Zadanie współfinansowane ze środków otrzymanych z Powiatu Lublinieckiego

CZĘSTOCHOWSKIE STOWARZYSZENIE ETOH

INFORMATOR PRAWNY

NR 7

Stan prawny

1 lipca 2021r.

2021

NR 7

INFORMATOR PRAWNY

Częstochowskiego Stowarzyszenia ETOH

W związku z korzystaniem z różnego rodzaju aukcji sprzedaży należy zachowywać odpowiednie środków ostrożności, jeśli zdecydujemy się na odbiór osobisty. Należy pamiętać najbezpieczniej jest dokonywać zakupu za pobraniem

.

Wpłata pieniędzy z góry na podany numer konta zawsze obarczona jest sporym ryzykiem. Często oszuści zakładają konta na tzw. słupów. Może się tak zdarzyć nie tylko przy kupnie przedmiotu, ale także przy opłacie za usługi oraz gdy sprzedający prosi o zapłatę za przesyłkę darmowego przedmiotu. W ten sposób możesz stracić pieniądze i nigdy nie zobaczyć zamówionego towaru.

Jeśli już decydujesz się na przelew poza płatnościami danego portalu Allegro, OLX dobrze jest sprawdź w internecie, czy podany przez sprzedającego numer konta bankowego nie był wykorzystywany w nieuczciwych celach. W żadnym wypadku nie należy wysyłać pieniędzy za granicę. Najbezpieczniej jest domagać się aby sprzedającego przesłał zakupiony przedmiot za pobraniem z możliwością sprawdzenia zawartości.

Należy również zwrócić uwagę w sytuacjach, kiedy sprzedający poprosi nas o przelew ekspresowy lub dokonanie płatności z użyciem BLIK-a. Często oszuści internetowi wybierają taką metodę płatności, aby szybciej zdobyć pieniądze na swoje konta.

Fraud nigeryjski

Tego typu rodzaj oszustwa polega na przesłaniu e- maili polegający na wciągnięciu ofiary w fikcyjny transfer wielkiej kwoty pieniędzy rzędu kilku milionów dolarów USA najczęściej z któregoś z krajów afrykańskich początkowo głównie do Nigerii

Na czym polega mechanizm oszustwa.

Mechanizm oszustwa polega na tym, że oszust proponuje ofierze podział pieniędzy, po dokonaniu przelewu na jej konto, ze źródła o wątpliwej legalności. Operacja ta często rzekomo wymaga dodatkowych działań w rodzaju założenia fikcyjnej działalności gospodarczej, przekupywania urzędników państwowych itp. Ofiara zwabiona chęcią zysku i nieznająca struktury urzędniczej państwa, z którego rzekomo mają zostać przelane pieniądze, godzi się na zainwestowanie własnych funduszy w celu przeprowadzenia „operacji". Opłaty ponoszone przez ofiarę są w rzeczywistości przechwytywane przez oszusta, który następnie znika, nie dokonując ostatecznie żadnej wpłaty na rzecz ofiary Przesyłane wiadomości są pisane zazwyczaj w języku angielskim. W większości przypadków wiadomość zawiera liczne błędy gramatyczne i ortograficzne. Niekiedy się zdarza, że list jest przesyłany w innym języku, całą wiadomość zaś przetłumaczono w translatorze

Przykłady wyłudzeń

- **A** jest spadkobiercą wielkiej kwoty po swoim krewnym, lecz w celu otrzymania pieniędzy musi opłacić prowizję dla firmy ubezpieczeniowej; **B** w zamian za udział w spadku ma dokonać tej wpłaty
- **A** był członkiem skorumpowanych władz lub osobą związaną z władzami któregoś z krajów afrykańskich i musiał opuścić kraj w następstwie zamachu stanu bądź innej formy zmiany władzy. W kraju pozostawił pokaźną sumę wcześniej zdefraudowanych pieniędzy. Do wyprowadzenia tych pieniędzy za granicę potrzebna jest pomoc **B**, w zamian za udział w zyskach.
- **A** jest pracownikiem korporacji w Nigerii, gdzie planuje zdefraudować firmowe pieniądze, podpisując umowę z firmą ofiary (**B**), założoną tylko na tę okoliczność. **B** podaje swoje dane osobowe potrzebne do założenia (podwójnie) fikcyjnej działalności, po czym otrzymuje sfałszowane dokumenty z „nigeryjskiego" ministerstwa zobowiązujące do dokonania rzekomych opłat administracyjnych.
- **A** pisze w e-mailu, że ma chore dziecko w szpitalu, które wymaga natychmiastowej pomocy lekarskiej i jeśli nie wpłaci stosownej kwoty na konto szpitala, to dziecko umrze. **A** prosi **B** o przysługę w postaci drobnej pomocy i pilną wpłatę kwoty od 2 do 10 tys. $ na opłacenie

