Podejrzany telefon z infolinii banku? Rzecznik Finansowy ostrzega przed nową metodą oszustów.

Do Rzecznika Finansowego trafiają skargi od klientów, którym oszuści wyczyścili konta bankowe wykorzystując do tego zaufanie klientów do banków. Oszuści znaleźli nową metodę – podszywają się pod pracownika banku i nakłaniają klientów do przekazywania środków oraz instalacji nieznanego oprogramowania. Rzecznik Finansowy apeluje o ostrożność i rozwagę, jeśli znajdziemy się w podobnej sytuacji.

Jak to wygląda w praktyce, można prześledzić na podstawie przypadków, które trafiają do Rzecznika. Model działania przestępców jest bardzo podobny – to oni kontaktują się z klientem banku i informują go, że właśnie padł ofiarą przestępstwa i ktoś włamał się na jego konto.

– *Wszystko było bardzo wiarygodne. Oszustka, która się ze mną kontaktowała, dzwoniła z infolinii banku, tego numeru podanego na ich stronie internetowej* – tak w pierwszych słowach wniosku do Rzecznika Finansowego wskazuje jedna z klientek.

– *Zadzwoniła do mnie osoba, która podała, że jest pracownikiem działu do spraw walki z cyberprzestępczością i powiedziała, że mają informację, iż ktoś na moje nazwisko podejmuje próbę wzięcia pożyczki na dużą kwotę i próbował dokonać przelewu na cudze konto na kwotę 600 zł. Przekazano mi, że za chwilę skontaktuje się ze mną pracownik banku i przekaże kolejne instrukcje. Za chwilę zadzwonił ktoś z infolinii. Sprawdziłem ten numer, to infolinia banku* – to kolejny opis klienta, który padł ofiarą oszustwa.

Klienci, mimo zachowania należytej ostrożności są przekonani, że mają kontakt z pracownikami banku, bowiem na wyświetlaczu ich telefonu wyświetla się nazwa banku czy numer oficjalnie podany na stronie internetowej, gdzie mają prowadzony rachunek bankowy. Oszuści informują o rzekomej próbie popełnienia przestępstwa: wypłaty środków w bankomacie, próbie zaciągnięcia pożyczki na dane klienta czy zmiany numeru telefonu przypisanego do numeru rachunku bankowego. Stosują „nakładkę", która ukrywa prawdziwy numer, z jakiego jest wykonywane połączenie, a klientom na wyświetlaczu ich telefonu pokazuje się właśnie numer infolinii czy nazwa banku. W ten sposób przestępcy zdobywają zaufanie klienta.

– *Dalsze działania przestępców są zróżnicowane i stosowane są różne metody, które w konsekwencji mają doprowadzić do przekazania przestępcom środków zgromadzonych na rachunku. Przestępcy przekonują klienta, że działają w jego interesie i wszystkie przekazywane rady czy polecenia służą zabezpieczeniu środków przed kradzieżą, czy nieautoryzowaną transakcją płatniczą* — opisuje **Marta Obroślak, z biura Rzecznika Finansowego.**

Najczęściej klienci skłaniani są do zainstalowania programu, który pozwala przestępcom na zdalne przejęcie kontroli nad komputerem lub telefonem klienta tzw. zdalny pulpit. Wszystko pod pozorem instalacji aplikacji służącej działowi technicznemu banku do zeskanowania urządzenia klienta oraz zabezpieczenia go przed dalszymi próbami przejęcia konta. W ten sposób przestępcy np. generują kody BLIK, dzięki którym wypłacają środki w bankomacie, zmieniają sposób autoryzacji czy dokonują kolejnych transakcji płatniczych najczęściej z wykorzystaniem usługi przelewów natychmiastowych.

– *Zdarza się, że klient jest manipulowany i skłaniany do zaciągnięcia zobowiązania kredytowego za pośrednictwem bankowości elektronicznej, które to wedle oświadczenia przestępców podających się za pracowników banku, ma być potem anulowane np. „kodami BLIK". Wydaje się, że w ten sposób klient jest nakłaniany do pomocy bankowi mającej na celu ujęcie przestępców „na gorącym uczynku". Klient jest proszony o przekazywanie kodów BLIK, które to mają służyć anulowaniu kredytów, a tak naprawdę w tym samym czasie przy ich wykorzystaniu przestępcy wypłacają środki pozyskane z kredytu w bankomacie* – wyjaśnia Marta Obroślak.

