https://poznan.wyborcza.pl/poznan/7,36001,27664412,mlodzi-i-wyksztalceni-traca-wszystkie-oszczednosci-oficer-policji.html?_ga=2.83153937.667515577.1633964513-2058663168.1624426496#S.main_topic_2-K.C-B.2-L.3.maly

Młodzi i wykształceni tracą wszystkie oszczędności. Oficer policji opowiada o "skrobaniu mamuta"

PIOTR ŻYTNICKI
11 PAŹDZIERNIKA 2021 | 06:00

SPOOFING - TAK OKREŚLA SIĘ NOWE PRZESTĘPSTWO INTERNETOWE. POLEGA NA PODSZYWANIU SIĘ I CZYSZCZENIU DO ZERA - A NAWET ZADŁUŻANIU - NASZYCH KONT.

Mają Facebooka i Instagrama, ale nie mają już pieniędzy. Każdego dnia polska policja dostaje nawet kilkaset zgłoszeń o nowym oszustwie i bezczelnych hakerach. Oto przestroga i kulisy przestępstwa.

W poniedziałek 4 października oficer dyżurny komendy wojewódzkiej policji w Poznaniu odbiera telefon. W słuchawce głos kobiety: - Dzień dobry, chciałam zapytać, czy numer 47 77 151 50 należy do wydziału od cyberprzestępczości?
- Tak, potwierdzam – odpowiada dyżurny.
- Dziękuję. Do widzenia – kobieta się żegna. Kilka godzin później orientuje się, że z jej bankowego konta zniknęły wszystkie pieniądze. Zgłasza przestępstwo i jeszcze ma pretensje – przecież rozmawiała z prawdziwym policjantem.

Policja: kilkaset prób "skrobania mamuta"

Andrzej (imię zmienione) przychodzi na spotkanie w czarnej marynarce, białym T-shircie i kolorowych adidasach. Jest oficerem operacyjnym wydziału ds. walki z cyberprzestępczością w komendzie wojewódzkiej w Poznaniu.
Przełożeni zgodzili się, by opowiedział nam o nowym oszustwie: - Codziennie w całej Polsce notujemy od kilkudziesięciu do kilkuset prób „skrobania mamuta", w większości udanych. Ofiarami nie są już zagubieni emeryci, jak w oszustwach na wnuczka. Pieniądze tracą młodzi, wykształceni ludzie. Mają smartfony, Facebooka, Instagrama. Inwencja przestępców wkroczyła na nowy poziom.
Policjanci posiłkują się angielskim słowem „spoofing", ale chodzi po prostu o podszywanie się i czyszczenie do zera – a nawet zadłużanie – naszych kont.
To udoskonala wersja znanej już metody „na policjanta CBŚ". Do tej pory oszuści dzwonili do przypadkowej osoby, informując, że zdeponowane w banku pieniądze są zagrożone, trzeba je pilnie wypłacić, a policja schowa je w depozycie. Ofiara szła do banku, wypłacała gotówkę i oddawała fałszywemu policjantowi. Ryzyko wpadki było jednak spore, bo prawdziwa policja mogła zrobić zasadzkę, media zaczęły ostrzegać przed tą metodą, a banki przeszkoliły pracowników. Oszuści poszli więc krok dalej.

Spoofing. Na telefonie zobaczysz, że dzwoni infolinia banku

- Sami czyszczą zdalnie konta swoich ofiar. Nadal mają legendę – podają się za pracowników banku, a także policjantów. Znaleźli jednak nowy sposób, by się uwiarygodnić. Nawet ostrożna z natury osoba może się na to złapać – mówi Andrzej.

I opowiada: - Przestępcy wykorzystują telefonię internetową, tzw. VoIP (Voice over Internet Protocol). Można z niej bez problemu połączyć się z tradycyjną telefonią komórkową GSM. Wystarczy zatem, że tylko sprawca używa telefonii internetowej. Pozwala mu to przed wykonaniem połączenia, za pomocą zainstalowanej aplikacji, wpisać w polu „nadawca" dowolny numer lub nazwę, które potem wyświetlą się na naszym telefonie. Na ekranie zobaczymy więc, że dzwoni infolinia naszego banku albo komenda policji. Numer telefonu będzie się zgadzał.

- Ale skąd wiedzą, w którym banku mam konto? Działają na chybił-trafił? – pytamy.

- To ataki celowane. Wiedzą, do kogo dzwonią. Korzystają z baz danych, które na przestrzeni lat wypływały z różnych instytucji finansowych lub administratorów różnych aplikacji. Hakerzy włamują się do niedoskonałych systemów i wykradają wykazy klientów. Potem proponują, że je zwrócą, ale za pieniądze. Jeśli administrator nie chce płacić, to wystawiają je na sprzedaż w darknecie [ukryte zasoby internetu]. Grupy zajmujące się spoofingiem kupują te wykazy i wybierają ofiary. Może się zdarzyć, że na przestrzeni lat ktoś zmienił bank, ale większość osób tego nie robi.

Pieniądze znikają z konta, czyli skrobanie mamuta

- Czyli już na starcie oszuści zyskują przewagę, bo zgadza się nazwa banku i numer telefonu.

- Dokładnie tak. Potem zaczyna się rozmowa: proszą o imię i nazwisko, pytają, czy jest pan lub pani posiadaczem rachunku. Mówią: „Zauważyliśmy nietypowy ruch na koncie, wypływają z niego pieniądze". Proszę o podanie numeru karty debetowej z kodem CVV bądź loginu i hasła do bankowości elektronicznej. A potem czyszczą konto. W ich żargonie nazywa się to skrobaniem mamuta. Czasem uruchamiają też linię kredytową i również czyszczą, zadłużając ofiarę.

