POLICJA ŚWIĘTOKRZYSKA

https://swietokrzyska.policja.gov.pl/kie/dzialania-policji/aktualnosci/58479,Tak-dzialaja-oszusci.html
2023-02-04, 13:48

TAK DZIAŁAJĄ OSZUŚCI!

Data publikacji 29.09.2022

Pamiętajmy, że zasada „ograniczonego zaufania” do nieznajomych obowiązuje nie tylko dzieci. Dorośli często o niej zapominają, stając się ofiarami własnej łatwowierności i braku rozwagi. Oszuści wykorzystują ufność oraz dobre serce osób, które nie potrafią odmówić pomocy w trudnej sytuacji. Należy pamiętać, że ci przestępcy nie próżnują i co jakiś czas modyfikują swoje działania. Przestępcy stosują co raz to bardziej pomysłowe metody, by dotrzeć nie tylko do seniorów. Ofiarą oszustów padają także młodsi, często przekonani chęcią szybkiego zysku. Poniżej przedstawiamy algorytmy postępowania oszustów.

Algorytm postępowania przestępców jest następujący:

„na wnuczka/krewnego/policjanta”

- dzwonią na numer stacjonarny i nawiązują rozmowę ze starszą osobą, podszywają się pod któregoś z członków rodziny. Po chwili jednak przerywają połączenie. Bardzo szybko telefon ponownie dzwoni. Tym razem przestępca podaje się za policjanta, funkcjonariusza CBŚP lub CBA. Oszust przekonuje swego rozmówcę, że np. rozpracowuje zorganizowaną grupę przestępczą i prosi, aby mu w tym pomóc – poprzez przekazanie gotówki. Głos w słuchawce podkreśla, że dzięki temu będzie można zatrzymać prawdziwych przestępców. W rzeczywistości działanie to jest bezprawne i nie ma nic wspólnego z postępowaniem funkcjonariuszy Policji, a jedynym celem jest zdobycie środków finansowych przez zorganizowane grupy przestępcze. Po przekazaniu pieniędzy lub wpłaceniu ich na wskazane przez oszusta konto - kontakt się urywa. Z reguły to właśnie w tym momencie - pokrzywdzony orientuje się, że padł ofiarą oszusta tracąc niejednokrotnie oszczędności życia.
- oszuści najpierw wykonują telefon podając się za członka rodziny (najczęściej wnuczka). Tłumaczą zmieniony głos chorobą, a następnie proszą o przekazanie dużej sumy pieniędzy. Zazwyczaj pieniądze, które ma przekazać osoba, do której dzwonią mają zostać wykorzystane na pokrycie szkód po wypadku drogowym, na ważną operację czy na zakup samochodu. Oszuści w trakcie rozmowy umiejętnie manipulują rozmówcą tak, by uzyskać o nim jak najwięcej informacji.
- oszust, który podaje się także za lekarza jednego ze szpitali. Przekazuje swojej ofierze informację o tym, że jej bliski jest ciężko chory na koronawirusa i może go uratować specjalistyczny lek. Za leczenie trzeba zapłacić kilkadziesiąt tysięcy zł., a po pieniądze zgłosi się pracownik szpitala.

„wykorzystanie systemu płatności internetowej”

- mechanizm przestępstwa polega na tym, że oszuści udają osoby zainteresowanie zakupem przedmiotów wystawionych na serwisach internetowych. Istotne, że kontakt ze sprzedającym nawiązują najczęściej za

pośrednictwem popularnego komunikatora lub e-maila, a nie samej platformy sprzedażowej. By sprawić wrażenie bardzo zainteresowanych zakupem towaru, często prowadzą obszerną korespondencję, szczegółowo wypytując o sprzedawany produkt. Finalizując transakcję podsyłają spreparowany link, który ma służyć do przyjęcia płatności przez sprzedającego. Link przenosi nas na stronę, gdzie wymagane jest podanie kompletnych danych karty płatniczej i jej posiadacza lub proszą o autoryzowanie transakcji kodem otrzymanym z banku. Jeśli to zrobimy, oszust wejdzie w posiadanie wszystkich naszych danych, które są mu niezbędne do wykonywania transakcji na naszym rachunku banków.

