

APEL POLICJI W SPRAWIE OSZUSTW

METODĄ „NA WNUCZKA”, „NA POLICJANTA”, „NA PRACOWNIKA BANKU”, itp.

Szanowni Państwo!

W trosce o bezpieczeństwo mieszkańców powiatu zamojskiego apelujemy o ostrożność i rozsądek w kontaktach z osobami obcymi, które mogą podawać się za naszych krewnych, policjantów, lub pracowników banku. W przypadku jakichkolwiek podejrzeń, że może to być próba wyłudzenia pieniędzy prosimy o natychmiastowe powiadomienie Policji dzwoniąc pod numer **112**”.

Przypominamy, że sposób działania przestępców oszukujących metodą „na wnuczka”, „na policjanta”, lub pracownika banku jest następujący:

Oszust telefonuje najczęściej na numer stacjonarny i podszywając się pod wnuczka lub innego krewnego, prosi o pilne wsparcie finansowe spowodowane nagłą sytuacją, np. wypadkiem drogowym, zatrzymaniem przez Policję lub potrzebą zapłacenia za nagłą operacji w szpitalu. Najczęściej oszust prosi o dochowanie tajemnicy. Nigdy nie odbiera pieniędzy osobiście, ale prosi o ich przekazanie swojemu znajomemu, który w rzeczywistości również jest oszustem.

Działając metodą „na policjanta” oszust informuje, że jest policjantem, funkcjonariuszem Centralnego Biura Śledczego, podaje stopień, imię, nazwisko i identyfikator służbowy, Prokuratorem, Sędziom, czy też żołnierzem. Podczas rozmowy przekonuje, że właśnie trwa akcja policyjna przeciwko oszustom i w celu ochrony naszych pieniędzy prosi o ich przekazanie na podany numer konta, wybranie z banku i pozostawienie w określonym miejscu lub przekazanie osobie, która się do nas zgłosi. Jednocześnie zapewnia, że po zakończeniu działań policyjnych niezwłocznie odda pieniądze.

Gotówka i kosztowności przekazywane są w miejscu zamieszkania oszukiwanej osoby albo na ulicy, bądź w placówkach bankowych. Zdarza się, że sprawcy przyjeżdżają po swoje ofiary taksówkami, z którymi razem jadą np. do banku w celu dokonania przelewu i pobrania gotówki.

Oszuści wykonują do swoich ofiar bardzo dużo połączeń telefonicznych, w krótkich odstępach czasu w celu wywarcia presji psychologicznej i nakłonienia do szybkiego przekazania pieniędzy. Takie częste telefony mają, także utrudnić osobie oszukiwanej nawiązanie kontaktu z członkami rodziny, rzekomo proszącymi o pomoc finansową.

Działając metodą na fałszywego pracownika banku oszuści dzwonią do ofiar ze spoofowanych numerów telefonów (wykrywanych jako prawdziwe numery telefonów banku!), przedstawiają się jako pracownicy banku i przestrzegają o nieautoryzowanej operacji na koncie, aby zapobiec rzekomemu oszustwu, konieczne jest zainstalowanie specjalnej aplikacji (AnyDesk lub TeamViewer QuickSupport). Aplikacje te dają przestępcom nieograniczony dostęp do telefonu i komputera, dzięki czemu mogą przechwycać wiadomości autoryzacyjne nasz bank i wykraść oszczędności znajdujące się na koncie lub zaciągnąć kredyt.

Pamiętajmy!!! Funkcjonariusze Policji nigdy nie proszą o przekazanie pieniędzy lub przelanie ich na jakiekolwiek konto!!!

Apelujemy również, by nigdy nie przekazywać żadnych pieniędzy osobom, których nie znamy zanim nie sprawdzimy i nie potwierdzimy, że nasi znajomi czy krewni ich faktycznie potrzebują!!

W przypadku jakichkolwiek podejrzeń, że może to być próba wyłudzenia pieniędzy prosimy o natychmiastowe powiadomienie Policji dzwoniąc pod numer **112**.

Nie dajmy przestępcom szansy! Nie pozwólmy, aby zabrali oszczędności naszego życia! Na Państwa sygnały policjanci czekają całą dobę.

Apelujemy również do osób młodych – informujcie waszych rodziców i dziadków o tym, że są osoby, które mogą chcieć wykorzystać ich ufność i życzliwość. Powiedzcie im jak zachować się w sytuacji, kiedy ktoś zadzwoni do nich z prośbą o pożyczenie dużej ilości pieniędzy. Zwróćcie uwagę na zagrożenie osobom starszym, o których wiemy, że mieszkają samotnie.

Ponadto uczulmy naszych najbliższych, że inni oszuści dokonują kradzieży bezpośrednio z naszym domów. Złodzieje pod pozorem wykonania w domu czy mieszkaniu różnych usług lub czynności, wykorzystują nieuwagę ofiary i dokonują kradzieży wartościowych przedmiotów. Często łupem padają również karty kredytowe czy dowody osobiste ofiar, które mogą posłużyć do wyłudzenia np. kredytu. Pomysłowość oszustów jest nieograniczona. Podają się oni za członków rodziny, za pracowników administracji, gazowni, elektrowni, inkasentów, kurierów czy hydraulików.

