncellemek, birçok çevrimiçi tehdide karşı ilk savunma hattını sağlar. Bunlara virüsler, kötü amaçlı yazılımlar, fidye yazılımları ve Kimlik avı girişimleri dahildir. Sisteminizi tehditlere karşı tarayabilir, şüpheli web sitelerini engelleyebilir ve kötü amaçlı yazılım saldırılarına karşı gerçek zamanlı koruma sağlayabilir.



Devlet kurumlarının taklidi şekilde manipölasyonlar



TEHLİKE ÖZELLİKLERİ:

Devlet yetkililerini taklit etmek, dolandırıcıların vergi daireleri, polis veya emeklilik fonları gibi çeşitli devlet kurumlarındanmış gibi davrandığı bir dolandırıcılık türüdür. Bu dolandırıcılıklar, bireylerin kişisel bilgileri ve finansal güvenlikleri için önemli bir tehdit oluşturur. Dolandırıcılar kurbanlarını aldatmak için farklı taktikler kullanır, ancak dikkat edilmesi gereken bazı genel işaretler vardır.

Devlet kurumlarının taklit edilmesinde manipölasyon türleri:

Dolandırıcılar genellikle kurbanlarla beklenmedik bir şekilde telefon, e-posta, mesaj veya hatta çevrimiçi reklam yoluyla iletişime geçerler. İlk amaç, kurbanları dolandırıcılarla iletişime geçmeye kandırmaktır. Genellikle, meşru görünmelerini sağlamak için amaçlanan kurbanın temel kişisel bilgilerine sahiptirler. İletişim kurulduktan sonra, dolandırıcılar kurbandan hassas bilgiler vermesini, "para cezaları" ödemesini (alışılmadık ödeme yöntemleriyle) veya başka eylemler gerçekleştirmesini talep edecektir.

Mağdurlarla yapılan görüşmelerde, kendileri ve görevleri hakkında çok sayıda yanlış bilgi veriyorlar ve resmi gibi görünen terimler kullanıyorlar, hükümetle bağlantılarını yanlış bir şekilde ima ediyorlar. Posta veya çevrimiçi iletişimde, resmi görünen hükümet mühürleri, logolar, pozisyonlardaki gerçek yetkililerin isimleri, sahte web siteleri ve e-posta alan adları kullanarak mağdurları kendilerine güvenmeye kandırıyorlar. E-postalar genellikle bir ek (genellikle bir PDF dosyası) ve ekteki belgeleri okumaları konusunda bir uyarı da içeriyor.

Dolandırıcılar, anında yanıt vermek için korkutma, son tarihler ve yasal işlem veya para cezası tehdidi kullanırlar. Örneğin, polisten geliyormuş gibi görünen bir e-posta, mağdur belirli bir zaman dilimi içinde yanıt vermezse cezai işlem başlatmakla tehdit edebilir. Bu taktikler paniğe yol açabilir ve muhakemeyi bozabilir, hatta genellikle mantıklı olan bireylerin bile korkudan tepki vermesine neden olabilir.

İstenmeyen
iletişim

Güvenilirmiş gibi
davranmak

Tehditler ve
aciliyet

Devlet kurumlarının taklidi şekilde manipölasyonlar



SONUÇLAR:

Hükümet sahtekarlığı dolandırıcılıkları, tam anlamıyla, yaşlıların büyük potansiyel kurbanlar olduğu gerçeğine dayanır çünkü yaşlı nesiller genellikle hükümet kuruluşlarına daha fazla güvenir ve otoriteye ve kurumlara daha fazla saygı duymaya alışkındır. Ayrıca, birikimleri vardır ve muhtemelen bir tür hükümet yardımı almaktadırlar.

01

Mali Sonuçlar

Mağdurlar, sahte vergi, yasal veya diğer yükümlölükleri çözmek için ödeme olarak dolandırıcılara aktardıkları parayı kaybederler. Kaybedilen paraya ek olarak, mağdurlar durumu çözmek için ek maliyetler ödeyebilirler. Dolandırıcılar banka hesaplarına erişirse, yetkisiz satın alımlar nedeniyle daha fazla mali kayba yol açabilir. En kötü senaryoda, hesap boşaltılabilir ve özellikle zor kazanılmış birikimlerini kaybetmiş olabilecek yaşlılar için telafisi imkansız hasara neden olabilir.

Devlet kurumlarının taklidi şekilde manipölasyonlar

02 Kimlik hırsızlığı

Bir kurban hassas kişisel verilerinin kaybını yaşarsa, dolandırıcılar kurbanın pasaport veya kimlik kartındaki bilgileri kullanarak yeni banka hesapları açabilir ve kurbanın bilgisi olmadan onun adına kredi alabilirler. Sağlık kimlik hırsızlığı durumunda, kurban sağlık yardımlarını kaybedebilirken, vergi Kimlik hırsızlığında vergi iadesi alamadan kalabilirler. Kimlik hırsızlığı travmatik bir deneyimdir ve suçluların kurbanın kimliğini suç işlemek için kullanması (siber suçlar dahil) gibi birçok başka sonucu vardır ve bu da kurbanın işlemediği eylemlerden dolayı yasal sonuçlarla karşılaşmasına yol açabilir.