rachunków za leczenie szpitalne dziecka, **A** Obiecuje **B**, że podzieli się z nim ogromną sumą ze swego konta. Oszust proponuje potencjalnej ofierze od 50% do nawet 80%, kapitału z konta, które tak naprawdę nie istnieje. **A** twierdzi, że pieniądze, które niby zgromadził na koncie, wobec śmiertelnej choroby jego dziecka, w tej chwili nie mają dla niego większego znaczenia. Na dowód przedstawia zeskanowane, wiarygodnie wyglądające, ale niestety sfałszowane i podrobione dokumenty bankowe. Po zainkasowaniu pieniędzy **A** znika bez śladu.

[1] https://pl.wikipedia.org/wiki/Nigeryjski_szwindel

OSZUSTWO wash-wash

Specyficznym rodzajem oszustwa jest metoda „wash-wash”. W niej przestępca, podający się najczęściej za pracownika prywatnej firmy, która posiada dużą ilość banknotów pokrytych substancją chemiczną, kontaktuje się z ofiarą. Następnie oszust nawiązuje bezpośredni kontakt z ofiarą. Potencjalna ofiara dowiaduje się, że jakiś czas temu firma otrzymała zlecenie wykonania pewnych czynności z oznaczonymi banknotami (np. oczyszczenia lub renowacji banknotów lub przygotowania specjalistycznego opakowania banknotów), jednak przed odebraniem towaru ze zleceniodawcą urwał się kontakt. Oszust w sytuacji wielomiesięcznej niemożności ustalenia właściciela pieniędzy, obserwuje i nawiązuje kontakt z przypadkowo napotkaną ofiarą. Miejscami spotkań są np. hotele, ośrodki hazardu i ośrodki wczasowe. Gdy dochodzi do spotkania, oszust prezentuje zabarwione banknoty (będące zazwyczaj wydrukowanymi banknotami lub wręcz czarnymi kartkami, odpowiadające wymiarami banknoty dolarowe lub euro). Oszust informuje, że znajduje się w trudnej sytuacji finansowej i odsprzeda walizkę z farbowanymi pieniędzmi za kwotę niższą niż wynosi nominalna wartość gotówki. Jedynym warunkiem jest kupno przez ofiarę specjalnego środka chemicznego do odbarwiania banknotów. Następnie oszust proponuje nowe spotkanie, do którego nigdy nie dochodzi.

Oszuści jako swoje ofiary upatrują osoby prowadzące działalność gospodarczą. Inicjują spotkania biznesowe, podczas których proponują zakup towaru na znaczną kwotę pieniędzy. Czasem dochodzi do kilku takich spotkań. W kontaktach zawsze są mili i uprzejmi, starają się pozyskać zaufanie swojej ofiary. Często są to osoby wykształcone. Gdy podczas spotkania dochodzi do rozmów na tematy finansowe, twierdzą, że są w pełni wypłacalni, ale pieniądze, którymi zapłacą za zamówienie, będą pochodzić z zagranicy.

Wtedy pokazują swojemu kontrahentowi kartkę papieru, która - pod wpływem pewnej nieustalonej substancji w płynie czy też w proszku - "staje się" banknotem euro. Wybieg taki tłumaczony jest tym, że nie mogą niepostrzeżenie wywieźć ze swojego kraju znacznej ilości gotówki, lub „niewidzialne” banknoty mają być zabezpieczeniem przed ich ewentualną kradzieżą w trakcie podróży. Gdy ofiara zgodzi się na zawarcie transakcji, oszuści przystępują do dalszego działania - proszą o udzielenie pożyczki w walucie euro, która jest im niezbędnie potrzebna na zakup i sprowadzenie odczynników chemicznych umożliwiających odbarwienie papieru, który zostanie przywieziony do kraju. Istnieje również inne

uzasadnienie pożyczki. Oszuści próbują wtedy wmówić, że dysponują słabszymi odczynnikami i potrzebują prawdziwych pieniędzy, aby przez przyłożenie do wstępnie przygotowanego banknotu w pełni go odbarwić.

