SENIORZE NIE DAJ SIĘ OSZUKAĆ!

METODA „NA POLICJANTA”

Metoda „na policjanta” to modyfikacja opisanej metody „na wnuczka”.

Schemat oszustwa może wyglądać w ten sposób, iż:

- najpierw dzwoni osoba podająca się za krewnego i prosząca o wsparcie finansowe [I etap może stanowić zatem klasyczną metodę „na wnuczka”],
- po kilku chwilach telefon dzwoni ponownie, przy czym po drugiej stronie tym razem odzywa się fałszywy policjant - opowiada o grupie przestępczej, która próbuje wyłudzić pieniądze metodą „na wnuczka”. Osoba taka doradza, by senior złożył swoje oszczędności do depozytu policyjnego. Po jakimś czasie do seniora trafia fałszywy funkcjonariusz, który „deponuje” przekazane pieniądze i znika z nimi.

PAMIĘTAJ!!!

- Policja oraz inne służby mundurowe nie informują telefonicznie obywateli o szczegółach prowadzonych spraw.
- Policja nigdy nie prosi obywateli o przekazywanie pieniędzy, biżuterii lub innych wartościowych przedmiotów do depozytu w sposób opisany powyżej.

INNE METODY OSZUSTW:

- metoda na agenta CBŚ itp.;
- metoda na fałszywego urzędnika np. ZUS, NFZ, US, pracownika socjalnego itp.;
- metoda na obowiązkowy remont (pobieranie zaliczek);
- metoda na wymianę drzwi wejściowych;
- metoda na hydraulika bądź innego fachowca.

PRZYDATNE ADRESY I STRONY INTERNETOWE:

- Ministerstwo Spraw Wewnętrznych i Administracji, ul. Stefana Batorego 5, 02-591 Warszawa; www.mswia.gov.pl, www.bezpiecznysenior.eu
- Policja - www.policja.pl
- www.oszustwanawnuczka.pl
- strona internetowa ogólnopolskiej kampanii społecznej: www.zanim-podpiszesz.pl
- strona internetowa ogólnopolskiego systemu bezpłatnej pomocy prawnej: www.darmowapomocprawna.ms.gov.pl

OGÓLNOPOLSKA FEDERACJA
STOWARZYSZEŃ UNIWERSYTETÓW TRZECIEGO WIEKU
UL. JAGIELLOŃSKA 18, 33-300 NOWY SĄCZ
tel./fax [18] 443 57 08
e-mail: federacjautw@interia.eu
www.federacjautw.pl

BEZPIECZNY SENIOR

BROSZURA EDUKACYJNO-INFORMACYJNA

PIENIĄDZE SENIORA

CO TO JEST KONTO INTERNETOWE?

Konto internetowe - [inaczej: homebanking, e-banking, bankowość internetowa, e-bankowość, mobilna bankowość] - to jedna z form całodobowej działalności bankowej, polegającej na umożliwieniu przez bank swoim klientom przeprowadzania określonych operacji na rachunku bankowym [np.: sprawdzenie historii, wykonywanie przelewów, zakładanie stałych zleceń] za pomocą nowoczesnych technologii [komputer, telefon, tablet].

JAK BEZPIECZNIE KORZYSTAĆ Z KONTA INTERNETOWEGO?

Warunkiem bezpiecznego korzystania z konta internetowego jest stosowanie się do podstawowych zasad korzystania z tego typu usług:

- należy starannie przechowywać login i hasło do konta oraz kartę kodów jednorazowych lub telefon, na który przysyłane są kody;
  Dane te najlepiej przechowywać w różnych miejscach. Nie powinno się nosić tych informacji przy sobie. Hasło i login najlepiej zapamiętać, ewentualnie zapisać, ale w formie zaszyfrowanej np. jako fikcyjny nr telefonu. Pamiętajmy, że nie powinniśmy nikomu udostępniać naszych danych dostępowych do konta. Warto podkreślić, że bank nigdy nie kieruje do swoich klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację drogą mailową/telefoniczną.

Ministerstwo Spraw Wewnętrznych i Administracji

Zadanie publiczne jest współfinansowane ze środków Ministra Spraw Wewnętrznych i Administracji

OGÓLNOPOLSKA FEDERACJA STOWARZYSZEŃ UNIWERSYTETÓW TRZECIEGO WIEKU

- <u>nie należy korzystać z przypadkowych komputerów/tabletów/smartfonów;</u>
  Z konta internetowego powinno się korzystać wyłącznie na znanych nam, bezpiecznych urządzeniach. Należy unikać komputerów udostępnionych w miejscach publicznych [kawiarenki internetowe, dworce autobusowe] - urządzenia te mogą mieć zainstalowane różnego rodzaju wirusy lub inne oprogramowanie przechwytujące wpisywane przez nas dane.

- <u>na urządzeniu, za pomocą którego uzyskujemy dostęp do konta bankowego, należy zainstalować legalne oprogramowanie antywirusowe (*antywirus, firewall*);</u>
  Program antywirusowy można pobrać bezpłatnie z internetu. Pamiętać również należy o bieżącym aktualizowaniu oprogramowania antywirusowego.