03 Kamu kurumlarına güven kaybı

Bu tür dolandırıcılıklar, mağdurların bu kurumlara karşı derin bir ihanete uğramışlık ve güven kaybı hissi yaşayabilmeleri nedeniyle bireylerin kamu kurumlarına olan güvenleri üzerinde önemli bir etkiye sahip olabilir. Bu, gerçek iletişimlere karşı şüpheli olmalarına ve meşru talepleri ve bilgileri sorgulamaya başlayabilecekleri için işbirliği yapmaya daha az istekli olmalarına neden olabilir ve bu da hükümet kurumlarıyla etkileşime girme isteksizliğine yol açabilir. Dolandırıcılık potansiyeline ilişkin artan endişe, kamuoyunu etkileyebilir ve hükümet organlarının vatandaşları etkili bir şekilde koruma ve hizmet etme becerisine olan güveni azaltabilir.

Devlet kurumlarının taklidi şekilde manipölasyonlar



ARKA PLANDA TARİHLE KORUMA YOLLARI



Simon, kendisini resmi bir tonda vergi dairesinin bir çalışanı olarak tanıtan bir kişiden bir çağrı aldı. Kadın, kendisine vergi borcu olduğunu ve borcunu hemen kripto paralardan biriyle ödememezse tutuklanıp hapse atılacağını söyledi. Arayan kişi ısrarcı ve korkutucu olmasına rağmen Simon telefonu kapattı.

Görüşmeyi sonlandırdıktan kısa bir süre sonra, görüşmeyle aynı içeriğe sahip, ayrıca vergi dairesinin internet sitesine şüpheli bir bağlantı içeren bir mesaj aldı.

Dolandırıcı için talihsizlik...

Simon, Vergi İdaresi tarafından düzenlenen devlet kimliği dolandırıcılığıyla ilgili eğitim seminerine katıldı.



ADIM 1: Uyarı işaretlerini tanıma

Simon ilk başta korktu ancak arayan kişinin, vergi ödemelerinde standart bir yöntem olmayan kripto para ile ödenmemiş vergi borçlarını ödediğinden bahsetmesi üzerine dolandırıcılık belirtilerini fark etti.

ADIM 2: Sıra dışı bir davranışın belirlenmesi

Arayan kişinin tutuklanma ve hapis tehdidinde bulunması üzerine Simon bu tür tehditlerin yasallığından şüphe etti ve derhal aramayı sonlandırdı.

ADIM 3: Doğrulama

Simon, telefon numarasının ilgili vergi dairesiyle ilişkili olup olmadığını hemen kontrol etti ve olmadığını gördü. Metin mesajında bulunan şüpheli alan adı yalnızca şüphelerini doğruladı, bu yüzden numarayı engelledi.

ADIM 4: Raporlama

Simon, resmi telefon numarasını kullanarak resmi vergi dairesine ulaştı ve dolandırıcılık girişimini bildirdi.

Devlet kurumlarının taklidi şekilde manipölasyonlar



KORUNMA YOLLARI:

Böyle bir durumla karşılaşmanız durumunda uygulayabileceğiniz bazı ek ipuçları:

Kapat, Sil, Cevaplama:

Devlet kurumlarından geldiğini iddia ederek sizden ödeme yapmanızı, hassas bilgileri doğrulamanızı veya başka bilgiler vermenizi isteyen çağrılar, e-postaları, mesajları ve sosyal medyadaki mesajları dikkate almayın.

Gerçek bir devlet kurumu asla sizi arayıp, e-posta gönderip, sosyal medyada mesaj atıp para veya bilgi talep etmez.



Dolandırıcılarla iletişim kurmayın ve kişisel bilgilerinizi vermeyin veya herhangi bir ödeme yapmayın!

Meşru kurumlar, ödemeler, mali yükümlölükler ve diğler idari konularla ilgili belirli prosedür ve kurallara uymaktadır ve sizden asla kripto para birimleri, para transfer hizmetleri, ödeme platformları vb. ödeme yöntemlerini kullanarak ödeme yapmanızı istemezler.

Devlet kurumlarının taklidi şekilde manipölasyonlar

KORUNMA YOLLARI:

E-posta ve SMS'lerde verilen iletişim bilgilerine güvenmeyin!

Devlet kurumundan geliyormuş gibi görünen yazışmalara cevap vermeden önce gönderenin kimliğini bağımsız olarak doğruladığınızdan emin olun.

İletişimin meşruiyetini sağlamak için ilgili kurumun resmi iletişim bilgilerini arayın ve onlarla doğrudan iletişime geçin!



**SCAM
ALERT**

Sizi tehdit etmeye veya sindirmeye çalışan herkesle derhal iletişimi kesin!

Tehditler ve korkutmalar duygusal sıkıntıya ve psikolojik zarara yol açabilir.

Hatırlayın!

Meşru devlet kurumları vergi yükümlölüklerinin veya diğer borçların ödenmesini sağlamak için tutuklama veya hapis tehdidinde bulunmazlar.

Dolandırıcılığın kurbanı olduysanız ve para transfer ettiyseniz ve daha sonra bunun bir dolandırıcılık olduğunu anladıysanız, derhal bankanızla iletişime geçin ve şikayette bulunun. Hasarı polise bildirin.

Dolandırıcılık sırasında başka kişisel bilgileriniz de ifşa olmuşsa, dolandırıcıların dolandırıcılık amaçları için kullandıkları ilgili kurumu derhal bilgilendirin.