(źródło https://policja.pl/pol/aktualnosci/56744,Wash-wash-i-za-kratki.html)

Oszustwo tzw. phishing

Phishing to jedna z metod, która wykorzystywana jest przez cyberprzestępców do wyłudzenia wrażliwych danych. W wyniku tego ataku możesz stracić nie tylko dostęp do konta mailowego, lecz także środki zgromadzone na rachunku bankowym.

.

Jak rozpoznać próby oszustwa i jak się przed nimi bronić.

Phishing to oszustwo stosowane przez internetowych przestępców w celu uzyskania cennych informacji, takich jak:

- **loginy i hasła,**
- numery **kart kredytowych**,
- numer **PESEL**

Nazwa budzi dźwiękowe skojarzenia z *fishingiem* – czyli łowieniem ryb. Przestępcy, podobnie jak wędkarze stosują, bowiem odpowiednio przygotowaną „przynętę". W tej roli wykorzystują najczęściej **fałszywe e-maile i SMS-y.** Coraz częściej oszuści działają także za pośrednictwem komunikatorów i portali społeczności.

Co zrobić żeby ustrzec się przed oszustwem tzw. Phishingu

Aby wzbudzić zaufanie ofiary, **phisherzy podszywają się pod powszechnie rozpoznawalne firmy i instytucje** – banki, urzędy, portale aukcyjne, firmy kurierskie i telekomunikacyjne. Za pomocą spreparowanych wiadomości próbują nakłonić ofiarę do kliknięcia

w umieszczony w wiadomości link. Przeważnie prowadzi on do **strony internetowej stworzonej przez oszustów.** Jest ona łudząco podobna do autentycznej witryny firmy czy instytucji, od której rzekomo pochodzi wiadomość – ale tak naprawdę stanowi pułapkę zastawioną na nieostrożnych internautów.

Przed phisingiem może ustrzec nas ostrożność i rozwaga w przeglądaniu poczy.

Pamiętaj

- ✓ Nigdy nie klikaj w linki w wiadomości e-mail lub na stronie internetowej, jeżeli nie masz pewności , że są one autentyczne i pochodzą ze sprawdzonego źródła.
- ✓ W przypadku jakichkolwiek wątpliwości, należy otworzyć w przeglądarce nowe okno i wpisać adres URL w pasku adresu.
- ✓ Uważać na e-maile z prośbą o podanie poufnych informacji - zwłaszcza, jeśli chodzi o dane osobowe lub informacje bankowe.
- ✓ W sieci należy stosować **zasadę ograniczonego zaufania.** Odruchowe klikanie w linki i pobieranie plików z nieznanych źródeł jest bardzo ryzykownym zachowaniem – zanim otworzysz wiadomość od „firmy kurierskiej", zastanów się, czy faktycznie czekasz na jakąś przesyłkę.
- ✓ Nie udostępniaj innym osobom haseł i loginów.
- ✓ Otwierając załącznik, dokładnie przeczytaj treść e-maila. Fałszywe wiadomość bardzo często zawierają **błędy ortograficzne, gramatyczne i interpunkcyjne.**
- ✓ Zwróć uwagę na dane nadawcy wiadomości. Adresy mailowe, którymi posługują się oszuści, mogą się różnić od tych autentycznych łatwymi do przeoczenia szczegółami, np. literówką w nazwie domeny – zamiast kontakt@bank.**pl** – kontakt@bank.**pppl**. Adresy mogą również zawierać przekręconą lub niepełną nazwę firmy czy instytucji.
- ✓ Przed kliknięciem w link dokładnie się mu przyjrzyj. Oszuści często wykorzystują pozornie banalne, ale trudne do wykrycia sztuczki – np. zastępują literę „l" cyfrą „1", a literę „O" – cyfrą „0". Jeżeli chcesz zalogować się do serwisu transakcyjnego banku, najbezpieczniej będzie, jeżeli **własnoręcznie wprowadzisz jego adres www.**
- ✓ jeżeli masz wątpliwości, czy wiadomość faktycznie pochodzi od danej firmy czy instytucji, skontaktuj się z jej przedstawicielem, np. za pośrednictwem infolinii.
- ✓ Upewnij się, czy korzystasz z najnowszej wersji przeglądarki internetowej i zaktualizowanego systemu operacyjnego, a na Twoim urządzeniu zainstalowane jest
- ✓ Oprogramowanie antywirusowe.