„na BLIK-a”

- oszuści podają się za znajomych wybranej ofiary. Kontaktują się poprzez portal społecznościowy, wcześniej uzyskując dostęp do konta jej przyjaciół, i proszą o „szybką pożyczkę”, tłumacząc się chwilową niedyspozycją. Obiecują zwrócić tego samego dnia pożyczoną gotówkę. Pokrzywdzeni nieświadomi niczego, przesyłają BLIK-iem umówioną kwotę i tym samym tracą swoje pieniądze.

„na kryptowaluty”

- przestępcy kontaktują się z wybraną ofiarą telefonicznie bądź przez portal społecznościowy i zachęcają do powiększenia swoich oszczędności. Oszust sprytnie i umiejętnie prowadzi rozmowę tak, by wzbudzić w nas zaufanie i przekonać do wpłaty najpierw mniejszej zaliczki, a potem pokazuje zyski i wybrana ofiara pod wpływem emocji inwestuje kolejne oszczędności, tym razem nieco wyższe. W ten sposób pokrzywdzeni tracą po kilkanaście, a nawet kilkadziesiąt tysięcy złotych. Bardzo często w tych przypadkach sprawcom udaje się osiągnąć dostęp zdalny do pulpitu ofiary i dzięki temu do konta bankowego, namawiając ofiary do zainstalowania specjalnego programu bądź aplikacji (AnyDesk).
- dzwoni osoba podająca się za pracownika firmy zajmującej się inwestycjami w kryptowaluty. Przedstawia szybką możliwość pomnożenia oszczędności. Poprzez dużą pewność siebie oraz odpowiednie słownictwo oszust zdobywa zaufanie potencjalnej ofiary, a następnie namawia aby ta na swoim telefonie komórkowym zainstalowała odpowiednią aplikację umożliwiającą śledzenie inwestycji. Pokrzywdzony wykonuje polecenie oszusta instalując aplikację, a dodatkowo o czym nie wie - program umożliwiający zdalny dostęp do telefonu (AnyDesk). Oszuści dysponując zdalnym dostępem wykonują operacje finansowe na koncie ofiary.

„na węgiel/opał”

- fikcyjna firma obiecuje nam dostarczenie ekogroszku, pelletu lub węgla po okazyjnej cenie po wpłacie przez nas całej kwoty lub zaliczki, a reszta ewentualnej zapłaty odbędzie się przy odbiorze. Niestety pomimo dokonania przelewu węgiel nie dociera do klienta, a samo ogłoszenie lub strona internetowa oszustów, jak i ich numery telefonów kontaktowych znikają po pewnym czasie. Może się zdarzyć, że wspomniani wcześniej sprzedawcy zastosują metodę bez zaliczki, lecz wtedy dowiadujemy się, że nasze zlecenie będzie zrealizowane w późniejszym, czasie – tym sposobem oszuści zachęcają nas mimo wszystko do dokonania zaliczki na wskazane konto.
- kolejnym sposobem wykorzystywanym przez oszustów jest podszywanie się pod strony firm zajmujących się wydobyciem lub sprzedażą opału. Spoofing, czyli podszywanie się oszustów pod rzeczywiste instytucje i urzędy jest popularnym typem ataków opartych na podszywaniu się pod strony internetowe, wiadomości e-mail lub SMS. Sposób ten polega na tym, że przestępcy internetowi próbują Cię oszukać i spowodować, abyś podjął działanie zgodnie z ich zamierzeniami. Cyberprzestępcy, podszywając się między innymi pod firmy kurierskie, urzędy administracji, a ostatnio również pod firmy zajmujące się sprzedażą węgla lub innego źródła energii, starają się wyłudzić nasze dane do logowania np. do kont bankowych lub używanych przez nas kont społecznościowych, czy systemów biznesowych.

„na pracownika banku”