REPORT

Deepfake teknolojisi kullanılarak yapılan manipölasyon



TEHLİKE ÖZELLİKLERİ:

Deepfake Sahtekarlığı, aldatmak amacıyla video, ses veya görüntü oluşturmak veya değiştirmek için yapay zekanın kullanıldığı bir dolandırıcılık türünü ifade eder. Bu genellikle bir bireyin sentetik içeriğini oluşturmayı, sesini, yüz ifadelerini ve tavırlarını taklit ederek sanki yapmadıkları veya söylemedikleri bir şeyi yapıyormuş veya söylüyormuş gibi göstermeyi içerir. Bu sahte videolar, ses klipleri veya görüntüler genellikle kurbanları kandırarak paralarını vermelerini, hassas bilgileri ifşa etmelerini veya itibarlarını zedelemelerini sağlamak için kullanılır. Özellikle yaşlılar, algılanan savunmasızlıkları ve bu tür karmaşık teknolojik tehditlere aşina olmamaları nedeniyle sıklıkla hedef alınmaktadır. Deepfake sahtekarlığı ayrıca şantaj, gasp, yanlış bilgi yayma veya güvenlik sistemlerini ihlal etme amacıyla da kullanılabilir. Yaşlılar üzerindeki önemli duygusal ve finansal etki göz önüne alındığında, farkındalık yaratmak ve onları bu aldatıcı dolandırıcılıkları nasıl tanıyacakları ve kendilerini nasıl koruyacakları konusunda eğitmek çok önemlidir.

Deepfake dolandırıcılığının türleri

Bu tür deepfake dolandırıcılığı, bir bireyin taklidini yapmak için onun sentetik bir videosunu oluşturmayı içerir. Dolandırıcı, bu videoyu kullanarak kurbanları gerçek kişiyle etkileşimde olduklarına inandırabilir ve bu da olası mali kayba veya kişisel bilgilerin çalınmasına yol açabilir.

**Kimlik
Hırsızlığı**

Bu tür dolandırıcılıkta, deepfake'ler yanlış bilgi veya propaganda yaymak için kullanılır. Bu, kamu figürlerinin asla yapmadıkları şeyleri söylediği veya yaptığı videoları oluşturmayı içerebilir, böylece halkı yanıltabilir ve fikirleri veya eylemleri etkileyebilir.

**Yanlış Bilgi
Yayılması**

Deepfake'ler ayrıca yüz tanıma teknolojisine dayanan güvenlik sistemlerini ihlal etmek için de kullanılabilir. Yetkili bir bireyin sentetik bir videosunu oluşturarak, dolandırıcılar bu sistemleri kandırabilir ve hassas alanlara veya sınıflandırılmış bilgilere yetkisiz erişim elde edebilir.

Güvenlik İhlali

Deepfake teknolojisi kullanılarak yapılan manipölasyon



SONUÇLAR:

Deepfake dolandırıcılığının şu gibi ciddi olumsuz etkileri olabilir:

01 Finansal Kayıp

Deepfake dolandırıcılığının kurbanları önemli miktarda mali kayba uğrayabilir. Bu, aldatıcı deepfake içeriklerine dayanarak fon transfer etmeye veya mali bilgileri ifşa etmeye kandırıldıklarında meydana gelebilir.

02 Duygusal Sıkıntı

Deepfake dolandırıcılığının kurbanı olmak ciddi duygusal sıkıntıya yol açabilir. Kişisel kimliğin ihlali ve kişisel bilgilerin potansiyel olarak ifşa edilmesi, kurbanların kendilerini savunmasız ve ihlal edilmiş hissetmelerine neden olabilir.

03 İtibarın Zarar Görmesi

Deepfake dolandırıcılığı, bireylere ve kuruluşlara ciddi itibar zararı verebilir. Deepfake'ler aracılığıyla yayılan yanlış bilgiler, kamu güvenini zedeleyebilir ve iş kaybına, yasal sorunlara ve diğer olumsuz sonuçlara yol açabilir.

Deepfake teknolojisi kullanılarak yapılan manipölasyon



SONUÇLAR:

04 Dezenformasyon

Deepfake'ler yanlış bilgi veya propaganda yaymak, halkı yanıltmak ve fikirleri veya eylemleri etkilemek için kullanılabilir. Bunun kurumlara olan güveni baltalamak veya seçim sonuçlarını manipüle etmek gibi ciddi sosyal ve politik sonuçları olabilir.

05 Kimlik Hırsızlığı

Deepfake teknolojisi, bireylerin sentetik videolarını veya ses kliplerini oluşturmak için kullanılabilir ve bu da kimlik hırsızlığına yol açabilir. Dolandırıcılar, kişisel bilgilere, finansal kaynaklara veya güvenli sistemlere erişmek için birini taklit edebilir.

06 Hukuki Sonuçlar

Sahtecilik yapmak veya yanlış bilgi yaymak için deepfake teknolojisinin kullanılması hem failler hem de mağdurlar için yasal sonuçlara yol açabilir. Mağdurlar masumiyetlerini kanıtlamada veya itibarlarını geri kazanmada yasal zorluklarla karşılaşabilirken, failer cezai suçlamalarla karşı karşıya kalabilir.

07 Sosyal Güven Erozyonu

Deepfake'lerin yaygınlığı toplumsal güveni aşındırabilir ve insanların dijital içeriklerin gerçekliğine şüpheyile yaklaşmasına neden olabilir. Bu, çevrimiçi olarak paylaşılan medya ve bilgilere karşı genel bir güvensizliğe yol açabilir ve iletişimi ve gerçek bilgilerin yayılmasını zorlaştırabilir.

