Spoofing czyli podszywanie się pod inny numer telefonu. Jak się bronić?

Oszustwo, które polega na podszywaniu się pod czyjś numer telefonu to tzw. spoofing (z ang. spoof – naciąganie). W przypadku tego rodzaju przestępstwa poszkodowanymi są zarówno osoby, które odbierają takie połączenie, jak i osoby, których wizerunek jest wykorzystywany. Oszuści, wykorzystując technologię i różne narzędzia internetowe, są w stanie podszyć się pod każdy numer.

Przestępcy aby zdobyć nasze zaufanie lub wydobyć od nas osobiste informacje, mogą zadzwonić jako przedstawiciele banku lub innej instytucji publicznej (np. policji czy ZUS-u), ale także mogą podawać się za osoby, które bardzo dobrze znamy. Przykładowo, dzwoniący może udawać członka naszej rodziny, a na telefonie wyświetli się numer wnuczka lub innej osoby. Niestety, kiedy widzimy znajomy i zapisany numer, nasza czujność zostaje uśpiona, a presja czasu i towarzyszące nam emocje mogą wpłynąć na nasze działania.

Najpopularniejsze sposoby oszustw telefonicznych to:

- metoda na wnuczka (np. wypadek, pilna potrzeba przesłania gotówki);
- metoda na policjanta, lekarza (np. wypadek z udziałem kogoś bliskiego);
- metoda na przedstawiciela banku i pomoc techniczną (np. podejrzana aktywność na naszym koncie bankowym, zablokowanie zgromadzonych środków);
- metoda na pracownika ZUS lub innej instytucji (np. problemy z wypłaceniem emerytury).

Co powinno wzbudzić naszą czujność?

- ton rozmówcy wywołujący silne emocje, ponaglanie i grożenie poważnymi konsekwencjami np. jeśli nie przekaże Pan/Pani pieniędzy, będą problemy prawne;
- presja czasu i konieczność podjęcia natychmiastowych działań;
- wszelkiego rodzaju informacje o potrzebie wpłacenia pieniędzy (np. na opłacenie leczenia poszkodowanego w wypadku członka rodziny);
- nakłanianie do podania danych osobowych lub prywatnych informacji.

Jak się chronić przed oszustwami telefonicznymi?

- Nie podejmuj żadnych działań pod wpływem presji i nacisków rozmówcy.
- Rozłącz się i sprawdź rozmówców; zadzwoń do instytucji, od której rzekomo otrzymałaś(-łeś) połączenie lub wiadomość. Udaj się do placówki i sprawdź, czy rzeczywiście próbowali się z Tobą

skontaktować. W przypadku telefonu od osoby bliskiej, wybierz jej numer na klawiaturze i zweryfikuj przedstawioną sytuację.

- Skontaktuj się z kimś zaufanym, np. rodziną, przyjaciółmi i powiedz o niepokojącym telefonie.
- Zwracaj uwagę na wszelkie nieścisłości w komunikatach lub pytania, które wydają się podejrzane, błędy językowe, nietypowe prośby, nerwową atmosferę.
- Nigdy nie podawaj nikomu wrażliwych danych (np. daty urodzenia, numeru PESEL), 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 wypłacaj 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

CERT Polska – zespół ekspertów powołany do reagowania na zdarzenia i incydenty naruszające bezpieczeństwo w internecie oraz oszustwa komputerowe.

***

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

***