

Nieoczekiwany telefon z banku lub policji? Zachowaj czujność, to może być oszustwo!

Oszustwo z wykorzystaniem połączeń telefonicznych to tzw. vishing (z ang. voice phishing). Innymi słowy przestępcy dzwonią do nas z nieznanymi numerami, podając się za policjantów, przedstawicieli banków i innych instytucji, a nawet za członków naszej rodziny! Wszystko w celu wyłudzenia danych lub pieniędzy od osoby odbierającej telefon.



Każdego dnia wykonujemy i odbieramy połączenia telefoniczne. Warto zwracać uwagę na to, kto i w jaki sposób się z nami kontaktuje. Może okazać się, że rozmówca próbuje nas zmanipulować i oszukać. Pamiętajmy, że metod, które stosują przestępcy, jest wiele, ale na przestępstwo z wykorzystaniem połączeń telefonicznych narażony jest każdy z nas! Jeśli rozmówca będzie żądał od nas danych osobowych lub podjęcia pewnych działań (np. zainstalowania aplikacji, zlecenia przelewu, wypłacenia gotówki) należy natychmiast rozłączyć się i zadzwonić lub udać się do najbliższej placówki banku, a w przypadku udostępnienia informacji także poinformować policję o zaistniałym zdarzeniu.

Najpopularniejsze przykłady oszustw telefonicznych to:

- metoda na wnuczka (np. wypadek, zepsuty telefon, pilnie potrzebne pieniądze),
- metoda na policjanta, lekarza (np. zatrzymanie członka rodziny, próba kradzieży naszych pieniędzy, pilna konsultacja lekarska),
- metoda na przedstawiciela banku i pomoc techniczną (np. zablokowanie naszych środków finansowych),
- metoda na pracownika ZUS lub innej instytucji (np. problem z wypłaceniem emerytury).

Co powinno wzbudzić nasz niepokój?

- Ton rozmówcy wywołuje silne i trudne emocje, które mogą skłonić do podjęcia różnych działań,
- dzwoniący ponagla do podjęcia działań, grozi poważnymi konsekwencjami dla nas (np. utrata oszczędności) lub naszych bliskich (np. jeśli nie przekaze Pan/Pani pieniędzy, wnuczek może trafić do więzienia),
- presja czasu, potrzeba natychmiastowego działania, namawianie do podążania za wskazówkami udzielanymi przez telefon,
- wszelkiego rodzaju informacje o potrzebie wpłacenia lub przekazania pieniędzy (np. na opłacenie leczenia poszkodowanego w wypadku członka rodziny),

- nakłanianie do podania danych osobowych (np. imię, nazwisko, panińskie nazwisko),
- w niektórych przypadkach połączenie z obcego numeru telefonu lub prywatnego.

Jak się chronić przed oszustwami telefonicznymi?

- Nie podejmuj żadnych pochopnych decyzji, nie działaj pod presją czasu.
- Unikaj odbierania telefonu słowami: „Tak, słucham”.
- Rozłącz się i zweryfikuj rozmówcę. Zadzwoń pod numer instytucji, która rzekomo się z Tobą kontaktuje lub odwiedź jej oddział. W przypadku telefonu od rodziny skontaktuj się bezpośrednio z osobą, za którą podają się oszuści.
- Porozmawiaj z kimś zaufanym, np. rodziną, przyjaciółmi i powiedz o niepokojącym telefonie.
- Zwracaj uwagę na wszelkie nieścisłości w komunikatach lub pytania, których nie rozumiesz lub wydają Ci się podejrzane. Zwracaj uwagę na błędy językowe lub inny akcent.
- Nigdy nie podawaj nikomu wrażliwych danych, haseł logowania i innych kodów autoryzacyjnych.
- Nie pobieraj ani nie instaluj aplikacji lub oprogramowania za czyjąś namową, może to umożliwić rozmówcy zdalny dostęp do Twojego urządzenia.
- Nie przekazuj żadnych pieniędzy ani nie zlecaj przelewów pod wpływem namowy dzwoniącego. Jeśli otrzymasz podejrzaną wiadomość, zgłoś ją do zespołu CERT Polska. Poproś zaufaną osobę, aby pomogła Ci wypełnić formularz i przesłać zgłoszenie. Podejrzane wiadomości SMS możesz przekazać na numer bezpłatny numer 8080.

Pamiętaj: żaden bank, policja, firma ani instytucja nie będą prosić o pieniądze ani o podanie Twoich danych, haseł do logowania, danych do kart płatniczych czy instalację dodatkowego oprogramowania. Jeśli dzwoniący tego wymaga, należy natychmiast rozłączyć się i zgłosić sprawę instytucji, za przedstawiciela której ktoś się podawał.

Materiał przygotowany w ramach kampanii pt. #Halo! Tu cyberbezpieczny Senior! przygotowanej przez NASK, Centralne Biuro Zwalczania Cyberprzestępczości w Policji oraz Warszawski Instytut Bankowości.

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