Deepfake teknolojisi kullanılarak yapılan manipölasyon

— ARKA PLANDA TARİHLE KORUMA YOLLARI

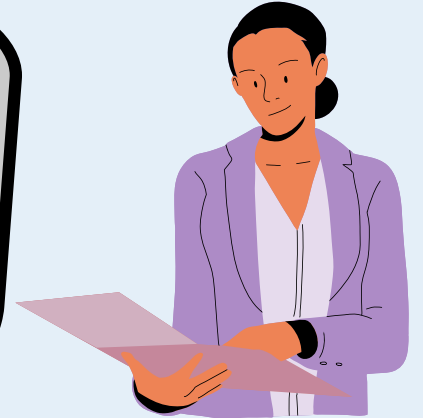


Bir gün Bill, torunu Jack'ten bir e-posta aldı. E-postada Jack'in yardım istediği görünen bir video vardı. Seyahat ederken cüzdanını kaybettiğini ve eve dönmek için biraz paraya ihtiyacı olduğunu söyledi. Video inanılmaz derecede gerçekçi görünüyordu çünkü Jack'in sesi ve tavırları en ince ayrıntısına kadar yansıtılmıştı.

Torunu için endişelenen Bill, parayı hemen transfer etti. Ancak daha sonra kızıyla konuştuğunda Jack'in aslında hiç seyahat etmediğini öğrendi.

Kafası karışmış ve şok olmuş bir halde, Bill bir deepfake dolandırıcılığının kurbanı olduğunu fark etti. Jack'in videosu gerçek değildi, bir deepfake'ti - yapay zeka kullanılarak üretilmiş sentetik bir video.

Bu hikaye, yaşlıların deepfake dolandırıcılığına karşı savunmasızlığını vurgulayarak, bu demografi arasında farkındalık ve eğitim ihtiyacını vurguluyor. Bill gibi yaşlılar, bu tür karmaşık dolandırıcılıkların farkında olmayabilir ve bu da onları kolay hedef haline getirebilir. Hikaye, yaşlıları deepfake teknolojisi hakkında bilgilendirmenin, onlara mali yardım taleplerini nasıl doğrulayacaklarını öğretmenin ve bu tür taleplerin gerçekliğini doğrulamak için aileler içinde açık iletişimi teşvik etmenin önemini vurguluyor.



ADIM 1: Doğrulama

Her zaman finansal yardım veya hassas bilgi taleplerini doğrulayın. Bill için bu, herhangi bir işlem yapmadan önce talebin gerçekliğini doğrulamak için bilinen ve güvenilir bir yöntemle, örneğin telefon görüşmesiyle torunuyla doğrudan iletişime geçmek anlamına gelir.

ADIM 3: Gelişmiş Güvenlik Önlemleri

Bill, e-posta ve sosyal medya hesapları için iki faktörlü kimlik doğrulama gibi gelişmiş güvenlik önlemlerini kullanmalıdır. Bu, yetkisiz erişime ve olası dolandırıcılıklara karşı ekstra bir koruma katmanı ekler.

ADIM 2: Eğitim ve Farkındalık

Bill, deepfake gibi en son teknolojik tehditler hakkında bilgi sahibi olmalıdır. Bunların nasıl çalıştığını ve dolandırıcılıklarda nasıl kullanılabileceğini anlamak, olası dolandırıcılık girişimlerini fark etmesine ve koruyucu önlemler almasına yardımcı olacaktır.

ADIM 4: Açık İletişim

Bill, ailesiyle aldığı alışılmadık istekler veya mesajlar hakkında açık iletişimi sürdürmelidir. Bunları güvendiği aile üyeleriyle görüşerek, potansiyel dolandırıcılıkları hızla tespit edebilir ve önleyebilir.

Deepfake teknolojisi kullanılarak yapılan manipölasyon



KORUNMA YOLLARI:

Deepfake dolandırıcılığı önemli miktarda mali kayba, duygusal sıkıntıya ve kişinin itibarının zedelenmesine yol açabilir. Ayrıca, yaşlılar bu tür dolandırıcılıklardan hem maddi hem de duygusal olarak kurtulmada zorluklarla karşılaşabilirler. Yaşlılar bu tehditlerin farkında olarak ve koruyucu önlemler alarak kişisel bilgilerini koruyabilir, mali güvenliklerini koruyabilir ve onurlarını ve gönül huzurlarını koruyabilirler.

Eğitim ve Farkındalık:

Deepfake'ler, potansiyel kullanımları ve bunları tespit etmek için mevcut en son araçlar hakkında bilgi sahibi olun. Bu tehditler ve bunlara karşı koruyucu önlemler hakkındaki bilginizi düzenli olarak güncelleyin.



Doğrulama:

Özellikle mali yardım veya hassas bilgi isteyen videoların kaynağını her zaman doğrulayın. Videoda görünen kişiyle güvenilir bir yöntemle iletişime geçerek videonun gerçekliğini doğrulayın.

Deepfake teknolojisi kullanılarak yapılan manipölasyon

KORUNMA YOLLARI:

Gelişmiş Kullanımı: Kişisel ve finansal bilgilerinizin güvenliğini sağlamak için iki faktörlü kimlik doğrulama ve biyometrik doğrulama gibi gelişmiş güvenlik önlemlerini kullanın.



Güvenilir Kaynaklara Güvenin: Hassas bilgileri yalnızca güvenilir kaynaklarla ve güvenli platformlar aracılığıyla paylaşın. Kişisel ayrıntılar veya finansal bilgiler isteyen istenmeyen iletişime karşı dikkatli olun.

