BEZPIECZEŃSTWO
W ŚWIECIE CYFROWYM

Praktyczne rozwiązania dla seniorów z analizą przypadków cyberprzestępczości

SPIS TREŚCI:

Funded by the European Union

CYBER SAFE SENIOR

Nowoczesne technologie coraz bardziej integrują się z naszym życiem, co podkreśla kluczowe znaczenie bezpieczeństwa w świecie wirtualnym. Kwestia ta jest szczególnie istotna dla seniorów, którzy często nie są tak biegli w nowoczesnych technologiach i są bardziej narażeni na cyberzagrożenia. E-book „Bezpieczeństwo w świecie cyfrowym. Praktyczne rozwiązania dla seniorów z analizą przypadków cyberprzestępczości" oferuje niezbędną wiedzę i narzędzia, które wspierają osoby starsze w ochronie przed zagrożeniami w Internecie.

E-book powstał w ramach projektu „Cyber Safe Senior" o numerze 2023-1-PL01-KA220-ADU-000160325 finansowanego przez Unię Europejską. Celem tego projektu jest podniesienie świadomości seniorów na temat zasad bezpieczeństwa w Internecie i rozwijanie ich umiejętności cyfrowych. Odpowiadając na rosnące zapotrzebowanie na edukację w zakresie bezpiecznego korzystania z Internetu, projekt dostarcza praktycznych wskazówek, studiów przypadków i analiz, aby pomóc seniorom unikać zagrożeń i reagować w sytuacjach awaryjnych.

E-book zawiera rozdziały na temat różnych aspektów cyberbezpieczeństwa, takich jak cyberataki, oszustwa finansowe, manipulacje społeczne, oszustwa związane z transakcjami online i kradzież tożsamości. Każdy rozdział zawiera studia przypadków ilustrujące działania cyberprzestępców i pokazujące, jak skutecznie się przed nimi bronić. Dzięki praktycznym poradom ten e-book jest cennym źródłem wiedzy dla seniorów, którzy chcą bezpiecznie korzystać z nowoczesnych technologii.

SIMBIOZA MED GENERACIJAMI

Instytut Nowych Technologii

ILKSENOL DERNEĞİ

Institute of Entrepreneurship Development iED

W ramach projektu przygotowaliśmy wyjątkowe materiały, które nie tylko dostarczają cennej wiedzy, ale również angażują i interesują użytkowników. Jednym z kluczowych elementów są profesjonalnie przygotowane klipy wideo - pięć dynamicznych, wizualnie atrakcyjnych filmów, które w przystępny sposób ilustrują rzeczywiste sytuacje, potencjalne zagrożenia i odpowiednie reakcje na niebezpieczeństwa. Filmy te mają na celu edukację poprzez praktyczne przykłady, co sprawia, że przekazywane informacje są łatwiejsze do zrozumienia i zapamiętania.

Przygotowaliśmy również pakiet interaktywnych quizów. Quizy te zostały opracowane w sposób nie tylko edukacyjny, ale również ciekawy i zabawny, aby uczestnicy mogli sprawdzić swoją wiedzę, dobrze się przy tym bawiąc. Taka forma angażowania odbiorców nie tylko uatrakcyjnia przekaz, ale także zwiększa jego skuteczność, zapewniając, że zdobyta wiedza zostanie z nimi na dłużej.

Elementy te, łączące w sobie edukację i rozrywkę, sprawiają, że projekt jest nie tylko wartościowy, ale także atrakcyjny i przyjemny dla każdego odbiorcy.

Funded by the European Union

CYBER SAFE SENIOR

FILMY:

Manipulacja emocjonalna - oszustwa charytatywne

Manipulacja finansowa

Łamanie haseł

Podszywanie się i deepfake

Pułapki zakupów online

QUIZY:

Oszustwa SMS-owe: Jak można się przed nimi chronić?

Ataki e-mailowe, oszustwa phishingowe, ryzyko związane ze słabymi hasłami, złośliwe oprogramowanie i wirusy komputerowe.

Technologie podszywania się i deepfake.

Kupowanie i sprzedawanie online: czy potrafisz rozpoznać zagrożenia?

Manipulacja finansowa i wykorzystywanie emocji seniorów.

SIMBIOZA MED GENERACIJAMI

Instytut Nowych Technologii

ILKSENOL DERNEĞİ

Institute of Entrepreneurship Development iED

ROZDZIAŁ 1.
CYBERATAKI I BEZPIECZEŃSTWO INTERNETOWE

W dzisiejszym cyfrowym świecie seniorzy są coraz bardziej podatni na cyberataki, które zagrażają ich bezpieczeństwu online. W tym rozdziale omówimy metody ataków i środki bezpieczeństwa, które mogą pomóc seniorom chronić się przed zagrożeniami.

Ataki na Wi-Fi obejmują zarówno sieci prywatne, jak i publiczne, które mogą być wykorzystywane przez przestępców do przechwytywania danych. Ważne jest, aby zrozumieć ryzyko związane z korzystaniem z publicznych hotspotów i umieć rozpoznawać bezpieczne sieci Wi-Fi.

Ataki e-mailowe, takie jak phishing, polegają na wysyłaniu fałszywych wiadomości, które wydają się pochodzić od zaufanych instytucji, w celu uzyskania danych osobowych. Słabe hasła to kolejny problem, który może ułatwić dostęp do prywatnych kont.

Malware i wirusy stanowią poważne zagrożenie, które może infiltrować urządzenia i kraść dane. Omówimy metody ochrony, takie jak regularne aktualizacje, oprogramowanie antywirusowe i unikanie podejrzanych linków.

Skupimy się na praktycznych wskazówkach i strategiach, które pomogą seniorom zrozumieć i uniknąć tych zagrożeń oraz chronić swoje dane i prywatność w Internecie.

Atak za pośrednictwem sieci Wi-Fi (prywatnych i publicznych)

CHARAKTERYSTYKA ZAGROŻENIA:

Publiczne sieci Wi-Fi umożliwiają bezpłatny dostęp do Internetu i są uważane za wielką wygodę. Są dostępne w wielu miejscach publicznych, w tym w bibliotekach, kawiarniach, na lotniskach, w restauracjach i hotelach. Jednak otwarte sieci Wi-Fi od dawna uważane są za ryzykowne środowisko online dla Twoich informacji. Chociaż żadna sieć Wi-Fi nie jest całkowicie wolna od ryzyka, bezpieczeństwo Twoich prywatnych danych w dużej mierze zależy od rodzaju sieci Wi-Fi. Ataki na sieci Wi-Fi, zarówno prywatne, jak i publiczne, mogą przybierać różne formy.

Oto pięć typów takich ataków:

Atak typu „Man in the Middle" (MitM)

W ataku MitM atakujący przechwytuje komunikację między dwoma urządzeniami w sieci Wi-Fi, podszywając się pod jedną ze stron. Dzięki temu może przechwytywać dane, takie jak loginy, hasła lub informacje bankowe bez wiedzy użytkowników.

Atak typu "Evil Twin"

W ataku Evil Twin atakujący tworzy fałszywą sieć Wi-Fi, która na pierwszy rzut oka wygląda identycznie jak legalna sieć. Użytkownicy, myśląc, że łączą się z prawdziwą siecią, łączą się z fałszywą siecią, co pozwala atakującemu przechwycić wszelkie przesyłane dane.

Atak za pośrednictwem sieci Wi-Fi (prywatnych i publicznych)

CHARAKTERYSTYKA ZAGROŻENIA:

Atak na hasło Wi-Fi typu "Brute Force Attack"

Atakujący próbuje odgadnąć hasło Wi-Fi, używając programów, które systematycznie testują różne kombinacje znaków. Gdy hasło jest słabe lub zbyt proste, atak ten może być skuteczny, umożliwiając nieautoryzowany dostęp do sieci.

Atak typu "Packet Sniffing"

W tym ataku atakujący używa specjalnego oprogramowania do przechwytywania i analizowania pakietów danych wysyłanych przez sieć Wi-Fi. Nawet w zabezpieczonej sieci, jeśli dane nie są odpowiednio zaszyfrowane, można je odczytać i wykorzystać.

Atak typu DoS (odmowa usługi)

W ataku DoS atakujący wysyła dużą liczbę nieprawidłowych żądań lub fałszywych sygnałów autoryzacji do punktu dostępu Wi-Fi, powodując przeciążenie sieci. Może to tymczasowo wyłączyć lub zakłócić działanie sieci, uniemożliwiając użytkownikom korzystanie z połączenia.

Atak za pośrednictwem sieci Wi-Fi (prywatnych i publicznych)

KONSEKWENCJE:

Korzystanie z publicznego i bezpłatnego dostępu do Internetu wiąże się z wieloma zagrożeniami, które mogą zagrozić poufnym danym i bezpieczeństwu online. Ważne jest, aby wiedzieć, jakie są zagrożenia podczas korzystania z publicznych sieci Wi-Fi.

Konsekwencje wynikające z różnych typów ataków na sieć Wi-Fi:

01 Man-in-the-Middle (MitM)

Osoby starsze mogą paść ofiarą kradzieży tożsamości lub stracić oszczędności, jeśli przestępca przechwyci dane logowania do kont bankowych lub serwisów społecznościowych.

02 Evil Twin

Użytkownicy mogą nieświadomie podawać swoje dane logowania, numery kart kredytowych lub inne poufne informacje, sądząc, że korzystają z bezpiecznej sieci.

Atak za pośrednictwem sieci Wi-Fi (prywatnych i publicznych)

KONSEKWENCJE:

03 Brute Force Attack

Jeśli seniorzy używają prostych lub powtarzalnych haseł, przestępcy mogą uzyskać dostęp do ich sieci, co może prowadzić do naruszenia prywatności, a także wyższych rachunków za Internet.

04 Packet Sniffing

Osoby starsze mogą być narażone na wyciek prywatnych informacji, takich jak adresy e-mail, hasła i dane osobowe, jeśli atakujący przechwycą niezaszyfrowane dane.

05 Odmowa usługi (DoS)

Atak typu DoS może uniemożliwić seniorom korzystanie z Internetu, co jest szczególnie problematyczne dla osób, które polegają na technologii w komunikacji z bliskimi lub załatwianiu codziennych spraw.

Atak za pośrednictwem sieci Wi-Fi (prywatnych i publicznych)

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Philip postanowił zjeść kolację w pobliskiej restauracji. Korzystając z publicznego Wi-Fi restauracji, otworzył pocztę e-mail, aby sprawdzić najnowsze wiadomości. Niestety, nieświadomy zagrożeń związanych z publicznymi sieciami Wi-Fi, nie zabezpieczył swojego połączenia. W wyniku ataku typu Man-in-the-Middle przestępca przechwycił dane logowania do jego poczty e-mail, co spowodowało nieautoryzowany dostęp do jego konta i potencjalny wyciek poufnych informacji.

Konsekwencje nierozpoznania zagrożenia:

KROK 1: Atak na sieć Wi-Fi w restauracji w miejscu publicznym

Philip skorzystał z publicznej sieci Wi-Fi w restauracji, aby sprawdzić swoją pocztę e-mail. Brak odpowiednich środków bezpieczeństwa, takich jak brak uwierzytelniania dwuskładnikowego, pozwolił przestępcy przechwycić dane logowania.

KROK 2: Nieautoryzowany dostęp do poczty e-mail

W wyniku ataku przestępca uzyskał nieautoryzowany dostęp do konta e-mail Philipa, zdobywając poufne informacje, takie jak prywatna korespondencja, kontakty i inne poufne dane.

KROK 3: Wyciek poufnych informacji

Przejęcie konta e-mail może doprowadzić do potencjalnego wycieku poufnych informacji Philipa, co może zagrozić jego prywatności i bezpieczeństwu. Przestępca może wykorzystać te dane do oszustwa, kradzieży tożsamości lub innych nielegalnych działań.

KROK 4: Konsekwencje emocjonalne

Philip doświadczył stresu, niepokoju i utraty pewności siebie podczas korzystania z publicznych sieci Wi-Fi. Ponadto konieczność zmiany haseł, monitorowania kont i podejmowania działań w celu zapobiegania dalszym atakom może wymagać dodatkowego czasu i wysiłku.

Atak za pośrednictwem sieci Wi-Fi (prywatnych i publicznych)

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Możesz uniknąć takich konsekwencji, stosując poniższe metody, aby chronić się przed atakami za pośrednictwem Wi-Fi.

Używaj silnych haseł:

Zabezpiecz swoją sieć Wi-Fi silnym, unikalnym hasłem. Pamiętaj, aby nie używać oczywistych haseł, takich jak imię, nazwisko, data urodzenia lub innych łatwych do odgadnięcia kombinacji znaków.

Aktualizacja oprogramowania:

Regularnie aktualizuj oprogramowanie routera, aby zabezpieczyć się przed znanymi lukami w zabezpieczeniach.

Atak za pośrednictwem sieci Wi-Fi (prywatnych i publicznych)

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Włącz szyfrowanie:

Upewnij się, że wszystkie przesyłane dane są szyfrowane, nawet w zabezpieczonych sieciach Wi-Fi.

Unikaj publicznych sieci Wi-Fi:

Jeśli to możliwe, unikaj korzystania z publicznych sieci Wi-Fi do przesyłania poufnych danych. Jeśli musisz z nich korzystać, użyj wirtualnej sieci prywatnej (VPN).

Monitoruj swoją sieć:

Regularnie sprawdzaj, jakie urządzenia są podłączone do Twojej sieci Wi-Fi, aby szybko wykryć urządzenia nieautoryzowane.

Ataki e-mailowe

CHARAKTERYSTYKA ZAGROŻENIA:

Ataki oparte na poczcie e-mail to złośliwe próby uzyskania nieautoryzowanego dostępu do systemów lub informacji za pośrednictwem kont e-mail. Istnieje wiele rodzajów ataków, na które podatni są seniorzy. Warto zapoznać się z niektórymi z najczęstszych.

Główne rodzaje ataków na skrzynki pocztowe:

Ataki phishingowe

Phishing to powszechna metoda, za pomocą której oszuści wysyłają fałszywe wiadomości e-mail, które wyglądają, jakby pochodziły od zaufanych źródeł (np. banków, urzędów państwowych).

Działania oszustów:

- Fałszywe linki i załączniki: Oszuści wysyłają wiadomości zawierające linki do fałszywych stron internetowych lub załączniki, których celem jest wyłudzenie poufnych informacji, takich jak hasła i numery kart kredytowych.
- Tworzenie poczucia pilności: wiadomości e-mail często zawierają informacje o problemach z kontem, konieczności natychmiastowej aktualizacji danych lub ostrzeżenia o podejrzanej aktywności.

Ataki typu spear phishing

Spear phishing to bardziej zaawansowana forma phishingu, w której ataki są spersonalizowane i wymierzone w konkretne osoby.

Działania oszustów:

- Spersonalizowane wiadomości: Oszuści zbierają informacje o ofierze z publicznych źródeł, takich jak media społecznościowe, w celu tworzenia legalnych wiadomości e-mail.
- Podszywanie się pod znajomego: Wiadomości te często sprawiają wrażenie, że wysyła je ktoś znany ofierze (np. kolega z pracy).

Ataki e-mailowe

CHARAKTERYSTYKA ZAGROŻENIA:

Ataki polegające na podszywaniu się pod e-mail

Podszywanie się pod wiadomość e-mail to technika polegająca na tym, że oszuści zmieniają nagłówki wiadomości e-mail, aby sprawiały wrażenie, że pochodzą one z zaufanego źródła.

Działania oszustów:

- Fałszywe nagłówki: Oszuści zmieniają nagłówki wiadomości, aby sprawiały wrażenie, że zostały wysłane z prawdziwego adresu, na przykład od znajomego, szefa lub zaufanej instytucji.
- Ukrywanie tożsamości: Wiadomości wydają się autentyczne, co utrudnia ich wykrycie przez odbiorców i systemy antyspamowe

Dystrybucja złośliwego oprogramowania i oprogramowania wymuszającego okup

Cyberprzestępcy często przejmują konta e-mail w celu rozsyłania złośliwego oprogramowania.

Działania oszustów:

- Zainfekowane załączniki: Wiadomości e-mail zawierają załączniki, które po otwarciu instalują złośliwe oprogramowanie na komputerze ofiary.
- Linki złośliwe: Wiadomości e-mail mogą zawierać linki do stron internetowych, które automatycznie pobierają i instalują złośliwe oprogramowanie na Twoim komputerze.

Ataki typu Man-in-the-middle (MiTM) na komunikację e-mailową

Atak MitM ma miejsce, gdy atakujący przechwytuje i przesyła dane między dwiema stronami bez wiedzy żadnej ze stron.

Działania oszustów:

- Przechwytywanie danych: Hakerzy przechwytują komunikację w celu uzyskania poufnych informacji, takich jak dane logowania lub tajemnice firmy.
- Podszywanie się: Mogą również wysyłać wiadomości w imieniu jednej ze stron, co umożliwia manipulowanie komunikacją.

Ataki e-mailowe

CHARAKTERYSTYKA ZAGROŻENIA:

Przejęcie poczty e-mail lub ataki przejęcia

Hakerzy próbują uzyskać dostęp do Twojego konta e-mail, zgadując hasło lub stosując inne metody.

Działania oszustów:

- Zgadywanie haseł: Hakerzy mogą używać technik takich jak siłowe odgadywanie haseł.
- Phishing: Mogą również stosować phishing lub inne techniki socjotechniczne, aby nakłonić Cię do podania danych logowania.

Ataki polegające na zbieraniu danych uwierzytelniających

Hakerzy uzyskują dostęp do kont e-mail, oszukując użytkowników i żądając od nich podania danych logowania.

Działania oszustów:

- Phishing: Użytkownik otrzymuje e-mail z fałszywą prośbą o podanie danych logowania.
- Wpływ społeczny: Hakerzy podszywają się pod kogoś innego i proszą o podanie nazwy użytkownika i hasła, często wykorzystując informacje z mediów społecznościowych, aby zwiększyć wiarygodność swojej prośby.

Ataki e-mailowe

KONSEKWENCJE:

Ataki e-mailowe mają szereg poważnych konsekwencji, które mogą zagrozić poufnym danym i bezpieczeństwu online. Aby się chronić, ważne jest, aby je rozpoznać.

01 Ataki phishingowe

- Kradzież tożsamości: Seniorzy mogą podawać swoje dane logowania i numery kart kredytowych, co może prowadzić do kradzieży tożsamości.
- Straty finansowe: Przesyłanie danych może prowadzić do nieautoryzowanych transakcji i strat finansowych.

02 Ataki typu spear phishing

- Naruszenie prywatności: Osoby starsze mogą udostępniać poufne informacje, sądząc, że komunikują się z kimś, komu ufają.
- Straty finansowe i emocjonalne: Można manipulować ludźmi, aby podejmowali działania skutkujące stratami finansowymi i emocjonalnymi.

03 Ataki polegające na podszywaniu się pod e-mail

- Naruszenie bezpieczeństwa: Osoby starsze mogą działać w oparciu o fałszywe informacje, co może prowadzić do naruszeń bezpieczeństwa.
- Instalacja złośliwego oprogramowania: Kliknięcie na linki lub załączniki może spowodować instalację złośliwego oprogramowania.

Ataki e-mailowe

KONSEKWENCJE:

04 Dystrybucja złośliwego oprogramowania i oprogramowania wymuszającego okup

- Uszkodzenie systemu: Złośliwe oprogramowanie może uszkodzić komputer i sprawić, że stanie się on bezużyteczny.
- Oprogramowanie wymuszające okup: Złośliwe oprogramowanie może szyfrować pliki na komputerze i żądać okupu za ich odblokowanie.

05 Ataki typu Man-in-the-middle (MitM) na komunikację e-mailową

- Utrata poufności: Osoby starsze mogą nieświadomie ujawnić poufne informacje.
- Manipulacja: atakujący mogą wprowadzić w błąd obie strony komunikacji.

06 Przejęcie poczty e-mail lub ataki przejęcia

- Kradzież tożsamości: Hakerzy mogą uzyskać dostęp do poufnych informacji i wykorzystać je w celu kradzieży tożsamości.
- Wysyłanie spamu: Zainfekowane konta mogą być wykorzystywane do wysyłania spamu i złośliwego oprogramowania.

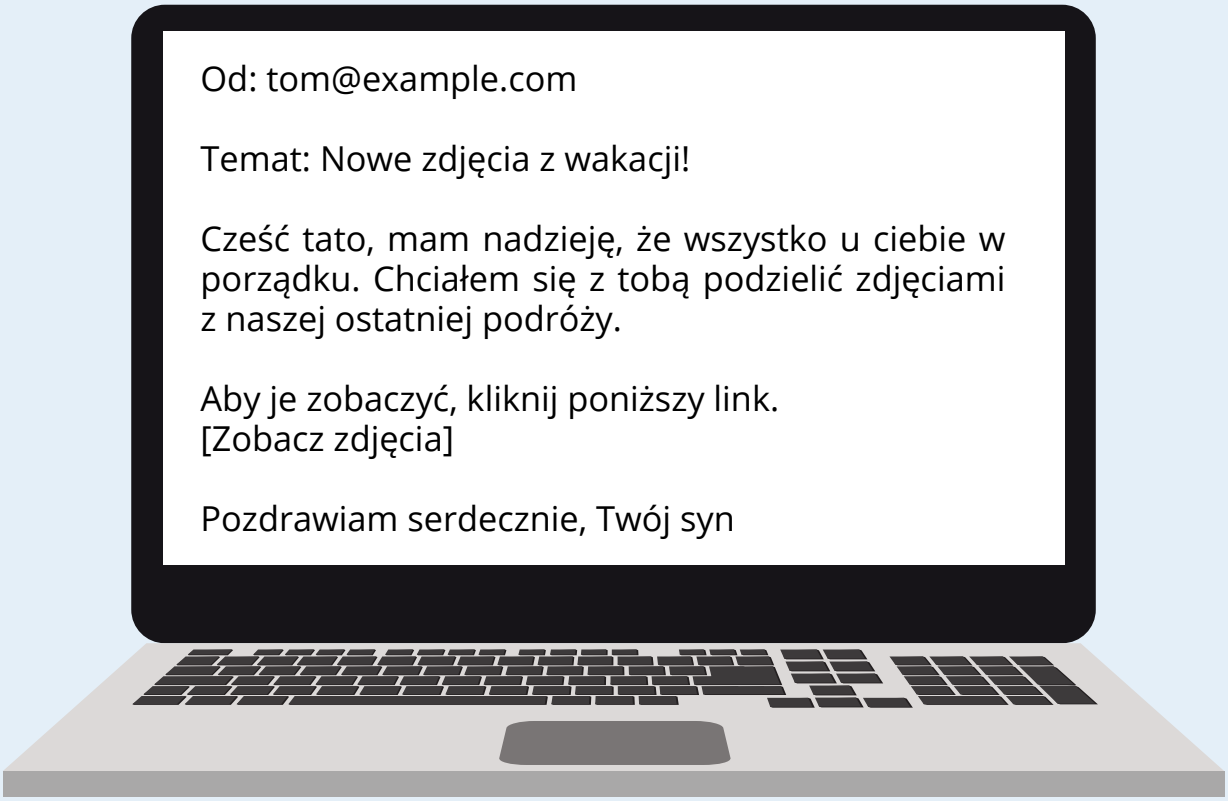
07 Ataki polegające na zbieraniu danych uwierzytelniających

- Utrata dostępu: Osoby starsze mogą utracić dostęp do swoich kont e-mail.
- Naruszenie prywatności: Hakerzy mogą uzyskać dostęp do prywatnych informacji i korespondencji.

Ataki e-mailowe

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Daniel regularnie używa poczty e-mail, aby utrzymywać kontakt z rodziną. Jego syn, który mieszkał za granicą, często wysyłał mu aktualizacje. Pewnego dnia Daniel otrzymał wiadomość e-mail, która wydawała się być wysłana przez jego syna.



Konsekwencje nierozpoznania zagrożenia:

KROK 1: Kliknięcie na link

Daniel, sądząc, że otrzymał wiadomość od syna, kliknął link.

KROK 2: Zainfekowanie komputera

Kliknięcie na link spowodowało pobranie złośliwego oprogramowania zainstalowanego na komputerze Daniela. Takie oprogramowanie może śledzić Twoją aktywność online, kraść hasła i inne poufne informacje.

Ataki e-mailowe

— SPOSOBY OCHRONY Z HISTORIĄ W TLE

Przykład Daniela pokazuje, jak niebezpieczne mogą być ataki na skrzynki pocztowe.

Link w wiadomości prowadził do strony internetowej, która automatycznie pobierała i instalowała złośliwe oprogramowanie na jego komputerze.

KROK 3: Zainfekowanie komputera

Złośliwe oprogramowanie uzyskało dostęp do danych osobowych Daniela, w tym numerów kont bankowych, haseł do różnych usług i prywatnych dokumentów.

KROK 4: Stres emocjonalny

Daniel poczuł się oszukany i martwił się, że ktoś podszywa się pod jego syna. Incydent ten wywołał u niego wielki stres i niepokój.

Ataki e-mailowe

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Możesz uniknąć takich konsekwencji, stosując poniższe metody ochrony przed atakami za pośrednictwem poczty elektronicznej.

Zachowaj ostrożność otwierając wiadomości e-mail:

Daniel powinien zachować ostrożność otwierając wiadomości e-mail:

Działanie:

- Zawsze sprawdzaj adres e-mail nadawcy, zwłaszcza jeśli wiadomość zawiera linki lub załączniki.
- Uważnie czytaj wiadomości i zwracaj uwagę na nietypowe prośby i błędy gramatyczne.

Aktualizacje oprogramowania antywirusowego:

Daniel powinien zadbać o to, aby jego komputer i telefon miały regularnie aktualizowane oprogramowanie antywirusowe.

Działanie:

- Regularna aktualizacja oprogramowania antywirusowego i skanowanie systemu.
- Instalacja najnowszych aktualizacji systemu operacyjnego i przeglądarki internetowej.

Ataki e-mailowe

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Uwierzytelnianie dwuskładnikowe (2FA):

Daniel powinien rozważyć aktywację dodatkowej warstwy zabezpieczeń, używając uwierzytelniania dwuskładnikowego (2FA) na wszystkich odpowiednich kontach. Takie podejście znacznie zwiększa poziom bezpieczeństwa, nawet jeśli hasło zostanie ujawnione.

Działanie:

- Dodatkowa warstwa zabezpieczeń: korzystanie z uwierzytelniania dwuskładnikowego (2FA) na wszystkich ważnych kontach, co zwiększa poziom bezpieczeństwa, nawet jeśli Twoje hasło zostanie ujawnione.

Warto rozważyć aktywację 2FA:

- podczas logowania się do swojego konta bankowego online, aby zapewnić sobie dostęp do swoich środków.
- podczas logowania się do konta poczty elektronicznej, na którym przechowywane są ważne informacje i korespondencja.
- podczas korzystania z platformy społecznościowej, zwłaszcza w celu komunikowania się z rodziną i znajomymi oraz udostępniania osobistych zdjęć i informacji.

Dzięki stosowaniu tych środków ostrożności Daniel może uniknąć wielu potencjalnych zagrożeń związanych z atakami na pocztę elektroniczną i innymi formami cyberprzestępczości.

Zapamiętaj moją radę, gdyż pomoże Ci ona poczuć się pewniej korzystając z Internetu oraz ochroni Twoje dane osobowe i finansowe przed nieautoryzowanym dostępem.

Ataki na słabe hasła

CHARAKTERYSTYKA ZAGROŻENIA:

Ataki wykorzystujące słabe hasła to jedna z najczęstszych metod stosowanych przez cyberprzestępców.

Główne rodzaje ataków na skrzynki pocztowe:

Atak słownikowy

Atak słownikowy polega na testowaniu dużej liczby potencjalnych haseł z wcześniej przygotowanej listy (słownika). Lista ta często zawiera popularne slogany i odmiany słów. Jest to skuteczna metoda, jeśli użytkownik używa łatwych do przewidzenia haseł, takich jak „password", „123456" lub „qwerty".

Atak siłowy

W ataku brute force atakujący systematycznie testuje wszystkie możliwe kombinacje znaków, aż znajdzie prawidłowe hasło. Chociaż ten typ ataku może zająć dużo czasu, może być skuteczny w przypadku krótkich i prostych haseł.

Atak polegający na wypełnianiu danych uwierzytelniających

Ten atak wykorzystuje dane zebrane z poprzednich wycieków informacji, takie jak loginy i hasła. Atakujący próbują używać tych samych kombinacji login-hasło na różnych stronach internetowych, licząc na to, że użytkownicy mają tendencję do ponownego używania tych samych danych logowania na wielu stronach internetowych.

Atak phishingowy

Chociaż nie jest to bezpośredni atak na hasło, phishing to technika, która próbuje oszukać użytkowników, aby dobrowolnie ujawnili swoje dane logowania. Atakujący tworzą fałszywe strony internetowe, które wyglądają identycznie jak prawdziwe strony internetowe (np. bankowość, e-mail) i wysyłają e-maile zachęcające ludzi do zalogowania się.