Co to jest spoofing ?

Definicja podszywania się

Spoofing, w odniesieniu do cyberbezpieczeństwa, ma miejsce wtedy, gdy ktoś lub coś udaje coś innego w celu zdobycia naszej pewności siebie, uzyskania dostępu do naszych systemów, kradzieży danych, kradzieży pieniędzy lub rozprzestrzeniania złośliwego oprogramowania. Ataki typu spoofing przybierają różne formy, przede wszystkim:

- Podszywanie się pod e-maile Podszywanie się pod witrynę internetową i/lub adres URL
- Podszywanie się pod identyfikator rozmówcy
- Podszywanie się pod wiadomości tekstowe
- Podszywanie się pod GPS

Ataki typu man-in-the-middle

- Podszywanie się pod rozszerzenie
- Podszywanie się pod IP
- Spoofing twarzy

W jaki sposób oszukują nas cyberprzestępcy

Często samo powołanie się na nazwę dużej, zaufanej organizacji wystarczy, aby skłonić nas do ujawnienia informacji lub podjęcia jakiegoś działania. Na przykład sfałszowana wiadomość e-mail z PayPal lub Amazon może zapytać o zakupy, których nigdy nie dokonałeś. W trosce o swoje konto możesz być zmotywowany do kliknięcia dołączonego linku.

Z tego złośliwego linku oszuści przekierowują Cię do pobrania złośliwego oprogramowania lub sfałszowanej strony logowania — wraz ze znanym logo i fałszywym adresem URL — w celu przechwycenia nazwy użytkownika i hasła.

Istnieje wiele innych sposobów, w jakie można przeprowadzić atak fałszowania. We wszystkich oszuści polegają na naiwności swoich ofiar. Jeśli nigdy nie wątpisz w wiarygodność witryny i nigdy nie podejrzewasz, że wiadomość e-mail została sfałszowana, prawdopodobnie w pewnym momencie staniesz się ofiarą ataku polegającego na podszywaniu się.

ODPOWIEDZIALNOŚĆ KARNA ZA SPOOFING

KK Art. 190a. [Uporczywe nękanie. Kradzież tożsamości]
§ 1. Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności do lat 3.
§ 2. Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej.
§ 3. Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od roku do lat 10.
§ 4. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Podszywanie się, w odniesieniu do cyberbezpieczeństwa, ma miejsce, gdy ktoś lub coś udaje coś innego w celu zdobycia naszej pewności siebie, uzyskania dostępu do naszych systemów, kradzieży danych, kradzieży pieniędzy lub rozprzestrzeniania złośliwego oprogramowania".

Formy podszywania się

Fałszowanie wiadomości e-mail. Ściśle mówiąc, fałszowanie wiadomości e-mail to wysyłanie wiadomości e-mail z fałszywymi adresami nadawcy, zwykle w ramach ataku phishingowego, którego celem jest kradzież informacji, zainfekowanie komputera złośliwym oprogramowaniem lub po prostu prośba o pieniądze. Typowe ładunki złośliwych wiadomości e-mail obejmują oprogramowanie ransomware, adware,cryptojackery,trojany (takie jak Emotet) lub złośliwe oprogramowanie, które zniewala Twój komputer w botnecie

Podszywanie się pod witrynę

Podszywanie się pod witrynę internetową polega na tym, aby złośliwa witryna wyglądała na legalną. Sfałszowana witryna będzie wyglądać jak strona logowania do witryny, którą często odwiedzasz — łącznie z brandingiem, interfejsem użytkownika, a nawet sfałszowaną nazwą domeny, która na pierwszy rzut oka wygląda tak samo. Cyberprzestępcy wykorzystują fałszywe witryny internetowe do przechwytywania nazwy użytkownika i hasła (tzw. podszywanie się pod login) lub umieszczania złośliwego oprogramowania na komputerze (drive-by download). Fałszywa strona internetowa będzie zwykle używana w połączeniu z podrobioną wiadomością e-mail, w której e-mail będzie zawierał link do witryny.

