8 sierpnia 2022

Czym jest spoofing? Jak go rozpoznać i nie dać się nabrać?

Spoofing to rodzaj ataku, w którym przestępcy podszywają się pod banki, instytucje i urzędy państwowe, firmy, a nawet osoby fizyczne w celu wyłudzenia od swoich ofiar danych lub pieniędzy.

Dzięki wykorzystaniu różnych technik, oszuści mogą podszyć się pod wybrany adres e-mail, numer telefonu, a nawet adres IP i w nieuczciwy sposób osiągnąć swoje cele.

Na czym polega spoofing telefoniczny?

Jednym z najpopularniejszych ataków spoofingowych są te wykorzystujące połączenia telefoniczne. Oficjalna nazwa tego typu ataku to Caller ID Spoofing. Cybeprzestępcy używają różnych ogólnodostępnych narzędzi w sieci, które pozwalają dzwoniącemu podszywać się pod dowolnie wybrany przez siebie numer. Najczęściej podają się za pracowników banków lub instytucji państwowych.

Najpopularniejsze scenariusze ataków:

Jednym z popularnych przykładów ataków spoofingowych jest telefon od „pracownika banku", który informuje ofiarę o włamaniu na konto lub o podejrzanych operacjach bankowych. Oszust prosi rozmówce nie tylko o podanie poufnych danych, ale również o zainstalowanie oprogramowania, które rzekomo może ochronić ofiarę – w rzeczywistości pozwala przejąć kontrolę nad jej urządzeniem. W konsekwencji przestępcy uzyskują dostęp do bankowości klienta, zmieniają hasło i wypłacają zgromadzone na koncie pieniądze.

Zdarza się, że oszuści podają się też za policjantów lub innych urzędników państwowych, próbując wyłudzić dane lub hasła dostępu do różnych usług i serwisów.

W jaki sposób możemy się chronić?

Przestępcy będą próbowali różnych sposobów, by w nieuczciwy sposób pozyskać Twoje dane lub wyłudzić od Ciebie pieniądze. Schematy i scenariusze działań, a także używane argumenty mogą być bardzo urozmaicone. Ataki z wykorzystaniem spoofingu są podobne do ataków phishingowych, dlatego najlepszą ochroną jest zdrowy rozsądek i zachowanie spokoju.

Poniżej przedstawiamy kilka wskazówek, które mogą uchronić Cię przed oszustami:

- Zachowaj szczególną ostrożność, gdy ktoś będzie do Ciebie dzwonił i przedstawiał się jako pracownik banku lub innej instytucji. Pamiętaj, że nawet jeśli numer, z którego dzwoni, jest taki sam, jak ten podany na oficjalnej stronie, połączenie może być sfałszowane. Skontaktuj się ze swoim bankiem, samodzielnie wybierz numer na klawiaturze telefonu i zweryfikuj, czy osoba, która do Ciebie dzwoniła, mówiła prawdę.
- Pamiętaj, że pracownik banku ani inny przedstawiciel instytucji nigdy nie będzie Cię prosił o podawanie prywatnych danych oraz jakichkolwiek haseł czy kodów dostępu. Jeśli ktoś do Ciebie zadzwoni i to zrobi, natychmiast się rozłącz i zgłoś sprawę do swojego banku.

- Sprawdź, jakie zabezpieczenia wprowadził Twój bank i w jaki sposób możesz zweryfikować, tożsamość pracownika, który się z Tobą kontaktuje. Coraz więcej banków udostępnia taką funkcję poprzez wykorzystanie swojej aplikacji mobilnej.
- Nie otwieraj przesłanych linków ani załączników, jeśli nie znasz nadawcy i nie masz pewności, co mogą zawierać otrzymane treści.
  Dbaj o bezpieczeństwo swoich haseł, stosuj weryfikację dwuetapową.
- Aplikacje pobieraj tylko z zaufanych źródeł.
- Aktualizuj swój sprzęt i oprogramowanie, z którego korzystasz.
- Korzystaj z oprogramowania antywirusowego.

Jeśli natrafisz w sieci na jakiekolwiek oszustwa internetowe, zgłoś je do zespołu CSIRT NASK

Źródło: www.gov.pl