- oszuści dzwoniąc podszywają się pod infolinię banku, na telefonie ofiary wyświetla się prawdziwy numer infolinii co uwiarygodnia słowa oszusta. Już na początku rozmowy rzekomy konsultant informuje ofiarę, że ktoś wziął na jej dane osobowe kredyt. Aby go anulować, poleca wziąć kredyt na tę samą kwotę. Ofiara postępując zgodnie z instrukcją fałszywego konsultanta zaciąga go za pomocą infolinii swojego banku. Potem przelewa na wskazane przez oszusta konto, do którego ma dostęp lub wpłaca je we wpłatomacie na rachunek podany przez oszusta.
- inny sposób to telefon od osoby przedstawiającej się jako pracownik banku. Rzekomy pracownik informuje swoja ofiarę, że pieniądze na jej koncie są zagrożone, dlatego jak najszybciej musi zalogować się na swoje konto, zainstalować aplikację i postępować zgodnie ze wskazówkami. Ofiara będąc pewna, że rozmawia z prawdziwym pracownikiem bankowym, postępuje zazwyczaj zgodnie z poleceniami rozmówcy. Niestety nie wie, że przestępca do oszustwa wykorzystał metodę *spoofingu*, czyli podszywania się oszustów pod rzeczywiste instytucje i urzędy. Klient banku instaluje przesłaną mu aplikację, przekazuje dane do logowania oraz przychodzące kody autoryzacyjne. Oszuści bądź wypłacają pieniądze znajdujące się na koncie bądź zaciągają kredyty.
- kolejny schemat oszustwa polega na tym, że zazwyczaj w słuchawce odzywa się męski głos, podający się za pracownika banku, w którym rozmówca ma konto. Na telefonie wyświetla się numer infolinii banku, dlatego połączenie nie wzbudza żadnych podejrzeń. Jest to tzw. *spoofing*, czyli podszywanie się pod rzeczywiste instytucje i urzędy. Rzekomy pracownik banku pyta, czy rozmówca złożył wniosek kredytowy. Po zaprzeczeniu oszust podaje, że w takim razie zrobiła to osoba trzecia w jego imieniu, dlatego też rozmowa zostanie przełączona do działu technicznego, w celu zabezpieczenia środków pieniężnych i konta. Po przełączeniu rozmowę z osobą pokrzywdzoną prowadzi już kolejny oszust, zazwyczaj jest to kobieta, która podaje nowy numer konta, które po zakończeniu procedury ma być własnością pokrzywdzonego. Zgodnie z podaną procedurą, oszukana osoba przelewa wszystkie swoje oszczędności na podane konto. Dodatkowo zaciąga jeszcze jeden lub kilka kredytów, gdzie wszystkie środki zostają przekazane na konto oszustów. Cała procedura, w tym rozmowy telefoniczne, mogą trwać nawet kilka dni. Następnego dnia rozmowę prowadzi kolejny oszust, który informuje ofiarę, by przez 24 godziny nie logowała się na swoje nowe konto bankowe, ponieważ będzie pod obserwacją Policji. Potem kontakt się urywa.

„na pracownika banku/policjanta/prokuratora”

- na telefon ofiary dzwoni osoba, która podaje się za pracownika banku. Rozmówca oświadcza, że pieniądze na koncie są zagrożone, gdyż widzi w systemie próbę wypłaty dużej sumy pieniędzy z konta ofiary lub próbę włamania na jej konto. Informuje także, że hakerzy są namierzani przez Policję, której funkcjonariusze będą się kontaktować z ofiarą telefonicznie. Po chwili dzwoni policjant lub nawet prokurator, który potwierdza słowa dzwoniącego wcześniej pracownika banku. Rzekomy policjant lub prokurator poleca przelać wszystkie pieniądze na wskazane konto, do którego tylko on ma dostęp, prosi też o dane do logowania lub inne dane osobowe, które służą następnie do zaciągnięcia kredytów.

Charakterystyczne dla tego rodzaju oszustw jest to, że przestępcy nie rozłączają się ze swoja ofiarą
i nawet gdy proszą o zweryfikowanie swoich danych, to odbywa się to na tym samym połączeniu, jednak już z drugim współpracującym oszustem. Dlatego tak ważne jest rozłączenie połączenia i zakończenie rozmowy!

Pamiętajmy, że oszuści umiejętnie manipulują rozmową tak, by uzyskać jak najwięcej informacji. Dlatego w kontaktach z nieznajomymi kierujmy się zawsze zasadą ograniczonego zaufania. Rozłączmy się i skontaktujmy z konsultantem swojego banku, aby zweryfikować, czy nasz rozmówca faktycznie jest tym, za kogo się podaje.

Oszuści bazują na naiwności i dobrym sercu ludzi, grają na ich uczuciach. Metody wykorzystywane przez oszustów często wpływają na nasze emocje, a te nie są dobrym doradcą, zwłaszcza kiedy trzeba działać szybko i zdecydowanie.