Podszywanie się pod identyfikator rozmówcy

Podszywanie się pod identyfikator dzwoniącego ma miejsce, gdy oszuści oszukują Twój identyfikator dzwoniącego, sprawiając, że połączenie wydaje się pochodzić z innego miejsca. Oszuści dowiedzieli się, że bardziej prawdopodobne jest, że odbierzesz telefon, jeśli identyfikator rozmówcy zawiera numer kierunkowy taki sam lub zbliżony do Twojego. W niektórych przypadkach oszuści fałszują nawet kilka pierwszych cyfr Twojego numeru telefonu oprócz numeru kierunkowego, aby stworzyć wrażenie, że połączenie pochodzi z Twojej okolicy (tzw. podszywanie się pod sąsiada). Tak się składa, że Malwarebytes na Androida i Malwarebytes na iOS blokują połączenia przychodzące z oszustwami, dzięki czemu fałszowanie identyfikatora dzwoniącego to już przeszłość.

Podszywanie się pod wiadomości tekstowe

Podszywanie się pod wiadomości tekstowe lub **podszywanie się pod** SMS to wysyłanie wiadomości tekstowej z numerem telefonu lub identyfikatorem nadawcy innej osoby. Jeśli kiedykolwiek wysłałeś wiadomość tekstową z laptopa, sfałszowałeś własny numer telefonu w celu wysłania SMS-a, ponieważ tekst nie pochodził z telefonu. Firmy często podszywają się pod własne numery w celach marketingowych i dla wygody konsumenta, zastępując długi numer krótkim i łatwym do zapamiętania alfanumerycznym identyfikatorem nadawcy. Oszuści robią to samo — ukrywają swoją prawdziwą tożsamość za alfanumerycznym identyfikatorem nadawcy, często podszywając się pod legalną firmę lub organizację. Sfałszowane teksty często zawierają łącza do stron phishingowych SMS (smishing) lub pobierania złośliwego oprogramowania.

Oszuści korzystający z wiadomości tekstowych wykorzystują teraz zdrowy rynek pracy, podszywając się pod agencje pracy i wysyłając ofiarom oferty pracy, które są dobre, aby były prawdziwe.

.

Atak Man-in-the-middle (MitM)

Atak typu -man-in-the-middle. Wszyscy lubimy darmowe Wi-Fi w lokalnej kawiarni. Zdarzają się przypadki, że cyberprzestępcy włamują się do sieci Wi-Fi lub tworzą inną nieuczciwą sieć Wi-Fi w tej samej lokalizacji. Cyberprzestępcy są w stanie przechwycić ruch sieciowy między dwiema stronami. Fałsz pojawia się, gdy przestępcy zmieniają komunikację między stronami w celu przekierowania środków lub pozyskania poufnych danych osobowych, takich jak numery kart kredytowych lub loginy.

Podszywanie się pod rozszerzenie

Spoofing rozszerzeń ma miejsce, gdy cyberprzestępcy muszą ukryć wykonywalne pliki złośliwego oprogramowania. Jednym z powszechnych sztuczek fałszowania rozszerzeń, których lubią używać przestępcy, jest nazwanie pliku na wzór „nazwapliku.txt.exe". Przestępcy wiedzą, że rozszerzenia plików są domyślnie ukryte w systemie Windows, więc dla przeciętnego użytkownika systemu Windows ten plik wykonywalny będzie widoczny, jako „nazwapliku.txt".

Podszywanie się pod IP

Spoofing IP jest używany, gdy ktoś chce ukryć lub zamaskować lokalizację, z której wysyła lub żąda danych online. Podobnie jak w przypadku cyberzagrożeń, fałszowanie adresów IP jest wykorzystywane w rozproszonych atakach typu „odmowa usługi " (DDoS), aby zapobiec odfiltrowaniu złośliwego ruchu i ukryciu lokalizacji atakującego.