- A po co im numer karty debetowej?

- Przy jej pomocy również można przelać pieniądze z jednego konta na drugie. I tak robią. Pieniądze płyną na konto założone na „słupa" [podstawiona osoba, zwykle niezdająca sobie z tego sprawy], ale najczęściej na konta za granicą w krajach takich jak Białoruś czy Ukraina.

- To chyba trudno ich namierzyć?

- Gdyby dzwonili przy użyciu tradycyjnej telefonii komórkowej GSM, można by próbować ich namierzyć. Ale telefonia internetowa pozwala im dość skutecznie anonimizować się w sieci. Pewne ślady zostawiają, ale co z tego, skoro na przykład numer IP prowadzi do dostawcy internetu na pewnej egzotycznej wyspie? Zwracamy się o pomoc międzynarodową do innych państw, ale to trwa. Nie poddajemy się jednak. Mamy pewne operacyjne ustalenia, o których nie mogą mówić.

Spoofing. Oszuści podszywają się pod policję

Andrzej przyznaje, że policja ma do czynienia z zawodowcami, a nie amatorami. Możliwe nawet, że w proceder zaangażowały się osoby pracujące wcześniej w tej branży. Są na tyle bezczelni, że w ostatnich dniach zaczęli podszywać się już nie tylko pod pracowników banków, ale także pod policjantów z wydziału do walki z cyberprzestępczością.

W poniedziałek, 4 października na telefonie mieszkanki Poznania wyświetlił się prawdziwy numer wydziału, w którym pracuje Andrzej. Dzwoniący mężczyzna podał się za policjanta z komendy wojewódzkiej w Poznaniu. Poinformował o włamaniu na bankowe konto. Dodał, że policja prowadzi działania razem z pracownikami działu bezpieczeństwa banku.

- Potrzebujemy pani pomocy, ale na początek proszę zweryfikować, że jesteśmy policjantami – powiedział oszust. Kazał kobiecie oddzwonić i potwierdzić, że numer należy do wydziału do walki z cyberprzestępczością.

Kobieta oddzwoniła i połączyła się z prawdziwą komendą. Było po południu, więc w sekretariacie wydziału nikt już nie pracował. Centrala przełączyła ją do oficera dyżurnego. Kobieta słyszała nagranie: „Komenda wojewódzka policji w Poznaniu, proszę czekać". Odebrał prawdziwy oficer dyżurny. A potem – nieświadomy przekrętu – potwierdził, że podany numer należy do wydziału do walki z cyberprzestępczością.

- Potwierdziła pani numer? – zapytał oszust przy kolejnym telefonie.

– Tak – odpowiedziała kobieta.

- To teraz proszę wykonywać polecenia.

Mieszkanka Poznania przekazała fałszywemu policjantowi dostęp do swojego konta. Dopiero po kilku godzinach zorientowała się, że wszystkie pieniądze zniknęły.

Spoofing. Jak się ochronić i uratować pieniądze?

Andrzej przyznaje, że policjanci nie mogli uwierzyć w bezczelność bandytów. W kolejnych dniach sytuacja się powtórzyła. – Ale oficerowie dyżurni byli już uprzedzeni, więc udało się zapobiec oszustwom. Teraz dyżurujemy przy telefonie naszego wydziału przez całą dobę, bo to może nie być koniec – mówi oficer.

- Co zatem robić, gdy na telefonie wyświetli się informacja, że dzwoni do nas policja lub nasz bank? – pytamy.

Andrzej odpowiada: - Ani policja, ani bank nie prosi nigdy o podanie numeru karty kredytowej i kodu CVV, a tym bardziej loginu i hasła do bankowości internetowej. Jeśli dzwoniący poprosi nas o takie dane, powinna zapalić nam się lampka ostrzegawcza. Należy przerwać połączenie i nie oddzwaniać. Wejdźmy na stronę banku, znajdźmy numer na infolinię, wpiszmy go do telefonu i zadzwońmy, by sprawdzić, czy rzeczywiście z naszym kontem coś się dzieje.

Spoofing. Banki nie uznają reklamacji

- A jeśli już daliśmy się nabrać?

- Zanim pójdziemy na policję zgłosić przestępstwo, skontaktujmy się ze swoim bankiem. Im szybciej to zrobimy, tym większe szanse, że pieniądze uda się uratować. Przelewy między bankami odbywają się bowiem w ciągu dnia w kilku sesjach, pomiędzy nimi pieniądze są w „kwarantannie". Można je jeszcze uratować.

- A jeśli nie zdążymy? Można złożyć w banku reklamację?

- Od ofiar wiemy, że banki nie uznają takich reklamacji. Wychodzą z założenia, że ich zabezpieczenia są dobre, a klient sam udostępnił innej osobie login czy hasło.

Oficer dodaje, że ofiary tracą od kilkuset złotych do nawet ponad 100 tys. zł: - To ludzie w różnym wieku, różnych profesji. Wielu młodych, wykształconych. Wydaje im się, że są bezpieczni, bo wiedzą, jak działa internet, mają dziesiątki aplikacji, Facebooka, Instagrama. Ale potem okazuje się, że dali się oszukać. Zgodziliśmy się na tę rozmowę, by za pośrednictwem gazety wszystkich ostrzec.