Şüpheli Aktiviteyi Bildirin: Potansiyel bir deepfake ile karşılaşırsanız, bunu ilgili yetkililere bildirin. Bu, başkalarının kurban olmasını önlemeye ve dolandırıcıların yakalanmasına yardımcı olabilir.



Devlet kurumlarını taklit eden hizmet dolandırıcılığı

TEHLİKE ÖZELLİKLERİ:

Devlet kurumlarını taklit eden hizmet dolandırıcılığı, resmi devlet kurumları veya hizmetleri gibi davranan dolandırıcıları içerir. Bu dolandırıcılar pasaport, vize veya sosyal güvenlik yardımları gibi resmi belgelerin işlenmesinde yardım teklif eder, ancak gerçek amaçları kişisel bilgilerinizi veya paranızı çalmaktır.

Hizmet dolandırıcılığında manipülasyon türleri:

Dolandırıcılar sahte web siteleri oluşturur veya devlet kurumlarından geliyormuş gibi görünen e-postalar gönderir. Meşru görünmek için resmi logolar ve dil kullanabilirler.

Bu dolandırıcılıklar genellikle aciliyet ifadesini kullanır ve hızlı davranmazsanız sonuçları konusunda sizi uyarır. Buna para cezası tehditleri, yasal işlem veya kaçırılan teslim tarihleri dahil olabilir.

Sosyal Güvenlik numaranız, banka hesap bilgileriniz veya pasaport bilgileriniz gibi hassas bilgiler isterler

Dolandırıcılar, "hizmetleri" için önceden ödeme talep ediyor; bu ödemeler genellikle havale, ön ödemeli kartlar veya kripto para birimi gibi izlenemeyen yöntemlerle yapılıyor.

Gerçek hükümet web siteleri net iletişim bilgileri ve müşteri hizmetleri seçenekleri sunar. Sahte siteler genellikle sınırlı veya sahte iletişim bilgilerine sahiptir.

Resmi
Hizmetlerin
Taklidi

Acil ve Yetkili
Dil

Kişisel Bilgi
Talepleri

Peşin
Ödemeler

Doğrudan
İletişim
Bilgilerinin
Eksikliği

Devlet kurumlarını taklit eden hizmet dolandırıcılığı

— SONUÇLAR:

Hizmet dolandırıcılığının aşağıdaki gibi ciddi olumsuz etkileri olabilir:

01 Hukuki ve İdari Sorunlar

Sahte hizmetlerin kullanılması, kurbanın bilmeden sahte belgeler sunması veya yasal gerekliliklere uymaması durumunda yasal sorunlara yol açabilir. Bu, para cezalarına, yaptırımlara veya ek yasal maliyetlere yol açabilir.

02 Kimlik Hırsızlığı

Dolandırıcılar genellikle devletle ilgili hizmetler için ihtiyaç duydukları bahanesiyle kişisel bilgileri toplarlar. Bu bilgiler kurbanın kimliğini çalmak için kullanılabilir ve bu da yetkisiz finansal işlemlere, adına yeni hesaplar açılmasına ve diğer dolandırıcılık faaliyetlerine yol açabilir.

03 Meşru Kurumlara Güvenin Kaybı

Devlet kurumu gibi davranan biri tarafından dolandırıldıktan sonra, yaşlılar gerçek devlet kurumlarına ve yetkililerine karşı güvensiz hale gelebilir. Bu, gerçekten ihtiyaç duydukları yardım veya hizmetleri arama isteklerini engelleyebilir.

04 Finansal Kayıp

Yaşlılar, var olmayan faydalar için işlem ücretleri veya resmi belgelerle ilgili yardım gibi sahte hizmetler için ödeme yapabilirler. Bu, özellikle sabit geliri olanlar için zararlı olabilecek doğrudan mali kayba yol açar.

Devlet kurumlarını taklit eden hizmet dolandırıcılığı



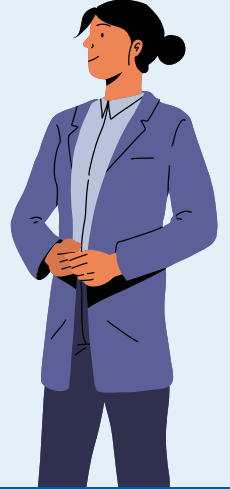
ARKA PLANDA TARİHLE KORUMA YOLLARI



Grace, cezalardan kaçınmak için pasaportunun acilen yenilenmesi gerektiğini belirten, hükümetten olduğunu iddia eden bir e-posta alır. E-posta, departmanın logosu ve resmi diliyle resmi görünen bir web sitesine bağlantı sağlar. Web sitesi, yenileme sürecini hızlandırmak için kişisel bilgiler ve 150 avroluk bir ücret ister. Grace ne yapmalıdır?

Devlet kurumlarını taklit eden hizmet dolandırıcılığı, özellikle yaşlılar için ciddi mali ve duygusal zararlara yol açabilir. Bilginin kaynağını doğrulayarak, acil taleplere karşı şüpheli davranarak, kişisel bilgileri koruyarak ve güvenli ödeme yöntemleri kullanarak kendinizi bu dolandırıcılıklardan koruyabilirsiniz.

Dolandırıcılıkların kurbanı olmamak için her zaman gerçek devlet web siteleri ve hizmetleriyle etkileşim kurduğunuzdan emin olun.