Spoofing twarzy

Fałszowanie twarzy. Najnowsza forma podszywania się może być najbardziej osobista ze względu na konsekwencje, jakie niesie dla przyszłości technologii i naszego życia osobistego. W obecnej postaci technologia identyfikacji twarzy jest dość ograniczona. Używamy twarzy do odblokowywania naszych urządzeń mobilnych i laptopów i niewiele więcej. Wkrótce jednak może się okazać, że

dokonujemy płatności i podpisujemy dokumenty twarzą. Wyobraź sobie konsekwencje, kiedy możesz otworzyć linię kredytową swoją twarzą. Straszna rzecz. Naukowcy wykazali, w jaki sposób modele twarzy 3D zbudowane na podstawie Twoich zdjęć w mediach społecznościowych mogą już zostać wykorzystane do włamania się do urządzenia zablokowanego za pomocą identyfikatora twarzy. Idąc krok dalej, blog Malwarebytes Labs doniósł o technologii deepfake wykorzystywane do tworzenia fałszywych filmów informacyjnych i fałszywych taśm erotycznych, zawierających głosy i podobizny polityków i celebrytów.

Jak działa podszywanie się?

W przypadku fałszowania wiadomości e-mail istnieje kilka sposobów, w jakie cyberprzestępcy są w stanie ukryć swoją prawdziwą tożsamość w podszytym e-mailu. Najbardziej niezawodną opcją jest zhakowanie niezabezpieczonego serwera pocztowego. W tym przypadku e-mail pochodzi, z technicznego punktu widzenia, od rzekomego nadawcy.

Opcja low-tech polega po prostu na wstawieniu dowolnego adresu w polu „Od”. Jedyny problem polega na tym, że jeśli ofiara odpowie lub z jakiegoś powodu wiadomość e-mail nie może zostać wysłana, odpowiedź zostanie przesłana do osoby wymienionej w polu „Od”, a nie do osoby atakującej. Ta technika jest powszechnie stosowana przez spamerów do wykorzystywania legalnych wiadomości e-mail w celu ominięcia filtrów spamu. Jeśli kiedykolwiek otrzymałeś odpowiedzi na wiadomości e-mail, których nigdy nie wysłałeś, jest to jeden z możliwych powodów, inny niż włamanie na Twoje konto e-mail. Nazywa się to rozproszeniem wstecznym lub spamem ubocznym.

Innym częstym sposobem fałszowania wiadomości e-mail przez atakujących jest zarejestrowanie nazwy domeny podobnej do tej, którą próbują sfałszować w ramach tzw. ataku homograficznego lub wizualnego podszywania się. Na przykład „rna1warebytes. Zwróć uwagę na użycie cyfry „1” zamiast litery „l”. Zwróć również uwagę na użycie liter „r” i „n” używanych do sfałszowania litery „m”. Dodatkową korzyścią jest udostępnienie atakującemu domeny, której może użyć do stworzenia sfałszowanej witryny.

Bez względu na to, jaka może być fałszywa, nie zawsze wystarczy rzucić w świat fałszywą stronę internetową lub wiadomość e-mail i mieć nadzieję na najlepsze. Skuteczne fałszowanie wymaga połączenia samego fałszowania i socjotechniki. Inżynieria społeczna odnosi się do metod stosowanych przez cyberprzestępców w celu nakłonienia nas do podania danych osobowych, kliknięcia złośliwego łącza lub otwarcia załącznika wyładowanego złośliwym oprogramowaniem. W podręczniku socjotechniki jest wiele sztuk. Cyberprzestępcy liczą na słabe punkty, które wszyscy nosimy, jako ludzie, takie jak strach, naiwność, chciwość i próżność, aby przekonać nas do zrobienia czegoś, czego naprawdę nie powinniśmy robić. Na przykład w przypadku oszustwa seksualnego możesz wysłać oszusta Bitcoin, ponieważ obawiasz się, że twoje przysłowiowe brudne pranie zostanie wyemitowane, aby wszyscy mogli je zobaczyć.

