

Oszustwa coraz bardziej wyrafinowane

Dziś chcemy ostrzec czytelników „Panaceum” przed wyjątkowo zuchwałymi próbami wyłudzeń pieniędzy. Chodzi o metody „na wniosek kredytowy” oraz „na fałszywą inwestycję”. W przypadku tej drugiej, w pułapkę można wpaść aż dwa razy!

Agnieszka Danowska-Tomczyk

W tym miejscu miał być inny tekst, jednak nasza stała autorka, Katarzyna Rulkiewicz, zaangażowała się w pomoc powodzianom. Naturalną kolejną rzeczą było więc, że przyjemny obowiązek pisanie do „Panaceum” zszedł na dalszy plan. Zbiegło się to z sytuacją, która mnie spotkała, a – jak się potem okazało – jest coraz powszechniejszą próbą wyłudzenia pieniędzy. Przybliżę Państwu tę i jeszcze drugą historię, ku przestrodze.

Metoda „na wniosek kredytowy”

Środek tygodnia, tuż przed godz. 9. Spieszę się do pracy, ale dzwoni telefon – numer mi nieznany, ale z racji zawodu odbieram takich dziesiątki. Pozornie numer wygląda normalnie, zaczyna się od 609... W słuchawce miły głos ze wschodnim akcentem, ale płynnie mówiący po polsku, przedstawia się i mówi, że dzwoni z „banku PKO”. Już wtedy troszkę mnie zdziwiło, że nie użył pełnej nazwy banku, jak choćby „moja pani” z banku, gdy wymawia wszystkie trzy człony nazwy, choć potocznie używamy jedynie pierwszej. Miły pan mówi, że dzwoni potwierdzić złożenie wniosku o kredyt. Pyta, czy to prawda, że go złożyłam. Teraz przedstawię Państwu cały dialog, w nawiasach uwzględniając didaskalia, nieco podprowadzające do przedstawienia mechanizmu oszustwa.

– Nie, to nieprawda – mówię.

– O, to wygląda na próbę oszustwa (wykazanie fałszywej troski). Ktoś próbuje się pod panią podszyć (podwójna troska!). Bo rozmawiam z panią Agnieszką, tak?

– Tak – słucham uważnie, choć dzielę uwagę z tym, co dzieje się na drodze (oczywiście podłączona do zestawu głośnomówiącego w samochodzie).

– Pani Agnieszko (zmniejszenie dystansu, a więc jeszcze większa troska), a w jakim banku ma pani konto? Bo pragnę panią poinformować o procedurze: teraz my wyślemy tę informację do pani banku, by oni nie wydali dyspozycji o wypłacie tych środków nieuprawnionej osobie (napięcie rośnie!) – mówi miły pan.

I przyznam, że tutaj już naprawdę zapaliła mi się czerwona lampka. System autoryzacji

transakcji w moim banku jest do bólu wielostopniowy, więc o żadnej szybkiej dyspozycji na wypłatę środków nie może być mowy. Nie jestem ekspertką w procedurach prób wyłudzeń, ale gdyby naprawdę PKO (BP czy SA – bez różnicy) chciało sprawdzić czy klientka Santander chce wziąć kredyt, to mogliby to zrobić bez kontaktu ze mną.

– Wie pan co, zrobimy inaczej: ja podam panu e-mail i poproszę wszystkie szczegóły tej sytuacji drogą mailową, a ja już sama poinformuję bank – zaproponowałam.

W tym momencie pan się bez słowa rozłączył.

Gdy opowiedziałam tę historię koleżankom z pracy (do której dotarłam nie tylko z lekkim opóźnieniem, ale przede wszystkim w wielkich emocjach), okazało się, że jeszcze dwie osoby z naszego kilkunastoosobowego zespołu miały podobną sytuację.

Co by było dalej? Byłoby jeszcze zuchwalej – po ujawnieniu nazwy banku, pan podziękowałby za rozmowę i się rozłączył. Po chwili doszłoby do tzw. spoofingu – zadzwoniłby telefon, a na wyświetlaczu pojawiłaby się informacja „Infolinia Santander” (znów – niepełna nazwa banku!). Miły pan 2, który zapewne siedzi obok naszego miłego pana nr 1, zadzwoniłby w celu weryfikacji danych, które rozstrzęsiona sytuacją osoba szybko poda.

Tym samym oszuści zdobyliby kluczowe informacje, które umożliwiłyby im dalsze działania, w tym potencjalnie wyłudzenie kredytu lub dostęp do konta.

Metoda „na fałszywą inwestycję” – podwójna pułapka

Warto także wspomnieć o innej, równie niebezpiecznej metodzie wyłudzeń, która pojawia się coraz częściej – „na fałszywą inwestycję”. W tym schemacie oszuści dzwonią do ofiary z propozycją inwestycji w „pewne” instrumenty finansowe, często obiecując szybki i wysoki zysk. Osoby zainteresowane tematem inwestycji mogą zostać skuszone wizją dużego zarobku przy minimalnym ryzyku.