Ataki na słabe hasła

KONSEKWENCJE:

Ataki z użyciem słabych haseł mają szereg poważnych konsekwencji dla seniorów i mogą zagrażać poufnym danym i bezpieczeństwu online. Aby się chronić, ważne jest, aby je znać.

01 Atak słownikowy

Osoby starsze, które używają łatwo przewidywalnych haseł, takich jak „password" lub „123456", mogą paść ofiarą tego ataku. W rezultacie ich prywatność może zostać naruszona, a dane osobowe lub finansowe mogą zostać skradzione.

02 Atak siłowy

Osoby starsze, które używają krótkich i prostych haseł, są narażone na ataki siłowe. Przestępcy mogą uzyskać dostęp do ich kont przez Wi-Fi, co może prowadzić do wycieków danych i kradzieży tożsamości.

03 Atak polegający na wypełnianiu danych uwierzytelniających

Seniorzy, którzy mają tendencję do używania tych samych danych logowania na wielu stronach internetowych, są podatni na tego typu ataki. Może to prowadzić do nieautoryzowanego dostępu do ich kont na różnych platformach online.

04 Atak phishingowy

Osoby starsze, które mogą być mniej świadome takich zagrożeń, są podatne na ataki phishingowe. Przestępcy mogą używać fałszywych stron internetowych lub wiadomości e-mail, aby oszukać ludzi i uzyskać dane logowania do konta, co może skutkować kradzieżą tożsamości lub oszustwem finansowym.

Ataki na słabe hasła

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Anna używa swojego konta na Facebooku, aby utrzymywać kontakt ze swoimi kolegami z pracy. Na co dzień publikuje tam zdjęcia, dzieli się ważnymi wydarzeniami i koordynuje projekty zawodowe. Niestety, padła ofiarą ataku, w którym jej hasło do Facebooka zostało złamane, a jej konto przejęli cyberprzestępcy.

Takie przypadki nie są rzadkością i dotyczą nie tylko seniorów, ale także osób aktywnych zawodowo i świadomych technologicznie. Każdy, niezależnie od wieku, może paść ofiarą cyberprzestępców, jeśli nie podejmie odpowiednich środków bezpieczeństwa online.

KROK 1: Używanie prostego hasła

Anna użyła prostego hasła, np. „12345678”, co ułatwiło przeprowadzenie ataku słownikowego.

KROK 2: Brak unikalnych haseł

Anna używała tego samego hasła na wielu stronach internetowych. Jej hasło było używane na innych stronach, co spowodowało wyciek danych.

Ataki na słabe hasła

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Możesz uniknąć takich konsekwencji, stosując poniższe metody ochrony przed atakami z wykorzystaniem słabych haseł.

Zmień swoje hasło na silne i niepowtarzalne:

Anna powinna natychmiast zmienić swoje hasło na Facebooku na silne, długie i unikalne hasło, którego nie używa się na żadnej innej stronie internetowej. Hasło powinno zawierać mieszankę liter, cyfr i znaków specjalnych.

Aktywuj uwierzytelnianie dwuskładnikowe (2FA):

Dobrym pomysłem jest włączenie uwierzytelniania dwuskładnikowego na koncie na Facebooku, co zapewni dodatkową warstwę bezpieczeństwa. Dzięki temu nawet jeśli ktoś zna hasło, nie będzie mógł się zalogować bez drugiego czynnika uwierzytelniania, np. kodu SMS.

Sprawdź ustawienia zabezpieczeń:

Powinieneś sprawdzić ustawienia zabezpieczeń Facebooka, aby sprawdzić, czy dodano jakieś nieznane urządzenia lub aplikacje, i wylogować się ze wszystkich urządzeń. Powinieneś również zmienić pytania bezpieczeństwa, jeśli są ustawione.

Ataki na słabe hasła

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Zgłoś incydent na Facebooku:

Prawidłowym rozwiązaniem jest skontaktowanie się z pomocą techniczną Facebooka i zgłoszenie, że Twoje konto zostało naruszone. Facebook może pomóc Ci odzyskać konto i chronić je przed dalszymi atakami.

Sprawdź inne konta:

Warto sprawdzić inne konta na stronach internetowych, na których mogła użyć tego samego hasła, i zmienić hasła na unikalne i silne. Zapobiegnie to dalszym przejęciom kont.

Edukacja na temat phishingu:

Dobrą praktyką jest również nauczenie się rozpoznawania prób phishingu, aby uniknąć tego typu ataków w przyszłości. Anna powinna zwracać uwagę na podejrzane e-maile, linki i dokładnie sprawdzać adresy URL stron logowania.

Phishing

CHARAKTERYSTYKA ZAGROŻENIA:

Phishing to forma cyberataku, w której oszuści próbują uzyskać poufne informacje. Słowo „phishing” pochodzi od angielskiego słowa „fishing”, które metaforycznie odnosi się do „łowienia” danych osobowych użytkowników.

Cztery główne zasady, na których opiera się phishing:

Podszywanie się pod zaufane źródła

- Metoda: Oszuści tworzą fałszywe strony internetowe, wiadomości e-mail lub wiadomości, które wyglądają, jakby pochodziły od zaufanych instytucji (np. banków, firm technologicznych, urzędów państwowych).
- Technika: Stosują logotypy, kolory i style komunikacji naśladujące oryginalne źródła.
- Cel: Zdobądź zaufanie ofiary, aby udostępniła swoje dane logowania lub inne poufne informacje

Tworzenie pilnych i emocjonalnych wiadomości

- Metoda: Wykorzystanie poczucia pilności lub strachu w celu zmuszenia ofiary do szybkiego działania.
- Technika: Wysyłanie wiadomości o domniemanym włamaniu na konto, zaległej płatności lub wyjątkowej okazji wymagającej natychmiastowej reakcji.
- Cel: Zwiększenie szansy, że ofiara będzie działać impulsywnie, bez dokładnego przemyślenia sprawy.

Phishing

CHARAKTERYSTYKA ZAGROŻENIA:

Korzystanie z fałszywych linków i załączników

- Metoda: Wysyłanie wiadomości z linkami do fałszywych stron internetowych lub załącznikami zawierającymi złośliwe oprogramowanie.
- Technika: Linki mogą wydawać się wiarygodne, ale prowadzą do fałszywych witryn, które zbierają dane logowania lub instalują złośliwe oprogramowanie na urządzeniu ofiary.
- Cel: przejęcie danych logowania, zainfekowanie urządzenia ofiary złośliwym oprogramowaniem lub próba wyłudzenia informacji.

Socjotechnika

- Metoda: Manipulowanie ofiarą poprzez stosowanie technik oszustwa psychologicznego.
- Technika: Korzystanie z publicznie dostępnych informacji, takich jak dane z mediów społecznościowych, w celu tworzenia spersonalizowanych wiadomości. Oszuści mogą również wykonywać połączenia telefoniczne, udając pracowników pomocy technicznej.
- Cel: Stworzenie fałszywego poczucia bezpieczeństwa i nakłonienie ofiary do ujawnienia poufnych informacji.

Phishing

KONSEKWENCJE:

Dlaczego phishing jest niebezpieczny? Konsekwencje udanego ataku phishingowego mogą być poważne - od utraty pieniędzy po kradzież tożsamości i zainfekowanie urządzenia złośliwym oprogramowaniem. Aby się chronić, ważne jest, aby je znać.

01 Podszywanie się pod zaufane źródła

- Kradzież tożsamości: Osoby starsze mogą nieświadomie udostępniać swoje dane osobowe, które następnie zostaną wykorzystane do zakładania fałszywych kont bankowych lub kredytowych na ich nazwisko.
- Straty finansowe: Udostępnienie danych logowania do konta bankowego może skutkować nieautoryzowanymi transakcjami i utratą oszczędności.

02 Tworzenie pilnych i emocjonalnych wiadomości

- Nieautoryzowane płatności: Seniorzy mogą szybko zareagować na fałszywe alarmy, podając swoje dane bankowe i dokonując niepotrzebnych przelewów.
- Utrata oszczędności: Pokusa szybkiego podejmowania decyzji może prowadzić do znacznych strat finansowych, zwłaszcza jeśli osoby starsze udostępnią oszustom dane swojej karty kredytowej.
- Większa podatność: Powtarzające się próby oszustw mogą sprawić, że seniorzy będą bardziej podatni na przyszłe ataki ze względu na stres i niepewność.

Phishing

KONSEKWENCJE:

03 Korzystanie z fałszywych linków i załączników

- Infekcja urządzenia: Złośliwe oprogramowanie może zainfekować komputer lub smartfon osoby starszej, powodując utratę kontroli nad urządzeniem i dostępu do poufnych informacji.
- Kradzież danych: Złośliwe oprogramowanie może przechwycić dane logowania, umożliwiając oszustom dostęp do kont bankowych i innych poufnych zasobów.
- Koszty naprawy: Usunięcie złośliwego oprogramowania i naprawa zainfekowanego urządzenia może wiązać się z wysokimi kosztami technicznymi, na które osoby starsze mogą nie być przygotowane.

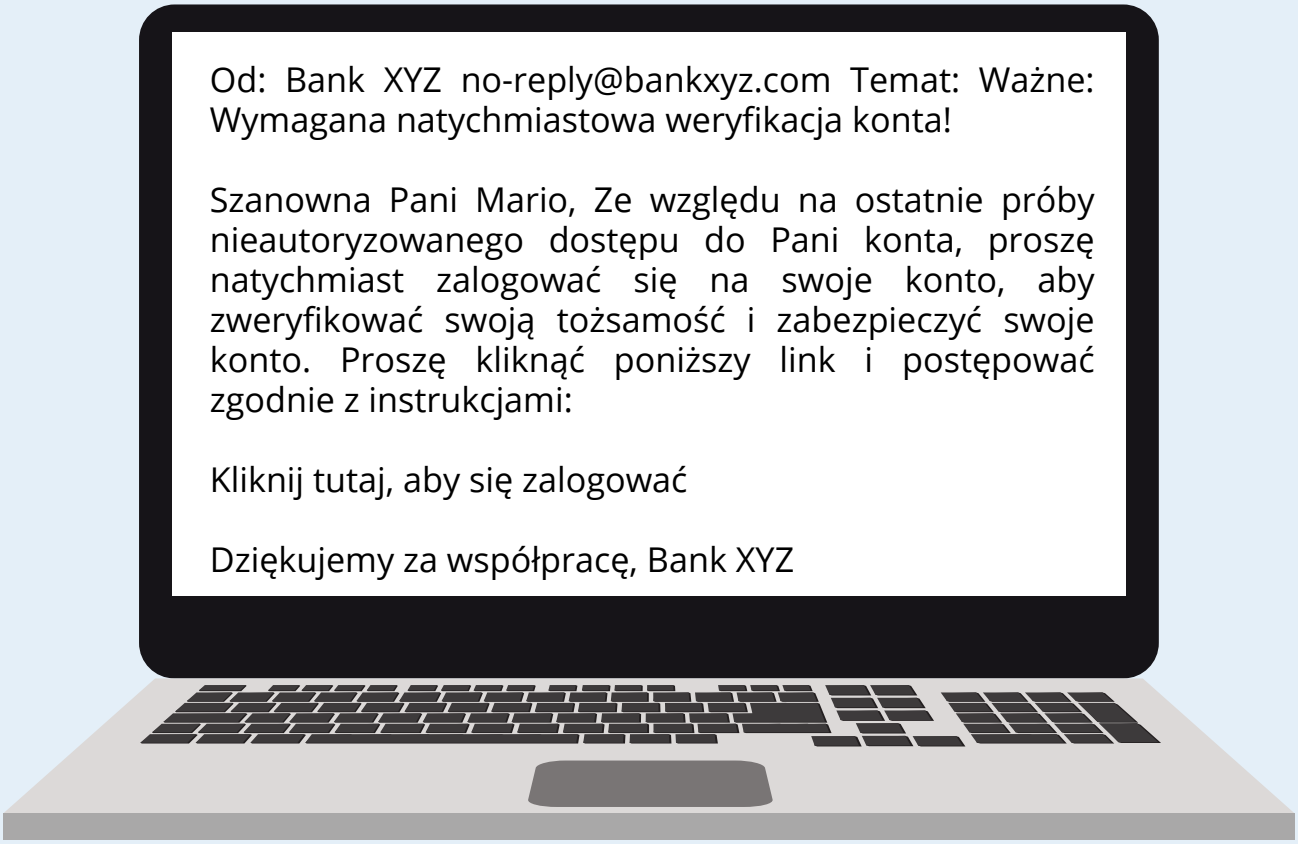
04 Socjotechnika

- Oszustwa telefoniczne: Seniorzy mogą zostać oszukani i podani przez telefon w celu uzyskania poufnych informacji, co może prowadzić do kradzieży tożsamości i strat finansowych.
- Utrata zaufania: Częste ataki socjotechniczne mogą prowadzić do braku zaufania do legalnych instytucji i ludzi, co utrudnia codzienne życie i zarządzanie finansami.
- Manipulacja emocjonalna: Takie psychologiczne efekty jak strach, stres i lęk mogą negatywnie wpływać na zdrowie psychiczne osób starszych.

Phishing

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Maria regularnie korzysta z Internetu, aby kontaktować się z rodziną, sprawdzać konta bankowe i czytać wiadomości. Pewnego dnia otrzymuje e-mail, który wydaje się pochodzić z jej banku.



Konsekwencje nierozpoznania zagrożenia:

KROK 1: Kliknięcie na link

Maria, zaniepokojona treścią wiadomości e-mail, klika na link, nie sprawdzając dokładnie jego autentyczności. Link prowadzi ją na stronę, która wygląda identycznie jak strona logowania do jej banku.

KROK 2: Podanie danych logowania

Maria wpisuje swoje dane logowania na fałszywej stronie internetowej, myśląc, że weryfikuje swoje konto.

Phishing

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Przykład Marii ilustruje powszechną metodę phishingu polegającą na podszywaniu się pod zaufane źródła. Przyjrzyjmy się konsekwencjom, które mogą wyniknąć z nierozpoznania tego zagrożenia przez Marię.

KROK 3: Dodatkowe załączniki

E-mail zawiera również załącznik. Maria pobiera załącznik zawierający złośliwe oprogramowanie. Po otwarciu pliku złośliwe oprogramowanie instaluje się na jej komputerze, umożliwiając oszustom zdalny dostęp do jej urządzenia.

KROK 4: Przechwytywanie danych i kradzież pieniędzy

Kiedy Maria kliknęła link, oszuści natychmiast przechwycili jej dane logowania i uzyskali dostęp do prawdziwego konta bankowego Marii.

KROK 5: Stres i niepokój

Maria jest załamana utratą oszczędności i boi się korzystać z bankowości internetowej i innych usług online w przyszłości.

KROK 6: Zainfekowanie urządzenia

Złośliwe oprogramowanie zainstalowane na komputerze Marii umożliwia oszustom monitorowanie jej aktywności w sieci, przechwytywanie danych logowania, a także potencjalne infekowanie innych plików.

Phishing

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Możesz uniknąć takich konsekwencji, stosując poniższe metody, aby chronić się przed oszustwami phishingowymi.

Sprawdzanie adresu e-mail nadawcy i linków:

Maria powinna dokładnie sprawdzić adres e-mail nadawcy oraz linki zawarte w wiadomości, zanim kliknie.

Działanie:

- Sprawdź adres e-mail: Upewnij się, że wiadomość e-mail pochodzi z prawdziwej domeny banku.

Konfigurowanie uwierzytelniania dwuskładnikowego (2FA):

Maria powinna włączyć uwierzytelnianie dwuskładnikowe (2FA) na swoim koncie bankowym, co dodaje dodatkową warstwę bezpieczeństwa. Nawet jeśli oszuści zdobędą Twoje hasło, będą potrzebować również drugiego elementu uwierzytelniania, takiego jak kod SMS.

Działanie:

- Aktywacja 2FA: Maria powinna skontaktować się ze swoim bankiem w celu włączenia 2FA.

Phishing

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Regularna aktualizacja oprogramowania antywirusowego i systemu operacyjnego:

Maria powinna zadbać o regularne aktualizacje oprogramowania antywirusowego i systemu operacyjnego, aby zapewnić sobie ochronę przed najnowszymi zagrożeniami związanymi ze złośliwym oprogramowaniem i phishingiem.

Działanie:

- Oprogramowanie antywirusowe: Maria powinna zainstalować oprogramowanie antywirusowe i dbać o jego aktualność. Należy pamiętać o jego regularnej aktualizacji.

Podejmując te środki ostrożności, Maria może zmniejszyć ryzyko stania się ofiarą phishingu, chroniąc swoje dane i finanse. Zawsze dokładnie sprawdzaj adres e-mail nadawcy i unikaj klikania linków lub załączników w nieoczekiwanych wiadomościach e-mail.

Złośliwe oprogramowanie i wirusy komputerowe

CHARAKTERYSTYKA ZAGROŻENIA:

Termin malware jest używany do opisywania złośliwych programów zaprojektowanych w celu uszkodzenia komputera lub wykonania na nim niepożądanych działań przez użytkownika. Wirus komputerowy jest jednym z najpoważniejszych zagrożeń, z jakimi borykają się użytkownicy komputerów. Malware jest w stanie wyrządzić ogromne szkody - od kradzieży danych po spowolnienie systemu i całkowite zniszczenie plików.

Typowe typy złośliwego oprogramowania:

Oprogramowanie wymuszające okup (Ransomware)

Rodzaj złośliwego oprogramowania, które blokuje dostęp do danych użytkownika poprzez ich szyfrowanie. Cyberprzestępca żąda okupu w zamian za klucz deszyfrujący, obiecując przywrócenie dostępu do danych. Jednak przestępcy często wycofują się z umowy, sprzedając poufne dane nawet po zapłaceniu okupu, a ofiary mogą ponownie stać się celem ataku.

Trojan

Rodzaj złośliwego oprogramowania, które podszywa się pod legalne oprogramowanie, aby zinfiltrować urządzenie użytkownika. Po zainstalowaniu otwierają dostęp do urządzenia, umożliwiając instalację innych rodzajów złośliwego oprogramowania, szpiegowanie użytkowników i kradzież poufnych informacji. Trojany często rozprzestrzeniają się za pomocą technik socjotechnicznych, takich jak phishing i podrabiane witryny, które zachęcają użytkownika do pobrania złośliwego pliku.

Złośliwe oprogramowanie i wirusy komputerowe

CHARAKTERYSTYKA ZAGROŻENIA:

Robaki

Rodzaj złośliwego oprogramowania podobnego do wirusów, ale nie wymagającego interakcji użytkownika do rozprzestrzeniania się. Wykorzystuje luki w urządzeniach instalacyjnych i replikacyjnych. Po zainfekowaniu urządzenia próbuje połączyć się z innymi urządzeniami w tej samej sieci i szuka dalszych luk, aby się na nie rozprzestrzenić.

Oprogramowanie szpiegujące (Spyware)

Oprogramowanie złośliwe, które instaluje się na urządzeniu ofiary w celu szpiegowania i zbierania poufnych informacji, takich jak dane uwierzytelniające i numery kart kredytowych. Oprogramowanie szpiegujące może być dołączone do innych programów lub możesz zainstalować je samodzielnie, klikając reklamę lub pobierając bezpłatne oprogramowanie z niewiarygodnych witryn. Po zainstalowaniu śledzi ono naciśnięcia klawiszy, historię przeglądania i korzysta z kamery i mikrofonu urządzenia.

Złośliwe oprogramowanie bezplikowe

Rodzaj złośliwego oprogramowania, które nie używa plików wykonywalnych zawierających złośliwy kod do infekowania urządzenia. Zamiast tego wprowadza zmiany w legalnych narzędziach systemowych urządzenia, umożliwiając wykonywanie złośliwych działań bez konieczności pobierania plików na dysk twardy. Złośliwy kod oprogramowania bezplikowego działa bezpośrednio w pamięci komputera, wykorzystując istniejące narzędzia systemowe do osiągnięcia swoich celów.

Złośliwe oprogramowanie i wirusy komputerowe

CHARAKTERYSTYKA ZAGROŻENIA:

Złośliwe oprogramowanie mobilne (Mobile malware)

Rodzaj złośliwego oprogramowania atakującego urządzenia mobilne, takie jak smartfony i tablety, w celu uzyskania dostępu do poufnych danych. Urządzenia bez odpowiednich środków bezpieczeństwa są podatne na tego typu ataki, ponieważ często brakuje im domyślnych mechanizmów obronnych wbudowanych w oryginalny system operacyjny.

Wirusy

Są to rodzaje złośliwego oprogramowania, które infekuje urządzenia i rozmnaża się, aby rozprzestrzeniać się na inne urządzenia. Zazwyczaj maskują się jako złośliwe pliki lub aplikacje instalowane przez ofiary. Atakujący często próbują przekonać użytkowników do pobrania tych plików, korzystając z ataków phishingowych. Gdy ofiara pobiera zainfekowany plik lub aplikację, wirus aktywuje się i zaczyna replikować na urządzeniu. Często zmienia pliki, aby uniknąć wykrycia i infekuje inne urządzenia. Wirus może kraść poufne dane, spowalniać urządzenie, zamrażać aplikacje oraz zmieniać i niszczyć pliki.

Złośliwe oprogramowanie i wirusy komputerowe

KONSEKWENCJE:

Konsekwencje zarażenia się złośliwym oprogramowaniem są bardzo poważne. Cyberprzestępcy kierują się chęcią zysku. Używają zainfekowanych urządzeń do przeprowadzania ataków, takich jak uzyskiwanie poświadczeń do usług bankowych, zbieranie danych osobowych w celu sprzedaży, sprzedawanie dostępu do zasobów komputerowych lub wymuszanie opłat od ofiar.

01 Oprogramowanie wymuszające okup (Ransomware)

Oprogramowanie może spowodować utratę dostępu do ważnych danych seniora, takich jak dokumenty finansowe lub zdjęcia rodzinne. Ponadto zapłacenie okupu nie gwarantuje odzyskania danych, co może prowadzić do dodatkowych strat finansowych.

02 Trojan

Oprogramowanie może spowodować kradzież poufnych informacji, takich jak hasła do kont bankowych lub numery kart kredytowych, narażając osoby starsze na ryzyko kradzieży tożsamości i strat finansowych.

03 Oprogramowanie szpiegujące

Oprogramowanie może służyć do podsłuchiwania rozmów osób starszych lub śledzenia ich aktywności w Internecie, co narusza ich prywatność i może doprowadzić do wykorzystania zebranych danych w celu szantażu lub oszustwa.

Złośliwe oprogramowanie i wirusy komputerowe

KONSEKWENCJE:

04 Robaki

Oprogramowanie może uszkodzić system operacyjny urządzenia osoby starszej lub przejąć nad nim kontrolę cyberprzestępcy. Może to uniemożliwić korzystanie z urządzenia lub doprowadzić do utraty ważnych danych.

05 Złośliwe oprogramowanie bezplikowe

Oprogramowanie może działać w tle, niezauważalnie zmieniając ustawienia urządzenia lub zużywając jego zasoby, co może prowadzić do spowolnienia działania urządzenia lub problemów z jego wydajnością.

06 Złośliwe oprogramowanie mobilne

Oprogramowanie może doprowadzić do utraty danych lub naruszenia prywatności osoby starszej poprzez dostęp do jej danych osobowych lub śledzenie jej lokalizacji.

07 Wirusy

Wirusy mogą kraść poufne dane, takie jak hasła, informacje finansowe lub dane osobowe, naruszając prywatność użytkowników. Mogą replikować się i rozprzestrzeniać na inne urządzenia w sieci, powodując dalsze infekcje i zwiększając skalę problemu.

Złośliwe oprogramowanie i wirusy komputerowe

— SPOSOBY OCHRONY Z HISTORIĄ W TLE

Aleksander przeglądał swoją pocztę. Zauważył pewne wiadomości, których się nie spodziewał i to go zaciekawiło. Kliknął na załącznik w tej wiadomości e-mail. Zauważył coś dziwnego. Coś zaczęło zmieniać pliki na jego komputerze, powodując znaczne zakłócenia w jego pracy. Co mogło się stać?

Przypadki podobne do Aleksandra są niestety dość powszechne. Kliknięcie podejrzanego załącznika e-mail może spowodować zainfekowanie komputera złośliwym oprogramowaniem. W rezultacie mogą wystąpić poważne zakłócenia w działaniu i bezpieczeństwie danych.

KROK 1: Kliknięcie załącznika do wiadomości e-mail

Aleksander przeglądał swoją pocztę elektroniczną i nieświadomie kliknął na załącznik w wiadomości.

KROK 2: Infekcja urządzenia

Kliknięcie fałszywego załącznika spowodowało zainfekowanie jego urządzenia wirusem.

KROK 3: Replikacja/rozmnażanie się wirusa

Złośliwy kod (załączony) zaczął szybko powielać się na komputerze Aleksandra, powodując zmiany w plikach i zakłócenia w jego pracy.

KROK 4: Możliwość kradzieży danych

Ponadto wirus mógł mieć zdolność kradzieży poufnych danych z urządzenia Alexandra, co mogłoby prowadzić do dalszych problemów z bezpieczeństwem i prywatnością.

Złośliwe oprogramowanie i wirusy komputerowe

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Możesz uniknąć takich konsekwencji, stosując opisane poniżej metody ochrony przed złośliwym oprogramowaniem.

Regularnie aktualizuj oprogramowanie za każdym razem, gdy pojawią się nowe komunikaty o podejrzanych zagrożeniach. Zmniejszy to ryzyko infekcji złośliwym oprogramowaniem wykorzystującym te luki w zabezpieczeniach.

Zachowaj ostrożność otwierając załączniki do wiadomości e-mail i pobierając pliki, zwłaszcza jeśli pochodzą one od nieznanych nadawców lub wydają się podejrzane.

Unikaj klikania podejrzanych linków i wyskakujących okienek, ponieważ mogą one prowadzić do infekcji lub przechwytywania danych.

Złośliwe oprogramowanie i wirusy komputerowe

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Używaj publicznych sieci Wi-Fi ostrożnie, ponieważ są podatne na ataki; rozważ użycie usługi VPN, aby zabezpieczyć połączenie internetowe. Korzystając z VPN, Twoje dane są szyfrowane podczas przesyłania przez sieci publiczne, co oznacza, że nikt nie może zobaczyć Twojego adresu IP ani przechwycić danych, które wysyłasz lub odbierasz z urządzenia.

Używaj programów antywirusowych i antymalware, które pomagają zapobiegać infekcjom i usuwać złośliwe oprogramowanie, w tym spyware i adware. Antywirusy skupiają się głównie na wykrywaniu i eliminowaniu wirusów, podczas gdy antimalware zajmuje się szerokim spektrum złośliwego oprogramowania, w tym złośliwymi aplikacjami, które nie są klasyfikowane jako wirusy.

Stosując się do tych zaleceń, Alexander i inni użytkownicy Internetu mogą uniknąć zagrożeń ze strony złośliwego oprogramowania. Pamiętaj, aby nie podejmować decyzji zbyt szybko i zawsze działać ostrożnie w wirtualnym świecie.

Więcej informacji

ATAK ZA POŚREDNICTWEM SIECI WI-FI (PRYWATNYCH I PUBLICZNYCH)

- 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/na popularne-rodzaje-atakow-na-wifi/

ATAKI E-MAILOWE

- www.powerdmarc.com/pl/what-are-email-based-atacks/
- 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/

ATAKI NA SŁABE HASŁA

- 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

PHISHING

- 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/

ZŁOŚLIWE OPROGRAMOWANIE I WIRUSY KOMPUTEROWE

- 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/

ROZDZIAŁ 2. OSZUSTWA FINANSOWE I INWESTYCYJNE

W dzisiejszym świecie seniorzy coraz częściej padają ofiarą oszustw finansowych, które przybierają różne formy i są nieustannie udoskonalane przez przestępców. Niniejszy rozdział ma na celu omówienie najczęstszych rodzajów oszustw, aby pomóc seniorom rozpoznawać zagrożenia i chronić swoje oszczędności.

Do najbardziej rozpowszechnionych metod należą manipulacje finansowe i inwestycyjne, oparte na fałszywych obietnicach szybkich zysków oraz oszustwa charytatywne wykorzystujące empatię seniorów. Innym niebezpieczeństwem jest obietnica dużych wygranych poprzez fałszywe nagrody i loterie, które wymagają zapłaty, aby je odebrać.

Oszustwa związane z walutami cyfrowymi, takimi jak Bitcoin, stają się coraz powszechniejsze, oferując nowe możliwości działalności przestępczej. Ważne jest również, aby wspomnieć o oszustwach nigeryjskich — międzynarodowych schematach oszustw opartych na fikcyjnych transakcjach.

