Ostrzeżenie - uwaga na próby wyłudzenia poufnych danych przez telefon – podszywanie się pod pracowników Banku nadal groźne!

03.2021. Ponownie ostrzegamy przed przestępcami podającymi się za pracowników banku – tzw. Vishing (Voice phising). Dla uwiarygodnienia swojej osoby mogą podawać się za pracowników działu IT lub bezpieczeństwa. Osoby te przez telefon wyłudzają poufne dane dotyczące haseł, kodów PIN/SMS.

Na czym polega Vishing (Voice phishing)?
To wyłudzenia poufnych danych z wykorzystaniem rozmowy telefonicznej (phishing głosowy). Przestępca dzwoniąc do ofiary podszywa się pod osoby lub instytucje godne zaufania. W ataku tym wykorzystywane są metody oparte na tzw. inżynierii społecznej (metody socjotechniczne)

Jak działają oszuści?
Informują rozmówcę, że dane te potrzebne są do zwiększenia bezpieczeństwa lub przeprowadzany jest test działania bankowości. Przestępcy mogą korzystać z techniki tzw. spoofingu numeru telefonu, tj. działać w taki sposób, by w telefonie ofiary wyświetlił się numer infolinii banku lub zaufanego pracownika banku.
W rzeczywistości celem oszustów jest m.in. zdobycie danych do logowania/ narzędzia autoryzacyjnego lub innych cennych danych, które nie powinny być upublicznione osobom postronnym.

Najczęściej stosowane metody:

- rozsyłanie wiadomości e-mail SMS ze wskazaniem numeru kontaktowego, pod którym można zaktualizować swoje dane,
- wykorzystanie oprogramowania wykonującego automatyczne połączenia telefoniczne wykorzystując dostępne w sieci Internet nr telefonów (np. z formularzy kontaktowych),
- bezpośrednie wykonywania połączenia telefonicznego przez oszusta wykorzystującego dostępne w sieci Internet nr telefonów (np. z formularzy kontaktowych),

We wszystkich powyższych scenariuszach cel jest ten sam - po wykonaniu połączenia, rozmówca lub automat prosi ofiarę o podanie danych poufnych celem weryfikacji tożsamości rozmówcy - np. loginu i hasła do bankowości elektronicznej, danych karty płatniczej (numer karty, data ważności, PIN).

Przypominamy:

- pracownicy Banku podczas rozmowy telefonicznej nigdy nie proszą o podanie haseł dostępu do konta bankowego, kodów PIN/SMS lub innych danych pozwalających na dokonanie transakcji,
- pracownicy Banku, nigdy nie proszą o zainstalowanie żadnego dodatkowego oprogramowania na komputerach lub urządzeniach mobilnych klienta,
- zawsze bądź ostrożny przy podawaniu danych telefonicznie i staraj się potwierdzić tożsamość rozmówcy – w przypadku jakichkolwiek wątpliwości zakończ rozmowę i skontaktuj się z Bankiem informując o zaistniałym o tym zdarzeniu,
- jeśli treść rozmowy wyda Ci się podejrzana i niestandardowa, a osoba dzwoniąca wymaga szybkiego podjęcia działań (np. podania danych, instalacji oprogramowania, podania kodów BLIK, kodów SMS, itp.) niezwłocznie zakończ rozmowę i skontaktuj się z Bankiem informując o zaistniałym zdarzeniu w celu potwierdzenia wiarygodności takiej rozmowy,

- jeśli podczas korzystania z elektronicznych kanałów dostępu spotkasz się z sytuacją, która wyda Ci się nietypowa, podejrzana lub wzbudzi Twoje zaniepokojenie, niezwłocznie skontaktuj się z Bankiem informując o zaistniałym zdarzeniu,
- nie podawaj nigdy przez telefon nadmiarowych informacji, nie zdradzaj szczegółów swoich transakcji, ani innych danych podlegających ochronie. Jeżeli masz jakiekolwiek wątpliwości – skontaktuj się osobiście z placówką Banku na znany Tobie numer telefonu (koniecznie wybierz numer ręcznie, najlepiej korzystając z innego urządzenia).