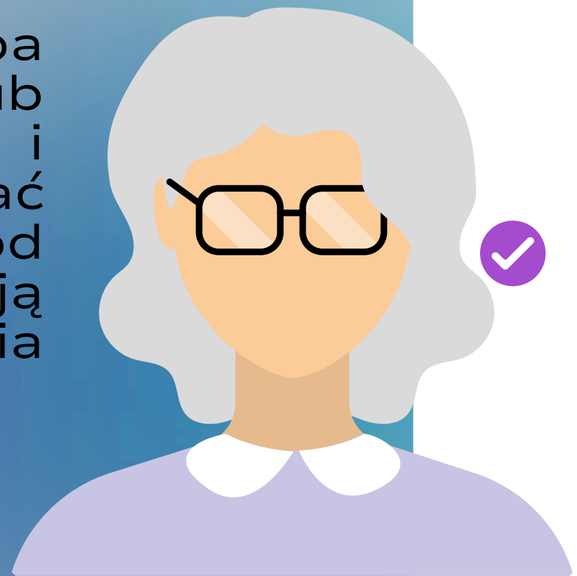
Zaborskie Towarzystwo Naukowe

Metody oszustw

W dobie powszechnego dostępu do technologii oraz rosnącej aktywności w internecie, przestępcy nieustannie rozwijają nowe sposoby na wyłudzanie pieniędzy i danych osobowych. Ofiarami oszustw mogą paść zarówno osoby starsze, jak i młodsi użytkownicy sieci, klienci banków czy użytkownicy mediów społecznościowych.

„Na wnuczka” – klasyka oszustwa

Metoda „na wnuczka” to jeden z najbardziej znanych i niestety wciąż skutecznych sposobów wyłudzania pieniędzy, głównie od osób starszych. Oszust podszywa się pod wnuka, siostrzeńca lub inną bliską osobę i dzwoni z dramatyczną historią – np. wypadkiem, nagłą chorobą czy aresztowaniem – w której potrzebna jest pilna pomoc finansowa.
Często rozmowę kontynuuje inna osoba podająca się za policjanta, lekarza lub prawnika, która potwierdza historię i wskazuje, gdzie należy przekazać pieniądze. Seniorzy, działając pod wpływem emocji, często nie weryfikują informacji i przekazują oszczędności życia nieznajomym.



Jak się bronić?

- Nigdy nie przekazuj pieniędzy osobie, której tożsamości nie jesteś w stanie potwierdzić.
- Zawsze dzwoń do członka rodziny, by upewnić się, czy rzeczywiście potrzebuje pomocy.
- Policja nigdy nie prosi o przekazanie pieniędzy „do ręki” czy pozostawienie ich w reklamówce przed domem.

„Na policjanta” lub „na CBŚ”

W tej metodzie oszust przedstawia się jako funkcjonariusz policji lub Centralnego Biura Śledczego i przekonuje ofiarę, że jej konto bankowe jest zagrożone. Następnie instruuje ją, aby przelała pieniądze „na bezpieczne konto” lub wypłaciła gotówkę i przekazała ją wskazanej osobie. Czasami oszuści namawiają do zainstalowania aplikacji zdalnego pulpitu, by „pomóc” zabezpieczyć konto, a w rzeczywistości uzyskują pełny dostęp do danych ofiary.

Jak się bronić?

Policja nigdy nie prosi o przelewy bankowe ani o wypłatę pieniędzy

Nie instaluj żadnego oprogramowania na polecenie nieznajomej osoby przez telefon

Zawsze zakończ rozmowę i samodzielnie zadzwoń na oficjalny numer policji lub swojego banku

Oszustwa internetowe

W dobie cyfryzacji jedną z najczęstszych metod oszustwa jest podszywanie się pod znane instytucje, np. banki, sklepy internetowe czy firmy kurierskie. Oszuści wysyłają e-maile lub SMS-y z linkami do fałszywych stron, które wyglądają niemal identycznie jak oryginalne. Po kliknięciu linku użytkownik zostaje poproszony o podanie loginu, hasła czy danych karty – które trafiają prosto do przestępców. Częstą formą jest również „oszustwo na paczkę” – ofiara dostaje SMS z prośbą o dopłatę kilku złotych do przesyłki, klikając w link do fałszywej bramki płatności

Jak się bronić?