Ludzkie luki też nie zawsze są złe. Ciekawość i empatia są ogólnie dobrymi cechami, ale przestępcy uwielbiają atakować ludzi, którzy je przejawiają. Przykładem może być oszustwo związane z wnukami, które porzuciły życie, w którym ukochana osoba jest rzekomo w więzieniu lub w szpitalu w obcym kraju i szybko potrzebuje pieniędzy. E-mail lub sms może brzmieć: „Dziadku Janie, aresztowano mnie za przemyt narkotyków w Niemczech. Proszę przesłać fundusze, och i btw, nie mów mamie i tacie. Jesteś najlepszy [trzy szczęśliwa buźka mrugająca emotikonami]!" Tutaj oszuści liczą na ogólny brak wiedzy dziadków na temat tego, gdzie w danym momencie przebywa jego wnuk.

„Pomyślne fałszowanie wymaga połączenia samego fałszowania i socjotechniki. Inżynieria społeczna odnosi się do metod stosowanych przez cyberprzestępców, aby nakłonić nas do podania danych osobowych, kliknięcia złośliwego łącza lub otwarcia załącznika wyładowanego złośliwym oprogramowaniem".

Jak wykryć podszywanie się?

Oto znaki, że jesteś podszywany. Jeśli widzisz te wskaźniki, naciśnij Usuń, kliknij przycisk Wstecz, zamknij przeglądarkę, nie przechodź.

Podszywanie się pod witrynę

- Brak symbolu kłódki lub zielonego paska. Wszystkie bezpieczne, renomowane witryny muszą mieć certyfikat SSL, co oznacza, że zewnętrzny urząd certyfikacji potwierdził, że adres internetowy faktycznie należy do weryfikowanej organizacji. Należy pamiętać, że certyfikaty SSL są teraz bezpłatne i łatwe do uzyskania. Chociaż strona może mieć kłódkę, nie oznacza to, że jest to prawdziwa okazja. Pamiętaj tylko, że nic w Internecie nie jest w 100% bezpieczne.
- Witryna nie korzysta z szyfrowania plików. Protokół HTTP lub Hypertext Transfer Protocol jest tak stary jak Internet i odnosi się do reguł używanych podczas udostępniania plików w Internecie. Prawidłowe witryny internetowe prawie zawsze używają protokołu HTTPS, zaszyfrowanej wersji protokołu HTTP podczas przesyłania danych tam, iż powrotem. Jeśli jesteś na stronie logowania i widzisz „http" zamiast „https" w pasku adresu przeglądarki, powinieneś być podejrzliwy.

- Użyj menedżera haseł. Menedżer haseł, taki jak 1Password, automatycznie wypełni Twoje dane logowania do każdej legalnej witryny, którą zapiszesz w skarbcu haseł. Jeśli jednak wejdziesz na
- sfałszowaną witrynę, menedżer haseł nie rozpozna tej witryny i nie wypełni za Ciebie pól nazwy użytkownika i hasła — to dobry znak, że jesteś sfałszowany.

Podszywanie się pod e-maile

- Sprawdź dokładnie adres nadawcy. Jak wspomniano, oszuści będą rejestrować fałszywe domeny, które wyglądają bardzo podobnie do legalnych.
- Google zawartość e-maila. Szybkie wyszukiwanie może być w stanie pokazać, czy znany e-mail phishingowy rozchodzi się po sieci.

- Osadzone linki mają nietypowe adresy URL. Możesz sprawdzić adresy URL przed kliknięciem, najeżdżając na nie kursorem.
- Literówki, zła gramatyka i nietypowa składnia. Oszuści nie sprawdzają swojej pracy.
- Treść e-maila jest zbyt piękna, aby była prawdziwa.
- Są załączniki. Uważaj na załączniki — zwłaszcza ,jeśli pochodzą od nieznanego nadawcy.

Podszywanie się pod identyfikator rozmówcy

- Identyfikator dzwoniącego można łatwo sfałszować. To smutny stan rzeczy, gdy nasze telefony stacjonarne stały się siedliskiem oszustw. Jest to szczególnie niepokojące, gdy weźmie się pod uwagę, że większość osób, które nadal mają telefony stacjonarne, to osoby starsze – grupa najbardziej podatna na oszustwa. Pozwól, aby połączenia z telefonem stacjonarnym od nieznanych rozmówców trafiały na pocztę głosową lub automatyczną sekretarkę.

