WYRAFINOWANE DZIAŁANIA OSZUSTÓW – CBŚP APELUJE O ROZWAGĘ

Data publikacji 20.11.2021

Uważajmy na fałszywe połączenia telefoniczne przestępców podszywających się pod policjantów CBŚP czy banki. Pamiętajmy! Policjanci nigdy nie proszą o pomoc w akcji osób prywatnych, tym bardziej nie żądają przekazania pieniędzy czy oddania kart bankomatowych wraz z podanym numerem PIN.

Pomimo licznych apeli, nie tylko Policji, ale również wielu organizacji i instytucji, nadal zdarzają się osoby, które padają ofiarami oszustów. Ponownie zwracamy się z prośbą o ostrożność i rozwagę w kontaktach z nieznajomymi. Zachęcamy, aby uczulić swoją rodzinę i znajomych na to, by zawsze stosowali zasadę ograniczonego zaufania. Ofiarami oszustwa padają głównie ludzie starsi, których wrażliwość i ufność wykorzystują przestępcy.

Szczególnie w ostatnim czasie zauważyliśmy, że zwiększyła się liczba oszustw, których sprawcy podszywają się pod policjantów CBŚP czy pracowników banków. Przestępcy wykorzystując różnego rodzaju techniki i narzędzia wyłudzają pieniądze od pokrzywdzonych lub nakłaniają do określonego zachowania np. przekazania informacji czy zainstalowania szkodliwej aplikacji.

Jest to rodzaj phishingu, nazywany vishingiem. Nazwa jest połączeniem słów „voice phishing”, czyli phishing głosowy. Celem jest pozyskanie poufnych informacji lub nakłonienie ofiary do wykonania określonych czynności (np. zainstalowania aplikacji dającej przestępcom zdalny dostęp do komputera ofiary).

Niestety przestępcy potrafią posługiwać się technikami manipulacji, stosują socjotechnikę w taki sposób, aby uwiarygodnić swoją opowieść. Ponadto w celu uwiarygodnienia kontaktu, potrafią na telefonie ofiary wyświetlić numer telefonu lub nazwę zaufanej instytucji np. CBŚP.

Przestępca wykorzystując numer telefonu danej instytucji, faktycznie wykonuje połączenie na telefon swojej ofiary z zupełnie innego numeru telefonu. Skutkuje to wyświetleniem na telefonie ofiary numeru telefonu instytucji lub nazwy kontaktu, gdy w rzeczywistości przestępca dzwoni z innego numeru. Pozwala na to technika określana jako spoofing numeru telefonu.

Spoofing polega na podszywaniu się pod inne urządzenie lub innego użytkownika, może dotyczyć m.in. numeru telefonu, ale także adresu e-mail, IP, nadawcy SMS i innych. Przestępcy wykorzystują znane sobie technologie, które oprócz podmiany numeru telefonu pozwalają m.in. na wybór płci osoby dzwoniącej, barwy, akcentu czy dodawanie efektów dźwiękowych.

Osoba, która odbiera telefon, informowana jest o rzekomej transakcji na swoim rachunku bankowym, a dzwoniący prosi o potwierdzenie jej wykonania. Oczywiście żadnego obciążenia nie ma, ale zdezorientowana ofiara, myśląc, że ratuje swoje środki, odpowiada na pytania dzwoniącego przekazując mu wiedzę pozwalającą przestępcy np. na dostęp do jej

konta.

Trochę inaczej działa przestępca podszywający się pod policjanta proszącego o pomoc w akcji. Na numer telefonu ofiary dzwoni sprawca, z reguły z informacją, że mundurowi rozpracowują grupę przestępczą zajmującą się oszustwami m.in. na wnuczka. I to właśnie pieniądze rozmówcy są zagrożone lub należy je przekazać jako „przynętę" w prowadzonych działaniach. Weryfikacją akcji bywają wymyślone dokumenty z napisem CBŚP przedstawiane ofierze, czy też odebrane środki są „kwitowane" na sfałszowanych drukach konkretnej instytucji.

Jedna z mieszkanek Warszawy została tak zmanipulowana przez przestępców, że oddała im kartę bankomatową razem z numerem PIN. Gdy urwał się kontakt z przestępcami podszywającymi się pod policjantów poszkodowana zgłosiła się do prawdziwych funkcjonariuszy.

Apelujemy o szczególną ostrożność w kontaktach telefonicznych z osobami podającymi się za funkcjonariuszy różnych służb lub proponującymi świadczenie usług finansowych lub bankowych. Bezwzględnie należy zweryfikować tożsamość dzwoniącej osoby. Nie należy ulegać namowom rozmówcy o wykonywanie jakichkolwiek przelewów, czy podawanie kodów do autoryzacji przelewów bankowych.

- Policjanci nigdy nie informują telefonicznie o prowadzonych tajnych akcjach i nie proszą o branie w nich udziału osób postronnych. Tym bardziej, ostrożność należy zachować wtedy, gdy osoby podające się za przedstawicieli służb czy banków, proszą o wykonanie przelewów, czy podanie kodów autoryzacyjnych. W takich przypadkach należy natychmiast powiadamiać Policję.
- Pamiętajmy, nawet fachowe słownictwo rozmówcy nie może być potwierdzeniem jego wiarygodności.
- Należy zawsze mieć świadomość, że wyświetlony numer telefonu lub nazwa banku nie są gwarancją, że rozmawiamy z prawdziwym przedstawicielem banku.
- Zawsze należy czytać treść SMS-ów jakie przychodzą na telefon lub komunikatów w aplikacji mobilnej w trakcie połączenia z rzekomym przedstawicielem banku lub innej instytucji. Z ich treści może wynikać, że akceptujemy transakcję, którą przeprowadzają przestępcy.
- Jeżeli rozmowa wzbudza jakiekolwiek wątpliwości lub niepokój, należy rozłączyć się, odczekać minimum 30 sekund, a następnie samodzielnie połączyć z instytucją, której rzekomy przedstawiciel dzwonił, koniecznie wybierając oficjalny numer na klawiaturze numerycznej, a nie oddzwaniając na wcześniejsze połączenie.
- Zachowajmy zdrowy rozsądek i zimną krew, nawet jeżeli zostało się poinformowanym o potencjalnym zagrożeniu np. utrata środków. Należy spokojnie przemyśleć, czy środki naprawdę mogą być w niebezpieczeństwie, czy może rozmowa prowadzona jest z oszustem, który dopiero sytuację chce wykorzystać. Dobrym krokiem będzie przerwanie połączenia i ponowne jego zainicjowanie zgodnie z zasadą powyżej.

Wykorzystano materiały KGP