Zrozumienie tych zagrożeń jest kluczowe dla seniorów, aby świadomie chronić swoje finanse.

Manipulacje finansowe i inwestycyjne

CHARAKTERYSTYKA ZAGROŻENIA:

Manipulacja finansowa i inwestycyjna odnosi się do oszukańczych praktyk mających na celu przekonanie osób do inwestowania swoich pieniędzy w oszukańcze lub nieodpowiednie schematy. Schematy te często obiecują wysokie zyski, ale ostatecznie skutkują stratami finansowymi dla inwestorów.

Rodzaje manipulacji w inwestycjach finansowych:

Fałszywe obietnice wysokich zysków

Oszuści stosują perswazyjne taktyki, aby obiecać inwestorom niezwykle wysokie zwroty z inwestycji. Te obietnice mogą wydawać się zbyt piękne, aby mogły być prawdziwe i często są skierowane do seniorów, którzy szukają sposobów na uzupełnienie dochodów emerytalnych.

Presja na szybką inwestycję

Oszuści często stosują taktykę sprzedaży pod presją, aby wywierać presję na osoby, aby podejmowały szybkie decyzje inwestycyjne bez dokładnego zbadania lub zrozumienia produktów inwestycyjnych. Mogą tworzyć poczucie pilności, twierdząc, że są to oferty ograniczone czasowo lub podkreślając strach przed przegapieniem lukratywnych okazji.

Skomplikowane i niejasne produkty inwestycyjne

Oszuści mogą polecać skomplikowane lub niejasne produkty inwestycyjne, które są trudne do zrozumienia dla inwestorów, zwłaszcza seniorów. Produkty te mogą wiązać się z wysokimi opłatami, ukrytym ryzykiem lub brakiem przejrzystości co do sposobu wykorzystania zainwestowanych środków.

Manipulacje finansowe i inwestycyjne

KONSEKWENCJE:

Manipulacje finansowe i inwestycyjne mogą mieć poważne negatywne skutki, takie jak:

01 Konsekwencje finansowe

Padnięcie ofiarą manipulacji finansowej może skutkować utratą ciężko zarobionych oszczędności i inwestycji. Możesz znaleźć się w sytuacji, w której będziesz mieć znacznie mniej pieniędzy niż się spodziewałeś, co wpłynie na Twoją zdolność do pokrycia codziennych wydatków i cieszenia się emeryturą.

02 Wpływ emocjonalny

Oszukiwanie przez oszustów finansowych może prowadzić do poczucia zdrady i rozczarowania. Możesz czuć się zakłopotany lub zawstydzony, że dałeś się nabrać na oszustwo, co wpłynie na twoją samoocenę i pewność siebie.

03 Konsekwencje osobiste

Padnięcie ofiarą manipulacji finansowej może nadwyrężyć zaufanie do innych, sprawiając, że będziesz bardziej ostrożny i sceptyczny w stosunku do przyszłych możliwości inwestycyjnych. Ta utrata zaufania może nadwyrężyć relacje i utrudnić Ci szukanie porady finansowej lub wsparcia.

Manipulacje finansowe i inwestycyjne

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Sofia otrzymuje e-mail od nieznanego nadawcy, który twierdzi, że oferuje lukratywną okazję inwestycyjną w nową firmę technologiczną. E-mail obiecuje wysokie zyski i namawia Sofię do szybkiego działania, aby zapewnić sobie miejsce w inwestycji.
Jednak Sofia pamięta, że przeczytała radę, by zachować ostrożność w przypadku niechcianych e-maili obiecujących duże zyski.

Historia Sofii niestety nie jest jedynym przypadkiem, ale pokazuje, jak ważne jest chronienie seniorów przed manipulacją finansową. Seniorzy powinni być świadomi różnych form manipulacji, z którymi mogą się zetknąć, i znać metody ich unikania.

KROK 1: Weryfikacja

Sofia postanawia zweryfikować autentyczność możliwości inwestycyjnej przed podjęciem jakichkolwiek działań.

KROK 2: Konsultacja

Sofia zwraca się o radę do zaufanego członka rodziny, który ma doświadczenie w finansach.

KROK 3: Potwierdzenie

Nadal sceptycznie nastawiona Sofia decyduje się skontaktować bezpośrednio ze spółką, aby zweryfikować możliwość inwestycji.

KROK 4: Raport

Sofia postanawia zgłosić podejrzany e-mail odpowiednim władzom.

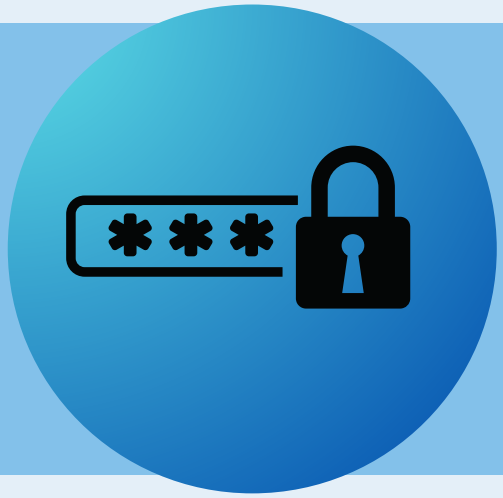
Manipulacje finansowe i inwestycyjne

SPOSOBY OCHRONY:

Ochrona siebie przed manipulacją finansową i inwestycyjną jest kluczowa dla ochrony ciężko zarobionych pieniędzy. Oto kilka prostych kroków, które możesz podjąć.

Uważaj na e-maile:

Jeśli otrzymasz niespodziewanego maila obiecującego duże zyski lub pilne transakcje finansowe, warto zachować ostrożność. Poświęć chwilę na sprawdzenie adresu e-mail nadawcy pod kątem dziwnych znaków. A jeśli coś wydaje się nie tak, nie klikaj żadnych linków ani nie pobieraj żadnych załączników.



Wzmocnij swoje hasła:

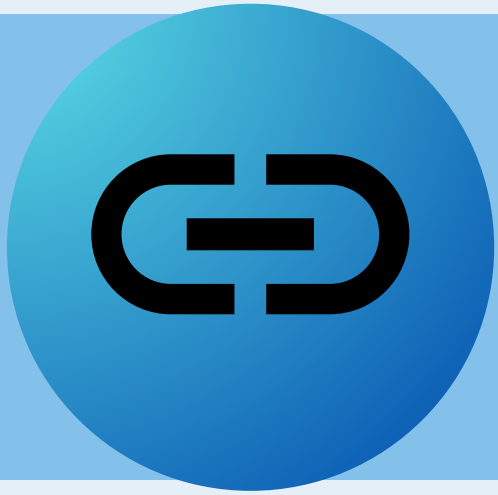
Podczas ustawiania haseł do kont online upewnij się, że są silne i niepowtarzalne. Używaj kombinacji liter, cyfr i symboli i unikaj używania łatwych do odgadnięcia informacji, takich jak data urodzenia lub imię zwierzaka.

Manipulacje finansowe i inwestycyjne

SPOSOBY OCHRONY:

Uważaj na podejrzane linki i strony internetowe:

Jeśli trafisz na stronę internetową, która wydaje się podejrzana lub nieznana, nie udostępniaj żadnych danych osobowych ani finansowych. Szukaj „https://” i symbolu kłódki na pasku adresu bezpiecznych stron internetowych.



Bądź na bieżąco z bezpieczeństwem w sieci:

Istnieje wiele źródeł i materiałów edukacyjnych, które pomogą Ci dowiedzieć się więcej na temat typowych oszustw wymierzonych w osoby starsze.

Na koniec, nie bój się prosić o pomoc:

Jeśli nie jesteś pewien decyzji finansowej lub podejrzewasz, że padłeś ofiarą oszustwa, zwróć się o poradę i wsparcie do członków rodziny, przyjaciół lub zaufanych specjalistów. A jeśli uważasz, że padłeś ofiarą manipulacji finansowej, natychmiast zgłoś to odpowiednim organom lub urzędom ochrony konsumentów w Twoim mieście.

Pozorny altruizm: oszustwa charytatywne

CHARAKTERYSTYKA ZAGROŻENIA:

Oszustwa charytatywne w Internecie często wykorzystują hojność i dobrą wolę osób fizycznych, szczególnie w przypadku seniorów w wieku 65 lat i starszych. Oszustwa te mogą obejmować fałszywe organizacje charytatywne podszywające się pod legalne organizacje, proszące o darowizny na rzekome cele, takie jak pomoc w przypadku katastrof, badania medyczne lub pomoc osobom mniej szczęśliwym.

Rodzaje manipulacji w oszustwach charytatywnych:

Taktyka wysokiego nacisku

Oszuści mogą używać języka perswazji lub odwoływać się do emocji, aby skłonić ofiary do szybkiego przekazania darowizny.

Podszywanie się pod legalne organizacje charytatywne

Oszuści mogą tworzyć fałszywe strony internetowe lub wysyłać wiadomości e-mail imitujące marki znanych organizacji charytatywnych, aby oszukać swoje ofiary.

Fałszywe historie i świadectwa

Oszuści mogą wymyślać poruszające historie lub podawać fałszywe świadectwa, aby wzbudzić współczucie i zachęcić do darowizn

Brak przejrzystości

Fałszywe organizacje charytatywne często podają niejasne lub wprowadzające w błąd informacje na temat swojej misji, celów i sposobu wykorzystania przekazanych środków.

Pozorny altruizm: oszustwa charytatywne

KONSEKWENCJE:

Stanie się ofiarą oszustw charytatywnych może być dla seniorów bardzo trudne, zarówno pod względem finansowym, jak i emocjonalnym.

01 Strata finansowa

Padnięcie ofiarą oszustwa charytatywnego może skutkować utratą ciężko zarobionych oszczędności i inwestycji. Możesz znaleźć się w sytuacji, w której będziesz mieć znacznie mniej pieniędzy niż się spodziewałeś, co wpłynie na Twoją zdolność do pokrycia codziennych wydatków i cieszenia się emeryturą.

02 Stres emocjonalny

Manipulacja oszustwem charytatywnym może sprawić, że poczujesz się zdradzony, winny i zawstydzony, że stałeś się ofiarą tego oszustwa.

03 Problemy z zaufaniem

Może to także utrudnić zaufanie prawdziwym organizacjom charytatywnym w przyszłości, ponieważ trudniej będzie odróżnić prawdziwe apele od fałszywych.

Pozorny altruizm: oszustwa charytatywne

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Alicja otrzymuje e-mail rzekomo od organizacji charytatywnej, która prosi o datki na pomoc dzieciom w potrzebie. E-mail zawiera emocjonalne historie i zdjęcia dzieci rzekomo korzystających z pracy organizacji charytatywnej.
Alicja pamięta jednak radę, jaką przeczytała, żeby zachować podejrzliwość w stosunku do e-maili, w których obiecywano wpłaty pieniędzy na cele charytatywne.

Historia Alice niestety nie jest jedynym przypadkiem, ale pokazuje, jak ważne jest chronienie seniorów przed oszustwami charytatywnymi. Seniorzy powinni być świadomi różnych form oszustw, na które mogą się natknąć, i znać metody ich unikania

Krok 1: Zbadaj organizację charytatywną

Przed dokonaniem darowizny Alicja sprawdza status rejestracji organizacji charytatywnej i opinie na jej temat na renomowanych stronach internetowych

Krok 2: Zachowaj ostrożność w przypadku niezamawianych próśb

Alicja zignorowała ten niespodziewany e-mail z prośbą o datki.

Krok 3: Nigdy nie udostępniaj danych osobowych

Alicja unikała udostępniania poufnych informacji, takich jak numer ubezpieczenia społecznego czy dane bankowe, nieznanym lub niezweryfikowanym organizacjom charytatywnym.

Krok 4: Przekaż darowiznę bezpośrednio

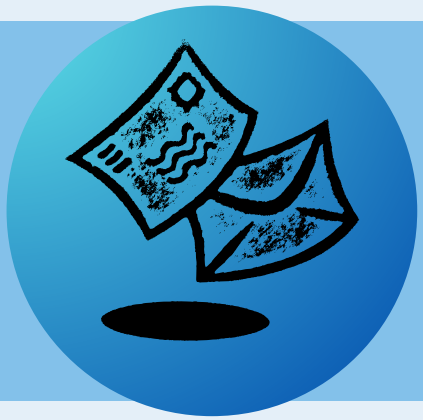
Jeśli Alicja chce przekazać darowiznę, zamiast klikać w linki w wiadomościach e-mail lub odpowiadać na telefony, może dokonać darowizny bezpośrednio za pośrednictwem oficjalnej strony internetowej organizacji charytatywnej.

Pozorny altruizm: oszustwa charytatywne

SPOSOBY OCHRONY:

Ochrona siebie przed oszustwami charytatywnymi i ich konsekwencjami jest bardzo ważna. Oto kilka prostych kroków, które możesz podjąć, aby uchronić się przed padnięciem ofiarą oszustwa charytatywnego:

Zbadaj organizacje charytatywne, sprawdzając ich status i opinie na legalnych stronach internetowych poświęconych tym organizacjom.



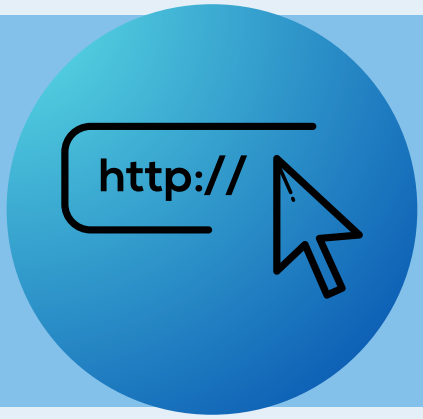
Zachowaj ostrożność w przypadku nieoczekiwanych próśb o darowizny otrzymywanych w wiadomościach e-mail, telefonicznie lub za pośrednictwem mediów społecznościowych, ponieważ prawdziwe organizacje charytatywne zazwyczaj nie stosują taktyk wywierania presji.

Nigdy nie udostępniaj danych osobowych, takich jak numer ubezpieczenia społecznego czy dane bankowe, nieznanym organizacjom charytatywnym.

Pozorny altruizm: oszustwo charytatywne

SPOSOBY OCHRONY:

Możesz dokonać darowizny bezpośrednio za pośrednictwem oficjalnej strony internetowej organizacji charytatywnej lub wysyłając czek na jej zweryfikowany adres.



Bądź na bieżąco z najczęstszymi oszustwami związanymi z działalnością charytatywną i naucz się rozpoznawać sygnały ostrzegawcze.

Nie wahaj się zwrócić o pomoc do rodziny, przyjaciół lub doradców finansowych, gdy oceniasz wnioski o wsparcie charytatywne lub gdy podejrzewasz oszustwo.

Kuszące iluzje: fikcyjne nagrody i konkursy

CHARAKTERYSTYKA ZAGROŻENIA:

Oszustwa oparte na fałszywych nagrodach, loteriach i konkursach są zwodnicze i celowo wykorzystują chęć wygranej u ludzi, przekonując ich, że wygrali duże nagrody. Oszuści namawiają ofiary do wypłacania im fałszywych wygranych, ale ostatecznie kradną pieniądze ofiary.

Rodzaje manipulacji w fikcyjnych nagrodach i loteriach:

Personifikacja

Oszuści często podszywają się pod przedstawicieli renomowanych firm lub loterii zarządzanych przez rządy (zwłaszcza zagraniczne) i stosują manipulacyjne taktyki, aby wykorzystać zaufanie swoich ofiar, mając nadzieję na wykorzystanie ich pragnienia bezpieczeństwa finansowego.

Elitaryzm

Oszuści próbują przekonać swoje ofiary, że zostały wybrane jako jedyni lub nieliczni szczęśliwcy, aby stworzyć im poczucie wyjątkowości i wyjątkowej okazji.

Nierealne obietnice

Oszuści obiecują nierealne kwoty nagród pieniężnych, luksusowe produkty itp., które są zbyt dobre, aby mogły być prawdziwe, stosując przy tym techniki wywierania presji, aby skłonić ofiary do natychmiastowej i pewnej reakcji.

Kuszące iluzje: fikcyjne nagrody i konkursy

KONSEKWENCJE:

Konsekwencje oszustw polegających na „kuszeniu iluzji” są różne i często długotrwałe.

01 Konsekwencje finansowe

Jedną z najgorszych konsekwencji takich oszustw jest katastrofa finansowa dla ofiar, a większość ofiar często ponosi znaczne straty finansowe. Ofiary mogą stracić oszczędności całego życia, popaść w nadmierne zadłużenie, a nawet zbankrutować. Wychodzenie z takich sytuacji finansowych może trwać latami.

02 Konsekwencje emocjonalne

Ofiary oszustw często doświadczają głębokiego cierpienia emocjonalnego i zmagają się z uczuciami zdrady, naruszenia, wstydu i winy. Emocjonalne zamieszanie spowodowane oszustwem i oszustwem może prowadzić do lęku, depresji, a nawet zespołu stresu pourazowego (PTSD), a także może wpływać na zdrowie fizyczne.

03 Konsekwencje prawne

W przypadku oszustw, w których ofiary są nakłaniane do przyjęcia fałszywych „czeków z nagrodą”, oprócz strat finansowych mogą one również ponieść konsekwencje prawne, w tym zarzuty prania pieniędzy i fałszerstwa.

Kuszące iluzje: fikcyjne nagrody i konkursy

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Greta otrzymała niespodziewaną wiadomość SMS informującą ją, że wygrała główną nagrodę w zagranicznej loterii i powinna natychmiast uiścić z góry „opłatę administracyjną", aby odebrać nagrodę pieniężną.
W wiadomości wyraźnie zaznaczyła, że nie wolno jej nikomu udostępniać informacji o wygranej na loterii ani o procedurze odbioru nagrody.

Niestety dla oszusta...

Greta niedawno uczestniczyła w kursie cyberbezpieczeństwa, w ramach którego odbywały się sesje na temat oszustw internetowych.

KROK 1: Rozpoznawanie sygnałów ostrzegawczych

Greta natychmiast wykryła oznaki oszustwa: nieoczekiwana wiadomość, wygrana na loterii (na którą nie kupiła losu) i prośba o zapłatę z góry.

KROK 2: Identyfikacja innych strategii oszustw

Greta zrozumiała, że polecenie, aby nie dzielić się szczegółami swoich wygranych na loterii z innymi, było taktyką mającą na celu jej izolację i ułatwienie jej padnięcia ofiarą oszustwa.

KROK 3: Unikanie angażowania się

Greta nie odpowiedziała na wiadomość tekstową, chroniąc w ten sposób swoje dane osobowe i unikając strat finansowych.

KROK 4: Raportowanie

Greta natychmiast powiadomiła swoją rodzinę, znajomych i odpowiednie władze o próbie oszustwa i udostępniła tę informację w mediach społecznościowych.

Kuszące iluzje: fikcyjne nagrody i konkursy

SPOSOBY OCHRONY:

Jeśli natkniesz się na próbę oszustwa typu „Kusząca iluzja”, pierwszą rzeczą, o której należy pamiętać, jest to, że nie ma darmowych pieniędzy i miej na uwadze znane powiedzenie: „Jeśli coś wygląda zbyt dobrze, aby było prawdziwe, prawdopodobnie takie nie jest”. Oto kilka dodatkowych wskazówek na wypadek, gdybyś znalazł się w takiej sytuacji.

Użyj zdrowego rozsądku:

Oprzyj się pokusie szybkiej reakcji na nieoczekiwane powiadomienia o nagrodach, które otrzymałeś e-mailem, w mediach społecznościowych lub SMS-em!

Zanim podejmiesz jakiekolwiek działania, zastanów się, czy kiedykolwiek brałeś udział w jakimś konkursie lub loterii.

Sprawdź legalność:

Sprawdź stronę internetową lub nadawcę powiadomienia innymi kanałami.

Sprawdź wiarygodność firmy w Internecie lub skonsultuj się z rodziną lub znajomymi!

Nie klikaj ani nie naciskaj linków w powiadomieniach, zwłaszcza jeśli wyglądają podejrzanie!

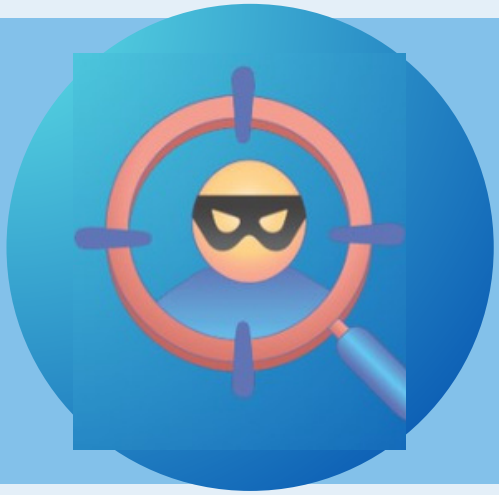
Kuszące iluzje: fikcyjne nagrody i konkursy

SPOSOBY OCHRONY:

Sprawdź szczegóły:

Sprawdź dokładnie wszystkie informacje, które otrzymałeś w powiadomieniu.

Należy zachować ostrożność w przypadku niejasnych lub nietypowych próśb, takich jak prośby o podanie danych osobowych, informacji finansowych lub o zapłatę z góry!



Pamiętaj:

Nigdy nie wysyłaj pieniędzy ani nie płać opłat za odbiór nagrody/pieniędzy w związku z nieoczekiwanym powiadomieniem o wygranej!

Legalne loterie nie wymagają żadnej płatności za uczestnictwo lub odebranie nagrody, natomiast udział w loteriach wiąże się z koniecznością zakupu losu.

Kuszące iluzje: fikcyjne nagrody i konkursy

SPOSOBY OCHRONY:

Jeśli ujawniłeś swoje dane osobowe lub finansowe oszustowi, powinieneś natychmiast zmienić hasła do swojego konta e-mail i wszystkich innych kont. Zmień również kody PIN do swoich kont bankowych, a jeśli korzystasz z bankowości internetowej, nie zapomnij zmienić hasła do bankowości internetowej.

Stosuj silne hasła, składające się z kombinacji wielkich i małych liter, cyfr oraz znaków specjalnych!

Jeśli otworzyłeś podejrzany link i udostępniłeś swoje dane finansowe lub osobowe albo poniosłeś stratę, natychmiast zgłoś to odpowiednim organom w swoim kraju!

Oszustwa związane z walutami cyfrowymi

CHARAKTERYSTYKA ZAGROŻENIA:

Oszustwa kryptowalutowe odnoszą się do wszelkich oszukańczych działań związanych z walutami cyfrowymi, takimi jak Bitcoin. Mogą przybierać różne formy, w tym oszustwa typu "initial coin offerings" (ICO), schematy Ponziego i oszukańcze okazje inwestycyjne. Te oszustwa zazwyczaj obiecują wysokie zyski, aby zwabić ofiary, które następnie tracą swoje inwestycje, gdy oszuści znikają z funduszami. Seniorzy są szczególnie podatni na tego typu oszustwa ze względu na ich nieznajomość technologii cyfrowych i Internetu. Oszuści często wykorzystują zaufanie i bezpieczeństwo finansowe seniorów, co sprawia, że konieczne jest podnoszenie świadomości i zapewnianie edukacji w celu ochrony ich przed takimi oszustwami.

Rodzaje oszustw związanych z kryptowalutami:

Oszustwa związane z początkowymi ofertami monet (ICO)

Tego typu oszustwa mają miejsce na etapie pozyskiwania funduszy na nowe kryptowaluty. Deweloperzy przedstawiają obiecującą nową walutę cyfrową, często ze szczegółowym dokumentem informacyjnym i obietnicami wysokiego zwrotu. Niestety, gdy zbierają wystarczającą ilość funduszy od inwestorów, ci deweloperzy znikają bez śladu, pozostawiając inwestorów z bezwartościowymi tokenami.

Schematy Ponziego

Te schematy obiecują wysokie, niskie ryzyko zwrotów. Jednak zwroty są wypłacane przy użyciu funduszy od nowych inwestorów, a nie z zysków. Schemat upada, gdy nie ma wystarczająco dużo nowych inwestorów, powodując znaczne straty dla ostatnich inwestorów.

Oszustwa związane z fałszywymi portfelami

Ten rodzaj oszustwa obejmuje aplikacje lub oprogramowanie, które twierdzą, że bezpiecznie przechowują kryptowaluty. Te portfele często mają profesjonalnie wyglądające interfejsy i mogą nawet naśladować legalne portfele. Jednak w rzeczywistości są zaprojektowane tak, aby wyprowadzać cyfrowe waluty. Gdy użytkownik zdeponuje swoje kryptowaluty w tych fałszywych portfelach, oszuści uzyskują do nich dostęp, co często skutkuje całkowitą utratą cyfrowych aktywów użytkownika.

Oszustwa związane z walutami cyfrowymi

KONSEKWENCJE:

Manipulacje finansowe i inwestycyjne mogą mieć poważne negatywne skutki, takie jak:

01 Strata finansowa

Najbardziej bezpośrednią i widoczną konsekwencją oszustwa kryptowalutowego jest strata finansowa. Ofiary często tracą całą inwestycję, co może być druzgocące, zwłaszcza jeśli zainwestowały dużą część swoich oszczędności.

02 Utrata zaufania

Ofiary oszustw kryptowalutowych często tracą zaufanie do walut cyfrowych i mogą wahać się przed inwestowaniem lub uczestnictwem w gospodarce cyfrowej w przyszłości. Może to utrudniać wzrost i akceptację kryptowalut.

03 Konsekwencje prawne

W niektórych przypadkach uczestnicy oszukańczych schematów, nawet nieświadomie, mogą ponieść konsekwencje prawne. Może to obejmować dochodzenie organów regulacyjnych i potencjalne zarzuty, jeśli nieświadomie pomogli ułatwić oszustwo.

Oszustwa związane z walutami cyfrowymi

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Pewnego dnia Helen otrzymała e-mail. Było to zaproszenie do zainwestowania w nową kryptowalutę, która obiecywała znaczne zyski. Zaintrygowana i chętna do rozbudowy swojego cyfrowego portfolio, postanowiła to zbadać.

E-mail pochodził od firmy o nazwie „CryptoGold", a ich strona internetowa była imponująca, pełna rekomendacji zadowolonych inwestorów i obietnic wysokich zysków. Okazja wydawała się zbyt dobra, aby ją przepuścić, więc postanowiła zainwestować niewielką część swoich oszczędności.

Dni zamieniły się w tygodnie, a Helen z niecierpliwością sprawdzała swój portfel internetowy każdego dnia, mając nadzieję, że jej inwestycja wzrośnie. Zamiast tego zauważyła, że jej inwestycja maleje. Zdezorientowana i zmartwiona, próbowała skontaktować się z „CryptoGold". Jednak wszystkie jej e-maile wracały, a niegdyś imponująca strona internetowa była teraz niedostępna.

Historia Hellen podkreśla potrzebę ochrony seniorów przed oszustwami kryptowalutowymi poprzez podnoszenie świadomości i edukację. Seniorzy mogą być narażeni z powodu cyfrowej nieznajomości, dlatego muszą zrozumieć ryzyko, oznaki oszustw i znaczenie sceptycyzmu wobec obietnic o wysokiej stopie zwrotu. Sieci wsparcia są również kluczowe dla bezpiecznej nawigacji cyfrowej.

KROK 1: Zbadaj firmę

Hellen powinna była dokładnie zbadać „CryptoGold" przed zainwestowaniem. Zamiast być pod wrażeniem strony internetowej i opinii, powinna sprawdzić, czy firma jest zarejestrowana i poszukać recenzji lub ostrzeżeń od innych użytkowników.

KROK 2: Zweryfikuj komunikację

Hellen otrzymała niezamawianą wiadomość e-mail i zaufała jej bez weryfikacji. Powinna była zachować ostrożność i zweryfikować tożsamość nadawcy, sprawdzając ją w zaufanych źródłach, takich jak oficjalne dane kontaktowe firmy lub znane fora kryptowalutowe.

KROK 3: Unikaj natychmiastowych decyzji

Hellen szybko zdecydowała się zainwestować, nie poświęcając czasu na pełne zrozumienie warunków i ryzyka. Powinna była unikać pochopnych decyzji inwestycyjnych i zasięgnąć porady u osób posiadających wiedzę lub doradców finansowych.

KROK 4: Regularnie monitoruj inwestycje

Hellen nie zauważyła żadnych natychmiastowych oznak oszustwa i nadal liczyła na pozytywne zwroty. Powinna była regularnie monitorować swoje inwestycje i natychmiast zgłaszać wszelkie nietypowe działania lub brak przejrzystości w celu dalszego zbadania.