Inny sposób działania przestępców, to informowanie przez rzekomych pracowników banku, że przestępca przełamał zabezpieczenia i ukradł pewną kwotę, najczęściej opiewającą na kilkaset złotych, przelewając ją na inny rachunek.

– *Klient jest zapewniany, że jedynym sposobem ochrony pozostałych środków jest ich przelanie na nowo utworzone konto przez bank dla klienta, bowiem trzymanie środków na obecnym rachunku nie jest już bezpieczne. W tym czasie klient jest namawiany do dokonywania kolejnych transakcji przelewem natychmiastowym i ich autoryzacji, niekiedy ich ponawiania ze względu na występowanie rzekomego błędu. Często zdarza się, że przestępca w celu kontroli działań podejmowanych przez klienta na rachunku bankowym czy przejęcia go i np. zwiększenia dziennego limitu przelewu lub dokonania transakcji, może nakłaniać klienta do zainstalowania oprogramowania, które pozwala na zdalne przejęcie kontroli nad komputerem* — mówi Marta Obroślak.

W związku z tym Rzecznik Finansowy apeluje o zachowanie szczególnej ostrożności w przypadku otrzymania telefonu z infolinii banku. Jeśli mamy jakiekolwiek podejrzenie, że może nie kontaktować się z nami pracownik banku należy niezwłocznie się rozłączyć i samodzielnie połączyć z infolinią banku. Podobnie należy postąpić w sytuacji, kiedy chcemy zweryfikować, czy kontaktuje się z nami pracownik banku.

Pamiętajmy, osoba kontaktująca się w imieniu banku nigdy nie poprosi nas o dane do logowania, podanie kodu BLIK czy zainstalowania aplikacji nieznanego pochodzenia!

Przypominamy! Kiedy bank powinien oddać Ci skradzione z konta pieniądze?

Przepisy określają termin zwrotu środków wynikających z nieautoryzowanej transakcji w oparciu o tzw. zasadę D+1. Zgodnie z nią pieniądze powinny wrócić na rachunek bankowy klienta nie później niż do końca dnia roboczego następującego po dniu

stwierdzenia wystąpienia nieautoryzowanej transakcji lub po dniu otrzymania zgłoszenia od klienta. Jedynym wyjątkiem od zasady zwrotu kwoty nieautoryzowanej transakcji w tym terminie jest uzasadnione i należycie udokumentowane podejrzenie próby oszustwa ze strony klienta. Równocześnie bank ma obowiązek na piśmie poinformować o takim podejrzeniu organy ścigania. W praktyce oznacza to, że bank zobligowany jest najpierw niezwłocznie oddać klientowi pieniądze, a następnie – jeżeli ma podstawy, by sądzić, że klient powinien w całości lub części odpowiadać za nieautoryzowaną transakcję – dochodzić tej kwoty od klienta na przykład przed sądem.

W sytuacji, gdy dojdzie do kradzieży środków pieniężnych z rachunku, klient może złożyć reklamację do podmiotu rynku finansowego. Reklamacja to wystąpienie skierowane do podmiotu rynku finansowego przez jego klienta, w którym klient zgłasza zastrzeżenia dotyczące usług świadczonych przez podmiot rynku finansowego. Reklamacja może być złożona w formie pisemnej, ustnie – telefonicznie albo osobiście do protokołu podczas wizyty klienta w jednostce lub w formie elektronicznej z wykorzystaniem środków komunikacji elektronicznej.

Równolegle, w sytuacji gdy utrata środków pieniężnych może być efektem działania przestępców, należy powiadomić policję i złożyć stosowne zawiadomienie.

Po wyczerpaniu trybu reklamacyjnego klient podmiotu rynku finansowego może złożyć do Rzecznika Finansowego wniosek o podjęcie interwencji z podmiotem rynku finansowego. Więcej informacji: https://rf.gov.pl/postepowania-interwencyjne/

Z kolei jeśli klient zdecyduje się na złożenie pozwu w sądzie lub został pozwany przez bank, może złożyć wniosek o wydanie tzw. istotnego poglądu w sprawie. Więcej informacji: https://rf.gov.pl/istotne-poglady/