01. Sprawdzaj adres nadawcy e-maila i nie klikaj w podejrzane linki.

02. Nigdy nie podawaj danych logowania ani numerów kart płatniczych poza oficjalnymi stronami.

03. Używaj dwustopniowego uwierzytelniania i aktualizuj oprogramowanie.

Oszustwa „na inwestycje” i kryptowaluty

Rosnąca popularność kryptowalut i szybkich zysków sprawiła, że oszuści chętnie wykorzystują ten temat. Oferują „niezwykle dochodowe” inwestycje, często powołując się na znanych celebrytów lub fałszywe rekomendacje. Ofiary są kuszone perspektywą szybkiego zarobku, a po wpłacie pierwszych pieniędzy otrzymują pozorowane zyski. Gdy chcą wypłacić środki – kontakt z firmą się urywa.
Czasem oszuści tworzą fikcyjne platformy inwestycyjne lub dzwonią do osób, przedstawiając się jako doradcy finansowi.

Jak się bronić?

- Nie inwestuj pieniędzy przez niezweryfikowane platformy lub telefonicznie.
- Sprawdzaj, czy firma ma licencję Komisji Nadzoru Finansowego (KNF).
- Pamiętaj, że szybki zysk to zwykle duże ryzyko – nikt nie gwarantuje pewnego zarobku.

Oszustwa w mediach społecznościowych

Jak się bronić?

- Nigdy nie podawaj kodów BLIK przez wiadomości, nawet znajomym – najpierw zadzwoń i potwierdź.
- Sprawdzaj opinie o sklepach i nie płać z góry w nieznanych miejscach.
- Włącz uwierzytelnianie dwuskładnikowe w mediach społecznościowych

Coraz więcej oszustw pojawia się także w serwisach społecznościowych – zwłaszcza na Facebooku i Instagramie. Oszuści mogą włamywać się na konta użytkowników i wysyłać do ich znajomych wiadomości z prośbą o „pożyczenie pieniędzy”, „opłacenie paczki” czy „potwierdzenie kodu BLIK”.
Wielu przestępców tworzy też fałszywe sklepy internetowe, oferujące atrakcyjne produkty w zaniżonych cenach – po wpłacie pieniędzy towar nigdy nie dociera.

Oszustwa „na pracę” i fałszywe oferty

Inna forma oszustwa to fałszywe ogłoszenia o pracę – często oferujące wysokie zarobki za prostą pracę zdalną. Po przesłaniu danych osobowych (CV, skanu dowodu) ofiara może paść ofiarą kradzieży tożsamości, a czasem proszona jest o „opłatę wstępną” za szkolenie lub narzędzia pracy.
Niektóre oszustwa wykorzystują również schemat tzw. „słupa” – ofiara zostaje nieświadomym pośrednikiem w praniu brudnych pieniędzy.

Jak się bronić?

- Nigdy nie wysyłaj skanu dowodu osobistego bez potrzeby
- Sprawdzaj firmę w KRS lub CEIDG
- Nie płać za możliwość pracy – to pracodawca powinien Ci płacić

Oszustwa przybierają coraz bardziej wyrafinowane formy, ale ich wspólnym mianownikiem jest próba wzbudzenia silnych emocji – strachu, pośpiechu, chciwości lub współczucia. Kluczem do obrony jest ostrożność, weryfikowanie informacji oraz świadomość zagrożeń.

Zasada ograniczonego zaufania powinna towarzyszyć nam w każdej sytuacji, która wymaga przekazania pieniędzy lub danych. Edukacja, czujność i szybkie reagowanie na podejrzane sytuacje to nasza najlepsza ochrona przed oszustami.

Chcesz dowiedzieć się więcej na ten temat? Odwiedź stronę darmowapomoc.com.pl lub udaj się do punktu nieodpłatnej pomocy prawnej i obywatelskiej.

Dziękujemy za uwagę

Zaborskie Towarzystwo Naukowe