Oszustwa związane z walutami cyfrowymi

SPOSOBY OCHRONY:

Ochrona przed oszustwami kryptowalutowymi jest kluczowa, zwłaszcza dla seniorów, ponieważ mogą być oni szczególnie podatni z powodu nieznajomości technologii cyfrowych. Oszuści często obierają sobie za cel seniorów, obiecując im wysokie zyski, wykorzystując ich zaufanie i bezpieczeństwo finansowe. Stanie się ofiarą tych oszustw może skutkować znacznymi stratami finansowymi, utratą zaufania do innowacji cyfrowych i potencjalnymi konsekwencjami prawnymi. Kształcenie się, przeprowadzanie dogłębnych badań i utrzymywanie zdrowego sceptycyzmu wobec ofert zbyt dobrych, aby były prawdziwe, to niezbędne kroki w celu zabezpieczenia swoich aktywów i zapewnienia sobie dobrobytu finansowego.

Edukacja:

Zrozumienie, jak działają kryptowaluty, to pierwszy krok do uniknięcia oszustwa. Obejmuje to zrozumienie technologii, która za nimi stoi, sposobu działania transakcji oraz bezpiecznego przechowywania i ochrony aktywów cyfrowych.

Badania:

Przed zainwestowaniem w jakąkolwiek kryptowalutę dokładnie zbadaj walutę cyfrową, zespół, który za nią stoi, i przeczytaj wszelkie dostępne oficjalne dokumenty. Uważaj na nowe kryptowaluty, które obiecują wysokie zyski przy niewielkim ryzyku.

Oszustwa związane z walutami cyfrowymi

SPOSOBY OCHRONY:

Zabezpiecz swój portfel:

Chroń swoje aktywa cyfrowe, używając bezpiecznego portfela. Może to być portfel sprzętowy, który przechowuje walutę offline lub renomowany portfel online z silnymi środkami bezpieczeństwa. Zawsze włączaj uwierzytelnianie dwuskładnikowe, jeśli jest dostępne.

Bądź sceptyczny:

Bądź sceptyczny wobec każdej inwestycji, która obiecuje wysokie zyski przy niewielkim ryzyku lub jego braku. Często są zbyt dobre, aby mogły być prawdziwe. Pamiętaj, że legalne inwestycje zazwyczaj nie gwarantują zysków i zawsze wiążą się z pewnym poziomem ryzyka.

Zgłoś podejrzaną aktywność:

Jeśli natkniesz się na potencjalne oszustwo kryptowalutowe, zgłoś je lokalnym władzom i wszelkim odpowiednim platformom internetowym. To nie tylko pomoże chronić Ciebie, ale także pomoże ostrzec i chronić innych.

Międzynarodowe oszustwa finansowe

CHARAKTERYSTYKA ZAGROŻENIA:

Oszustwo 419, znane również jako oszustwo nigeryjskie, to znane oszustwo polegające na pobieraniu zaliczki. Ma ono swój początek w Nigerii. Trwa od początków istnienia Internetu i stało się jednym z najbardziej rozpowszechnionych oszustw na świecie.

Rodzaje manipulacji w oszustwie 419:

Personifikacja *(wariant 1)*

Jeśli w temacie wiadomości znajduje się słowo „Pozdrowienia", powita Cię bogaty nigeryjski książę (a może nawet nigeryjski astronauta), bogaty prawnik lub biznesmen i zaoferuje Ci dużą sumę pieniędzy za pomoc w przelaniu pieniędzy z Nigerii (lub umożliwienie mu dostępu do konta) w zamian za niewielką zaliczkę pokrywającą rzekome koszty transakcji.

Personifikacja *(wariant 2)*

Jeśli w temacie wiadomości znajduje się słowo „Pozdrowienia", zostaniesz powitany przez osobę, która zmaga się z trudną sytuacją życiową, taką jak porwanie dzieci tej osoby; lub osobę, która z powodu sytuacji politycznej stała się zbiegiem lub niewinnym więźniem itp. Jednak wszyscy oni mają długą i smutną historię o tym, dlaczego nie mogą odebrać swoich pieniędzy, więc proszą o Twoją pomoc.

Międzynarodowe oszustwa finansowe

Gra na ludzkich emocjach

Za nigeryjskimi oszustwami stoją profesjonalni oszuści, którzy stosują systematyczne podejście i sprawdzone techniki, aby manipulować ludzkimi emocjami i słabościami. Stosują oni wstępnie przygotowany podręcznik, znany w nigeryjskim oszustwie jako „scenariusz" lub „format". Często obejmuje on rozbudowane historie, fałszywe tożsamości i sfałszowane dokumenty, które wydają się legalne, a oszuści po prostu kopiują je i wykorzystują w komunikacji z ofiarami.

Wyłączne korzystanie z pisemnej komunikacji cyfrowej

W przypadku oszustwa nigeryjskiego komunikacja odbywa się wyłącznie za pośrednictwem poczty e-mail, wiadomości tekstowych lub sieci społecznościowych. W tym typie oszustwa oszuści nie komunikują się z ofiarami za pośrednictwem wideo ani telefonu. Otrzymane wiadomości zawierają błędy gramatyczne i słabe formatowanie tekstu.

Zniknięcie

Gdy ofiara nie poda pieniędzy ani danych osobowych albo zorientuje się, że padła ofiarą oszustwa, oszuści natychmiast przestają odpowiadać na korespondencję i po prostu znikają.

Międzynarodowe oszustwa finansowe

KONSEKWENCJE:

To oszustwo może zagrozić osobom w każdym wieku, zwłaszcza tym, którzy wierzą w schematy szybkiego wzbogacenia się lub są naiwni finansowo. Jednak seniorzy są jeszcze bardziej podatni, ponieważ zazwyczaj bardziej ufają innym i mniej wiedzą o bezpieczeństwie online.

01 Konsekwencje finansowe

Ofiary mogą stracić duże sumy pieniędzy, co prowadzi do poważnych problemów finansowych. Kiedy ofiary odpowiadają pozytywnie, wpadają w pułapkę, w której oszuści proszą je o coraz więcej pieniędzy, wymyślając wszelkiego rodzaju fałszywe wymówki lub propozycje dodatkowych płatności. W takim przypadku może pojawić się również "błąd kosztów utopionych", gdzie ofiary nadal dążą do czegoś, w co już mocno zainwestowały (czy to pieniądze, czas, wysiłek, energię emocjonalną itp.), mimo że poddanie się byłoby znacznie lepszym pomysłem.

02 Konsekwencje emocjonalne

Gdy wstyd lub zażenowanie zachęcają do zachowań skrytych, może to często prowadzić do tego, że ofiary padają ofiarą kolejnych oszustw.

03 Konsekwencje społeczne

Po padnięciu ofiarą oszustwa zaufanie człowieka do innych ludzi może znacznie spaść, co może prowadzić do izolacji oraz trudności w utrzymywaniu i budowaniu relacji.

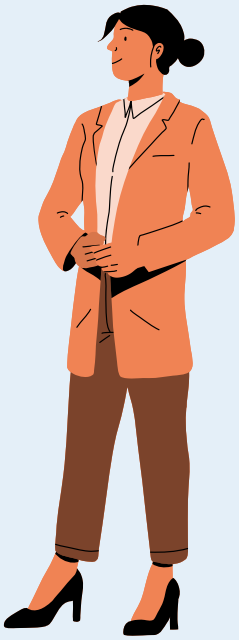
Międzynarodowy oszustwo finansowe

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Emma przeglądała sieć, gdy otrzymała wiadomość e-mail zatytułowaną „Pozdrowienia”. Nadawcą wiadomości był nigeryjski „książę”, który potrzebował jej pomocy w przelaniu dużej sumy pieniędzy z Nigerii. W zamian miała otrzymać procent środków za pomoc, w zamian za niewielką opłatę za ułatwienie transakcji.
Mimo kuszącej oferty Emma nabrała podejrzeń!

Niestety dla oszusta...

Emma niedawno przeczytała w internecie artykuł o oszustwach 419 i poznała wszystkie ich odmiany.



KROK 1: Rozpoznawanie sygnałów ostrzegawczych w komunikacji
Emma zauważyła, że treść wiadomości e-mail była napisana bardzo słabą angielszczyzną i nie miała żadnego sensu.

KROK 2: Wykorzystanie wiedzy
Emma dowiedziała się również z artykułu w internecie o oszustwach 419, że w Nigerii nie ma żadnych rodzin królewskich.

KROK 3: Podejmowanie zdecydowanych działań
Emma natychmiast oznaczyła e-mail jako spam i usunęła go. To samo zrobiła z innymi e-mailami, które pochodziły od „rzekomego” nigeryjskiego księcia.

KROK 4: Wspieranie społeczności świadomych i czujnych osób
Emma podzieliła się swoimi doświadczeniami z mężem, rodziną i przyjaciółmi, a także udostępniła te informacje w mediach społecznościowych.

Międzynarodowe oszustwa finansowe

SPOSOBY OCHRONY:

Jeśli natkniesz się na próbę oszustwa typu 419, pierwszą rzeczą, o której musisz pamiętać, jest to, że nikt nie otrzymał dużej sumy pieniędzy z powodu nieoczekiwanej wiadomości w skrzynce odbiorczej!

Poniżej znajdziesz kilka dodatkowych wskazówek, na wypadek gdybyś znalazł się w podobnej sytuacji.

Jeśli otrzymasz ofertę oszustwa 419 i będziesz chciał ją przyjąć, zatrzymaj się i zadaj sobie dwa proste, zdroworozsądkowe pytania:

Dlaczego miałbyś dzielić się swoimi danymi osobowymi i finansowymi z zupełnie obcą osobą (pochodzącą z kraju, z którym nie masz żadnych kontaktów) i dlaczego ta obca osoba miałaby wybrać ciebie, aby podzielić się z tobą majątkiem?

Nawet jeśli historia „porwania dziecka” poruszyła Cię do głębi serca, nigdy nie wysyłaj pieniędzy (ani innych informacji finansowych) bez sprawdzenia autentyczności osoby proszącej Cię o pomoc finansową!

Pamiętaj również, że oszustwa 419 nakłaniają do płacenia za pomocą przelewów bankowych! (zazwyczaj Western Union)

Międzynarodowe oszustwa finansowe

SPOSOBY OCHRONY:

Sprawdź autentyczność treści:

Ponieważ oszuści 419 wielokrotnie używają skryptów, możesz sprawdzić autentyczność wiadomości e-mail, po prostu wstawiając krótki fragment treści do wyszukiwarki (Google, Bing itp.). Jeśli treść jest częścią znanych lub nieodkrytych wiadomości o oszustwie, znajdziesz strony internetowe ostrzegające przed tym oszustwem, które zostały już zgłoszone przez inne ofiary.

Nie odpowiadaj na oszukańcze wiadomości e-mail (nawet nie jako żart)!

Usuń je natychmiast!

Pamiętaj, że jeśli odpowiesz, najprawdopodobniej wpadniesz w pułapkę finansową!

Międzynarodowe oszustwa finansowe

SPOSOBY OCHRONY:

Jeśli ujawniłeś swoje dane finansowe oszustowi, zmień kod PIN i hasło logowania (jeśli korzystasz z bankowości internetowej).

Stosuj dodatkowe środki bezpieczeństwa przy transakcjach finansowych, takie jak uwierzytelnianie dwuskładnikowe (2FA) i funkcja powiadomień o transakcjach, a także regularnie monitoruj saldo swojego konta.

Jeśli poniosłeś stratę finansową, natychmiast zgłoś to swojemu bankowi i innym odpowiednim organom w swoim kraju!

Dodatkowe informacje

MANIPULACJE FINANSOWE I INWESTYCYJNE

- https://faircanada.ca/investing-basics/protecting-vulnerable-investors-from-financial-abuse/
- https://economictimes.indiatimes.com/wealth/legal/will/how-can-senior-citizens-protect-themselves-from-financial-exploitations-by-their-own-families/articleshow/103877992.cms?from= mdr
- 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

POZORNY ALTRUIZM: OSZUSTWA CHARYTATYWNE

- https://www.bbc.com/news/uk-34530586
- https://www.youtube.com/watch?app=desktop&v=MTm-fq0OUQQ
- https://www.americanseniioralliance.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

Dodatkowe informacje

KUSZĄCE ZŁUDZENIA: FIKCYJNE NAGRODY I KONKURSY

- 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.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

OSZUSTWA ZWIĄZANE Z WALUTĄ CYFROWĄ

- https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams https://www.coindesk.com/learn/crypto-scams-types-of-crypto-schemes-and -jak-nie dać się-oszukać
- 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 -zgłoszono-utratę-więcej-1-miliarda-oszustw-kryptowalutowych-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-analytic-reveals-consumers-lost-nearly-500-million-cryptocurrency-scams
- https://www.kaspersky.com/resource-center/threats/top-seven-tips-for-preventing-cryptocurrency-scams

Dodatkowe informacje

MIĘDZYNARODOWE OSZUSTWA FINANSOWE

- 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

ROZDZIAŁ 3. MANIPULACJA SPOŁECZNA I OSZUSTWA EMOCJONALNE

Współczesne oszustwa coraz częściej przybierają formę manipulacji społecznej i emocjonalnej, co sprawia, że seniorzy są szczególnie podatni na te zagrożenia. Przestępcy wykorzystują emocje, zaufanie i naiwność, aby osiągnąć swoje cele, często rujnując finansowe i emocjonalne samopoczucie swoich ofiar. Niniejszy rozdział ma na celu omówienie najczęstszych oszustw opartych na manipulacji emocjonalnej i społecznej, pomagając seniorom rozpoznawać i chronić się przed tymi zagrożeniami.

Do najniebezpieczniejszych należą oszustwa romantyczne, w których przestępcy budują relacje, aby wyłudzić pieniądze. Smishing i oszustwa telefoniczne również stanowią poważne zagrożenie, ponieważ oszuści podszywają się pod zaufane osoby lub instytucje, aby uzyskać dane osobowe lub fundusze.

Innymi metodami manipulacji są oszustwa na wnuczka, w których oszuści podszywają się pod członków rodziny, a także oszustwa związane z produktami medycznymi.
Zrozumienie tych zagrożeń jest kluczowe dla ochrony dobrobytu finansowego i emocjonalnego osób starszych.

Oszustwa w związkach damsko-męskich

CHARAKTERYSTYKA ZAGROŻENIA:

Oszustwo randkowe online, znane również jako oszustwo romantyczne, ma miejsce, gdy ofiara zostaje oszukana i wierzy, że jest w związku romantycznym z kimś, kogo poznała online. Jednak jej domniemany partner jest oszustem.

Rodzaje manipulacji w romansie online:

Fałszywa tożsamość

Oszuści tworzą fałszywe profile internetowe i przedstawiają się jako osoby mieszkające daleko od ofiary, najczęściej za granicą, będące na misji (lekarz, żołnierz, filantrop), pracujące na platformie wiertniczej itp.

Doskonałość

Zainteresowania i hobby oszusta są niemal dokładnie takie same jak ofiar... a zdjęcia są po prostu... WOW! Chociaż poza kilkoma „doskonałymi zdjęciami" nie ma zbyt wielu (lub żadnych) innych zdjęć przedstawiających go/ją w różnych sytuacjach życiowych.

Szybki postęp

Kiedy wszystko zaczyna wyglądać wspaniale (wyznanie miłości, oświadczyny itp.), oszust zaprasza ofiary do prywatnej rozmowy (uzyskując w ten sposób numer telefonu, adres e-mail i inne informacje) i obiecuje wkrótce spotkać się z ofiarą osobiście.

Prośba o... PIENIĄDZE

A kiedy wszystko zaczęło wyglądać jeszcze lepiej, pojawiła się prośba o pieniądze, której towarzyszyła historia budząca empatię i prośba o podanie konkretnych metod płatności (przelew bankowy, nowo założone konto bankowe na nazwisko ofiary itp.).

Oszustwa w związkach damsko-męskich

KONSEKWENCJE:

Oszustwa romantyczne mogą prowadzić do poważnych strat finansowych i znacznego cierpienia emocjonalnego u ofiar.

01 Konsekwencje finansowe

Ponieważ ofiary często wierzą, że pomagają bliskiej osobie w potrzebie, są skłonne wykorzystać swoje pieniądze i zainwestować je w związek. Dla dobra „miłości" niektóre ofiary poświęcają nawet wszystkie swoje oszczędności, zaciągają dodatkowe pożyczki, a nawet sprzedają swoje aktywa. Dane, które oszuści uzyskują od ofiar (konto bankowe, informacje o karcie kredytowej) mogą być wykorzystywane do dokonywania nieautoryzowanych transakcji lub wypłat, co prowadzi do znacznych strat finansowych.

02 Konsekwencje emocjonalne

Oszustwa związane z randkami online są szczególnie okrutne, ponieważ grają na emocjach ludzi. Ujawnienie, że związek online jest oszustwem, powoduje podobne szkody emocjonalne u ofiary, jak nagły koniec związku opartego na interakcji fizycznej. Często utrudnia to ofiarom zerwanie uczucia, jakie czują do oszusta, nawet gdy zdają sobie sprawę, że zostały oszukane.

03 Konsekwencje prawne

Ofiary romantycznych oszustw są podatne na ból psychiczny, taki jak wstyd, zażenowanie, stres, lęk, depresja i strach. Ofiary mogą doświadczać objawów przypominających poważne zaburzenie depresyjne, żałobę lub zespół stresu pourazowego (PTSD).

Oszustwa w związkach damsko-męskich

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Dwa lata po śmierci męża wnuki Margot przekonały ją do zapisania się na stronę randkową online. Wkrótce zaczęła czatować z mężczyzną o imieniu Tom, lekarzem na misji humanitarnej w Afryce.
Po kilku tygodniach szczerych rozmów Tom stwierdził, że ma „problemy z przepływem gotówki" i potrzebuje pieniędzy na pokrycie wydatków. Margot nabrała podejrzeń i omówiła niezwykłą prośbę ze swoimi wnukami. Razem zbadali jego profil i odkryli, że Tom jest oszustem.

Niestety dla oszusta...

Margot podjęła właściwą decyzję, kiedy otwarcie powiedziała bliskim o swoich podejrzeniach co do oszustwa.

KROK 1: Podążanie za intuicją
Margot wyczuła, że coś jest nie tak. Zaufała swoim instynktom i nie spieszyła się, by mu pomóc, ale najpierw pomyślała o dziwności jego prośby.

KROK 2: Poszukaj porady u zaufanych osób
Zamiast podjąć decyzję sama, Margot skonsultowała się z wnukami. Podzieliła się z nimi szczegółami prośby Toma i poprosiła ich o radę.

KROK 3: Badanie
Razem zbadali profil Toma i odkryli, że był oszustem. Ta świadomość powstrzymała Margot przed wysłaniem mu pieniędzy i rzuceniem się w wir oszustwa.

KROK 4: Raportowanie
Margot poinformowała o tym portal randkowy, skontaktowała się z administratorem serwisu i zgłosiła Toma podejrzanego o oszustwo.

Oszustwa w związkach damsko-męskich

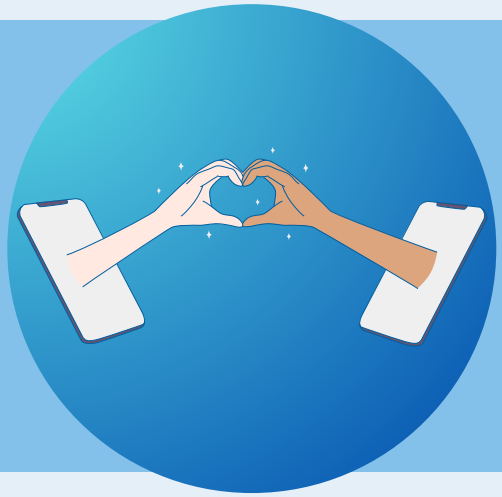
SPOSOBY OCHRONY:

Oszuści wykorzystują samotność osób starszych, zwłaszcza tych, które niedawno owdowiały lub się rozwiodły, wykorzystując ich bezbronność i zasoby finansowe, aby nawiązywać fałszywe relacje romantyczne online w mediach społecznościowych, na stronach randkowych itp.

Poniżej znajdziesz kilka dodatkowych wskazówek, na wypadek gdybyś znalazł się w podobnej sytuacji.

Uważaj na to, co udostępniasz w Internecie:

Informacje, którymi dzielisz się publicznie (zainteresowania, hobby, styl życia itp.) mogą zostać wykorzystane przez oszustów do stworzenia fałszywej persony, mającej na celu przyciągnięcie Twojej romantycznej sympatii.



W przypadku wszelkich relacji online zachowaj swoje dane osobowe i finansowe dla siebie:

Nie podawaj zbyt wielu informacji osobistych potencjalnemu partnerowi, z którym poznasz się online, i na pewno nie ujawniaj swoich danych finansowych.

Ale przede wszystkim - nie wysyłaj pieniędzy i nie kupuj wartościowych przedmiotów nikomu, kogo nigdy nie spotkałeś!

Oszustwo w związku damsko-męskim

SPOSOBY OCHRONY:

Zweryfikować:

Chociaż nie możesz zweryfikować wszystkiego, co mówi Ci romantyczny partner online, możesz sprawdzić pewne konkretne szczegóły, korzystając z Internetu, aby zweryfikować jego imię, nazwisko, miejsce zamieszkania, profile w mediach społecznościowych, autentyczność zamieszczonych i wysłanych zdjęć, a także sprawdzić, czy w komunikacji nie używa powtarzanych historii lub wyrażeń, ponieważ oszuści często powtarzają te same historie i kwestie.

Pamiętaj!

Jeśli Twój partner/partnerka w sieci odmawia spotkania się z Tobą twarzą w twarz, wymyśla wymówki, dlaczego nie może się spotkać lub nigdy nie bierze udziału w rozmowie wideo lub innych formach „interakcji” na żywo, może to oznaczać, że masz do czynienia z oszustem.

Oszustwo w związku damsko-męskim

SPOSOBY OCHRONY:

Jeśli udostępniłeś hasła do swoich kont i wykryłeś podejrzaną aktywność, natychmiast sprawdź, czy jakieś ustawienia zostały zmienione, i sprawdź ostatnie logowania i aktywność na swoich kontach. Jeśli zauważysz jakiekolwiek nieznane lub podejrzane logowania, poinformuj swojego dostawcę usług i swoje kontakty i uprzedź ich, aby byli czujni na podejrzane wiadomości, które mogą pochodzić od Ciebie.

Najlepszą radą jest zmiana wszystkich haseł, którym udzieliłeś dostępu!

Jeśli podejrzewasz, że Twój internetowy związek jest próbą oszustwa, natychmiast przerwij komunikację i zablokuj oszusta w mediach społecznościowych, poczcie e-mail, aplikacjach do przesyłania wiadomości, witrynach randkowych itp.

Jeżeli ktoś wykorzystał Twoje konto bankowe lub kredytowe, skontaktuj się z bankiem lub policją!

Rozpowszechnij tę wiadomość!

Oszustwa SMS-owe typu smishing

CHARAKTERYSTYKA ZAGROŻENIA:

Smishing to połączenie słów „SMS” (krótkie wiadomości tekstowe) i „phishing”. W tych atakach cyberprzestępcy wysyłają fałszywe wiadomości tekstowe i próbują oszukać lub zmanipulować ofiary, aby ujawniły dane osobowe lub finansowe, nagrywały złośliwe linki lub pobierały szkodliwe oprogramowanie lub aplikacje.

Rodzaje manipulacji w smishingu:

Personifikacja

Oszuści oszukują ofiary, podszywając się pod instytucje prawne, firmy lub inne organizacje za pośrednictwem wiadomości tekstowych. Wiadomości te skłaniają ofiary do podjęcia natychmiastowych działań, takich jak kliknięcie łącza w wiadomości, odpowiedź z danymi osobowymi lub wybranie określonego numeru.

Możliwy i prawdopodobny kontekst

Wykorzystanie sytuacji, która może być istotna dla ofiar (wiadomość z banku, usług związanych z kartami kredytowymi, obsługa klienta itp.) pozwala oszustom na stworzenie skutecznego kamuflażu i pomaga im rozwiać wszelkie podejrzenia, że jest to spam.

Granie na emocjach

Poprzez nasilenie emocji ofiary wiadomość wydaje się spersonalizowana i wywołuje określoną reakcję emocjonalną, taką jak pilność, strach lub ciekawość. Stosując te taktyki, oszuści tworzą wiadomości mające na celu skłonienie ofiar do natychmiastowego działania.

Oszustwa typu smishing-SMS

KONSEKWENCJE:

Ze względu na ograniczone doświadczenie z nowoczesnymi technologiami i wiedzą na temat cyberbezpieczeństwa, seniorzy często mają trudności z rozpoznawaniem oznak zagrożenia w wiadomościach smishingowych, takich jak fałszywe wezwania do działania lub podejrzane linki. Są mniej podejrzliwi i bardziej skłonni uwierzyć w oszukańcze wiadomości smishingowe.

01 Konsekwencje finansowe

Jeśli ofiary ujawnią swoje dane osobowe lub finansowe, takie jak numery kart kredytowych lub numery kont bankowych, mogą ponieść większe straty finansowe, ponieważ oszuści wykorzystują te informacje do przeprowadzania nieautoryzowanych transakcji lub wypłacania pieniędzy z konta ofiary. Konsekwencje te mogą powodować poważne problemy finansowe i długoterminowe szkody.

02 Kradzież tożsamości

W przypadku kradzieży tożsamości Twoje dane osobowe są niewłaściwie wykorzystywane, co wpływa na Twoje bezpieczeństwo osobiste i prywatność. Jeśli zostaną powiązane z nielegalną działalnością, możesz również ponieść konsekwencje prawne. Odzyskanie tożsamości może być bardzo czasochłonne, ponieważ obejmuje wiele procedur administracyjnych (a także prawnych).

03 Konsekwencje psychologiczne

Smishing często wykorzystuje emocje takie jak strach, panika czy dezorientacja, co może mieć wpływ na samopoczucie psychiczne ofiar.

Oszustwa SMS-owe typu smishing

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Peter otrzymał wiadomość tekstową na smartfonie od swojego banku informującą go, że jego konto zostało tymczasowo zablokowane. Wiadomość zawierała niezwykłą prośbę, aby NATYCHMIAST kliknął link, aby aktywować swoje konto.
Chociaż Piotr na chwilę spanikował, postanowił nie klikać na link, gdyż wiadomość wydała mu się bardzo podejrzana.

Niestety dla oszusta...

Peter niedawno obejrzał w Internecie film edukacyjny na temat smishingu i dowiedział się, na czym polegają tego typu oszustwa.

KROK 1: Rozpoznawanie sygnałów ostrzegawczych
Peter zauważył również błędy ortograficzne i niezręcznie sformułowane zdania w wiadomości, co wskazywało na to, że wiadomość nie była uwierzytelniona.

KROK 2: Zauważenie braku osobistego kontaktu
Peter zauważył również, że wiadomość była anonimowa i nie zawierała danych banku ani danych osoby kontaktowej, z którą klient mógłby się skontaktować w celu uzyskania dalszych informacji.

KROK 3: Weryfikacja informacji

Zamiast kliknąć link, Peter zadzwonił do banku, korzystając z numeru telefonu ze swojej książki telefonicznej, i sprawdził, czy wiadomość jest prawdziwa.

KROK 4: Informowanie/zgłaszanie

Po tym, jak Peter poinformował bank, który potwierdził próbę oszustwa, bank poinformował wszystkich swoich klientów i zgłosił próbę oszustwa odpowiednim organom.

Oszustwa SMS-owe typu smishing

SPOSOBY OCHRONY:

Łatwo jest chronić się przed potencjalnymi konsekwencjami tych ataków - po prostu je ignoruj. Oczywiście nie należy ignorować wszystkich wiadomości, ponieważ wiadomości tekstowe są legalnym narzędziem dla wielu sprzedawców detalicznych i innych instytucji, aby się z Tobą skontaktować.

Poniżej znajdziesz kilka dodatkowych wskazówek, na wypadek gdybyś znalazł się w podobnej sytuacji.

Nie odpowiadaj:

Otrzymanie nieoczekiwanej lub podejrzanej wiadomości tekstowej, a nawet prośby o odpowiedź, np. o wysłanie wiadomości „STOP" z prośbą o anulowanie subskrypcji, może być próbą identyfikacji aktywnych numerów telefonów i prowadzić do oszustwa.

- **Przykład 3**

Nie panikuj:

Jeśli wiadomość wydaje się pilna, nie spiesz się i czytaj ją wolniej.

PILNE aktualizacje konta lub PILNE oferty ograniczone czasowo należy traktować jako potencjalne oznaki smishingu.

Zachowaj ostrożność!

Oszustwa SMS-owe typu smishing

SPOSOBY OCHRONY:

Nie korzystaj z linków i danych kontaktowych podanych w wiadomości!
Zweryfikuj, sprawdź i skontaktuj się bezpośrednio za pośrednictwem oficjalnych kanałów komunikacji, a nie za pośrednictwem szczegółów lub informacji podanych w tekście.

Pamiętaj o!
Legalne instytucje (np. banki, urzędy państwowe itp.) nigdy nie żądają podania poufnych danych za pośrednictwem wiadomości SMS lub niecertyfikowanych połączeń.