Jak mogę chronić się przed podszywaniem się?

Przede wszystkim powinieneś nauczyć się rozpoznawać atak typu spoofing.

Włącz filtr spamu. Dzięki temu większość fałszywych e-maili nigdy nie trafi do Twojej skrzynki odbiorczej.
Nie klikaj linków ani nie otwieraj załączników w wiadomościach e-mail, jeśli e-mail pochodzi od nieznanego nadawcy. Jeśli istnieje szansa, że wiadomość e-mail jest wiarygodna, skontaktuj się z nadawcą innym kanałem i potwierdź treść wiadomości e-mail.

Zaloguj się przez osobną kartę lub okno. Jeśli otrzymasz podejrzaną wiadomość e-mail lub SMS z prośbą o zalogowanie się na swoje konto i podjęcie jakiegoś działania, np. zweryfikowanie swoich danych, nie klikaj podanego linku. Zamiast tego otwórz inną kartę lub okno i przejdź bezpośrednio do witryny. Możesz też zalogować się przez dedykowaną aplikację na swoim telefonie lub tablecie.

Odbierz telefon. Jeśli otrzymasz podejrzaną wiadomość e-mail, rzekomo od kogoś, kogo znasz, nie bój się zadzwonić lub wysłać SMS-a do nadawcy i potwierdzić, że rzeczywiście wysłał wiadomość. Ta rada jest szczególnie słuszna, jeśli nadawca wysyła prośbę nietypową, np. „Hej, czy możesz kupić 100 kart upominkowych iTunes i przesłać mi numery kart?

Pokaż rozszerzenia plików w systemie Windows. System Windows domyślnie nie wyświetla rozszerzeń plików, ale możesz zmienić to ustawienie, klikając kartę „Widok" w Eksploratorze plików, a następnie zaznaczając pole, aby wyświetlić rozszerzenia plików. Chociaż nie powstrzyma to cyberprzestępców przed fałszowaniem rozszerzeń plików, przynajmniej będziesz mógł zobaczyć sfałszowane rozszerzenia i uniknąć otwierania tych złośliwych plików.

Zainwestuj w dobry program cyberbezpieczeństwa. W przypadku kliknięcia złego łącza lub załącznika nie martw się, dobry program do cyberbezpieczeństwa będzie w stanie ostrzec Cię o zagrożeniu, zatrzymać pobieranie i zapobiec przedostawaniu się złośliwego oprogramowania do systemu lub sieci.

Programy będą blokować połączenia i wiadomości tekstowe ze znanych numerów oszustw. To świetna poprawka dla rodziców i dziadków, którzy wciąż polegają na starym telefonie stacjonarnym. Odetnij przewód i skonfiguruj je za pomocą podstawowego smartfona z już zainstalowanym Malwarebytes

.

Jak zapobiec podszywaniu się pod wiadomości tekstowe:

- W miarę możliwości unikaj klikania linków w wiadomościach tekstowych. Jeśli wiadomość SMS, która wydaje się pochodzić od znanej Ci firmy, prosi o podjęcie pilnych działań, odwiedź jej witrynę bezpośrednio, wpisując adres URL samodzielnie lub wyszukując w wyszukiwarce i nie klikaj łącza SMS.
- W szczególności nigdy nie klikaj linków „resetowanie hasła" w wiadomościach SMS – są to bardzo prawdopodobne oszustwa.

- Pamiętaj, że banki, firmy telekomunikacyjne i inni legalni dostawcy usług nigdy nie proszą o podanie danych osobowych za pośrednictwem SMS-ów – więc nie podawaj danych osobowych w ten sposób.
- Zachowaj ostrożność w przypadku jakichkolwiek „zbyt pięknych, aby mogły być prawdziwe” alertów SMS o nagrodach lub zniżkach – prawdopodobnie będą to oszustwa.

REGON: 240530048, NIP: 9492019492
adres ul. ALEJA POKOJU, nr 12, lok. ---, miejsc. CZESTOCHOWA, kod 42-207,
Numer KRS: 0000266366

Zadanie publiczne współfinansowane ze środków otrzymanych z Powiatu Lublinieckiego

PUBLIKACJA WYDANA PRZEZ CZĘSTOCHOWSKIE STOWARZYSZENIE ETOH