

## Uważaj na oszustów, którzy mogą do Ciebie zadzwonić i podawać się za pracownika Twojego banku lub znanej Ci firmy



**Uważaj na oszukańcze telefony lub maile. Nie daj się nabrać, zwróć uwagę kto naprawdę do Ciebie dzwoni. Tylko oszuści pytają o login czy hasło, proszą o zainstalowanie aplikacji lub o pełny numer karty, datę jej ważności czy o kod CVV2/CVC2. Trzeba uważać na popularny ostatnio sposób działania przestępców, którzy podszywają się pod znane instytucje finansowe.**

Mnożą się sposoby wyłudzenia i nieuprawnionego wykorzystania skradzionych danych. Metod, jakimi posługują się złodzieje danych jest bardzo wiele. Do jednych z bardziej niebezpiecznych sposobów oszustów należą chwytły socjotechniczne. To, co je łączy, to element zaskoczenia oraz bazowanie na ludzkiej naiwności lub nieuwadze.

**W ostatnim czasie eksperci BIK zaobserwowali zwiększoną aktywność telefoniczną oszustów podszywających się pod rozmaite instytucje zaufania publicznego w celu zebrania danych personalnych.** Pojawiły się przypadki podawania się za pracowników BIK i nakłaniania rozmówców do ujawnienia danych osobowych pod pretekstem zweryfikowania informacji o rzekomo niedokończonym wniosku kredytowym lub próbie wyłudzenia kredytu. Na szczęście klienci bankowości są coraz bardziej świadomi i nie ulegają oszustom.

### **Nie daj się zaskoczyć, weryfikuj**

Dane osobowe i kontaktowe w rękach złodziei oznaczają dla nas wysokie ryzyko utraty pieniędzy. A dla złodziei szansę na zarobek. Dlatego oszuści stosują wyszukane metody socjotechniczne. Obecnie plagą stały się tzw. spoofing – metoda telefoniczna lub mailowa, polegająca na podszywaniu się pod prawdziwe organizacje (w tym banki czy BIK) oraz phishing. Złodzieje wykorzystują narzędzia umożliwiające wykonanie połączenia telefonicznego z wyświetleniem prawdziwego numeru wiarygodniejszej instytucji, np. znanego dostawcy usług lub banku.

Przestępca nawiązuje bliski i przekonujący kontakt z ofiarą, namawiając do podania danych, np. do wykonania przelewu lub dokonania transakcji kartowej. Wszystkie szczegóły są zmyślone: przestępcy podają fikcyjne uzasadnienie, fikcyjne kwoty zobowiązań, nieistniejące dane odbiorcy.

Rozmowy mogą trwać długo, przestępcy przełączają rozmowę do innych „konsultantów”, żeby stworzyć pozory prawdziwego kontaktu np. z bankiem. Rozmówca jest zmanipulowany,

zaczyna wierzyć, że jego pieniądze są w niebezpieczeństwie. Często zdarza się, że jest nakłaniany do zainstalowania na swoim komputerze lub smartfonie aplikacji, która zwiększy bezpieczeństwo pieniędzy. W rzeczywistości ten program czy aplikacja umożliwi oszustom przejęcie kontroli nad telefonem lub komputerem ofiary.

*- Zwracam uwagę na konieczność zachowania szczególnej ostrożności przez nas wszystkich. BIK nigdy nie wymaga podania wrażliwych informacji przez telefon. Wszelkie tego typu sytuacje należy zgłaszać do [Centrum Obsługi Klientów BIK](#). Nowoczesna bankowość i coraz częstsze przenoszenie operacji związanych z wykorzystaniem naszych danych do internetu wymagają od nas czujności i świadomego korzystania z nowych możliwości. Praktycznie wszystkie zidentyfikowane przypadki ingerencji oszustów wynikają z niefrasobliwości i łatwowierności klientów. Jeżeli kogoś zaskakuje telefon z firmy, której nie zna, natychmiast powinien przerwać rozmowę i skontaktować się z biurem obsługi danej firmy na podstawie informacji z oficjalnej strony. Nie wdawajmy się w dyskusję z nieznanymi – mówi Andrzej Karpiński, Szef Bezpieczeństwa Biura Informacji Kredytowej.*

### **Ważne rady, jak nie dać się oszukać**

Charakter wszystkich działań złodziei danych jest ten sam - mają one na celu uzyskanie korzyści finansowych.

- Pielęgnuj dobre nawyki bezpieczeństwa danych - zwracaj uwagę, gdzie i komu je udostępniasz, rozważnie dokonuj transakcji płatniczych w sieci, dokładnie sprawdzaj adresy portali internetowych;
- Nie oddzwaniaj na nieznaną numer ani nie odpisuj anonimowym nadawcom. Jeśli masz wątpliwości co do wiarygodności osoby, która dzwoni – natychmiast rozłącz się, a następnie zadzwoń na oficjalną infolinię firmy, aby potwierdzić czy faktycznie jej pracownik kontaktował się z Tobą;
- Pamiętaj, pracownik BIK, Związku Banków Polskich, Twojego banku NIGDY nie pyta się o login i hasło do logowania na Twoje konto w banku, nie prosi o pełny numer Twojej karty, jej daty ważności oraz kod CVV2/CVC2, ani nie namawia do zainstalowania aplikacji na Twoim komputerze lub smartfonie;
- Nie potwierdzaj operacji, których sam nie zlecasz albo których do końca nie rozumiesz;
- Nie daj się zwieść atrakcyjnym ofertom inwestycyjnym pod pozorem szybkiego zarobku (Komenda Główna Policji i FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP stale ostrzegają przed próbami oszustw przy inwestowaniu w kryptowaluty oraz na rynku Forex);
- Nigdy nie wiadomo, kiedy i skąd nasze dane zostaną skradzione, dlatego [miej włączone Alerty BIK – ostrzeżenia sms](#), które otrzymasz, gdy ktoś na Twoje dane zaciąga kredyt, pożyczkę, umowę z operatorem telekomunikacyjnym, dokonuje zakupów na raty.

Działaj ostrożnie i rozsądnie - Twoje zachowanie ma wpływ na bezpieczeństwo Twoich pieniędzy.

*Biuro Informacji Kredytowej jest partnerem programu edukacyjnego Nowoczesne Zarządzanie Biznesem, w module „Zarządzanie ryzykiem finansowym w biznesie i życiu osobistym”.*

Więcej: [www.nzb.pl](http://www.nzb.pl) oraz [www.facebook.com/NowoczesneZarzadzanieBiznesem](https://www.facebook.com/NowoczesneZarzadzanieBiznesem)