Jeśli podejrzewasz próbę ataku smishing, natychmiast zmień wszystkie hasła i kody PIN do swoich kont.

Monitoruj również swoje finanse i konta internetowe pod kątem nietypowych miejsc logowania i podejrzanych działań.

Jeśli padłeś ofiarą smishingu, skontaktuj się z odpowiednimi instytucjami, które mogą Ci natychmiast pomóc. W przypadku ataku finansowego skontaktuj się ze swoim bankiem, aby zamrozić konto lub anulować karty kredytowe.

Oszustwa telefoniczne z udziałem seniorów

CHARAKTERYSTYKA ZAGROŻENIA:

Oszustwa telefoniczne, znane również jako vishing, są szczególnie skuteczne w przypadku osób starszych. Typowe taktyki obejmują nieoczekiwane połączenia z nieznanych lub zagranicznych numerów, fałszywych numerów lub platform takich jak Viber i WhatsApp. Połączenia vishingowe mogą pochodzić od prawdziwej osoby lub nagranego wcześniej robocall. Oszuści wykorzystują taktykę głosową w celu kradzieży poufnych danych osobowych, takich jak informacje identyfikacyjne, numery kont bankowych, dane logowania i hasła.

Rodzaje manipulacji w vishingu:

Personifikacja

Oszuści często podszywają się pod pracowników banków, agencji rządowych, firm ubezpieczeniowych lub innych znanych firm, aby wydawać się legalnymi i uzyskać informacje finansowe i osobiste. Stosują taktyki psychologiczne, aby stworzyć poczucie pilności, przekonując ofiary, że mają kłopoty. Mogą grozić i próbować je przestraszyć.

Perswazyjność

Oszuści mogą również używać języka perswazyjnego i tonu, aby przekonać ofiarę, że są po ich stronie. Dlatego często prowadzą rozmowę w przyjazny, przystępny, współczujący sposób i wydają się być pomocni, a często używają dwuznacznego języka lub zmieniają temat podczas rozmowy, aby odwrócić uwagę ofiary.

Trwałość

Oszuści charakteryzują się uporem, w tym powtarzaniem połączeń z tego samego numeru (mogą nawet kontaktować się z ofiarą kilka razy dziennie itd.). Na swój sposób, powoli i systematycznie, zyskują zaufanie ofiary. Ta taktyka jest stosowana w celu zdobycia zaufania ofiary i skłonienia jej do ujawnienia poufnych informacji.

Oszustwa telefoniczne z udziałem seniorów

KONSEKWENCJE:

Seniorzy często uważają rozmowy telefoniczne za ważny sposób komunikacji i cenią sobie osobistą interakcję, jaką zapewnia rozmowa telefoniczna. To właśnie ten wysoki poziom zaufania do osobistej komunikacji przez telefon sprawia, że są bardziej podatni na różne rodzaje oszustw telefonicznych i łatwiej wierzą wprowadzającym w błąd prośbom o informacje lub działaniom podejmowanym przez oszustów.

01 Konsekwencje finansowe

Ofiary oszustw telefonicznych często ponoszą bezpośrednie straty finansowe. Oszuści mogą oszukać ofiary, aby dokonały płatności lub podały informacje bankowe, co prowadzi do nieautoryzowanych transakcji lub opróżnienia kont bankowych. Może to znacząco wpłynąć na ich oszczędności i bezpieczeństwo finansowe.

02 Kradzież tożsamości

Oszustwa telefoniczne często obejmują kradzież danych osobowych, takich jak numery ubezpieczenia społecznego, daty urodzenia i adresy. Ofiary mogą napotkać poważne trudności w rozwiązywaniu tych problemów i odzyskiwaniu tożsamości.

03 Uszkodzenie reputacji

W przypadkach, gdy oszustwo jest wynikiem nieautoryzowanych działań lub transakcji finansowych, ofiara może również ponieść szkody na swojej reputacji finansowej. Odbudowa reputacji może być trudna i wymaga obszernej dokumentacji i komunikacji z instytucjami finansowymi.

Oszustwa telefoniczne z udziałem seniorów

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Andrew odebrał telefon od osoby podającej się za przedstawiciela firmy ubezpieczeniowej i potrzebującej dodatkowych informacji, aby zaktualizować swoją dokumentację medyczną. Dzwoniący był bardzo przyjazny, ale nie przedstawił się swoim imieniem i nazwiskiem. Powiedział tylko, że dzwoni w imieniu firmy ubezpieczeniowej i wyjaśnił, że to rutynowa kontrola.
Kiedy zaczął pytać o dane osobowe, takie jak numer ubezpieczenia i datę urodzenia, Andrew nabrał podejrzeń.

Niestety dla oszusta...

Andrew aktywnie uczestniczy w forach i społecznościach internetowych, gdzie omawiane są kwestie bezpieczeństwa i wymieniane są doświadczenia związane z oszustwami.

KROK 1: Weryfikacja tożsamości osoby dzwoniącej
Andrew nie był w stanie zweryfikować tożsamości osoby dzwoniącej na oficjalnej stronie internetowej firmy ubezpieczeniowej, ponieważ domniemany pracownik firmy nie podał jego pełnego imienia i nazwiska, więc Andrew nabrał podejrzeń.

KROK 3: Wykorzystanie dotychczasowej wiedzy
Andrew rozpoznał oznaki oszustwa, ponieważ aktywnie uczestniczył w dyskusjach na forach internetowych na temat bezpieczeństwa, co pozwoliło mu szybko wychwycić podejrzane elementy rozmowy.

KROK 2: Bądź uważny na podejrzane prośby

Kiedy rozmówca zaczął pytać o dane osobowe, takie jak numer ubezpieczenia i datę urodzenia, Andrew zaczął wątpić w autentyczność połączenia i natychmiast się rozłączył.

KROK 4: Informowanie/zgłaszanie

Andrew zadzwonił bezpośrednio do swojego ubezpieczyciela, aby sprawdzić, czy nie jest to próba oszustwa, i rozpowszechnił informację na forach i w mediach społecznościach, w których jest aktywny.

Oszustwa telefoniczne z udziałem seniorów

SPOSOBY OCHRONY:

Ze względu na przyspieszony postęp technologii telekomunikacyjnych oszuści wykorzystali anonimowość i łatwy dostęp do połączeń telefonicznych, aby prowadzić oszukańcze działania. Dlatego też niezwykle ważne jest, aby osoby starsze zachowały wysoki poziom czujności i były świadome ryzyka związanego z komunikacją przez telefon.

Poniżej znajdziesz kilka dodatkowych wskazówek, na wypadek gdybyś znalazł się w podobnej sytuacji.

Ignoruj nieoczekiwane połączenia z nieznanych numerów lub po prostu pozwól, aby połączenia zostały przekierowane na pocztę głosową, a następnie na podstawie podanych informacji zdecyduj, czy oddzwonić.

Unikaj korzystania z jakiegokolwiek numeru oddzwaniania, który podają, ponieważ może to być część oszustwa. Zamiast tego wyszukaj oficjalny numer telefonu i zadzwoń do nich bezpośrednio, aby potwierdzić zasadność prośby.

Nigdy nie podawaj informacji finansowych ani osobistych przez telefon!

Natychmiast się rozłącz, jeżeli będą próbowali wydobyć od ciebie tego typu informacje!

Oszustwa telefoniczne z udziałem seniorów

SPOSOBY OCHRONY:

Sprawdź linię:

Pamiętaj, że oszuści mogą utrzymać Twoją linię telefoniczną otwartą nawet po zakończeniu rozmowy.

Użyj innego telefonu, aby sprawdzić, czy linia jest wolna, lub odczekaj co najmniej 10–15 minut, aby mieć pewność, że oszuści się rozłączyli.

Spróbuj zablokować połączenia:

Aktywuj funkcje blokowania połączeń w telefonie, aby odfiltrować możliwe oszustwa vishingowe. Większość smartfonów oferuje tę funkcję.

Jeśli nie masz smartfona, skontaktuj się ze swoim operatorem telefonii komórkowej, aby dowiedzieć się, jakie usługi blokowania niechcianych połączeń oferuje.

Jeśli padłeś ofiarą vishingu, natychmiast skontaktuj się z odpowiednimi instytucjami, które mogą Ci pomóc

Oszustwa wykorzystujące emocjonalne więzi rodzinne

CHARAKTERYSTYKA ZAGROŻENIA:

Oszustwo na dziadków to rodzaj oszustwa, w którym oszuści żerują na więziach emocjonalnych między dziadkami i wnukami. Oszuści zazwyczaj udają wnuka w potrzebie, potrzebującego natychmiastowej pomocy finansowej.

Rodzaje manipulacji w oszustwie na wnuczka:

Pilność

Oszuści wykorzystują poczucie pilności, aby powstrzymać dziadków przed zbytnim myśleniem lub kontaktowaniem się z innymi członkami rodziny.

Tajność

Oszuści mogą prosić dziadków o zachowanie tajemnicy, tłumacząc się wstydem lub obawą przed większymi kłopotami.

Manipulujący emocjonalnie

Oszuści wykorzystują miłość i troskę dziadków o wnuki, aby uzyskać szybką odpowiedź.

Oszustwa wykorzystujące emocjonalne więzi rodzinne

KONSEKWENCJE:

Padnięcie ofiarą oszustwa podszywającego się pod wnuczka może mieć poważne konsekwencje.

01 Strata finansowa

Finansowo możesz stracić ciężko zarobione pieniądze, ponieważ oszuści często proszą o duże sumy, które mogą wyczerpać Twoje oszczędności. Jeśli podasz swoje dane bankowe, mogą ukraść jeszcze więcej

02 Stres emocjonalny

Pod względem emocjonalnym fałszywe sytuacje awaryjne powodują znaczny stres i niepokój, a odkrycie, że to oszustwo, może wywołać poczucie głębokiej zdrady i zranienia.

03 Utrata zaufania

Takie doświadczenie może prowadzić do utraty zaufania, sprawiając, że zaczniesz wątpić w prawdziwe sytuacje kryzysowe i będziesz podejrzliwy wobec każdego nieoczekiwanego kontaktu, nawet ze strony legalnych osób.

04 Izolacja

Dodatkowo możesz odczuwać zażenowanie lub wstyd, co może prowadzić do niechęci do rozmawiania o sprawach finansowych z rodziną i znajomymi. W takiej sytuacji oszuści mogą ponownie wziąć cię na celownik, widząc w tobie łatwy cel.

Oszustwa wykorzystujące emocjonalne więzi rodzinne

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Mary mieszka sama i cieszy się bliską relacją ze swoją rodziną, zwłaszcza wnukami. Pewnego wieczoru Mary odebrała telefon od kogoś, kto twierdził, że jest jej wnukiem, Jackiem, i pilnie poprosił o dużą sumę pieniędzy. Ten telefon doprowadził do przygnębiającego i kosztownego doświadczenia dla Mary.
Mary pamięta jednak, że wnuk radził jej, by zachować ostrożność podczas rozmów telefonicznych z ludźmi proszącymi o pieniądze.

Doświadczenie Mary podkreśla znaczenie pozostawania poinformowanym o typowych oszustwach i weryfikowania wszelkich pilnych i emocjonalnych próśb o pieniądze. Rozumiejąc taktyki stosowane przez oszustów, takie jak tworzenie pilności, żądanie zachowania tajemnicy i manipulowanie emocjami, seniorzy mogą lepiej chronić się przed zostaniem ofiarami. W razie wątpliwości zawsze weryfikuj informacje z innymi członkami rodziny i nigdy nie spiesz się z wysyłaniem pieniędzy.

Krok 1: Weryfikacja

Mary zadała rozmówcy pytania, o których wiedział tylko Jack, ale poświęciła chwilę, aby zadzwonić bezpośrednio do Jacka, aby uniknąć oszustwa.

Krok 2: Świadomość

Wiedza o takich oszustwach z wyprzedzeniem pomogła Mary rozpoznać sygnały ostrzegawcze.

Krok 3: Komunikacja

Mary już rozmawiała z rodziną o potencjalnych oszustwach, a ustalenie rodzinnego hasła na wypadek sytuacji awaryjnych może zapewnić dodatkową ochronę.

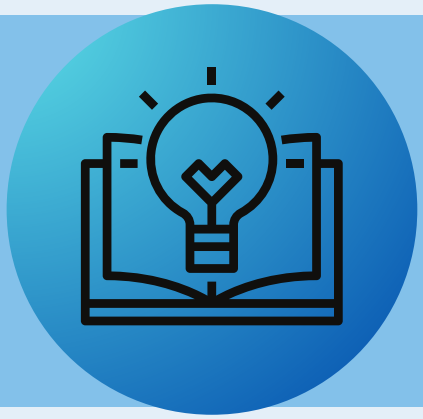
Oszustwa wykorzystujące emocjonalne więzi rodzinne

SPOSOBY OCHRONY:

Ochrona siebie przed oszustwami wykorzystującymi emocjonalne więzi rodzinne jest kluczowa dla ochrony ciężko zarobionych pieniędzy. Oto kilka prostych kroków, które możesz podjąć.

Bądź na bieżąco:

Dowiedz się i poznaj bliżej swoich bliskich na temat częstych oszustw wymierzonych w osoby starsze, w tym oszustw na wnuczęta.
Bądź na bieżąco z nowymi taktykami oszustów, śledząc wiarygodne źródła informacji.



Weryfikacja tożsamości:

Zawsze zadawaj pytania, na które może odpowiedzieć tylko członek rodziny, na przykład dotyczące imienia zwierzęcia domowego lub konkretnego wydarzenia rodzinnego.
W razie wątpliwości należy oddzwonić pod znany numer, aby potwierdzić tożsamość dzwoniącego.

Ustal hasło rodzinne:

Ustal z rodziną tajne hasło, które będą znane tylko zaufanym osobom.
Użyj tego hasła w nagłych wypadkach, aby zweryfikować tożsamość osób dzwoniących, podających się za członków rodziny.

Oszustwa wykorzystujące emocjonalne więzi rodzinne

SPOSOBY OCHRONY:

Unikaj pochopnych decyzji:

Nie spiesz się, gdy otrzymasz nieoczekiwaną lub pilną prośbę o pieniądze.
Oszuści wykorzystują pośpiech, aby uniemożliwić Ci zakwestionowanie ich historii lub zwrócenie się do innych o poradę.

Użyj identyfikatora dzwoniącego i blokowania połączeń:

Użyj identyfikatora dzwoniącego, aby filtrować połączenia przychodzące i blokować nieznane lub podejrzane numery.
Oszukańcze połączenia telefoniczne należy zgłaszać operatorowi telefonii komórkowej lub odpowiednim władzom.

Chroń swoje dane osobowe

Zachowaj ostrożność udostępniając informacje osobiste i finansowe przez telefon lub Internet.
Unikaj podawania poufnych informacji, chyba że masz pewność co do tożsamości odbiorcy.

Oszustwa związane z produktami medycznymi

CHARAKTERYSTYKA ZAGROŻENIA:

W ostatnich latach oszuści coraz częściej obierają sobie za cel osoby podatne na zagrożenia, w tym seniorów, stosując oszukańcze schematy obejmujące produkty medyczne. Te oszustwa często wykorzystują emocje i obawy związane z problemami zdrowotnymi, obiecując cudowne lekarstwa, terapie lub środki zaradcze, które są zbyt dobre, aby mogły być prawdziwe.

Rodzaje manipulacji w oszustwach związanych z produktami leczniczymi:

Fałszywe obietnice

Oszuści wygłaszają śmiałe zapewnienia na temat swoich produktów, obiecując cudowne rezultaty, mimo że mają niewiele dowodów naukowych lub nie mają ich wcale.

Taktyka wysokiego ciśnienia

Często stosują agresywne techniki sprzedaży, namawiając do szybkiego zakupu, zanim „oferta ograniczona czasowo” wygaśnie.

Manipulacja emocjonalna

Tego typu oszustwa grają na emocjach, wykorzystują obawy związane ze zdrowiem i oferują fałszywą nadzieję na szybkie i łatwe rozwiązanie.

Oszustwa związane z produktami medycznymi

KONSEKWENCJE:

Manipulowanie produktami medycznymi może mieć poważne negatywne skutki, takie jak:

01 Strata finansowa

Padnięcie ofiarą oszustwa związanego z produktami medycznymi może skutkować wydaniem dużych sum pieniędzy na nieskuteczne lub nawet niebezpieczne produkty, co uszczupli Twoje oszczędności.

02 Zagrożenia dla zdrowia

W niektórych przypadkach oszuści wykorzystują nieuregulowane lub podrobione produkty medyczne, które mogą prowadzić do poważnych komplikacji zdrowotnych lub interakcji z istniejącymi lekami.

03 Stres emocjonalny

Bycie oszukanym może prowadzić do uczucia wstydu, winy i zażenowania. Możesz czuć się zdradzony i niespokojny, co może negatywnie wpłynąć na Twoje ogólne zdrowie psychiczne i dobre samopoczucie.

04 Pogorszenie jakości życia

Połączone skutki strat finansowych, zagrożeń dla zdrowia i stresu emocjonalnego mogą prowadzić do znacznego pogorszenia jakości życia ofiar. Mogą mieć trudności z zarządzaniem codziennymi czynnościami i utrzymaniem niezależności.

Oszustwa związane z produktami medycznymi

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Thomas otrzymuje e-mail z reklamą nowego „cudownego suplementu", który rzekomo leczy artretyzm, cukrzycę i wysokie ciśnienie krwi z dnia na dzień. E-mail oferuje ograniczoną czasowo zniżkę i namawia go do zakupu teraz, aby nie przegapić okazji na lepsze zdrowie.
Thomas pamięta jednak, że przeczytał radę, aby zachować ostrożność w stosowaniu cudownych metod leczenia.

Niestety historia Thomasa nie jest jedynym przypadkiem. Oszustwa związane z produktami medycznymi żerują na podatnościach i emocjach seniorów, obiecując szybkie rozwiązania złożonych problemów zdrowotnych. Pozostając poinformowanym, sceptycznym i konsultując się z pracownikami służby zdrowia, możesz uchronić się przed padnięciem ofiarą tych oszukańczych schematów. Pamiętaj, że Twoje zdrowie jest bezcenne i nie ma skrótów do prawdziwego dobrego samopoczucia.

Krok 1: Zachowaj sceptycyzm

Thomas pamiętał, że prawdziwe przełomy medyczne są dokładnie testowane i weryfikowane przez ekspertów.

Krok 2: Skonsultuj się ze specjalistami

Thomas zadzwonił do swojego lekarza pierwszego kontaktu i omówił z nim wszelkie nowe metody leczenia i suplementy.

Krok 3: Badania

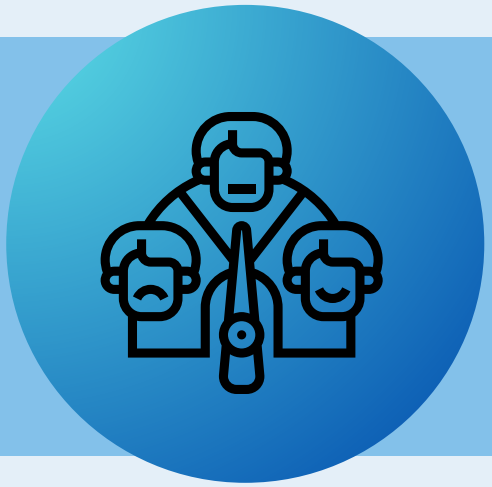
Przed podjęciem decyzji o zakupie Thomas szukał obiektywnych opinii i dowodów naukowych potwierdzających skuteczność produktu.

Oszustwa związane z produktami medycznymi

SPOSOBY OCHRONY:

Pamiętaj, że ochrona przed oszustwami związanymi z produktami medycznymi jest kluczowa dla ochrony ciężko zarobionych pieniędzy i zdrowia. Jednym z najważniejszych kroków jest poszukiwanie wsparcia emocjonalnego. Oto kilka prostych kroków, które możesz podjąć.

Szukaj wsparcia emocjonalnego:
Wsparcie społeczne ze strony rodziny, przyjaciół i członków społeczności może zapewnić seniorom siłę emocjonalną i pewność, których potrzebują, aby oprzeć się manipulacji. Kiedy seniorzy czują się wspierani i doceniani, jest mniej prawdopodobne, że padną ofiarą oszustów, którzy wykorzystują emocjonalne słabości.



Bądź na bieżąco:
Sieci społecznościowe mogą być ważnym źródłem informacji. Członkowie rodziny i przyjaciele mogą dzielić się ostrzeżeniami o trwających oszustwach, udzielać wskazówek, jak rozpoznawać oszustwa, i sugerować zaufane źródła produktów medycznych i metod leczenia. Pozostawanie poinformowanym dzięki wsparciu społecznemu może znacznie zmniejszyć ryzyko wpadnięcia w pułapkę oszustw.

Oszustwa związane z produktami medycznymi

SPOSOBY OCHRONY:

Skonsultuj się z personelem medycznym:
Przed wypróbowaniem jakiegokolwiek nowego produktu medycznego lub metody leczenia skonsultuj się z lekarzem, aby upewnić się, że jest ona bezpieczna i skuteczna.

Podchodź sceptycznie do twierdzeń o cudach:
Jeśli produkt obiecuje wyleczyć kilka niezwiązanych ze sobą schorzeń lub oferuje szybkie i bezproblemowe rezultaty, to prawdopodobnie jest to zbyt piękne, aby mogło być prawdziwe.

Przeprowadź dokładne badania:
Poświęć czas na zbadanie produktu i firmy, która za nim stoi. Poszukaj recenzji z renomowanych źródeł i sprawdź, czy produkt jest zatwierdzony przez agencje regulacyjne.

Dodatkowe informacje

OSZUSTWA W RELACJACH DAMSKO-MĘSKICH

- 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/

OSZUSTWA SMS-OWE SMISHING

- https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-bronić-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/czym-jest_smishing/#jak_chronic_sie_przed_smishingiem_sekcja
- https://www.techtarget.com/searchmobilecomputing/definition/SMiShing
- https://cyberready.com/category/the-complete-guide-to-smishing
- https://www.rd.com/article/what-is-smishing/

Dodatkowe informacje

OSZUSTWA TELEFONICZNE Z UDZIAŁEM SENIORÓW

- 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

OSZUSTWA WYKORZYSTUJĄCE EMOCJONALNE WIĘZI RODZINNE

- 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%20overseas.
- https://www.cbsnews.com/news/what-being-targeted-by-grandparent-scam-sounds-like-60-minuty/
- https://www.youtube.com/watch?v=v2VFy2igHPE
- https://globalnews.ca/video/9901367/calgary-senior-falls-victim-to-grandparents-scam-costing-her-thousands

Dodatkowe informacje

OSZUSTWA ZWIĄZANE Z PRODUKTAMI MEDYCZNYMI

- 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

ROZDZIAŁ 4. OSZUSTWA ZWIĄZANE Z TRANSAKCJAMI ONLINE

W erze płatności i transakcji online coraz częściej pojawiają się doniesienia o oszustwach online. Przestępcy mają dostęp do wielu seniorów, korzystając z nowych technologii, co czyni ich bardziej wyrafinowanymi w oszukańczych praktykach. W tej sekcji omówimy najczęstsze oszustwa z postępowaniami online, aby pomóc seniorom je rozwiązać i uniknąć.

Oszustwa związane z podróżami i biletami obejmują oferowanie fikcyjnych ofert, które nigdy się nie materializują. W oszustwach subskrypcyjnych seniorzy są oszukiwani, aby akceptować usługi, które automatycznie pobierają opłaty. Fałszywe sklepy internetowe wymuszają płatności za niedostarczone produkty. Oszustwa kupna-sprzedaży obejmują oszukańcze zakupy, w których produkty nie są wymienione lub nie są dostępne, a seniorzy sprzedają swoje rzeczy za darmo na stronach z ogłoszeniami.

Zrozumienie tych zagrożeń jest kluczowe, aby seniorzy mogli bezpiecznie korzystać z możliwości oferowanych przez Internet i chronić swoje finanse przed oszustwami.

Oszustwa związane z podróżami i sprzedażą biletów

CHARAKTERYSTYKA ZAGROŻENIA:

Oszustwa związane z podróżami i biletami odnoszą się do oszukańczych schematów, które obejmują sprzedaż fałszywych pakietów podróży, wycieczek i biletów. Ten rodzaj oszustwa często występuje w Internecie, gdzie oszuści zakładają profesjonalnie wyglądające strony internetowe lub wysyłają e-maile oferujące mocno obniżone oferty. Seniorzy, którzy mogą być mniej zaznajomieni z nowoczesnymi taktykami oszustw online, są szczególnie podatni na te oszustwa. Nieświadomi klienci, zwłaszcza seniorzy przyciągnięci tymi ofertami, dokonują płatności za te nieistniejące usługi i pozostają bez możliwości odwołania się, gdy zdają sobie sprawę, że zostali oszukani. Ważne jest, aby edukować seniorów na temat tych oszukańczych schematów, aby pomóc im uniknąć znacznych strat finansowych i stresu emocjonalnego.

Rodzaje oszustw związanych z podróżowaniem i biletami:

Fałszywe bilety lotnicze

Polega ona na tym, że oszuści sprzedają nieistniejące bilety lotnicze. Mogą zakładać fałszywe strony internetowe, które wyglądają jak prawdziwe strony linii lotniczych, wabić klientów obniżonymi cenami biletów, a następnie znikać po otrzymaniu płatności.

Oszukańcze pakiety wakacyjne

Dzieje się tak, gdy oszuści oferują kompleksowe pakiety wakacyjne po mocno obniżonych cenach. Po dokonaniu płatności przez klienta odkrywają, że pakiet nie istnieje lub nie zawiera tego, co obiecano.

Oszustwa związane z timeshare'ami

Oszuści mogą podszywać się pod sprzedawców lub odsprzedawców timeshare, obiecując świetne okazje na nieruchomości typu timeshare. Mogą żądać opłat z góry, a następnie zniknąć po dokonaniu płatności.

Oszustwa związane z podróżami i sprzedażą biletów

KONSEKWENCJE:

Oszustwa związane z podróżami i biletami mogą mieć poważne negatywne skutki, takie jak:

01 Strata finansowa

Najbardziej bezpośrednią konsekwencją oszustw związanych z podróżami i biletami jest strata finansowa. Oszuści pobierają płatności za nieistniejące usługi, pozostawiając ofiary bez możliwości odzyskania pieniędzy.

02 Kradzież tożsamości

Często oszustwa te polegają na tym, że ofiara podaje poufne dane osobowe i finansowe pod pretekstem rezerwacji podróży. Informacje te mogą być następnie wykorzystane do kradzieży tożsamości.

03 Stres emocjonalny

Padnięcie ofiarą takiego oszustwa może prowadzić do znacznego cierpienia emocjonalnego. Ekscytacja związana z zaplanowaną podróżą przeradza się w rozczarowanie i frustrację, nie wspominając o uczuciach naruszenia i bezbronności po oszukaniu.

Oszustwa związane z podróżami i sprzedażą biletów

SPOSOBY OCHRONY Z HISTORIĄ W TLE:

Pewnego dnia George otrzymał e-mail od internetowej agencji turystycznej oferującej fantastyczną ofertę na europejski pakiet wakacyjny. Oferta obejmowała loty, zakwaterowanie i wycieczki krajoznawcze do Rzymu, Paryża i Londynu. Pakiet był mocno przeceniony, a George, podekscytowany perspektywą wymarzonej podróży, postanowił zbadać sprawę dokładniej.
Kliknął na stronę internetową agencji turystycznej, która wyglądała profesjonalnie, z wysokiej jakości zdjęciami miejsc docelowych i entuzjastycznymi opiniami zadowolonych klientów. Przekonany George postanowił zarezerwować pakiet wakacyjny. Wprowadził dane swojej karty kredytowej i otrzymał e-mail potwierdzający rezerwację.
Dni zamieniły się w tygodnie, a George nie otrzymał żadnej dalszej wiadomości o swojej podróży. Zaczął się martwić i próbował skontaktować się z biurem podróży, ale okazało się, że ich numer telefonu jest wyłączony, a na jego e-maile nie ma odpowiedzi.

Historia George'a podkreśla potrzebę edukowania seniorów na temat oszustw internetowych. Im bardziej są obeznani z technologią, tym większe ryzyko im grożą. Poinformowanie ich o oznakach oszustwa, takich jak zbyt atrakcyjne oferty i znaczenie weryfikacji autentyczności firmy przed zakupem, może pomóc im zachować bezpieczeństwo. Dzielenie się takimi doświadczeniami może skutecznie ostrzegać seniorów przed oszustwami internetowymi.

KROK 1: Zweryfikuj autentyczność w porównaniu z natychmiastowym zaufaniem
George zaufał agencji turystycznej na podstawie jej profesjonalnie wyglądającej strony internetowej i referencji bez dalszej weryfikacji. George powinien był zweryfikować autentyczność agencji turystycznej, sprawdzając opinie klientów, potwierdzając jej rejestrację i adres fizyczny oraz oceniając wskaźnik odpowiedzi, kontaktując się z nią bezpośrednio.