Ostrzegamy!
AnyDesk, TeamViewer, Splashtop to aplikacje, które umożliwiają zdalne połączenie z komputerami oraz urządzeniami

mobilnymi. Niestety oszuści bardzo często wykorzystują za ich pomocą metodę „na zdalny pulpit”. Internetowi przestępcy posługują się różnymi wariantami, chodzi jednak o to, by skłonić ofiarę do zainstalowania programu zdalnej obsługi komputera, a potem polecić jej by zalogowała się do swojego konta w banku. Czyniąc to, uzyskują pełny dostęp do konta oraz zgromadzonych na nim pieniędzy, co natychmiast wykorzystują.

Pamiętając o kilku podstawowych zasadach, możemy uniknąć kłopotów i utraty oszczędności naszego życia.

- Policja nigdy nie prosi o przekazanie pieniędzy i nigdy nie dzwoni z takim żądaniem! Policja nigdy nie informuje telefonicznie o prowadzonych działaniach! Jeżeli odebrałeś taki telefon, bądź pewien, że dzwoni oszust!

- Nigdy w takich sytuacjach nie przekazuj pieniędzy, nie podpisuj dokumentów, nie zakładaj kont w banku i nie przekazuj nikomu swoich danych, numerów PIN i haseł dostępu!

- Po takiej rozmowie natychmiast zadzwoń do kogoś bliskiego na znany Ci numer i opowiedz o tym zdarzeniu. Poinformuj policję, zadzwoń na numer alarmowy 112.

- Zawsze rozłączaj połączenie przed wykonaniem kolejnego. Na tym często bazują oszuści!

- Za każdym razem, gdy proszeni jesteśmy o wykonanie transakcji z naszego rachunku bankowego, przekazanie danych służących do logowania na konto bądź gotówki nieznanej nam osobiście osobie, jest to potencjalne oszustwo i wówczas należy bezwzględnie starać się zweryfikować wiarygodność osoby, która do nas dzwoni, albo kontaktuje się z nami
  w inny sposób - poprzez SMS, komunikator internetowy czy pocztę elektroniczną. Warto dwa razy zastanowić się i dokładnie wszystko sprawdzić przed wykonaniem czynności zleconej nam przez głos w słuchawce, aby nie stracić życiowych oszczędności.

- Pod żadnym pozorem nie przekazujmy jakiejkolwiek osobie, co do tożsamości której nie jesteśmy stuprocentowo pewni, loginu i hasła do bankowości internetowej oraz danych karty płatniczej. Są to informacje poufne i powinny być tylko w posiadaniu ich użytkownika. Nikt nie ma prawa wymagać od nas ich podania. Prawdziwy przedstawiciel banku nigdy o to nie zapyta;

- Nawet jeśli zostaliśmy poinformowani o potencjalnym zagrożeniu np. ataku hakerów na nasze konto bankowe, należy spokojnie przemyśleć, czy środki zgromadzone na rachunku naprawdę mogą być w niebezpieczeństwie, czy może rozmowa prowadzona jest
  z oszustem. Musimy zawsze mieć świadomość, że wyświetlony numer telefonu lub nazwa banku nie są gwarancją, że rozmawiamy z prawdziwym przedstawicielem tej instytucji.

- Jeśli o „szybką pożyczkę” zwracają się do nas znajomi poprzez portal społecznościowy- pisząc, że np. stoją przy kasie, zabrakło im środków na koncie, a muszą zapłacić za zakupy – proszą o przesłanie pieniędzy BLIKiem, weryfikujmy takie informacje. Lepiej zadzwonić do takiego znajomego i upewnić się czy na pewno to on do nas pisze.

- Nigdy nie przekazuj dostępu do swoich urządzeń osobom, których nie znasz.

- Nie ufaj oferowanej "pomocy", o którą nie prosiłeś! Żaden bank ani firma nie poproszą Cię przez telefon o pobranie oprogramowania! Jeśli „konsultant” proponuje Ci zainstalowanie oprogramowania typu AnyDesk, możesz być pewien, że to oszustwo.

- Jeśli osoba podająca się za pracownika banku żąda zweryfikowania Twoich danych i danych konta lub zainstalowania jakiegokolwiek oprogramowania rozłącz się i zadzwoń do biura obsługi klienta Twojego banku.

- Pracownicy banku nie wymagają od klientów podawania haseł i loginów do konta!

Oprac. M S-B

Źródło: KWP w Kielcach.