Co gorsza, po pierwszej wpłacie, która wydaje się bezpieczna, oszuści kontynuują swoją grę, zachęcając do kolejnych inwestycji. W najbardziej perfidnych scenariuszach zachęcają jeszcze do pobrania aplikacji, która umożliwia podgląd tego, jak pieniądze zarabiają. W rzeczywistości są to programy śledzące, przechwytyjące hasła i dostępy m.in. do aplikacji bankowej. W wielu przypadkach po jakimś czasie ofiary orientują się, że straciły pieniądze, a kontakt z „doradcą” się urywa. Pieniądze najczęściej są już ulokowane za granicą, nierzadko w kryptowalutach. Pokrzywdzony zgłasza sprawę na policję, ale odzyskanie straconych pieniędzy to rzadkość. W Internecie nietrudno znaleźć ofiary, które w ten sposób straciły oszczędności życia, idący w setki tysięcy

złotych.

Niestety, może nastąpić drugi cios i to w dwojaki sposób – po jakimś czasie ofiara dostaje kolejny telefon od innej osoby, która twierdzi, że reprezentuje firmę specjalizującą się w odzyskiwaniu utraconych inwestycji. Nowi oszuści obiecują odzyskanie środków, jednak za odpowiednią opłatą – jednak nierzadko to ci sami oszuści! Drugim sposobem ponownego oszustwa na tej samej osobie jest kontakt z ramienia rzekomej kancelarii adwokackiej, która przygotowuje zbiorowy pozew i znalazła nas na grupach/forach dla pokrzywdzonych. Przygotowaniu pozwu i postępowania sądowego oczywiście kosztuje, więc... w ten sposób ofiara może paść ofiarą wyłudzenia dwa razy.

Codziennie ktoś zgłasza próbę wyłudzenia

Banki przyznają, że oba oszustwa są im dobrze znane. – Nie ma dnia, żeby ktoś nie przyszedł do oddziału i nie zgłosił próby lub samego oszustwa. Odbieramy też po kilkadziesiąt takich telefonów dziennie – mówi mi osoba z infolinii mojego banku, gdy zgłaszam ten incydent. Kinga Wojciechowska-Rulka, rzeczniczka prasowa mBanku z kolei dodaje: – To są naprawdę wyrafinowane i wyrachowane próby wyłudzeń. Nabrać się może nawet osoba, która uważa się za świadomą i czujną – podkreśla. Z kolei z komunikatów ostrzegających, publikowanych przez policję możemy dowiedzieć się, że takimi działaniami nie stoją już pojedyncze osoby, np. hakerzy, ale zorganizowane na dużą skalę grupy przestępcze.

Oszustwa często opracowane są na podstawie wiedzy psychologicznej: ktoś próbuje wywierać presję, sugerując, że jeśli ofiara nie zareaguje natychmiast, to kredyt zostanie zatwierdzony, a pieniądze zostaną wyłudzone. Manipulacja emocjami (strach, niepewność, panika) sprawia, że ofiara podejmuje pochopne decyzje, które prowadzą do przekazania oszustom wrażliwych informacji lub wykonania przelewów bankowych.

Jak reagować na podejrzane telefony?

Jeśli odbierzesz telefon, w którym rozmówca twierdzi, że ktoś złożył wniosek o kredyt na twoje nazwisko lub podejrzewa nieautoryzowane działania na twoim koncie, zachowaj spokój i postępuj według poniższych kroków:

1. **Nie podawaj żadnych danych osobowych ani bankowych.** Żadna instytucja bankowa nie poprosi cię przez telefon o PESEL, numer dowodu osobistego, hasła czy kody autoryzacyjne.
2. **Nie instaluj żadnego oprogramowania na polecenie osoby dzwoniącej.** Nie odwiedzaj stron internetowych ani nie pobieraj aplikacji, które ktoś sugeruje podczas rozmowy telefonicznej.

3. **Zakończ rozmowę.** W razie jakichkolwiek podejrzeń najlepiej zakończyć rozmowę i zadzwonić do swojego banku, korzystając z oficjalnego numeru kontaktowego widniejącego na stronie internetowej lub karcie bankowej. Bank zweryfikuje, czy rzeczywiście istnieje problem.
4. **Sprawdź swoje konto bankowe.** Zaloguj się na swoje konto, ale korzystaj tylko z własnego, zaufanego urządzenia, aby upewnić się, że nie ma żadnych podejrzanych transakcji.
5. **Nie działaj pod presją czasu.** Oszuści będą wywierać presję, abyś działał natychmiast, ale pamiętaj, że w rzeczywistości masz czas na spokojne sprawdzenie sytuacji.

Jak się chronić?

- **Nie podawaj danych przez telefon.** Banki nigdy nie proszą o podanie pełnych danych osobowych czy numerów kart przez telefon.
- **Sprawdź numer dzwoniącego.** Jeśli masz wątpliwości, zakończ rozmowę i skontaktuj się bezpośrednio z infolinią swojego banku.
- **Zachowaj ostrożność przy inwestycjach.** Zawsze dokładnie weryfikuj ofertę inwestycyjną, sprawdzaj firmy w oficjalnych rejestrach, np. KNF, i nie ufaj obietnicom szybkich zysków.
- **Zgłaszaj próby oszustwa.** Jeżeli staniesz się celem oszustwa, natychmiast zgłoś sprawę do banku, policji oraz do odpowiednich służb, takich jak CERT Polska.