KROK 2: Używaj bezpiecznych metod płatności zamiast podawać dane karty kredytowej
George wpisał dane swojej karty kredytowej bezpośrednio na stronie internetowej biura podróży, nie zapewniając bezpieczeństwa procesu płatności. George powinien był użyć bezpiecznych metod płatności, które oferują ochronę kupującego, takich jak karty kredytowe za pośrednictwem zaufanej platformy płatniczej, i unikać udostępniania danych karty kredytowej bezpośrednio na nieznanych stronach internetowych.

KROK 3: Komunikacja następcza kontra czekanie bez działania
George czekał tygodnie, nie otrzymując żadnej dalszej informacji o swojej podróży i próbował skontaktować się z agencją dopiero, gdy zaczął się martwić. George powinien był skontaktować się z agencją podróży wkrótce po dokonaniu rezerwacji, aby potwierdzić szczegóły i zapewnić ciągłą komunikację.

KROK 4: Zgłoś podejrzaną aktywność w porównaniu z opóźnioną reakcją
George odwlekał kontakt z firmą obsługującą jego kartę kredytową, dopóki nie zorientował się, że coś jest nie tak. George powinien był natychmiast zgłosić wszelkie podejrzane działania lub brak komunikacji do firmy obsługującej jego kartę kredytową, aby potencjalnie wstrzymać transakcję i zbadać sprawę.

Oszustwa związane z podróżami i sprzedażą biletów

SPOSOBY OCHRONY:

Dla seniorów kluczowe jest zabezpieczenie się przed oszustwami w podróżach i biletach, aby uniknąć znacznych strat finansowych, stresu emocjonalnego i potencjalnej kradzieży tożsamości. Oszuści często atakują seniorów, którzy mogą być mniej zaznajomieni z taktyką oszustw internetowych, wykorzystując ich zaufanie i ekscytację ofertami podróży. Chroniąc się, seniorzy mogą mieć pewność, że ich ciężko zarobione pieniądze nie zostaną skradzione, ich dane osobowe pozostaną bezpieczne, a ich plany podróży nie zostaną zrujnowane przez oszukańcze schematy.

Dokładnie zbadaj firmę:

Przed dokonaniem jakichkolwiek zakupów zawsze upewnij się, że przeprowadziłeś kompleksowe badanie firmy. Upewnij się, że poszukałeś opinii i ocen klientów, aby określić wiarygodność firmy i upewnić się co do jej legalności. Dzięki temu lepiej zrozumiesz reputację firmy wśród jej poprzednich klientów.

Używaj wyłącznie bezpiecznych metod płatności:

Podczas zakupów online, kluczowe jest korzystanie wyłącznie z bezpiecznych metod płatności. Unikaj dokonywania bezpośrednich przelewów bankowych i powstrzymaj się od udostępniania danych karty kredytowej na platformach, które nie są zabezpieczone. Zawsze bezpieczniej jest korzystać z opcji płatności, które oferują ochronę kupującego.

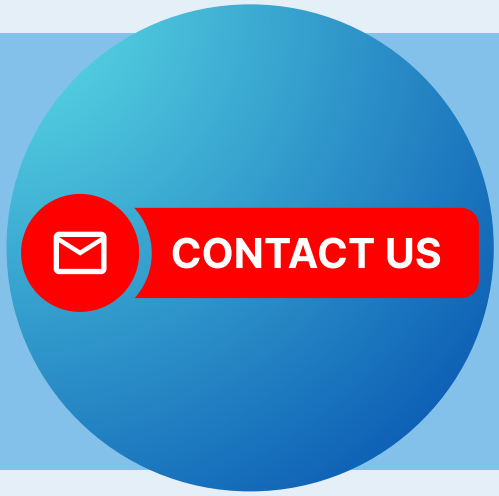
Oszustwa związane z podróżami i sprzedażą biletów

SPOSOBY OCHRONY:

Uważaj na oferty, które wydają się zbyt dobre, żeby były prawdziwe:

Jeśli oferta lub zniżka wydaje się zbyt dobra, aby była prawdziwa, prawdopodobnie taka jest. Bądź szczególnie ostrożny w przypadku mocno przecenionych cen takich rzeczy jak bilety lotnicze lub pakiety wakacyjne. Zawsze lepiej jest przeprowadzić trochę badań rynku, zanim rzucisz się na takie okazje.

- Przykład 3



Skontaktuj się bezpośrednio z linią lotniczą lub hotelem:

Jeśli otrzymasz wiadomość e-mail z ofertą tańszego lotu lub pobytu w hotelu, dobrym pomysłem jest skontaktowanie się bezpośrednio z linią lotniczą lub hotelem, aby zweryfikować ofertę. Dzięki temu upewnisz się, że oferta jest legalna i nie jest oszustwem.

Zapewnij bezpieczeństwo swoich danych osobowych:

Zachowaj ostrożność, udostępniając dane osobowe. Zawsze sprawdzaj, czy platforma jest bezpieczna, zanim wprowadzisz jakiekolwiek poufne informacje. Nigdy nie udostępniaj ważnych danych osobowych na platformach, które nie mają odpowiednich środków bezpieczeństwa.

Oszustwa subskrypcyjne

CHARAKTERYSTYKA ZAGROŻENIA:

Oszustwa subskrypcyjne to rodzaj oszustwa, w którym osoby są oszukiwane i nakłaniane do zapisywania się na drogie członkostwa lub usługi bez ich wiedzy. Oszustwa te często skutkują powtarzającymi się opłatami, które trudno anulować, co wpływa na osoby podatne na zagrożenia, w tym seniorów.

Rodzaje manipulacji w oszustwach subskrypcyjnych:

Oszukańcze reklamy i linki

Oszuści wykorzystują wprowadzające w błąd reklamy lub wyskakujące linki, aby nakłonić Cię do zapisania się na coś, co wydaje się być bezpłatną wersją próbną lub niedrogą usługą.

Ukryte warunki

Warunki subskrypcji, w tym koszt i czas trwania, są często ukryte drobnym drukiem lub nie są jasno wyjaśnione.

Automatyczne odnawianie

Po zapisaniu się subskrypcja odnawia się automatycznie, co wiąże się z nieoczekiwanymi opłatami na Twojej karcie kredytowej lub koncie bankowym.

Trudności z anulowaniem

Anulowanie subskrypcji jest celowo utrudniane poprzez skomplikowane procedury, obojętną obsługę klienta i niejasne zasady anulowania.

Oszustwa subskrypcyjne

KONSEKWENCJE:

Oszustwa subskrypcyjne mogą mieć poważne negatywne skutki, takie jak:

01 Strata finansowa

Padnięcie ofiarą oszustwa subskrypcyjnego może skutkować utratą ciężko zarobionych oszczędności. Możesz stracić znaczne kwoty pieniędzy z powodu powtarzających się opłat, których nie przewidzieli lub na które się nie zgodzili.

02 Kradzież tożsamości

Podawanie danych osobowych i danych płatniczych na fałszywych stronach internetowych może prowadzić do kradzieży tożsamości i dalszych szkód finansowych.

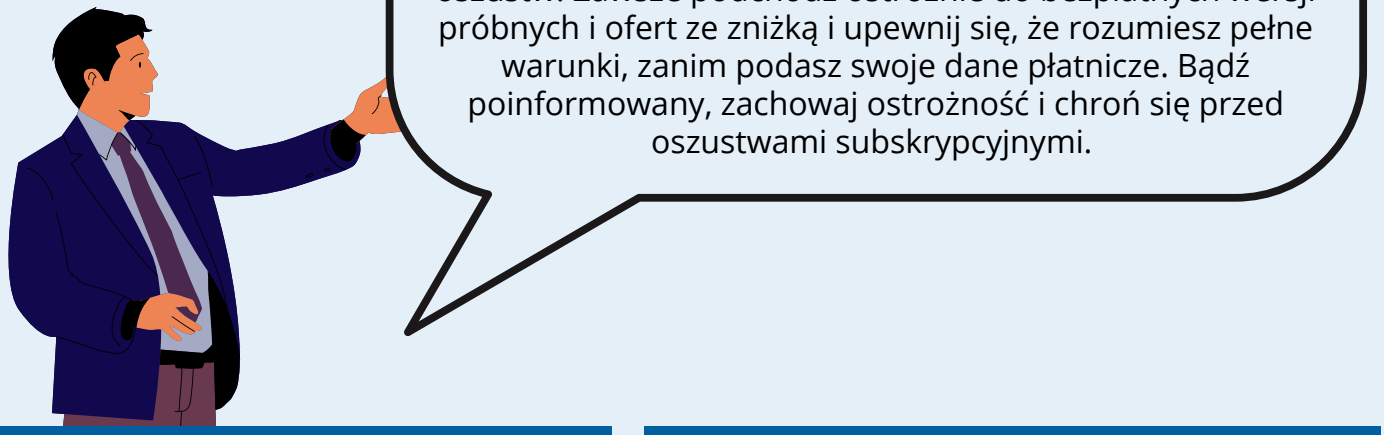
03 Stres emocjonalny

Frustracja i stres związane z koniecznością płacenia nieautoryzowanych opłat i próbami anulowania subskrypcji mogą mieć negatywny wpływ na Twoje samopoczucie emocjonalne.

Oszustwa subskrypcyjne

SPOSOBY OCHRONY Z HISTORIĄ W TLE

David zobaczył reklamę online oferującą bezpłatny okres próbny nowego suplementu witaminowego. Reklama głosiła, że wystarczy zapłacić niewielką opłatę za wysyłkę, aby się zapisać, a następnie otrzyma nieograniczoną ilość witamin do końca roku. Podekscytowany możliwością wypróbowania suplementu, postanowił podać dane swojej karty kredytowej, aby pokryć koszt wysyłki.
Podczas gdy to robił, David przypomniał sobie to, co przeczytał o pewnych stronach internetowych, które wyłudzały pieniądze od niewinnych ludzi.
Co więc zrobił Dawid?



Krok 1: Przeczytaj drobny druk

Zanim się zarejestrował, sprawdził, czy są jakieś wzmianki o trwających subskrypcjach lub dodatkowych opłatach.

Krok 2: Badania

Wyszukał firmę i przeczytał recenzje, aby dowiedzieć się, czy inni mieli podobne problemy

Krok 3: Monitoruj oświadczenia

Regularnie sprawdzał wyciągi, aby wcześnie wykryć nieautoryzowane opłaty.

Oszustwa subskrypcyjne

SPOSOBY OCHRONY:

Ochrona przed oszustwami subskrypcyjnymi jest kluczowa dla ochrony ciężko zarobionych pieniędzy. Oto kilka prostych kroków, które możesz podjąć.

Przeczytaj drobny druk:

Zawsze czytaj regulamin przed zapisaniem się do jakiejkolwiek usługi, zwłaszcza jeśli obejmuje ona bezpłatny okres próbny lub ofertę zniżkową

Uważaj na bezpłatne wersje próbne:

Uważaj na bezpłatne wersje próbne, które wymagają podania danych karty kredytowej. Sprawdź, czy wersja próbna przekształca się w płatną subskrypcję i jakie będą koszty.

Zbadaj firmę:

Sprawdź recenzje i oceny firmy oferującej subskrypcję. Upewnij się, że mają dobrą reputację i niezawodną obsługę klienta.

Oszustwa subskrypcyjne

SPOSOBY OCHRONY:

Monitoruj wyciągi bankowe:

Regularnie sprawdzaj wyciągi bankowe i wyciągi z kart kredytowych pod kątem nieautoryzowanych lub podejrzanych opłat.

Skonfiguruj alerty:

Użyj alertów konta, aby powiadomić Cię o wszelkich nowych opłatach lub transakcjach. W ten sposób możesz szybko zidentyfikować i zakwestionować nieautoryzowane opłaty.

Szukaj pomocy:

Jeśli padłeś ofiarą oszustwa subskrypcyjnego, skontaktuj się natychmiast ze swoim bankiem lub firmą obsługującą kartę kredytową, aby zgłosić nieautoryzowane opłaty. Mogą pomóc Ci zatrzymać dalsze opłaty i odzyskać pieniądze

Oszustwa polegające na tworzeniu fałszywych sklepów internetowych

CHARAKTERYSTYKA ZAGROŻENIA:

Fałszywe sklepy internetowe to fałszywe witryny stworzone tak, aby wyglądały jak legalne witryny handlowe. Ci oszuści stosują zwodnicze taktyki sprzedaży, aby nakłonić ludzi do dokonania zakupów. Zamiast otrzymać zamówione przedmioty, ofiary często otrzymują podrobione towary, przedmioty niskiej jakości lub nic. Ten rodzaj oszustwa może znacząco wpłynąć na osoby podatne na ataki, w tym osoby starsze.

Rodzaje manipulacji w fałszywych sklepach internetowych:

Ceny zbyt dobre, żeby były prawdziwe

Oszuści wabią klientów niewiarygodnie niskimi cenami lub ogromnymi zniżkami na popularne produkty.

Słaby projekt strony internetowej

Choć niektóre fałszywe strony są bardzo zaawansowane, wiele z nich ma kiepską konstrukcję, uszkodzone linki lub obrazy niskiej jakości.

Ograniczone informacje kontaktowe

Legalne firmy podają jasne dane kontaktowe, obejmujące adresy fizyczne i numery telefonów do działu obsługi klienta.

Brak recenzji lub fałszywe recenzje

Brak prawdziwych opinii klientów lub obecność wyłącznie pozytywnych i ogólnikowych recenzji może być sygnałem ostrzegawczym.

Brak bezpiecznego połączenia

Legalne witryny zakupowe używają bezpiecznych połączeń, aby chronić Twoje dane. Szukaj „https” i ikony kłódki na pasku adresu przeglądarki.

Oszustwa polegające na tworzeniu fałszywych sklepów internetowych

KONSEKWENCJE:

Oszustwa związane z fałszywymi sklepami internetowymi mogą powodować poważne negatywne skutki, takie jak:

01 Strata finansowa

Padnięcie ofiarą oszustwa dotyczącego fałszywych sklepów internetowych może skutkować utratą oszczędności. Możesz znaleźć się w sytuacji, w której będziesz mieć znacznie mniej pieniędzy niż się spodziewałeś, co wpłynie na Twoją zdolność do pokrycia codziennych wydatków i cieszenia się emeryturą.

02 Stres emocjonalny

Uświadomienie sobie, że zostali oszukani, może powodować znaczny stres emocjonalny. Seniorzy mogą czuć się zawstydzeni lub winni, że dali się nabrać na oszustwo. Ten wpływ emocjonalny może prowadzić do niepokoju, depresji i spadku zaufania do zakupów online i instytucji finansowych.

03 Kradzież informacji Persolan

Fałszywe sklepy internetowe często zbierają dane osobowe i finansowe podczas procesu realizacji transakcji. Informacje te mogą być wykorzystywane do kradzieży tożsamości, co prowadzi do nieautoryzowanych transakcji, otwierania nowych kont kredytowych w imieniu ofiary i innych form oszustw.

Oszustwa polegające na tworzeniu fałszywych sklepów internetowych

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Eva zobaczyła w mediach społecznościowych reklamę wysokiej klasy blendera ze zniżką 75%. Podekscytowana świetną okazją, kliknęła link i została przekierowana na stronę internetową, która wyglądała profesjonalnie, ale oferowała ograniczone dane kontaktowe. Strona nalegała na płatność przelewem bankowym, aby zapewnić sobie niską cenę.
Po dokonaniu płatności blender nie został dostarczony, a próby skontaktowania się z obsługą klienta pozostały bez odpowiedzi.

Co Ewa powinna była zrobić, żeby uniknąć oszustwa?

Fałszywe sklepy internetowe mogą być oszukańcze i powodować znaczne szkody finansowe i emocjonalne, zwłaszcza u osób starszych. Pozostając poinformowanym i stosując się do środków ochronnych opisanych poniżej, możesz zmniejszyć ryzyko stania się ofiarą tych oszustw. Zawsze poświęć czas na zbadanie i zweryfikowanie sklepów internetowych przed dokonaniem jakichkolwiek zakupów, aby zapewnić sobie bezpieczne i pewne zakupy.

Krok 1: Zbadaj witrynę
Powinna sprawdzić recenzje i poszukać danych kontaktowych sklepu.

Krok 2: Sprawdź bezpieczne połączenia
Upewnij się, że witryna ma „https” i ikonę kłódki.

Krok 3: Podchodź sceptycznie do ofert
Podważaj zniżki, które wydają się zbyt dobre, żeby były prawdziwe.

Krok 4: Używaj bezpiecznych metod płatności
Unikaj przelewów bankowych; zamiast tego używaj karty kredytowej.

Oszustwa polegające na tworzeniu fałszywych sklepów internetowych

SPOSOBY OCHRONY:

Pamiętajcie, drodzy seniorzy, ochrona przed fałszywymi sklepami internetowymi jest kluczowa dla ochrony waszych pieniędzy i emocji. Oto kilka prostych kroków, które możecie podjąć.

Zbadaj witrynę:

Sprawdź recenzje i oceny innych klientów. Skorzystaj z zaufanych witryn z recenzjami, aby zweryfikować wiarygodność sklepu. Wyszukaj dane kontaktowe sklepu i spróbuj skontaktować się z nim przed dokonaniem zakupu.

Sprawdź bezpieczne połączenia:

Upewnij się, że strona internetowa używa bezpiecznego połączenia („https” i ikona kłódki). Unikaj wprowadzania danych osobowych lub płatniczych na stronach bez bezpiecznego połączenia.

Podchodź sceptycznie do ofert, które wydają się zbyt dobre, żeby były prawdziwe:

Jeśli ceny wydają się niewiarygodnie niskie lub oferty są zbyt dobre, aby mogły być prawdziwe, prawdopodobnie takie są. Porównaj ceny z cenami innych renomowanych sprzedawców detalicznych.

Oszustwa polegające na tworzeniu fałszywych sklepów internetowych

SPOSOBY OCHRONY:

Używaj bezpiecznych metod płatności:

Używaj kart kredytowych do zakupów online, ponieważ oferują lepszą ochronę przed oszustwami. Unikaj korzystania z przelewów bankowych, kart przedpłaconych lub kryptowaluty do płatności.

Sprawdź szczegóły witryny:

Szukaj jasnych, szczegółowych opisów produktów i profesjonalnych zdjęć. Sprawdź dane kontaktowe witryny, w tym numery telefonów i adresy fizyczne

Zapoznaj się z polityką zwrotów:

Legalne sklepy mają jasne zasady zwrotu. Zachowaj ostrożność, jeśli brakuje tych informacji lub są one niejasne.

Oszukańcze zakupy za pośrednictwem reklam internetowych (kupowanie)

CHARAKTERYSTYKA ZAGROŻENIA:

Oszukańcza reklama online stanowi poważne zagrożenie, a oszuści wykorzystują platformy mediów społecznościowych, popularne strony internetowe, a nawet wyszukiwarki, takie jak Google. Fałszywe reklamy mogą przybierać różne formy, w tym wyskakujące okienka, banery, reklamy w mediach społecznościowych i treści sponsorowane. Te oszukańcze reklamy online mają na celu oszukanie niczego niepodejrzewających użytkowników, aby kliknęli je, co potencjalnie prowadzi do oszukańczych zakupów.

Rodzaje manipulacji zakupowych za pośrednictwem reklam internetowych:

Imitacja

Oszuści zazwyczaj wykorzystują materiały promocyjne (logo, podpisy, slogany itp.) pochodzące od prawdziwych, znanych marek. Następnie zaczynają wyświetlać reklamy ukierunkowane na ofiary oszustw. Oszuści mogą również stosować taktyki inżynierii społecznej, takie jak kuszące oferty, aby nakłonić użytkowników do klikania w te fałszywe reklamy.

Brak „prawdziwych" towarów

Ponieważ fałszywe reklamy mogą wydawać się bardzo profesjonalne i przekonujące, trudno je odróżnić od legalnych reklam. Kiedy ofiara klika reklamę, zazwyczaj trafia do fałszywego sklepu – gdzie może dojść do phishingu – lub do sklepu, który sprzedaje podróbki. W takich przypadkach (oprócz phishingu) istnieje również ryzyko, że ofiara nie otrzyma produktu lub otrzyma produkt o niższej jakości niż zapłacony.

Reklama złośliwa

Oszuści często używają fałszywych reklam z osadzonym złośliwym kodem, który może zainfekować urządzenia użytkowników po kliknięciu. Ta metoda, znana jako malvertising, stała się powszechną taktyką stosowaną przez cyberprzestępców w celu rozprzestrzeniania złośliwego oprogramowania za pośrednictwem fałszywych reklam.

Oszukańcze zakupy za pośrednictwem reklam internetowych (kupowanie)

KONSEKWENCJE

Bez względu na wybraną metodę, oszuści kryjący się za fałszywymi reklamami zawsze kierują się chęcią zysku finansowego.

01 Konsekwencje finansowe - bezpośrednia kradzież finansowa

Fałszywe reklamy oferujące mocno przecenione produkty znanych marek często ukrywają sklepy, których celem jest przechwycenie danych płatniczych i poufnych informacji podczas realizacji transakcji. Informacje te mogą zostać wykorzystane do kradzieży pieniędzy z kont, zainicjowania dodatkowych cyberataków lub sprzedaży innym cyberprzestępcom. W wielu przypadkach ofiary otrzymują podrobione towary lub nic.

02 Konsekwencje finansowe - koszty oprogramowania ransomware

Z powodu naruszenia systemu i naruszenia danych za pomocą metody malvertisingu mogą również wystąpić konsekwencje finansowe. Po kliknięciu reklamy złośliwe oprogramowanie zaczyna pobierać i instalować ransomware - rodzaj złośliwego oprogramowania, które szyfruje pliki - oszuści żądają zapłaty za jego uwolnienie. Koszty związane z zapłaceniem okupu, naprawą systemu i usunięciem złośliwego oprogramowania mogą być znaczne.

03 Kradzież tożsamości

Za pomocą metody phishingu oszuści podszywają się pod legalne marki, próbując nakłonić ofiary do udostępnienia swoich danych osobowych lub instalując oprogramowanie szpiegujące (za pomocą metody malvertsig), które potajemnie zbiera poufne informacje z urządzenia, takie jak dane logowania i dane finansowe, co może prowadzić do poważnej kradzieży tożsamości, podczas której poufne dane ofiar zostają wykorzystane w niewłaściwy sposób.

Oszukańcze zakupy za pośrednictwem reklam internetowych (kupowanie)

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Liza, regularna użytkowniczka różnych platform mediów społecznościowych, przeglądała Facebooka, gdy natknęła się na reklamę internetową oferującą bardzo ładny blender. Reklama pokazywała zdjęcie blendera najwyższej klasy w niezwykle niskiej cenie z obietnicą szybkiej dostawy.
Reklama wydawała się zbyt dobra, żeby była prawdziwa, ale Liza kliknęła ją przez pomyłkę i została przekierowana do sklepu internetowego, który początkowo wydawał się legalny... Jednak Liza rozpoznała znaki ostrzegawcze!

Niestety dla oszusta...

Liza wzięła udział w zaawansowanych warsztatach na temat oszustw w mediach społecznościowych.

KROK 1: Kontrola jakości

Po przekierowaniu Liza od razu zauważyła, że strona była źle zaprojektowana, zawierała wiele błędów gramatycznych, a jakość zdjęć była słaba w porównaniu do reklamy.

KROK 2: Kontrola techniczna

Liza zauważyła, że adres URL witryny nie odpowiadał nazwie marki. Zamiast tego tytuł składał się z losowych liter i cyfr.

KROK 3: Sprawdzanie legalności

Kiedy Liza sprawdziła stronę internetową, odkryła, że brakowało w niej kluczowych danych kontaktowych, takich jak adres firmy, numer telefonu i adres e-mail działu obsługi klienta.

KROK 4: Sprawdzanie opinii

Liza zauważyła również, że na stronie nie ma żadnych recenzji ani opinii klientów. Prawdziwy handlowiec internetowy zazwyczaj udostępnia recenzje i opinie od poprzednich klientów.

Oszukańcze zakupy za pośrednictwem reklam internetowych (kupowanie)

SPOSOBY OCHRONY:

Oszustwa z fałszywymi reklamami, w których przestępcy sprzedają fałszywe lub nieistniejące produkty w atrakcyjnych cenach i wykorzystują zainteresowanie seniorów zniżkami. Oszuści mogą przedłużać oszustwo, wymyślając wymówki na opóźnienia w dostawie, co dodatkowo zwiększa szkody finansowe dla ofiar.

Poniżej znajdziesz kilka dodatkowych wskazówek, na wypadek gdybyś znalazł się w podobnej sytuacji.

Aby chronić się przed potencjalnymi oszustwami, najbezpieczniej jest ignorować reklamy, zwłaszcza te, które wydają się podejrzane!

Uważaj też, gdzie klikasz lub stukasz! Zwracanie uwagi na to, gdzie na ekranie znajduje się twoja mysz lub palce, a także zwracanie uwagi na to, po której części strony się przewijasz, może pomóc ci uniknąć przypadkowych kliknięć lub stuknięć!

Należy zachować ostrożność klikając lub klikając jakikolwiek link, nawet ten znajdujący się na górze wyników wyszukiwania.

Zwróć szczególną uwagę na rozróżnienie reklam i prawdziwych wyników wyszukiwania. Reklamy zazwyczaj pojawiają się jako pierwsze i są oznaczone jako „Reklama”.

Uważaj, oszuści celowo płacą za umieszczanie reklam w wyszukiwarkach!

Oszukańcze zakupy za pośrednictwem reklam internetowych (kupowanie)

SPOSOBY OCHRONY:

Zawsze wpisuj adres URL witryny bezpośrednio w przeglądarce:

Aby upewnić się, że przeglądarka jest bezpieczna, poszukaj ikony kłódki i „https”, zweryfikuj adres URL (najedź kursorem na adres URL).

Chroń swój komputer:

Ważne jest, aby zainstalować i regularnie aktualizować oprogramowanie antywirusowe i zabezpieczające na swoim komputerze. Zapewni to ochronę komputera przed różnymi typami zagrożeń, takimi jak wirusy, ataki hakerów i złośliwe oprogramowanie.

Włącz funkcję blokowania wyskakujących okienek w swojej przeglądarce internetowej!

Oszukańcze zakupy za pośrednictwem reklam internetowych (kupowanie)

SPOSOBY OCHRONY:

Fałszywi sprzedawcy internetowi/oszuści zazwyczaj żądają zapłaty za pośrednictwem mało niezawodnych metod, takich jak przelewy bankowe (gdyż w porównaniu z innymi metodami płatności, takimi jak karty kredytowe, oferują one mniejszą ochronę w przypadku oszustwa) lub nieznanych platform płatniczych.

Nigdy nie dokonuj płatności w ten sposób! Ponadto nigdy nie ujawniaj swoich danych finansowych lub innych poufnych informacji!

Jeśli padniesz ofiarą oszustwa, postaraj się zebrać jak najwięcej dowodów i natychmiast zgłoś sprawę odpowiednim organom!

Zgłoś! Większość platform ma mechanizmy raportowania, aby rozwiązać takie problemy.

Skorzystaj z funkcji raportowania na platformie, dostępnej zazwyczaj za pośrednictwem przycisku „Zgłoś” w reklamie lub profilu użytkownika.

Po zgłoszeniu problemu należy oczekiwać na instrukcje od zespołu wsparcia platformy i zaprzestać wszelkich kontaktów z podejrzaną osobą.

Oszukańcze zakupy za pośrednictwem serwisów ogłoszeniowych (sprzedaż)

CHARAKTERYSTYKA ZAGROŻENIA:

Internetowe targi mogą być świetnym sposobem dla seniorów na zarobienie dodatkowych pieniędzy, ponieważ mogą sprzedawać swoje przedmioty, takie jak rękodzieło, antyki lub niepotrzebne artykuły gospodarstwa domowego itp. Umożliwia im to zarobienie dodatkowych pieniędzy, które mogą być wykorzystane na poprawę ich standardu życia lub na specjalne okazje. Seniorzy muszą być szczególnie czujni podczas sprzedaży, ponieważ te targi są również podatne na oszustów podszywających się pod potencjalnych nabywców.

Rodzaje manipulacji w oszustwach na rzecz tajnych nabywców:

Brak kontaktu osobistego

Oszuści są skłonni „kupić" przedmiot bez jego obejrzenia i często używają różnych wymówek, takich jak choroba, miesiąc miodowy lub podróż za granicę itp. Kontaktują się z ofiarami wyłącznie za pośrednictwem wiadomości tekstowych lub e-maili i unikają połączeń telefonicznych lub wideorozmów. Często proszą o wysłanie przedmiotu do ich „agenta wysyłkowego" lub organizują kuriera, który go odbierze. Wszystkie te metody komunikacji pozwalają oszustom ukryć swoją tożsamość.

