Co to jest Vishing?

Przestępcy podszywają się pod przedstawicieli banku lub innej firmy, policję, a nawet rodzinę i znajomych. Wszystko w celu wyłudzenia danych osobistych, loginów i haseł, danych kart kredytowych czy innych informacji. Tego typu oszustwo może zacząć się od telefonu z banku. Osoba podająca się za konsultanta początkowo informuje ofiarę o nietypowej aktywności na jej koncie. Wizja utraty zgromadzonych na rachunku środków finansowych wywołuje emocje, przy jednoczesnej potrzebie podjęcia natychmiastowych działań. Tego typu zdarzenie może prowadzić do ślepego podążania za instrukcjami dzwoniącego. Fałszywy konsultant może poinformować o tym, że w celu zabezpieczenia naszych pieniędzy konto zostanie tymczasowo zablokowane, a za chwilę zadzwoni dedykowana bankowi pomoc techniczna, która wesprze w procesie „bezpiecznego" dostępu do zgromadzonych oszczędności.

Kiedy pierwsza rozmowa zostaje zakończona, chwilę później można spodziewać się kolejnego połączenia, tym razem od wsparcia technicznego, które zostało wspomniane przy okazji pierwszego kontaktu.

Czego możemy spodziewać się od rozmówcy podającego się za pomoc techniczną?

- nakłaniania do pobrania i instalacji programu, poprzez który oszust uzyska dostęp do naszego urządzenia,
- nakłaniania do podania loginu i hasła, kodów dostępu do naszego konta bankowego poprzez wpisanie poświadczeń na stronie, którą podał oszust,
- nakłaniania do wykonania przelewu na udostępnione tymczasowe konto, w momencie kiedy oszuści przekonali rozmówcę do zablokowanego konta bankowego.

Jak reagować na telefony z banku czy inne instytucji?

- nie podejmuj żadnych pochopnych decyzji i nie działaj pod wpływem emocji,
- rozłącz się i zweryfikuj rozmówcę, wybierz na klawiaturze numer instytucji, od której dostaliśmy wiadomość i zadzwoń, ewentualnie odwiedź jej oddział,
- skontaktuj się z kimś zaufanym np. rodziną, przyjaciółmi i powiedzmy o niepokojącym telefonie,
- zwracaj uwagę na wszelkie nieścisłości i niejasności w komunikatach lub pytania, które wydają się podejrzane, zawierają błędy językowe,
- nigdy nie podawaj nikomu wrażliwych danych, loginów czy haseł lub kodów autoryzacyjnych,
- nie pobieraj ani nie instaluj aplikacji lub oprogramowania za czyjąś namową,
- nie wypłacaj pieniędzy ani nie zlecaj przelewów pod wpływem namowy osób dzwoniących.

Pamiętaj! Jeśli dzwoniący wymaga podania danych osobistych, haseł dostępu, kodów autoryzacyjnych lun numery kart płatniczych, należy natychmiast rozłączyć się i zgłosić sprawę do instytucji, za którą ktoś się podawał.

Wszystkie incydenty związane z bezpieczeństwem internetowym zgłaszaj do zespołu CERT Polska.