ADIM 1: Kaynağı doğrulayın

Yenileme sürecini onaylamak için doğrudan Dışişleri Bakanlığı'nın resmi web sitesini kontrol edin veya müşteri hizmetlerini arayın.

ADIM 2: Acil taleplere karşı şüpheli olun

Gerçek devlet kurumlarının acil yenileme taleplerini e-posta yoluyla göndermeyeceğini unutmayın.

ADIM 3: Kişisel bilgilerinizi paylaşmayın

Doğruluğunu teyit edene kadar kişisel bilgilerinizi sağlanan web sitesine girmekten kaçının.

ADIM 4: Güvenli ödeme yöntemlerini kullanın

Ödeme talepleri konusunda dikkatli olun ve hükümetin bu tür ücret ve hizmetleri sağlayıp sağlamadığını kontrol edin.

Devlet kurumlarını taklit eden hizmet dolandırıcılığı



KORUNMA YOLLARI:

Devlet kurumunu taklit eden hizmet dolandırıcılığından kendinizi korumak, kişisel bilgilerinizi, paranızı ve duygularınızı korumak için çok önemlidir. İşte atabileceğiniz bazı basit adımlar.

Kişisel Bilgilerinizi Paylaşmayın:

Sosyal Güvenlik numaranız, banka bilgileriniz veya pasaport bilgileriniz gibi hassas bilgilerinizi, web sitesinin meşru olduğundan emin olmadığınız sürece çevrimiçi olarak vermekten kaçının.



Kaynağı Doğrulayın:

Resmi bir hükümet web sitesinde olduğunuzdan emin olun. Hükümet kurumları tarafından kullanılan web adresinde ".gov" ifadesini arayın. Şüpheli e-postada veya web sitesinde sağlanan iletişim bilgileri yerine resmi bir kaynaktan gelen bilgileri kullanarak doğrudan hükümet kurumuyla iletişime geçin



Acil Taleplere Şüpheyle Yaklaşın:

Acil veya tehdit edici, hemen eylem veya ödeme talep eden mesajlar alırsanız dikkatli olun. Gerçek devlet kurumları bu şekilde çalışmaz.



Sahte hesaplar aracılığıyla dolandırıcılık

TEHLİKE ÖZELLİKLERİ:

Sahte hesaplar kullanarak şantaj yapmak, dolandırıcıların sahte sosyal medya profilleri oluşturduğu ve genellikle kurbanın tanıdığı veya güvendiği birini taklit ettiği aldatıcı bir uygulamadır. Bu dolandırıcılık özellikle dijital platformlara daha az aşina olabilecek yaşlıları hedef alır. Dolandırıcılar genellikle arkadaşlık isteği göndererek iletişimi başlatır, ardından açık veya zararlı içerik paylaşmaya devam eder. Dolandırıcı daha sonra para veya diğer ödeme biçimlerini talep eder ve yaşlının itibarını uygunsuz içerikle ilişkilendirerek zarar vermekle tehdit eder.

Sahte hesaplar kullanılarak yapılan şantaj türleri:

Dolandırıcı, kurbanın tanıdığı biriymiş gibi davranarak sahte bir hesap oluşturur, kurbanın güvenini kazanır ve ardından bu güveni kullanarak şantajı başlatır.

Arkadaş veya
Tanıdık Taklidi

Dolandırıcı sahte bir kimlik yaratır, genellikle kurbana romantik ilgi duyan bir kişi. Kurban duygusal olarak yatırım yaptığında, dolandırıcı şantajı başlatır.

Yayın
balıkçılığı

Dolandırıcı, bir ünlünün veya kamu figürünün sahte hesabını oluşturur. Daha sonra hayranlarıyla veya takipçileriyle iletişime geçerek açık içerikler paylaşır ve hayranın itibarını zedeleme tehdidiyle para talep eder.

Ünlü veya
Kamuya Mal
Olmuş Bir
Kişinin Taklidi

Sahte hesaplar aracılığıyla dolandırıcılık



SONUÇLAR:

Sahte hesaplar kullanılarak yapılan şantajın ciddi olumsuz etkileri olabilir, örneğin:

01 Duygusal ve Psikolojik Sıkıntı

Bir kurbanın karşılaşılabileceği birincil etkilerden biri önemli duygusal ve psikolojik sıkıntıdır. Bu genellikle dolandırıcının yaptığı amansız tehditlerin ve sürekli tacizin doğrudan bir sonucudur. Bu sıkıntı korku, kaygı, depresyon ve uyku bozukluğu gibi çok sayıda şekilde ortaya çıkabilir ve kurbanın günlük hayatını önemli ölçüde etkileyebilir.

02 Finansal Kayıp

Mağdurların maruz kaldığı bir diğer risk ise önemli miktarda maddi kayıp yaşama olasılığıdır. Bu durum genellikle mağdurun dolandırıcının katı talepleri karşısında köşeye sıkıştığını ve bunaldığını hissettiğinde ve sonunda pes ettiğinde ortaya çıkar. Sonuç olarak, sadece zor kazanılmış paralarını kaybetmekle kalmayıp, bu kayba eşlik eden stres ve kaygıyı da yaşayabilirler.

03 İtibarın Zarar Görmesi

Son olarak, kurbanın itibarına ciddi zarar verme riski vardır. Bu, dolandırıcı tehditlerini yerine getirmeye karar verirse ve kurban hakkında potansiyel olarak zararlı veya hassas bilgiler ifşa ederse gerçekleşebilir. Bu, kurbanın sosyal statüsünde önemli bir düşüşe yol açabilir ve kişisel ve profesyonel ilişkilerinin yanı sıra gelecekteki fırsatlarını da etkileyebilir.