Brak gotówki

Oszuści proszą wyłącznie o płatność czekiem, przekazem pieniężnym, przelewem bankowym, międzynarodowym przelewem środków, aplikacjami do płatności mobilnych itp., wysyłając fałszywe potwierdzenia płatności i mając nadzieję, że ofiary wyślą przedmiot, zanim zorientują się, że jest to oszustwo. Mogą używać „wymówek", takich jak problem z wysłaną płatnością, mogą prosić ofiary o zapłatę z góry za koszty transportu lub wysyłki i obiecać zwrot kosztów itp.

Nadpłata

Oszuści zazwyczaj oferują ofiarom więcej pieniędzy niż żądana cena. Powody są różne - mogą twierdzić, że rekompensują „kłopoty" ofiary, pokrywają rzekome koszty wysyłki lub udają, że popełnili błąd w kwocie płatności. Jednak gdy ofiary otrzymają nadpłatę, oszuści zażądają zwrotu nadwyżki.

Oszukańcze zakupy za pośrednictwem serwisów ogłoszeniowych (sprzedaż)

KONSEKWENCJE

Ofiary oszustw typu „not to buy” mogą doświadczyć następujących negatywnych skutków:

01 Konsekwencje finansowe

Ofiary mogą ponieść konsekwencje finansowe, takie jak strata pieniężna wartości przedmiotów, jeśli wysłały przedmioty bez otrzymania zapłaty. Jeśli nastąpiła nadpłata i ofiary zwróciły pieniądze, prawdopodobnie odkryją, że początkowa płatność była oszustwem — czek zostanie odliczony lub płatność online klienta zostanie odrzucona — w takim przypadku ofiary straciły pieniądze, które „zwróciły”, i wartość pieniężną przedmiotów.

02 Konsekwencje emocjonalne

U ofiary mogą rozwinąć się różne objawy, w tym negatywne myśli o sobie. Ofiary mogą myśleć, że nie są mądre lub że coś jest nie tak z ich zdolnością do oceniania innych. Często obwiniają siebie za przestępstwo, czując, że były zbyt ufne, i czują się złe, smutne, zdradzone, bezradne i zawstydzone.

03 Konsekwencje prawne

Jeśli ofiara zgodziła się i przyjęła płatność czekiem, ale czek został sfałszowany, nieświadoma ofiara będzie pociągnięta do odpowiedzialności prawnej za próbę zrealizowania nielegalnego czeku, gdy bank wykryje fałszerstwo. Ponadto ofiara może mieć trudności w przyszłych transakcjach finansowych.

Oszukańcze zakupy za pośrednictwem serwisów ogłoszeniowych (sprzedaż)

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Leon zamieścił ogłoszenie na portalu Facebook Marketplace, w którym domagał się kupna używanego roweru za 200 euro, i natychmiast otrzymał wiadomość od „Tima", który chciał go kupić bez negocjacji ceny i zaoferował nawet 30 euro więcej na pokrycie kosztów przesyłki.
Leonowi wydało się dziwne, że Tim nie chciał zobaczyć produktu osobiście, mimo że mieszkał w tym samym mieście. Tim chciał również zapłacić za produkt przez PayPal i poprosił o numer ubezpieczenia społecznego i adres domowy Leona. Wtedy Leon szybko się wycofał!

Niestety dla oszusta...

Leon monitorował kampanię informacyjną wśród społeczności użytkowników i zdobywał wiedzę na temat częstych prób tego typu oszustw oraz środków zapobiegawczych.

KROK 1: Rozpoznawanie podejrzanego zachowania

Leon uważał za dziwne, że Tim nie chciał zobaczyć produktu osobiście, mimo że mieszkał w tym samym mieście. To był pierwszy znak ostrzegawczy, ponieważ uczciwi kupujący zazwyczaj wolą obejrzeć przedmioty przed dokonaniem zakupu.

KROK 2: Badanie

Leon zbadał profil Tima i znalazł podejrzane dane kontaktowe i niespójną komunikację. Leon zablokował Tima i natychmiast przerwał wszelką komunikację, zapobiegając w ten sposób dalszym zagrożeniom.

KROK 3: Ochrona

Tim chciał zapłacić przez PayPal, co samo w sobie nie jest podejrzane, ale poprosił również o numer ubezpieczenia społecznego i adres domowy Leona, co jest bardzo nietypowe i niepotrzebne. Leon świadomie postanowił nie dzielić się tymi informacjami.

KROK 4: Informowanie/zgłaszanie

Leon podzielił się swoim doświadczeniem ze społecznością i zgłosił profil Tima na platformie. Dzięki temu pomógł zwiększyć świadomość i chronić innych użytkowników.

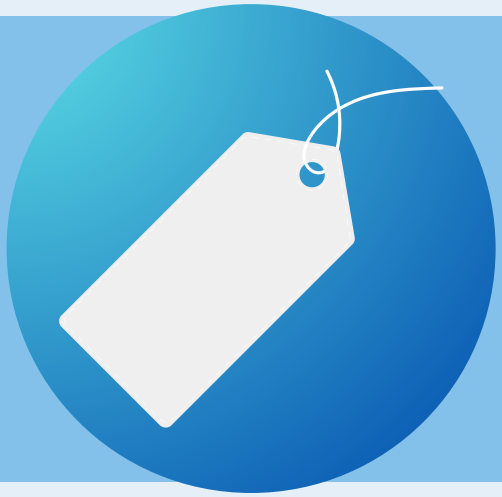
Oszukańcze zakupy za pośrednictwem serwisów ogłoszeniowych (sprzedaż)

SPOSOBY OCHRONY:

Jeśli wystawiasz swoje przedmioty na sprzedaż za pośrednictwem internetowych portali ogłoszeniowych, zapoznaj się z poniższymi prostymi wskazówkami, które pozwolą Ci zwiększyć swoją pewność siebie i ochronić się przed oszustami podającymi się za potencjalnych nabywców.

Zachowaj ostrożność, gdy ktoś oferuje Ci więcej niż żądana cena (chyba że sprzedajesz przedmiot z wieloma konkurencyjnymi ofertami). Nie wchodź w interakcję z nikim, kto oferuje Ci płatność w wyższej kwocie, oczekując, że odeślesz nadwyżkę.

Natychmiast odrzuć taką płatność i nalegaj na otrzymanie prawidłowej kwoty w nowej transakcji.



Poproś o płatność gotówką:

Jeśli nie jest to możliwe, nie wysyłaj przedmiotu do momentu otrzymania zapłaty i upewnij się, że płatność jest prawidłowa.

Jeśli wyślesz przesyłkę przed zapłatą, nie będziesz miał możliwości jej zwrotu!

Oszukańcze zakupy za pośrednictwem serwisów ogłoszeniowych (sprzedaż)

SPOSOBY OCHRONY:

Nie ufaj potwierdzeniom płatności e-mailem – mogą być fałszywe! Sprawdź bezpośrednio swoje konto bankowe, aby zobaczyć, czy płatność została otrzymana

Najlepiej jest mieć do czynienia z lokalnymi kupcami, których możesz spotkać osobiście i akceptować tylko gotówkę, aby uniknąć możliwych oszustw. Nie płać żadnych widocznych kosztów wysyłki ani opłat za przelew. Zaleca się szczególną ostrożność przy sprzedaży kupującym za granicą.

Zignoruj wszelkie prośby o podanie zbędnych informacji. Podaj tylko informacje ściśle niezbędne do sfinalizowania transakcji.

Jeśli sprzedajesz przedmiot, nie klikaj na żaden link przesłany Ci przez kupującego i nie wysyłaj kupującemu żadnych informacji, które mogłyby umożliwić mu dostęp do Twojego konta bankowego.

Zgłoś! Większość platform ma mechanizmy raportowania, aby rozwiązać takie problemy.
Skorzystaj z funkcji raportowania na platformie, dostępnej zazwyczaj za pośrednictwem przycisku „Zgłoś" w reklamie lub profilu użytkownika.
Po zgłoszeniu problemu należy oczekiwać na instrukcje od zespołu wsparcia platformy i zaprzestać wszelkich kontaktów z podejrzaną osobą.

Dodatkowe informacje

OSZUSTWA ZWIĄZANE Z PODRÓŻAMI I BILETAMI

- 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-bilions-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

OSZUSTWA ZWIĄZANE Z SUBSKRYPCJĄ

- 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/coordyned-actions/consumer-frequent-traps-and-scams_en
- https://www.evz.de/en/shopping-internet/oszustwa-internetowe/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. Which.co.uk/news/article/5-subscription-scams-and-traps-to-watch-out-for-aYwJA0u8EFZ9

Dodatkowe informacje

OSZUSTWA POLEGAJĄCE NA TWORZENIU FAŁSZYWYCH SKLEPÓW INTERNETOWYCH

- 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=ltI7DXrNQCA
- https://www.youtube.com/watch?v=CQYmfcLW_oc

OSZUKAŃCZE ZAKUPY POPRZEZ REKLAMY ONLINE (KUPNO)

- 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/ przykłady 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/pl/artykuły/85/oszustwa-adresowe-w-mediach-społecznościowych
- https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_fradulentadvertisingonline_execsummary_july2020_final.pdf
- https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

Dodatkowe informacje

OSZUSTWA W ZAKUPACH NA PORTALACH OGŁOSZENIOWYCH (SPRZEDAŻ)

- 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 -sites-small-ads/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

ROZDZIAŁ 5. MANIPULACJA TOŻSAMOŚCIĄ I WYKORZYSTYWANIE ZAUFANIA PUBLICZNEGO

Współczesne oszustwa coraz częściej polegają na manipulacji tożsamością i wykorzystywaniu zaufania do instytucji publicznych, co stawia seniorów w szczególnie bezbronnej sytuacji. Przestępcy nie tylko podszywają się pod godne zaufania instytucje, ale także wykorzystują zaawansowane technologie, aby osiągnąć swoje cele. W tym rozdziale omówimy najczęstsze oszustwa dotyczące tożsamości i zaufania, aby pomóc seniorom rozpoznać i uniknąć tych zagrożeń.

Poważne zagrożenia dla seniorów obejmują fałszywe oskarżenia o popełnienie przestępstwa, w których oszuści fałszywie oskarżają seniorów w celu wyłudzenia pieniędzy lub informacji. Podszywanie się pod rząd to kolejna niebezpieczna metoda, w której przestępcy podszywają się pod rząd, aby uzyskać dane osobowe lub pieniądze. Technologia deepfake umożliwia tworzenie fałszywych, ale przekonujących nagrań, co może prowadzić do poważnych konsekwencji. Oszustwa usługowe podszywające się pod instytucje rządowe często obejmują fałszywe oferty, których celem jest wyłudzenie pieniędzy. Fałszywe konta są wykorzystywane do szantażu seniorów poprzez groźby ujawnienia fałszywych informacji.

Zrozumienie tych zagrożeń i ich mechanizmów jest kluczowe dla seniorów, aby skutecznie chronić swoją tożsamość, finanse i zaufanie do instytucji publicznych. W tym rozdziale omówimy te kwestie szczegółowo, aby pomóc Ci rozpoznać i uniknąć takich oszustw.

Zarzuty udziału w przestępstwie

CHARAKTERYSTYKA ZAGROŻENIA:

Oszukiwanie użytkownika na pieniądze poprzez podszywanie się pod sędziego, policjanta lub prokuratora i twierdzenie, że jego nazwisko jest powiązane z terroryzmem. „Zarzuty udziału w przestępstwie" odnoszą się do zarzutów lub oskarżeń, że osoba, organizacja lub nawet seniorzy uczestniczyli w nielegalnych działaniach. Zarzuty te nie zostały jeszcze udowodnione i wymagają dochodzenia w celu ustalenia ich zasadności. Charakter przestępstwa może być bardzo różny, w tym oszustwo, kradzież lub inne bezprawne działania, a takie zarzuty mogą mieć poważne konsekwencje prawne i społeczne dla oskarżonego, w tym seniorów. Seniorzy mogą być szczególnie podatni na takie zarzuty ze względu na ich potencjalny brak znajomości technologii cyfrowej i typowych taktyk oszustw.

Rodzaje zarzutów o udział w przestępstwie:

Zaangażowanie w sieć finansowania terroryzmu

Twierdzenie, że konto bankowe ofiary zostało powiązane z transakcjami finansującymi działalność terrorystyczną, jest rodzajem oszustwa, którego celem jest zastraszenie ofiary i wywołanie paniki. W tym scenariuszu oszust podkreśla powagę zarzutu. Oszust zazwyczaj będzie żądał natychmiastowego działania od ofiary, co może oznaczać zapłacenie „grzywny" lub „opłaty". Podczas całej interakcji oszust stosuje taktykę manipulacji psychologicznej, aby wywołać panikę u ofiary i zmanipulować ją, aby udostępniła swoje dane osobowe i/lub pieniądze. Może nawet ostrzec ofiarę, aby nie kontaktowała się z nikim i zachowała to w tajemnicy.

Powiązania ze znanymi organizacjami terrorystycznymi

W tym scenariuszu oszust może skontaktować się z ofiarą i przedstawić się jako osoba autorytetu, twierdząc, że jest częścią organu ścigania lub systemu sądowniczego. Ostrzega ofiarę, że jej nazwisko zostanie znalezione na liście osób powiązanych ze znaną organizacją terrorystyczną. Może podać zmyślone dane, aby przestraszyć ofiarę i wywołać panikę. Żądając od ofiary natychmiastowego działania, może użyć gróźb lub zastraszającej mowy, aby utrzymać kontrolę.

Podejrzana historia podróży lub aktywności

W tym scenariuszu oszust kontaktuje się z ofiarą, podszywając się pod policjanta, sędziego lub prokuratora. Informuje ofiarę, że jej historia podróży lub pewne działania wzbudziły podejrzenia. Może wspomnieć o konkretnych miejscach, które ofiara faktycznie odwiedziła. Aby było to bardziej wiarygodne, może dodać szczegóły, takie jak daty podróży lub nazwiska podejrzanych terrorystów, z którymi, jak sądzi, się kontaktowałeś. Podobnie jak w innych scenariuszach, oszust wywiera presję na ofiarę, aby podejmowała szybkie decyzje i stosuje taktykę manipulacji, aby uzyskać od niej dane osobowe.

Zarzuty udziału w przestępstwie

KONSEKWENCJE:

Błędy wynikające z udziału w przestępstwie mogą mieć poważne negatywne skutki, takie jak:

01 Uszkodzenie reputacji

Bycie powiązanym z przestępstwem, nawet jeśli zarzuty nie są udowodnione, może mieć poważne konsekwencje dla reputacji danej osoby. Może to wpłynąć na relacje osobiste, a także na możliwości zawodowe.

02 Konsekwencje prawne

Jeśli zarzuty doprowadzą do dochodzenia karnego i osoba zostanie uznana za winną, może ponieść konsekwencje prawne. Mogą one obejmować grzywny, okres próbny, a nawet pozbawienie wolności.

03 Stres emocjonalny

Oskarżenie o popełnienie przestępstwa może powodować znaczny stres emocjonalny. Osoba może odczuwać strach, wstyd lub zażenowanie, a te emocje mogą mieć długofalowe skutki dla jej dobrego samopoczucia psychicznego.

Zarzuty udziału w przestępstwie

KONSEKWENCJE:

04 Kradzież tożsamości i wykorzystywanie jej do popełniania kolejnych przestępstw

Oskarżenia o kradzież tożsamości mogą doprowadzić do dalszych działań przestępczych podejmowanych w imieniu ofiary, co zaostrzy konsekwencje prawne i osobiste.

05 Utrata środków

Ofiary oskarżeń o przestępstwa, zwłaszcza te obejmujące oszustwa finansowe, mogą ponieść znaczne straty finansowe, bezpośrednio z powodu kradzieży lub pośrednio z powodu kosztów prawnych i innych wydatków związanych z obroną.

06 Zarażanie urządzeń wirusami

W sprawach dotyczących oskarżeń o cyberprzestępstwa istnieje ryzyko, że urządzenia oskarżonego mogą stać się celem ataku i zostać zainfekowane wirusami lub złośliwym oprogramowaniem, co może doprowadzić do naruszenia bezpieczeństwa danych i dalszych komplikacji.

Zarzuty udziału w przestępstwie

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Pewnego dnia Rita otrzymała e-mail z informacją, że jej nazwisko jest zamieszane w głośne śledztwo w sprawie przestępstwa związanego z oszukańczą transakcją online. E-mail wydawał się pochodzić z lokalnego wydziału policji i był dość szczegółowy, co wywołało poczucie pilności i strachu.

W e-mailu polecono Ricie kliknąć link i wprowadzić swoje dane osobowe, w tym numer ubezpieczenia społecznego i dane konta bankowego, rzekomo w celu zweryfikowania jej tożsamości i oczyszczenia jej nazwiska ze śledztwa. Przerażona oskarżeniami i zdesperowana, by natychmiast rozwiązać problem, Rita zastosowała się do instrukcji.

Kilka dni później otrzymała telefon z banku informujący o podejrzanych działaniach na jej koncie. W tym momencie Rita zdała sobie sprawę, że została oszukana przez oszusta, który wykorzystał oskarżenia o udział w przestępstwie jako podstęp.

Ta historia podkreśla znaczenie edukowania seniorów na temat ryzyka i taktyk oszustw internetowych. Jak wykazano w przypadku Rity, oszuści mogą wykorzystywać ich brak znajomości świata cyfrowego i stosować taktyki straszenia, aby nakłonić ich do ujawnienia poufnych danych osobowych. Edukując seniorów na temat tych zagrożeń i ucząc ich, jak weryfikować zasadność takich próśb, możemy chronić ich przed padnięciem ofiarą takich oszustw.

KROK 1: Weryfikacja
Jeśli Rita otrzymała nieoczekiwanego maila, zwłaszcza od rzekomego organu rządowego lub organów ścigania, nie powinna odpowiadać bezpośrednio. Powinna znaleźć oficjalne dane kontaktowe niezależnie i zweryfikować.

KROK 2: Chroń dane osobowe
Rita nie powinna udostępniać poufnych informacji, takich jak numer ubezpieczenia społecznego lub dane bankowe, za pośrednictwem poczty e-mail. Legalne organizacje nie proszą o to za pośrednictwem poczty e-mail.

KROK 3: Monitoruj konta
Rita powinna regularnie sprawdzać swoje konta finansowe i internetowe pod kątem podejrzanej aktywności, aby wcześnie wykryć oszustwa i zabezpieczyć swoje konta.

KROK 4: Użyj oprogramowania zabezpieczającego
Instalowanie i aktualizowanie oprogramowania zabezpieczającego może chronić Ritę przed zagrożeniami online, takimi jak wirusy, malware i phishing. Oprogramowanie może skanować w poszukiwaniu zagrożeń i blokować podejrzane witryny.

Zarzuty udziału w przestępstwie

SPOSOBY OCHRONY:

Seniorzy muszą chronić się przed oskarżeniami o przestępstwa, które mogą zaszkodzić ich reputacji, prowadzić do problemów prawnych i powodować cierpienie emocjonalne. Często padają ofiarą oszustw z powodu nieznajomości technologii cyfrowych, co czyni ich podatnymi na oszustwa. Środki zapobiegawcze mogą chronić ich finanse, dane osobowe i dobre samopoczucie.

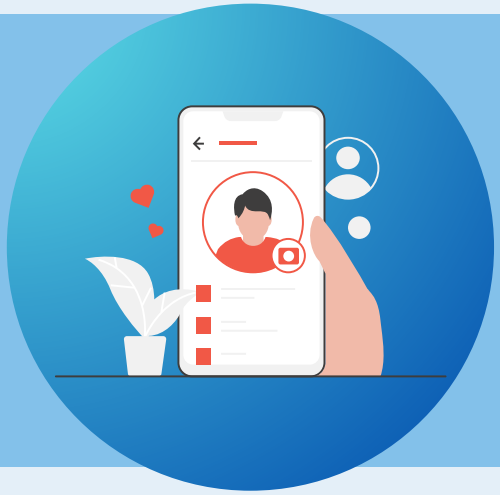
Weryfikacja nieoczekiwanych żądań:
Zawsze bądź czujny, gdy otrzymasz nieoczekiwane e-maile lub komunikaty, zwłaszcza ze źródła podającego się za organ rządowy, agencję ścigania lub usługę, z której korzystasz. Zamiast odpowiadać bezpośrednio na e-mail lub klikać na jakiekolwiek linki, niezależnie znajdź oficjalne dane kontaktowe organizacji i skontaktuj się z nią w celu weryfikacji. W ten sposób możesz potwierdzić, czy prośba jest uzasadniona, czy też jest potencjalnym oszustwem.

Zachowaj ostrożność przy udostępnianiu danych osobowych:
Twoje dane osobowe są cenne i powinny być chronione za wszelką cenę. Nigdy nie podawaj poufnych danych osobowych, takich jak numer ubezpieczenia społecznego, dane konta bankowego lub inne dane osobowe w odpowiedzi na prośbę e-mailową lub niezweryfikowane źródło. Legalne organizacje zazwyczaj nie proszą o tego rodzaju informacje za pośrednictwem poczty e-mail lub niezamawianej komunikacji.

Zarzuty udziału w przestępstwie

SPOSOBY OCHRONY:

Regularne monitorowanie kont:
Regularne monitorowanie kont finansowych i internetowych może pomóc Ci wcześnie wykryć podejrzaną aktywność. Jest to kluczowe dla zapobiegania dalszym szkodom, ponieważ możesz natychmiast zgłosić aktywność odpowiednim organom lub dostawcy usług i podjąć kroki w celu zabezpieczenia swojego konta.



Stosowanie bezpiecznych i unikalnych haseł:
Używanie silnych i unikalnych haseł do wszystkich kont online jest podstawowym środkiem bezpieczeństwa. Silne hasło zawiera mieszankę liter, cyfr i symboli i nie jest łatwe do odgadnięcia. Nie używaj tego samego hasła na wielu kontach. Jeśli jedno konto zostanie naruszone, inne pozostaną bezpieczne.

Instalacja oprogramowania zabezpieczającego:
Instalowanie i regularne aktualizowanie oprogramowania zabezpieczającego na komputerze zapewnia pierwszą linię obrony przed wieloma zagrożeniami online. Obejmuje to wirusy, złośliwe oprogramowanie, ransomware i próby phishingu. Może ono skanować system pod kątem zagrożeń, blokować podejrzane witryny i zapewniać ochronę w czasie rzeczywistym przed atakami złośliwego oprogramowania.

Manipulacje podszywające się pod instytucje państwowe

CHARAKTERYSTYKA ZAGROŻENIA:

Podszywanie się pod urzędników państwowych to rodzaj oszustwa, w którym oszuści podszywają się pod przedstawicieli różnych agencji rządowych, takich jak organy podatkowe, policja lub fundusze emerytalne. Oszustwa te stanowią poważne zagrożenie dla danych osobowych i bezpieczeństwa finansowego osób fizycznych. Oszuści stosują różne taktyki, aby oszukać swoje ofiary, ale istnieje kilka typowych oznak, na które należy zwrócić uwagę.

Rodzaje manipulacji podszywających się pod instytucje państwowe:

Niezamawiana komunikacja

Oszuści zazwyczaj kontaktują się z ofiarami niespodziewanie przez telefon, e-mail, SMS-y, a nawet reklamy online. Początkowym celem jest oszukanie ofiar, aby nawiązały kontakt ze oszustami. Zazwyczaj mają podstawowe dane osobowe zamierzonej ofiary, aby sprawiać wrażenie legalnej. Po nawiązaniu kontaktu oszuści zażądają od ofiary podania poufnych informacji, zapłacenia „kary" (za pomocą nietypowych metod płatności) lub wykonania innych czynności.

Udawanie godnego zaufania

W rozmowach z ofiarami podają wiele fałszywych informacji o sobie i swoich obowiązkach, a także używają oficjalnie brzmiących terminów, fałszywie sugerując przynależność do rządu. W komunikacji za pośrednictwem poczty lub online używają oficjalnie wyglądających pieczęci rządowych, logotypów, nazwisk prawdziwych urzędników na stanowiskach, fałszywych stron internetowych i domen e-mail, aby oszukać ofiary i zmusić je do zaufania. Wiadomości e-mail często zawierają również załącznik (zazwyczaj plik PDF) i ostrzeżenie o konieczności przeczytania załączonych dokumentów.

Zagrożenia i pilność

Oszuści stosują zastraszanie, terminy i grożą podjęciem kroków prawnych lub grzywnami, aby wymusić natychmiastową odpowiedź. Na przykład e-mail rzekomo pochodzący od policji może grozić wszczęciem postępowania karnego, jeśli ofiara nie odpowie w określonym czasie. Te taktyki mogą wywołać panikę i osłabić osąd, powodując, że nawet osoby zazwyczaj racjonalne reagują ze strachu.

Manipulacje podszywające się pod instytucje państwowe

KONSEKWENCJE

Oszustwa rządowe polegają dosłownie na fakcie, że seniorzy są świetnymi potencjalnymi ofiarami, ponieważ starsze pokolenia często bardziej ufają instytucjom rządowym i są przyzwyczajone do większego szacunku dla władzy i instytucji. Ponadto mają oszczędności i prawdopodobnie otrzymują jakąś formę świadczeń rządowych.

01 Konsekwencje finansowe

Ofiary tracą pieniądze, które przekazują oszustom jako zapłatę za rozwiązanie fikcyjnych zobowiązań podatkowych, prawnych lub innych. Oprócz utraconych pieniędzy ofiary mogą ponieść dodatkowe koszty rozwiązania sytuacji. Jeśli oszuści uzyskają dostęp do ich konta bankowego, może to doprowadzić do dalszych strat finansowych z powodu nieautoryzowanych zakupów. W najgorszym przypadku konto może zostać opróżnione, powodując nieodwracalne szkody, zwłaszcza u osób starszych, które mogły stracić ciężko zarobione oszczędności.

Manipulacje podszywające się pod instytucje państwowe

02 Kradzież tożsamości

Jeśli ofiara doświadczy utraty poufnych danych osobowych, może to prowadzić do dalszych strat finansowych, ponieważ oszuści mogą wykorzystać informacje z paszportu lub dowodu osobistego do otwarcia nowych kont bankowych i zaciągnięcia pożyczek w imieniu ofiary bez jej wiedzy. W przypadku kradzieży tożsamości w służbie zdrowia ofiara może stracić świadczenia zdrowotne, podczas gdy w przypadku kradzieży tożsamości podatkowej może zostać bez zwrotu podatku. Kradzież tożsamości jest traumatycznym doświadczeniem i ma wiele innych konsekwencji, takich jak wykorzystywanie tożsamości ofiary przez przestępców do popełniania przestępstw (w tym cyberprzestępstw), co potencjalnie prowadzi do tego, że ofiara poniesie konsekwencje prawne za działania, których nie popełniła.

03 Utrata zaufania do instytucji publicznych

Tego typu oszustwa mogą mieć znaczący wpływ na zaufanie jednostek do instytucji publicznych, ponieważ ofiary mogą odczuwać głębokie poczucie zdrady i utraty zaufania do tych instytucji. Może to spowodować, że staną się sceptyczni wobec prawdziwych komunikatów i mniej chętni do współpracy, ponieważ mogą zacząć kwestionować uzasadnione prośby i informacje, co prowadzi do braku chęci do angażowania się w instytucje rządowe. Zwiększone obawy dotyczące potencjalnych oszustw mogą również wpłynąć na opinię publiczną i zmniejszyć zaufanie do zdolności organów rządowych do skutecznej ochrony i służby obywatelom.

Manipulacje podszywające się pod instytucje państwowe

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Simon odebrał telefon od osoby, która oficjalnym tonem przedstawiła się jako pracownica urzędu skarbowego. Powiedziała mu, że zalega z podatkami i zostanie aresztowany i osadzony w więzieniu, jeśli nie spłaci długu natychmiast, płacąc jedną z kryptowalut. Pomimo uporczywości i zastraszania rozmówcy, Simon odłożył słuchawkę.

Niedługo po zakończeniu rozmowy otrzymał wiadomość o tej samej treści, co rozmowa, która zawierała również podejrzany link do strony internetowej urzędu skarbowego.

Niestety dla oszusta...

Simon wziął udział w wykładzie edukacyjnym na temat oszustw podszywających się pod przedstawicieli rządu, zorganizowanym przez Administrację Podatkową.

KROK 1: Rozpoznawanie sygnałów ostrzegawczych
Simon początkowo się przestraszył, ale rozpoznał oznaki oszustwa, gdy rozmówca wspomniał o uregulowaniu zaległych zobowiązań podatkowych za pomocą kryptowaluty, co nie jest standardową metodą rozliczania podatków.

KROK 2: Identyfikacja nietypowego zachowania
Ponieważ rozmówca groził aresztowaniem i uwięzieniem, Simon miał wątpliwości co do legalności tych gróźb i natychmiast zakończył rozmowę.