- <u>wchodząc na stronę bankową należy upewnić się, czy nie nastąpiło przekierowanie na inną stronę podobną do strony naszego banku;</u>
  Logowanie się do konta powinno następować za pomocą nazwy strony internetowej banku, którą znamy. Nie wolno logować się za pomocą podesłanych linków. Szczególną ostrożność należy zachować w przypadku korespondencji mailowej z banku - zwłaszcza tej, w której bank zaleca nam szybkie zalogowanie się na koncie np. w celu sprawdzenia nowych usług. Pamiętajmy, że banki w przesłanej do nas korespondencji nigdy nie proszą o podanie naszego loginu i hasła do konta. Aby upewnić się, czy znajdujemy się na prawdziwej stronie bankowej, należy koniecznie zwrócić uwagę, czy adres witryny rozpoczyna się od <u>https://</u> oraz, czy w pasku dialogowym znajduje się symbol zamkniętej kłódki.

- <u>nie należy otwierać wiadomości i dołączonych do nich załączników jeśli pochodzą z nieznanego źródła;</u>
  Otwarcie takiego załącznika może doprowadzić do pobrania złośliwego oprogramowania.

- <u>nie wolno zapamiętywać w przeglądarce loginów i haseł;</u>
  Jest to szczególnie niebezpieczne, gdy z naszego urządzenia korzystają również inne osoby.

- <u>kończąc pracę z kontem internetowym zawsze należy użyć opcji: WYLOGUJ SIĘ;</u>
  Uniemożliwi to osobom trzecim np. przypadkowe uzyskanie dostępu do naszego konta.

- <u>wszystkie wyżej wymienione zasady należy stosować równolegle/łącznie!</u>
  Odstępstwo od którejkolwiek z wyżej wskazanych zasad postępowania w przypadku korzystania z bankowości elektronicznej może doprowadzić do sytuacji, w której osoby nieuprawnione uzyskają dostęp do naszego konta. Łączne i konsekwentne stosowanie się do tych zasad powoduje z kolei, iż konto internetowe jest produktem bezpiecznym.

WAŻNE DEFINICJE:

LOGIN - [inaczej: nazwa użytkownika, numer klienta], jest to indywidualny identyfikator niezbędny do uzyskania przez klienta dostępu do konta internetowego. Login otrzymujemy z banku. Login może występować jako ciąg liter, znaków lub cyfr.

HASŁO - jest to ciąg znaków [liter małych i dużych, cyfr, znaków specjalnych] niezbędny - obok loginu - do uzyskania dostępu do konta internetowego.

HASŁO PIERWSZEGO LOGOWANIA - jest to hasło, które klient otrzymuje z banku w celu pierwszego [jednokrotnego] uzyskania dostępu do konta internetowego. System informatyczny po pierwszym zalogowaniu wymaga, by klient wprowadził inne, indywidulane hasło, które następnie służy do kolejnych „wejść" do rachunku bankowego.

PRZELEW INTERNETOWY - [przelew on-line] jest to przelew wykonywany za pomocą konta internetowego.

SENIORZE NIE DAJ SIĘ OSZUKAĆ!

Osoby starsze to grupa wiekowa, która często jest wykorzystywana i okradana za pomocą różnych podstępnych metod. Jedną z najpopularniejszych i zarazem najskuteczniejszych są metody wyłudzania pieniędzy tzw. na wnuczka i na policjanta oraz różne ich odmiany.

METODA „NA WNUCZKA"

Metoda „na wnuczka" charakteryzuje się tym, że przestępca dzwoniąc do ofiary podaje się za jej krewnego [najczęściej wnuka]. Rozmowę prowadzi w taki sposób, aby przekonać seniora, że jest tą osobą, za którą się podaje. Przedmiotem rozmowy jest najczęściej jakieś nieszczęście [np. wypadek samochodowy, porwanie, choroba] lub niepowtarzalna okazja [np. zakupu samochodu, zakupu mieszkania] i jednoczesna prośba o natychmiastową pomoc finansową [np. pożyczkę]. W zależności od informacji jakie uda się uzyskać oszustowi w trakcie rozmowy senior proszony jest o przygotowanie gotówki, wykonanie przelewu lub np. proponowane jest mu wspólne wyjście do banku - przy czym po pieniądze do potencjalnej ofiary zawsze wysyłany jest jakiś znajomy fałszywego wnuczka [np. kolega, przyjaciółka]. Osoba starsza pozostając w przekonaniu, że udziela koniecznego wsparcia najbliższemu będącemu w potrzebie, zostaje oszukana i okradziona.

PAMIĘTAJ!!!

- Nigdy nie przekazuj pieniędzy nieznajomym!
- Gdy ktoś w rozmowie telefonicznej podaje się za Twojego krewnego i prosi o pieniądze - **zachowaj szczególną ostrożność!**
- Gdy ktoś w imieniu Twojego krewnego prosi o pieniądze - **odmów!**
- Każdą prośbę o wsparcie czy pożyczkę potwierdź - **zadzwoń do takiej osoby lub skontaktuj się z nią w inny sposób [np. idź do niej]**.
- Gdy masz jakieś wątpliwości i podejrzewasz, że ktoś próbuje dokonać oszustwa, **zawiadom Policję dzwoniąc pod nr 112**.