Pamiętajmy:

- Nie wpuszczajmy do mieszkania nieznajomych osób - nie każdy jest tym, za kogo się podaje.
- Oszuści wykorzystują dobre serce, ufność i gościnność swoich ofiar.
- Miła powierzchowność sprawcy pomaga zdobyć zaufanie ofiary.
- Nie wierzymy w „życiowe okazje” oferowane przez nieznajomych (np. „super, zdrową i relaksującą” pościel czy też „niezniszczalny” komplet garnków).
- Upewniamy się, kogo wpuszczamy do domu. Zanim to uczynimy, żądamy okazania legitymacji lub identyfikatora. Zadzwonimy do instytucji, na które nieznajomi się powołują.

Gdy podejrzewamy, że mamy do czynienia z oszustem, nie wahajmy się zadzwonić na Policję pod numer 112.

Nie bądźmy łatwowierni, nie dajmy się oszukać!

Pamiętaj każda z tych osób może okazać się niebezpiecznym przestępcą.

Badź ostrożny, pamiętaj:

- jeżeli rozmówca proponuje Ci, że możesz potwierdzić autentyczność dzwoniącego policjanta pod numerem 112 - zanim zadzwonisz pod ten telefon, sprawdź czy rozłączyłeś poprzednią rozmowę,
- Policja nigdy nie prosi o przekazanie pieniędzy,
- nie działaj pochopnie pod presją czasu,
- po rozmowie zadzwoń do kogoś bliskiego na znany Ci numer telefonu, by opowiedzieć o zdarzeniu – nie może być ono tajemnicą,
- jeśli nie możesz skontaktować się z najbliższymi, niezwłocznie powiadom Policję o takim zdarzeniu, dzwoniąc pod numer 112.

NIE POZWÓL SIĘ OSZUKAĆ PODCZAS TRANSAKCJI INTERNETOWYCH

JAK DZIAŁAJĄ OSZUŚCI?

- Wystawiasz coś do sprzedaży. Znajduje się kupiec. Odzywa się najczęściej za pośrednictwem aplikacji WhatsApp. Twierdzi, że kupił przedmiot i za niego zapłacił, a pieniądze możesz odebrać po wejściu w link.
- Teraz oszust wysłał Ci linka. Klikasz i trafiasz na stronę ładną podobną do strony np. OLX, Vinted. Na stronie jest formularz z prośbą o podanie danych Twojej karty i stan Twojego konta. Wypełniasz formularz.
- Przychodzi do Ciebie SMS z banku, z kodem do autoryzacji. Ty nie czytasz go uważnie i wpisujesz kod do formularza. W SMS-ie jest jasno napisane, że autoryzujesz dodanie Twojej karty do Google Pay lub Apple Pay. Oszust Cię okrada. Płaci Twoją kartą za pomocą aplikacji płatniczej lub wypłaca nią gotówkę w bankomacie.
- Koniec. Twoje konto jest PUSTE.

JAK UNIKNĄĆ OSZUSTWA?

- **Nie klikaj w linki przesyłane mailem lub SMS-em, nie ujawniaj danych swojej karty płatniczej.**
- Czytaj SMS-y od Banków. **Zwróć uwagę na to, co autoryzujesz.**
- Poznaj zasady bezpieczeństwa swojego banku i stosuj się do nich gdy korzystasz z portali aukcyjnych.
- Miej ograniczone zaufanie do potencjalnych kontrahentów.
- Rozliczaj się bezpośrednio przez dany portal. **Unikaj bezpośrednich transakcji.** Uważaj na próby nawiązania kontaktu poza portalem, np. przez WhatsApp czy Messenger. Zobacz instrukcje płatności z OLX.
- Oszuści mogą podrobić stronę portalu aukcyjnego – np. Allegro lub Vinted – tak samo jak i każdą inną stronę. Dlatego **zwracaj uwagę na adres widoczny w przeglądarce.** Zobacz poradnik OLX
- Zwróć uwagę na **poprawność językową strony**, na której przekazujesz dane karty. Fałszywe strony często zawierają błędy, są napisane niegramatycznie.

„Pamiętaj, że portale nie generuje żadnych linków do opłacenia zakupu, czy do podania danych do otrzymania płatności za oferowany przez Ciebie przedmiot.

Apelujemy o zachowanie szczególnej ostrożności. Nie korzystajcie nigdy z linków, które przychodzą w wiadomościach. Najbezpieczniej jest wpisać samodzielnie adres internetowy strony danego serwisu ogłoszeniowego lub banku. Sprawdzajmy zawsze, czy witryna jest bezpieczna. Jeśli korzystamy z kodów autoryzacyjnych przesłanych SMS-em przez bank lub inne instytucje sprawdzajmy zawsze, czy zawiera polskie znaki.

Pamiętaj! Weryfikuj kto i co do Ciebie pisze. Nie wpisuj nigdzie numeru swojej karty. Nie klikaj w nieznajome linki do stron.