Sahte hesaplar aracılığıyla dolandırıcılık



ARKA PLANDA TARİHLE KORUMA YOLLARI



Bir gün, Susan uzun zamandır görüşmediği bir arkadaşının adını taşıyan bir hesaptan arkadaşlık isteği aldı. Yeniden bağlantı kurma ihtimalinden çok memnun olan Susan, isteği kabul etti. Kısa süre sonra, eski zamanları anarak mesaj alışverişinde bulunmaya başladılar. Ancak, arkadaş açık içerik paylaşmaya başladığında ve içerikle adını ilişkilendirerek itibarını zedelemekle tehdit ederek para talep ettiğinde işler kötü bir hal aldı.

Ani değişiklikten sarsılan Susan, gerçek arkadaşına farklı bir mecradan ulaşmaya karar verdi. Arkadaşının bu hesaptan haberi olmadığını öğrendiğinde, sahte bir hesapla etkileşimde bulunduğunu fark etti.

Bu hikaye, yaşlıların çevrimiçi ortamda bilinmeyen varlıklarla etkileşime girmenin potansiyel riskleri konusunda eğitilmesinin önemini vurguluyor. Yaşlıların dijital platformlara aşina olmama potansiyelleri nedeniyle sahte hesaplar üzerinden şantaj gibi dolandırıcılıklara hedef olabileceğini vurguluyor. Hikaye, yaşlılara çevrimiçi olarak kişilerle etkileşime girmeden önce kimliklerini doğrulamaları ve şüpheli faaliyetleri platforma veya yerel yetkililere bildirmeleri konusunda bir hatırlatma görevi görüyor. Dijital dünyada refahlarını ve finansal güvenliklerini korumak için farkındalık ve uyanıklık ihtiyacını vurguluyor.



ADIM 1: Arkadaşlık isteklerini doğrulayın

Susan, uzun zamandır görmediği bir arkadaşı olduğuna inandığı bir hesaptan gelen arkadaşlık isteğini, gerçekliğini doğrulamadan kabul etti. Susan, arkadaşlık isteğini kabul etmeden önce gerçek arkadaşıyla başka bir mecradan iletişime geçip gerçekliğini doğrulamalıydı.

ADIM 3: Şüpheli davranışları tanıyın

Susan, açık içerik paylaşmaya ve taleplerde bulunmaya başladıktan sonra bile hesapla etkileşime girmeye devam etti. Şüpheli davranışı fark ettiğinde, Susan hemen hesapla etkileşimi kesmeli ve şüpheli olarak işaretlemeliydi.

ADIM 2: Kişisel bilgiler konusunda dikkatli olun

Susan, herhangi bir kötü niyetli davranıştan şüphelenmeden sohbetlere katıldı ve kişisel anılarını paylaştı. Susan, diğer tarafın kimliğinden emin olana kadar dikkatli olmalı ve kişisel bilgileri paylaşmaktan veya hassas sohbetlere girmekten kaçınmalıydı.

ADIM 4: Raporlama ve eğitim

Hesabın sahte olduğunu fark ettikten sonra Susan olayı bildirdi ve deneyimini arkadaşları ve ailesiyle paylaştı. Susan'ın hesabı bildirme ve başkalarını eğitime eylemleri uygundu. Çevrimiçi dolandırıcılıklara karşı farkındalık ve uyanıklık için savunuculuk yapmaya devam etmelidir.

Sahte hesaplar aracılığıyla dolandırıcılık



KORUNMA YOLLARI:

Sahte hesaplar kullanarak şantajdan korunmak, özellikle yaşlılar için çok önemlidir çünkü duygusal ve psikolojik sıkıntıyı, maddi kaybı ve itibar kaybını önlemeye yardımcı olur. Yaşlılar, dijital platformlara aşina olmama potansiyelleri nedeniyle bu dolandırıcılıklara karşı daha savunmasız olabilir. Yaşlılar çevrimiçi ortamda dikkatli ve temkinli davranarak refahlarını ve mali güvenliklerini koruyabilir, daha güvenli ve daha keyifli bir çevrimiçi deneyim sağlayabilirler.

Arkadaşlık İsteklerinin Doğrulanması:

Arkadaşlık isteği gönderen kişinin kimliğini her zaman doğrulayın, özellikle de bir süredir onlarla iletişim kurmadıysanız. Bu, daha önce iletişim kurmak için kullandığınız başka bir ortam aracılığıyla onlara ulaşarak yapılabilir.



Gizlilik Ayarları:

Sosyal medya hesaplarınızın en yüksek gizlilik ayarlarına ayarlandığından emin olun. Bu, arkadaş listenizde olmayan kişiler tarafından görülebilecek bilgi miktarını sınırlayacaktır.

Sahte hesaplar aracılığıyla dolandırıcılık

KORUNMA YOLLARI:

Hassas Bilgileri Paylaşmayın: Kişisel veya hassas bilgileri çevrimiçi olarak paylaşmaktan kaçının. İletişim kurduğunuz kişi şüpheli davranmaya veya para talep etmeye başlarsa, konuşmayı hemen sonlandırın.



Şüpheli Aktiviteyi Bildirin:

Şüpheli bir hesapla karşılaşırsanız veya birileri uygunsuz içerikler paylaşmaya veya tehditler savurmaya başlarsa, hesabı sosyal medya platformuna ve yerel yetkililere bildirin.