KROK 3: Weryfikacja
Simon natychmiast sprawdził, czy numer telefonu jest powiązany z odpowiednim organem podatkowym i stwierdził, że nie. Podejrzana domena zawarta w wiadomości tekstowej tylko potwierdziła jego podejrzenia, więc zablokował numer.

KROK 4: Raportowanie
Simon skontaktował się z oficjalnym urzędem skarbowym, korzystając z oficjalnego numeru telefonu, i poinformował o próbie oszustwa.

Manipulacje podszywające się pod instytucje państwowe

SPOSOBY OCHRONY:

Poniżej znajdziesz kilka dodatkowych wskazówek, na wypadek gdybyś znalazł się w podobnej sytuacji.

Rozłącz się, Usuń, Nie odpowiadaj:

Ignoruj połączenia, wiadomości e-mail, SMS-y i wiadomości w mediach społecznościowych, które rzekomo pochodzą od instytucji rządowych i w których proszą o zapłatę, potwierdzenie poufnych informacji lub podanie innych informacji.

Prawdziwa instytucja rządowa nigdy nie zadzwoni, nie wyśle wiadomości e-mail, SMS ani wiadomości w mediach społecznościowych, aby żądać pieniędzy lub informacji.

Nie utrzymuj kontaktu ze oszustami, nie podawaj im swoich danych osobowych i nie dokonuj żadnych płatności!

Legalne instytucje stosują się do określonych procedur i zasad dotyczących płatności, zobowiązań finansowych i innych kwestii administracyjnych. Nigdy nie poproszą Cię o zapłatę przy użyciu takich metod płatności, jak kryptowaluty, usługi przekazów pieniężnych, platformy płatnicze itp.

Manipulacje podszywające się pod instytucje państwowe

SPOSOBY OCHRONY:

Nie polegaj wyłącznie na danych kontaktowych podanych w wiadomościach e-mail i SMS!
Zanim odpowiesz na korespondencję rzekomo pochodzącą z instytucji rządowej, upewnij się, że samodzielnie potwierdzisz tożsamość nadawcy.

Aby mieć pewność, że komunikacja jest autentyczna, poszukaj oficjalnych danych kontaktowych odpowiedniej agencji i skontaktuj się z nią bezpośrednio!

Natychmiast zerwij kontakt z osobą, która próbuje Ci grozić lub zastraszać!
Groźby i zastraszanie mogą prowadzić do cierpienia emocjonalnego i szkód psychologicznych.

Pamiętaj!

Legalne instytucje rządowe nie stosują gróźb aresztowania lub więzienia w celu wyegzekwowania zobowiązań podatkowych lub innych długów.

Jeśli stałeś się ofiarą oszustwa i przelałeś pieniądze, a później zorientowałeś się, że to było oszustwo, natychmiast skontaktuj się ze swoim bankiem i złóż skargę. Zgłoś szkodę na policję.

Jeżeli podczas oszustwa ujawniono jakiekolwiek dane osobowe, należy niezwłocznie powiadomić odpowiednią instytucję, którą oszuści wykorzystali do swoich celów.

Manipulacja przy użyciu technologii deepfake

CHARAKTERYSTYKA ZAGROŻENIA:

Deepfake Fraud odnosi się do rodzaju oszustwa, w którym sztuczna inteligencja jest używana do tworzenia lub modyfikowania wideo, audio lub obrazów w celu oszukiwania. Często wiąże się to z tworzeniem syntetycznej treści danej osoby, naśladowaniem jej głosu, mimiki twarzy i manier, aby sprawiać wrażenie, że robi lub mówi coś, czego nie zrobiła. Te oszukańcze filmy, klipy audio lub obrazy są często wykorzystywane do oszukiwania ofiar, aby rozstały się z pieniędzmi, ujawniły poufne informacje lub zaszkodziły reputacji. Osoby starsze są często celem ataków ze względu na ich postrzeganą podatność i brak znajomości tak wyrafinowanych zagrożeń technologicznych. Oszustwa deepfake mogą być również wykorzystywane do szantażu, wymuszenia, rozpowszechniania fałszywych informacji lub naruszania systemów bezpieczeństwa. Biorąc pod uwagę znaczący wpływ emocjonalny i finansowy na osoby starsze, kluczowe jest podniesienie świadomości i edukowanie ich na temat tego, jak rozpoznawać i chronić się przed tymi oszukańczymi oszustwami.

Rodzaje oszustw deepfake:

Kradzież tożsamości

Ten rodzaj oszustwa deepfake polega na stworzeniu syntetycznego wideo osoby, aby się pod nią podszyć. Oszust może użyć tego wideo, aby oszukać ofiary i sprawić, że uwierzą, że wchodzą w interakcję z prawdziwą osobą, co może prowadzić do potencjalnych strat finansowych lub kradzieży danych osobowych.

Rozpowszechnianie fałszywych informacji

W tym typie oszustwa deepfakes są wykorzystywane do rozpowszechniania dezinformacji lub propagandy. Może to obejmować tworzenie filmów osób publicznych mówiących lub robiących rzeczy, których nigdy nie zrobiły, wprowadzając w ten sposób opinię publiczną w błąd i wpływając na opinie lub działania.

Naruszenie bezpieczeństwa

Deepfakes mogą być również wykorzystywane do łamania systemów bezpieczeństwa, które opierają się na technologii rozpoznawania twarzy. Tworząc syntetyczne wideo upoważnionej osoby, oszuści mogą oszukać te systemy i uzyskać nieautoryzowany dostęp do wrażliwych obszarów lub tajnych informacji.

Manipulacja przy użyciu technologii deepfake

KONSEKWENCJE:

Oszustwa typu deepfake mogą mieć poważne negatywne skutki, takie jak:

01 Strata finansowa

Ofiary oszustw deepfake mogą ponieść znaczne straty finansowe. Może się to zdarzyć, gdy zostaną oszukane i zmuszone do przekazania środków lub ujawnienia informacji finansowych na podstawie oszukańczej treści deepfake.

02 Stres emocjonalny

Bycie ofiarą oszustwa deepfake może prowadzić do poważnego cierpienia emocjonalnego. Naruszenie tożsamości osobistej i potencjalne ujawnienie danych osobowych może sprawić, że ofiary poczują się bezbronne i naruszone.

03 Uszkodzenie reputacji

Oszustwa typu deepfake mogą spowodować poważne szkody wizerunkowe dla osób i organizacji. Fałszywe informacje rozprzestrzeniane za pośrednictwem deepfake mogą podważyć zaufanie publiczne i doprowadzić do utraty działalności, problemów prawnych i innych negatywnych konsekwencji.

Manipulacja przy użyciu technologii deepfake

KONSEKWENCJE:

04 Dezinformacja

Deepfakes mogą być wykorzystywane do rozpowszechniania fałszywych informacji lub propagandy, wprowadzania opinii publicznej w błąd i wpływania na opinie lub działania. Może to mieć poważne konsekwencje społeczne i polityczne, takie jak podważanie zaufania do instytucji lub manipulowanie wynikami wyborów.

05 Kradzież tożsamości

Technologia deepfake może być używana do tworzenia syntetycznych filmów wideo lub klipów audio osób, co prowadzi do kradzieży tożsamości. Oszuści mogą podszywać się pod kogoś, aby uzyskać dostęp do danych osobowych, zasobów finansowych lub bezpiecznych systemów.

06 Konsekwencje prawne

Wykorzystanie technologii deepfake do popełniania oszustw lub rozpowszechniania fałszywych informacji może prowadzić do konsekwencji prawnych zarówno dla sprawców, jak i ofiar. Ofiary mogą stanąć przed wyzwaniami prawnymi w udowodnieniu swojej niewinności lub odzyskaniu reputacji, podczas gdy sprawcy mogą stanąć przed zarzutami karnymi.

07 Erozja zaufania społecznego

Rozpowszechnienie deepfake'ów może podważyć zaufanie społeczne, sprawiając, że ludzie będą sceptyczni co do autentyczności treści cyfrowych. Może to prowadzić do ogólnej nieufności wobec mediów i informacji udostępnianych online, co komplikuje komunikację i rozprzestrzenianie się prawdziwych informacji.

Manipulacja przy użyciu technologii deepfake

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Pewnego dnia Bill otrzymał e-mail od swojego wnuka, Jacka. E-mail zawierał film, na którym Jack najwyraźniej prosił o pomoc. Powiedział, że zgubił portfel podczas podróży i potrzebuje pieniędzy, aby wrócić do domu. Film wyglądał niesamowicie autentycznie, ponieważ miał głos i maniery Jacka dopracowane do perfekcji.

Bill, zaniepokojony o wnuka, natychmiast przelał pieniądze. Dopiero później, gdy rozmawiał z córką, dowiedział się, że Jack w ogóle nie odbył tej podróży.

Zdezorientowany i zszokowany Bill zdał sobie sprawę, że padł ofiarą oszustwa deepfake. Wideo Jacka nie było prawdziwe, ale było deepfake - syntetycznym wideo wyprodukowanym przy użyciu sztucznej inteligencji.

Ta historia podkreśla podatność seniorów na oszustwa deepfake, podkreślając potrzebę świadomości i edukacji wśród tej grupy demograficznej. Seniorzy, tacy jak Bill, mogą nie być świadomi tak wyrafinowanych oszustw, co czyni ich łatwymi celami. Narracja podkreśla znaczenie informowania seniorów o technologii deepfake, nauczania ich, jak weryfikować wnioski o pomoc finansową i zachęcania do otwartej komunikacji w rodzinach w celu potwierdzenia autentyczności takich wniosków.

KROK 1: Weryfikacja
Zawsze weryfikuj wszelkie prośby o pomoc finansową lub poufne informacje. Dla Billa oznacza to skontaktowanie się z wnukiem bezpośrednio za pomocą znanej i zaufanej metody, takiej jak rozmowa telefoniczna, aby potwierdzić autentyczność prośby przed podjęciem jakichkolwiek działań.

KROK 2: Edukacja i świadomość
Bill powinien być na bieżąco z najnowszymi zagrożeniami technologicznymi, takimi jak deepfakes. Zrozumienie, jak działają i jak mogą być wykorzystywane w oszustwach, pomoże mu rozpoznać potencjalne próby oszustwa i podjąć środki ochronne.

KROK 3: Zaawansowane środki bezpieczeństwa
Bill powinien używać zaawansowanych środków bezpieczeństwa, takich jak uwierzytelnianie dwuskładnikowe dla swoich kont e-mail i mediów społecznościowych. Dodaje to dodatkową warstwę ochrony przed nieautoryzowanym dostępem i potencjalnymi oszustwami.

KROK 4: Otwarta komunikacja
Bill powinien utrzymywać otwartą komunikację ze swoją rodziną na temat wszelkich nietypowych próśb lub wiadomości, które otrzymuje. Omawiając je z zaufanymi członkami rodziny, może szybko zidentyfikować i uniknąć potencjalnych oszustw.

Manipulacja przy użyciu technologii deepfake

SPOSOBY OCHRONY:

Oszustwa deepfake mogą prowadzić do znacznych strat finansowych, cierpienia emocjonalnego i szkody dla reputacji. Ponadto seniorzy mogą mieć trudności z odzyskaniem się po takich oszustwach, zarówno finansowo, jak i emocjonalnie. Mając świadomość tych zagrożeń i podejmując środki ochronne, seniorzy mogą chronić swoje dane osobowe, zachować bezpieczeństwo finansowe i zachować godność i spokój ducha.

Edukacja i świadomość:
Bądź na bieżąco z deepfake'ami, ich potencjalnymi zastosowaniami i najnowszymi narzędziami dostępnymi do ich wykrywania. Regularnie aktualizuj swoją wiedzę na temat tych zagrożeń i środków ochronnych przed nimi.

Weryfikacja:
Zawsze weryfikuj źródło filmów, zwłaszcza tych, które zachęcają do pomocy finansowej lub poufnych informacji. Skontaktuj się z osobą pojawiającą się w filmie za pomocą zaufanej metody, aby potwierdzić jego autentyczność.

Manipulacja przy użyciu technologii deepfake

SPOSOBY OCHRONY:

Stosowanie zaawansowanych środków bezpieczeństwa:
Stosuj zaawansowane środki bezpieczeństwa, takie jak uwierzytelnianie dwuskładnikowe i weryfikacja biometryczna, aby chronić swoje dane osobowe i finansowe.

Polegaj na zaufanych źródłach:
Udostępniaj poufne informacje tylko zaufanym źródłom i za pośrednictwem bezpiecznych platform. Uważaj na niechciane wiadomości z prośbą o podanie danych osobowych lub informacji finansowych.

Zgłoś podejrzaną aktywność:
Jeśli natrafisz na potencjalny deepfake, zgłoś go odpowiednim organom. Może to pomóc zapobiec staniu się ofiarą innych osób i pomóc w zatrzymaniu oszustów.

Oszuści podszywający się pod instytucje państwowe

CHARAKTERYSTYKA ZAGROŻENIA:

Oszustwa usługowe podszywające się pod instytucje państwowe obejmują oszustów podszywających się pod oficjalne agencje rządowe lub służby. Oszuści ci oferują pomoc w przetwarzaniu dokumentów urzędowych, takich jak paszporty, wizy lub świadczenia z ubezpieczenia społecznego, ale ich prawdziwym celem jest kradzież Twoich danych osobowych lub pieniędzy.

Rodzaje manipulacji w oszustwach usługowych:

Podszywanie się pod oficjalne służby

Oszuści tworzą fałszywe strony internetowe lub wysyłają e-maile, które wyglądają, jakby pochodziły od agencji rządowych. Mogą używać oficjalnych logo i języka, aby sprawiać wrażenie legalnych.

Język pilny i autorytatywny

Te oszustwa często używają pilnego języka, ostrzegając Cię o konsekwencjach, jeśli nie zareagujesz szybko. Może to obejmować groźby grzywien, działań prawnych lub niedotrzymania terminów.

Prośby o informacje osobiste

Proszą o poufne informacje, takie jak numer ubezpieczenia społecznego, dane konta bankowego lub dane paszportowe.

Płatności z góry

Oszuści żądają zapłaty za swoje „usługi” z góry, często za pomocą niemożliwych do wyśledzenia metod, takich jak przelewy bankowe, karty przedpłacone lub kryptowaluta.

Brak bezpośrednich informacji kontaktowych

Prawdziwe strony rządowe zapewniają jasne informacje kontaktowe i opcje obsługi klienta. Fałszywe strony często mają ograniczone lub fałszywe dane kontaktowe.

Oszuści podszywający się pod instytucje państwowe

KONSEKWENCJE:

Oszustwa związane z usługami mogą mieć poważne negatywne skutki, takie jak:

01 Problemy prawne i administracyjne

Korzystanie z fałszywych usług może skutkować problemami prawnymi, jeśli ofiara nieświadomie złoży fałszywe dokumenty lub nie zastosuje się do wymogów prawnych. Może to skutkować grzywnami, karami lub dodatkowymi kosztami prawnymi.

02 Kradzież tożsamości

Oszuści często zbierają dane osobowe pod pretekstem, że potrzebują ich do usług państwowych. Informacje te mogą zostać wykorzystane do kradzieży tożsamości ofiary, co prowadzi do nieautoryzowanych transakcji finansowych, zakładania nowych kont na jej nazwisko i innych oszukańczych działań.

03 Utrata zaufania do legalnych instytucji

Po tym, jak ktoś podszywa się pod instytucję państwową, oszukani seniorzy mogą stać się nieufni wobec prawdziwych agencji rządowych i urzędników. Może to utrudnić im chęć szukania pomocy lub usług, których naprawdę potrzebują.

04 Strata finansowa

Seniorzy mogą płacić za fałszywe usługi, takie jak opłaty za przetwarzanie nieistniejących świadczeń lub pomoc w zakresie dokumentów urzędowych. Powoduje to bezpośrednie straty finansowe, które mogą być szczególnie szkodliwe dla osób o stałych dochodach.

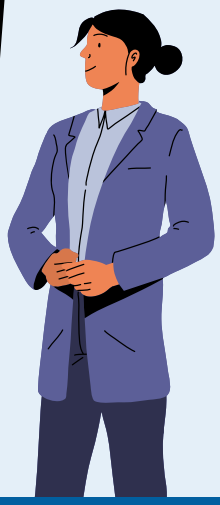
Oszuści podszywający się pod instytucje państwowe

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Grace otrzymuje e-mail rzekomo od urzędu, w którym stwierdza się, że jej paszport wymaga pilnego odnowienia, aby uniknąć kar. E-mail zawierał link do strony internetowej, która wyglądała na oficjalną, z logo departamentu i oficjalnym językiem. Strona internetowa poprosiła o podanie danych osobowych i opłatę w wysokości 150 euro, aby przyspieszyć proces odnowienia. Co powinna zrobić Grace?

Oszustwa usługowe podszywające się pod instytucje państwowe mogą prowadzić do poważnych szkód finansowych i emocjonalnych, zwłaszcza dla seniorów. Weryfikując źródło informacji, zachowując sceptycyzm wobec pilnych próśb, chroniąc dane osobowe i korzystając z bezpiecznych metod płatności, możesz zabezpieczyć się przed tymi oszustwami.

Zawsze upewniaj się, że korzystasz z prawdziwych witryn i usług rządowych, aby nie paść ofiarą oszustw.



Krok 1: Zweryfikuj źródło

Sprawdź bezpośrednio oficjalną stronę internetową urzędu lub zadzwoń do działu obsługi klienta, aby potwierdzić proces odnowienia.

Krok 2: Podchodź sceptycznie do pilnych próśb

Należy pamiętać, że prawdziwe instytucje rządowe nie będą wysyłać pilnych próśb o odnowienie za pośrednictwem poczty elektronicznej.

Krok 3: Nie udostępniaj danych osobowych

Nie podawaj swoich danych osobowych na podanej stronie internetowej, dopóki nie zweryfikujesz ich autentyczności.

Krok 4: Używaj bezpiecznych metod płatności

Należy zachować ostrożność w przypadku próśb o zapłatę i sprawdzić, czy rząd pobiera takie opłaty i świadczy takie usługi.

Oszuści podszywający się pod instytucje państwowe

SPOSOBY OCHRONY:

Ochrona siebie przed oszustwami usługowymi podszywającymi się pod państwową instytucję jest kluczowa dla ochrony Twoich danych osobowych, pieniędzy i emocji. Oto kilka prostych kroków, które możesz podjąć.

Nie udostępniaj danych osobowych:

Unikaj podawania poufnych informacji, takich jak numer ubezpieczenia społecznego, dane bankowe lub dane paszportowe, jeśli nie masz pewności, że dana strona internetowa jest legalna.

Sprawdź źródło:

Upewnij się, że jesteś na oficjalnej stronie rządowej. Szukaj „gov” w adresie internetowym, który jest używany przez instytucje rządowe. Skontaktuj się z agencją rządową bezpośrednio, korzystając z informacji z oficjalnego źródła, a nie danych kontaktowych podanych w podejrzanym e-mailu lub na stronie internetowej.

Podchodź sceptycznie do pilnych próśb:

Zachowaj ostrożność, jeśli otrzymasz pilne lub groźne wiadomości wymagające natychmiastowego działania lub zapłaty. Prawdziwe instytucje rządowe nie działają w ten sposób.

Oszustwo za pomocą fałszywych kont

CHARAKTERYSTYKA ZAGROŻENIA:

Szantaż za pomocą fałszywych kont odnosi się do oszukańczej praktyki, w której oszuści tworzą fałszywe profile w mediach społecznościowych, często podszywając się pod kogoś, kogo ofiara zna lub komu ufa. To oszustwo jest szczególnie skierowane do seniorów, którzy mogą być mniej zaznajomieni z platformami cyfrowymi. Oszuści zazwyczaj nawiązują kontakt, wysyłając prośby o dodanie do znajomych, a następnie udostępniają treści o charakterze jawnym lub szkodliwym. Następnie oszust żąda pieniędzy lub innych form płatności, grożąc uszkodzeniem reputacji seniora poprzez powiązanie go z nieodpowiednimi treściami.

Rodzaje szantażu z wykorzystaniem fałszywych kont:

Podszywanie się pod znajomego lub przyjaciela

Oszust tworzy fałszywe konto, podszywając się pod kogoś, kogo ofiara zna, zyskuje jej zaufanie, a następnie wykorzystuje to zaufanie, aby rozpocząć szantaż.

Łowienie sumów

Oszust tworzy fałszywą tożsamość, często osobę, która jest romantycznie zainteresowana ofiarą. Gdy ofiara jest emocjonalnie zaangażowana, oszust rozpoczyna szantaż.

Podszywanie się pod celebrytę lub osobę publiczną

Oszust tworzy fałszywe konto celebryty lub osoby publicznej. Następnie kontaktuje się z fanami lub obserwatorami, udostępniając treści o charakterze pornograficznym i żądając pieniędzy, grożąc zszarganiem reputacji fana.

Oszustwo za pomocą fałszywych kont

KONSEKWENCJE:

Szantażowanie przy użyciu fałszywych kont może mieć poważne negatywne skutki, takie jak:

01 Cierpienie emocjonalne i psychiczne

Jednym z głównych skutków, z jakimi może się zmierzyć ofiara, jest znaczny stres emocjonalny i psychologiczny. Często jest to bezpośredni skutek nieustannych gróźb i nieustannego nękania dokonywanego przez oszusta. Taki stres może objawiać się na wiele sposobów, w tym strachem, lękiem, depresją i zaburzeniami snu, znacząco wpływając na codzienne życie ofiary.

02 Strata finansowa

Kolejnym ryzykiem, na jakie narażone są ofiary, jest potencjalna znaczna strata finansowa. Zazwyczaj dzieje się tak, gdy ofiara, czując się osaczona i przytłoczona nieustępliwymi żądaniami oszusta, ostatecznie ulega. W rezultacie może doświadczyć nie tylko utraty ciężko zarobionych pieniędzy, ale także stresu i niepokoju, które towarzyszą takiej stracie.

03 Uszkodzenie reputacji

Na koniec, istnieje ryzyko poważnego uszkodzenia reputacji ofiary. Może się to zdarzyć, jeśli oszust zdecyduje się zrealizować swoje groźby, potencjalnie ujawniając szkodliwe lub poufne informacje o ofierze. Może to doprowadzić do znacznego spadku pozycji społecznej ofiary i wpłynąć na jej osobiste i zawodowe relacje, a także przyszłe możliwości.

Oszustwo za pomocą fałszywych kont

SPOSOBY OCHRONY Z HISTORIĄ W TLE

Pewnego dnia Susan otrzymała prośbę o dodanie do znajomych z konta noszącego imię dawno niewidzianego przyjaciela. Zachwycona perspektywą ponownego połączenia, zaakceptowała prośbę. Niedługo potem zaczęły wymieniać wiadomości, wspominając stare czasy. Jednak sytuacja stała się złowroga, gdy przyjaciel zaczął udostępniać treści o charakterze pornograficznym i zażądał pieniędzy, grożąc zszarganiem jej reputacji poprzez skojarzenie jej imienia z treścią.

Wstrząśnięta nagłą zmianą Susan postanowiła skontaktować się ze swoją prawdziwą przyjaciółką za pośrednictwem innego medium. Kiedy dowiedziała się, że jej przyjaciółka nie ma pojęcia o tym koncie, zdała sobie sprawę, że wchodziła w interakcję z fałszywym kontem.

Ta historia podkreśla, jak ważne jest edukowanie seniorów na temat potencjalnych zagrożeń, jakie niesie ze sobą interakcja z nieznanymi podmiotami w Internecie.
Podkreśla, w jaki sposób seniorzy mogą paść ofiarą oszustw, takich jak szantaż za pomocą fałszywych kont, ze względu na ich potencjalny brak znajomości platform cyfrowych. Historia ta służy jako przypomnienie dla seniorów, aby weryfikowali tożsamość osób przed nawiązaniem z nimi kontaktu online i zgłaszali wszelkie podejrzane działania platformie lub lokalnym władzom. Podkreśla potrzebę świadomości i czujności w świecie cyfrowym w celu ochrony ich dobrostanu i bezpieczeństwa finansowego.

KROK 1: Zweryfikuj prośby o dodanie do znajomych
Susan zaakceptowała prośbę o dodanie do znajomych z konta, które uważała za dawno niewidzianego znajomego, bez weryfikacji jego autentyczności. Susan powinna była skontaktować się ze swoim prawdziwym znajomym za pośrednictwem innego medium, aby zweryfikować autentyczność prośby o dodanie do znajomych przed jej zaakceptowaniem.

KROK 2: Bądź ostrożny z informacjami osobistymi
Susan angażowała się w rozmowy i dzieliła się osobistymi wspomnieniami, nie podejrzewając żadnej nieczystej gry. Susan powinna była zachować ostrożność i unikać udostępniania informacji osobistych lub angażowania się w delikatne rozmowy, dopóki nie była pewna tożsamości drugiej osoby.

KROK 3: Rozpoznaj podejrzane zachowanie
Susan kontynuowała interakcję z kontem, nawet po tym, jak zaczęli udostępniać treści o charakterze pornograficznym i stawiać żądania. Po zauważeniu podejrzanego zachowania Susan powinna była natychmiast zaprzestać interakcji z kontem i oznaczyć je jako podejrzane.

KROK 4: Zgłoś i edukuj
Po uświadomieniu sobie, że konto jest fałszywe, Susan zgłosiła incydent i podzieliła się swoim doświadczeniem ze znajomymi i rodziną. Działania Susan związane ze zgłoszeniem konta i edukacją innych były właściwe. Powinna nadal propagować świadomość i czujność w stosunku do oszustw internetowych.

Oszustwo za pomocą fałszywych kont

SPOSOBY OCHRONY:

Ochrona przed szantażem za pomocą fałszywych kont jest kluczowa, zwłaszcza dla seniorów, ponieważ pomaga zapobiegać stresowi emocjonalnemu i psychicznemu, stratom finansowym i szkodom dla reputacji. Seniorzy mogą być bardziej podatni na te oszustwa ze względu na potencjalny brak znajomości platform cyfrowych. Będąc czujnymi i ostrożnymi w Internecie, seniorzy mogą chronić swoje dobre samopoczucie i bezpieczeństwo finansowe, zapewniając bezpieczniejsze i przyjemniejsze korzystanie z Internetu.

Weryfikacja próśb o dodanie do znajomych:
Zawsze uwierzytelniaj tożsamość osoby wysyłającej prośbę o dodanie do znajomych, szczególnie jeśli nie kontaktowałeś się z nią przez jakiś czas. Można to zrobić, kontaktując się z nią za pośrednictwem innego medium, którego wcześniej używałeś do komunikacji.

Ustawienia prywatności:
Upewnij się, że Twoje konta w mediach społecznościowych są ustawione na najwyższe ustawienia prywatności. Ograniczy to ilość informacji, które mogą zobaczyć osoby, które nie znajdują się na Twojej liście znajomych.

Oszustwo za pomocą fałszywych kont

SPOSOBY OCHRONY:

Nie udostępniaj poufnych informacji: Unikaj udostępniania osobistych lub poufnych informacji online. Jeśli osoba, z którą się komunikujesz, zaczyna zachowywać się podejrzanie lub żądać pieniędzy, natychmiast przerwij rozmowę.

Zgłoś podejrzaną aktywność: Jeśli natkniesz się na podejrzane konto lub ktoś zacznie udostępniać nieodpowiednie treści lub grozić, zgłoś to konto serwisowi społecznościowemu i lokalnym władzom.

Kształć siebie i innych: Dowiedz się o typowych oznakach oszustw internetowych i naucz innych o tych oznakach. Może to pomóc Tobie i Twoim bliskim uniknąć stania się ofiarą takich oszustw.

Dodatkowe informacje

ZARZUTY UDZIAŁU W PRZESTĘPSTWIE

- 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/

MANIPULACJE PODSZYWAJĄCE SIĘ POD INSTYTUCJE PAŃSTWOWE

- 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

Dodatkowe informacje

MANIPULACJA PRZY UŻYCIU TECHNOLOGII DEEPFAKE

- 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/technology/ai-and-automation/audio-deepfake-scams-the-growing-threat-explored
- https://readwrite.com/are-deepfakes-illegal-ais-dark-side-explained/

OSZUŚCI PODSZYWAJĄCY SIĘ POD INSTYTUCJE PAŃSTWOWE

- 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

Dodatkowe informacje

OSZUSTWA ZA POMOCĄ FAŁSZYWYCH KONT

- 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-technology/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

Institute of Entrepreneurship Development
iED

İLKSENOL
DERNEĞİ

SIMBIOZA
MED GENERACIJAMI

„Finansowane przez UE. Wyrażone poglądy i opinie są poglądami i opiniami autora(-ów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Narodowej Agencji Erasmus+. Unia Europejska, ani grantodawca nie ponoszą za nie odpowiedzialności”.