**Seniorze nie daj się oszukać: Jak odróżnić oszusta od pracownika banku**

Nowoczesna bankowość jest coraz bardziej wygodna i do załatwienia większości spraw nie wymagana już jest wizyta w placówce. Pandemia pokazała, jak ważne jest, by móc korzystać z usług bankowych przez internet czy telefon. To również ogromne ułatwienie dla osób z ograniczoną mobilnością i seniorów. Niestety zmiany w bankowości próbują wykorzystać oszuści, którzy dzwonią do naszych domów podszywając się pod pracowników banku. Na szczęście można ich dość łatwo zdemaskować!

Oszuści co chwila wymyślają nowe sposoby by wykraść nasze oszczędności, ale też dane. Potrafią przez telefon podać się za policjanta, pracownika naszego banku, przedstawiciela Komisji Nadzoru Finansowego czy Biura Informacji Kredytowej. Mówią, że dzwonią w ważnej, pilnej sprawie, bo np. ktoś włamuje się na nasze konto albo pojawia się wyjątkowa okazja inwestycyjna. Wzbudzają zaufanie, usypiają czujność, a potem wypytują o ważne informacje, lub proszą o wykonanie pewnych czynności na naszym komputerze czy telefonie. Jeżeli uda im się wyłudzić np. dane do logowania albo skłonić nas do zainstalowania złośliwego oprogramowania mogą wyczyścić konto bankowe lub wziąć kredyt w naszym imieniu!

**Po czym poznać oszusta?**

To właśnie nietypowe pytania i oczekiwania rozmówcy podającego się za pracownika banku powinny wzbudzić naszą czujność. Przedstawiciele banku **nigdy** nie proszą o dane do logowania do systemów bankowych, tj. numer klienta, login czy hasło. **Nie oczekują** dyktowania kodów BLIK, czy haseł jednorazowych. Takie informacje potrzebne są złodziejom, by dostać się na twoje konto!

Pracownicy banku nie pytają również o pełen numer PESEL czy dane dokumentu tożsamości. Te dane już znajdują się w systemie twojego banku. Oszuści mogą je jednak wykorzystać np. do zaciągnięcia pożyczki w twoim imieniu.

Przedstawiciele banku nie będą oczekiwać od ciebie również klikania w linki wysyłane mailem czy SMS-em ani instalowania aplikacji na telefonie czy komputerze. Nie będą wymagać również aktualizowania aplikacji. Oszuści pod tym pretekstem próbują skłonić cię do zainstalowania na twoim urządzeniu złośliwego programowania. Ostatnio coraz częściej instalują w ten sposób tzw. pulpit zdalny, który pozwala przejąć pełną kontrolę nad komputerem czy smartfonem. Dzięki temu mogą łatwo dostać się na twoje konto i ukraść pieniądze.

**Co robić, gdy podejrzewasz oszustwo?**

Jeżeli podczas rozmowy z osobą podająca się za pracownika banku (urzędnika, funkcjonariusza itp.) coś wzbudzi twoje podejrzenia to po prostu **przerwij rozmowę**. Nie przejmuj się, że rozmówca się obrazi, **bezpieczeństwo twoich pieniędzy jest ważniejsze**! Następnie zadzwoń na oficjalny numer infolinii twojego banku z pytaniem czy rzeczywiście ktoś z banku się z tobą przed chwilą kontaktował. Możesz również zgłosić sprawę na policję.

**Pamiętaj!**

Pracownik banku podczas rozmowy telefonicznej nigdy nie prosi o:

- login i hasło ( do bankowości internetowej, mobilnej ani do systemu telefonicznego),
- pełen numer PESEL,
- serię i numer dowodu osobistego,
- numer karty płatniczej, dane karty ani o kod CVV/CVC,
- podanie hasła jednorazowego,
- podanie kodu BLIK,
- instalację żadnego programu, aktualizacji ani aplikacji,
- kliknięcie w link wysłany e-mailem lub SMS-em.

O zdalnym pulpicie i o tym jak odróżnić oszusta od pracownika banku opowiada Cezary Pazura w filmie kampanii edukacyjnej „Bankowcy dla CyberEdukacji".

Zobacz!: https://youtu.be/wwP1dUTpbDk

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