Czym jest spoofing i gdzie zgłosić ataki?

Spoofing jest rodzajem oszustwa, do którego przestępcy wykorzystują e-mail lub rozmowę telefoniczną. Podszywają się pod banki, instytucje państwowe czy firmy, by wyłudzić wrażliwe dane lub pieniądze. Przed atakiem spoofingowym może ochronić nas czujność i zasada ograniczonego zaufania do przychodzących połączeń telefonicznych i e-maili.

Jednym z najpopularniejszych ataków spoofingowych są te wykorzystujące połączenia telefoniczne. Cyberprzestępcy używają specjalnych narzędzi, które pozwalają dzwoniącemu podszywać się pod dowolnie wybrany przez siebie numer. Oznacza to, że na ekranie naszego telefonu może wyświetlać się informacja, że dzwoni do nas bankowa infolinia lub nasz operator telefoniczny, a nawet ktoś z naszej rodziny czy znajomych. Niestety ze względu na stosowaną technologię połączeń telefonicznych nie można skutecznie wyeliminować możliwości podszywania się pod cudze numery. Dlatego, jeśli to nie my wykręciliśmy numer, zawsze powinniśmy zachować ostrożność, bo nasz rozmówca może nie być tym, za kogo się podaje.

Przestępcy często podszywają się pod pracowników banków, ponieważ najczęściej zależy im po prostu na kradzieży pieniędzy. W najczęstszym scenariuszu oszuści twierdzą, że bank właśnie zatrzymał próbę wypłaty środków z konta klienta przez złodziei. Rzekomy pracownik banku ma pomóc rozmówcy w zabezpieczeniu konta na przyszłość, dlatego pyta o dane osobowe, hasło, login do banku a także instruuje, jak zainstalować specjalny program ochronny na telefonie lub komputerze. W rzeczywistości dzięki tym informacjom zdobywa dostęp do konta klienta, a zainstalowany program przejmuje kontrolę nad urządzeniem. Następnym etapem jest wyczyszczenie rachunku bankowego ze wszystkich środków.

Spooferzy podszywają się nie tylko pod pracowników banków, ale również pod policjantów, pracowników nadzoru finansowego czy nawet specjalistów od zwalczania cyberprzestępczości. Scenariusze rozmowy i ataku mogą być bardzo zróżnicowane, ale w pewnym momencie rozmówca będzie dopytywał się o dane osobowe albo hasła dostępu lub też będzie prosił o przesłanie pieniędzy czy zainstalowanie wskazanego oprogramowania. To znak, że rozmawiamy z oszustem! Pracownik banku, innej instytucji, żaden funkcjonariusz publiczny nigdy nie będzie zwracał się z takim żądaniem.
W e-mailowej wersji spoofingu również mamy do czynienia z podszywaniem się pod banki i inne instytucje. W tym przypadku podstawowa zasada brzmi - jeśli masz wątpliwości co do adresata, nie klikaj w wysłane mailem linki ani nie otwieraj załączników. Zawsze możesz zweryfikować, czy bank wysłał ci e-mail z taką wiadomością dzwoniąc na infolinię swojego banku.

Jak się bronić przed spoofingiem?

Jeżeli zachowasz czujność, dość łatwo możesz zorientować się, że rozmawiasz z oszustem. W takim przypadku najlepiej rozłączyć się i samodzielnie zadzwonić do instytucji, z której rzekomo dzwonił nasz rozmówca. W ten sposób zweryfikujesz, czy rzeczywiście stałeś się celem ataku spoofingowego.
W takim przypadku należy sprawę zgłosić na policję oraz do CERT Polska (zespół reagowania na incydenty cyberbezpieczeństwa działający w NASK). Można to zrobić pod **tym adresem**, jeśli dotyczy to ciebie/twojej rodziny/znajomego, trzeba wybrać opcję: „osoba fizyczna”.

Program sektorowy „Bankowcy dla Edukacji” to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Zapraszamy na stronę **www.bde.wib.org.pl**

BANKOWCY DLA EDUKACJI
program sektorowy