Kendinizi ve Başkalarını Eğitin:

Çevrimiçi dolandırıcılıkların yaygın belirtilerini öğrenin ve başkalarına da bu belirtileri öğretin. Bu, sizin ve sevdiklerinizin bu tür dolandırıcılıkların kurbanı olmaktan kaçınmanıza yardımcı olabilir.



Daha fazla okuma



SUÇA KARIŞMA İDDİALARI

- <https://www.legalmatch.com/law-library/article/allegations-of-criminal-involvement.html>
- <https://www.findlaw.com/criminal/criminal-charges/defending-against-criminal-charges.html>
- <https://www.nolo.com/legal-encyclopedia/criminal-defense-strategies>
- <https://www.lawinfo.com/resources/criminal-defense/>
- <https://www.justia.com/criminal/>
- <https://www.avvo.com/topics/criminal-charges>
- <https://www.legalzoom.com/articles/what-to-do-if-youre-accused-of-a-crime>
- <https://www.hg.org/criminal.html> <https://www.lawyers.com/legal-info/criminal/>
- https://www.americanbar.org/groups/criminal_justice/



DEVLET KURUMLARININ TAKLİDİ ŞEKLİNDE MANİPÜLASYONLAR

- <https://www.ncoa.org/article/government-imposter-scams-what-they-are-and-how-to-spot-them>
- <https://www.nia.nih.gov/news/high-vulnerability-government-impersonation-scams-among-older-adults>
- <https://www.idnow.io/glossary/impostor-fraud/>
- <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/senior-citizens-financial-scams/>
- <https://consumer.ftc.gov/articles/how-avoid-government-impersonation-scam#whattoknow>
- <https://regtechtimes.com/government-impersonation-scams-your-shield/>
- <https://www.europol.europa.eu/media-press/newsroom/news/beware-of-scams-involving-fake-correspondence-europol>

Daha fazla okuma



DEEFAKE TEKNOLOJİSİ KULLANILARAK YAPILAN MANİPÜLASYON

- <https://www.bitdefender.com/blog/labs/deepfakes-what-they-are-how-they-work-and-how-to-protect-against-malicious-usage-in-the-digital-age>
- <https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained>
- <https://www.media.mit.edu/posts/deepfakes-explained/>
- <https://www.sentinelone.com/blog/what-are-deepfakes-how-can-you-spot-them/>
- <https://www.datavisor.com/blog/how-deepfakes-are-made-and-how-fraudsters-use-them/>
- <https://www.iproov.com/blog/deepfake-fraud-identity-theft-explained>
- <https://techmonitor.ai/teknoloji/ai-and-automation/audio-deepfake-scams-the-growing-threat-explored>
- <https://readwrite.com/are-deepfakes-illegal-ais-dark-side-explained/>



DEVLET KURUMLARINI TAKLİT EDEN HİZMET DOLANDIRICILIĞI

- <https://www.c-span.org/video/?468676-1/social-security-scams>
- <https://www.nia.nih.gov/news/high-vulnerability-government-impersonation-scams-among-older-adults>
- <https://www.bressler.com/news-1882>
- <https://consumer.ftc.gov/articles/how-avoid-government-impersonation-scam>
- https://www.facebook.com/europol/videos/%EF%B8%8F-beware-scammers-impersonating-europol-officers-europol-never-contacts-members-/1097501060976901/?_rdr

Daha fazla okuma



SAHTE HESAPLAR ARACILIĞIYLA DOLANDIRICILIK

- <https://www.malwaretips.com/i-have-your-secrets-fake-blackmail-sextortion-scam-email>
- <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/sextortion-scams>
- https://www.scamnet.wa.gov.au/scamnet/Fight_back.htm
- <https://www.antivirus.com/blackmail-and-sextortion-emails>
- <https://www.malwaretips.com/hello-perv-blackmail-emails-are-fake>
- <https://www.womenslaw.org/about-abuse/abuse-using-teknoloji/impersonation>
- <https://www.minclaw.com/how-to-deal-with-google-chat-blackmail>
- <https://www.digitalinvestigation.com/blog/blackmail-on-tiktok>
- <https://www.justice.gov/opa/pr/us-law-enforcement-joins-international-partners-disrupt-international-sextortion-ring>
- <https://www.cyber.gov.au/acsc/view-all-content/publications/sextortion-scams>



www.cybersafesenior.eu



Cyber-Safe-Senior



Funded by
the European Union

CYBER SAFE
SENIOR 



Instytut
Nowych Technologii



SIMBIOZA
MED GENERACIJAMI

"AB tarafından finanse edilmiştir. İfade edilen görüş ve düşünceler yazar(lar)a aittir ve Avrupa Birliği veya Erasmus+ Ulusal Ajansı'nın görüşlerini yansıtmaz.

Bunlardan Avrupa Birliği veya hibe eden kuruluş sorumlu değildir."



Bu materyal açık CC.3.0 BY-NC-ND 3.0 PL lisansı (Atıf-Ticari Olmayan-Türev Eser Yok 3.0 Polska) altında sunulmaktadır.

Lisans, eseri yalnızca ticari olmayan amaçlar için ve özgün haliyle (türev eserler olmadan) muhafaza edilmesi koşuluyla dağıtmanıza, sunmanıza ve icra etmenize izin verir. Daha fazla bilgi için: <https://creativecommons.org/licenses/by-nd/3.0/pl/legalcode>

