Utrudniaj robotę przestępcom

Nawet doświadczeni specjaliści do spraw bezpieczeństwa padają ofiarami ataków cyberprzestępców. Dlatego można przyjąć, że **Ty też kiedyś możesz dać się podejść**. Zabezpiecz się wcześniej przed skutkami takiego ataku.

1. W każdym z serwisów internetowych **włącz dwuskładnikowe uwierzytelnienie w oparciu o aplikację lub kod wysyłany SMS-em na Twój numer telefonu**. Jeśli posiadasz sprzętowy klucz U2F lub Twoje urządzenia wspiera mechanizm tzw. passkeys, w pierwszej kolejności skorzystaj z tych rozwiązań, bo to jedyne metody, których nie da się obejść.

2. **Ustaw limity na przelewy i operacje dokonywane kartą w Twoim banku.** Jeśli stracisz kontrolę nad swoim rachunkiem, przestępcom będzie trudniej okraść Cię z kwot większych niż ustawiony limit.

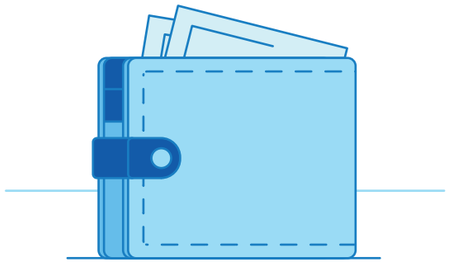
3. **Włącz profilowanie biometryczne**, jeśli Twój bank oferuje takie zabezpieczenie. Dzięki niemu systemy bankowe mają większe szanse rozpoznać, że to nie Ty zlecasz operacje na swoim rachunku, i zablokują transakcję.

4. **Korzystaj z managerów haseł**, czyli aplikacji, które „pilnują", by hasła do poszczególnych kont się różniły. Dzięki temu, po wycieku danych z jednego z serwisów, z których korzystasz, cyberprzestępcy nie włamią się na Twoje pozostałe konta.

5. **Zainstaluj oprogramowanie antywirusowe.** Nie da Ci ono 100-procentowej ochrony przed wirusami, ale całkiem dobrze poradzi sobie ze znanymi zagrożeniami.

6. **Pobieraj tylko legalne oprogramowanie, wyłącznie ze strony producenta.** Wiele z tzw. pirackich wersji popularnych narzędzi jest zainfekowanych wirusami.

Pamiętaj, że oszuści chcą wyłudzić od Ciebie pieniądze lub Twoje dane. Dlatego zawsze zachowuj czujność, korzystając z internetu.



Notatki

A kto tu się **podszywa**?

KAMPANIA PREWENCYJNA

POLICJA 112

PZU

Z myślą o bezpieczeństwie

801 102 102 pzu.pl
Opłata zgodna z taryfą operatora

PZU

Cyberprzestępcy coraz częściej atakują Polaków. Najczęściej podszywają się pod znane Ci instytucje, takie jak banki, policja czy firmy kurierskie. Celem takich ataków jest wyłudzenie od Ciebie informacji, które umożliwią oszustom **kradzież Twoich pieniędzy lub danych**. Na szczęście, znajomość sposobów działania oszustów pomoże Ci obronić się przed nimi.

Od czego może się rozpocząć atak?

Oszuści mogą próbować kontaktować się z Tobą:

- **wysyłając wiadomość e-mail**, której rzekomym nadawcą jest np. firma kurierska,
- **wysyłając wiadomość SMS**, której rzekomym nadawcą jest np. Twój bank,
- **wysyłając wiadomość na czacie** w serwisie internetowym, grze albo aplikacji (np. randkowej),
- **umieszczając reklamę** np. na portalu społecznościowym, która przypomina znaną reklamę lub wykorzystuje np. wizerunek popularnego polityka, muzyka, sportowca lub dziennikarza,
- **dzwoniąc do Ciebie** z dokładnie takiego numeru, z którego korzystają znane Ci firmy i instytucje.

Opisane ataki mogą być bardzo wiarygodne, bo:

- cyberprzestępcy znają Twoje imię, bank, z którego korzystasz, a nawet pełen numer Twojej karty płatniczej. Te informacje odczytują z historycznych baz danych, które wyciekły po cyberatakach np. na sklepy internetowe, z których kiedyś korzystałeś,
- dzięki technicznym niedoskonałościom sieci teleinformatycznych cyberoszuści mogą się podszyć pod konkretną markę lub firmę: są w stanie wysłać SMS-a, używając takiej samej nazwy, co znana Ci firma, kiedy komunikuje się z Tobą SMS-owo. Fałszywy SMS pojawi się wtedy tuż pod wcześniejszymi, prawdziwymi wiadomościami od tej firmy, co bardzo podnosi wiarygodność ataku,
- oszuści mogą zadzwonić do Ciebie z dokładnie tego samego numeru co firmy lub instytucje, z których usług korzystasz.

Większość fałszywych wiadomości zawiera albo **linki prowadzące do strony wyłudzającej dane, albo załącznik, albo link do pliku**, którego uruchomienie zainfekuje Twoje urządzenie. Cyberprzestępcy pod różnymi pretekstami będą **Cię nakłaniać do kliknięcia w link albo załącznik**. Mogą np. **grozić**, że jeśli tego nie zrobisz, Twoje **konto zostanie zablokowane albo przesyłka nie zostanie dostarczona**. Usiłują Cię przestraszyć lub zmanipulować, aby wymusić Twoją szybką reakcję. Niedawne kampanie cyberprzestępców zachęcały do kliknięcia w link, aby odebrać zwrot podatku. Oszuści są bardzo pomysłowi i często nawiązują do bieżących wydarzeń.

Jak sobie radzić z cyberatakami?

Pamiętaj, że **nadawca e-maila, SMS-a lub rozmówca na czacie to niekoniecznie instytucja lub osoba, o której myślisz**. Przestępcy potrafią się podszywać, wykorzystując znane Ci adresy e-mail, nadawców SMS i numery telefonów. Dlatego poniżej przedstawiamy kilka podstawowych zasad bezpieczeństwa.

- **Jeśli dzwoni do Ciebie ktoś z banku, rozłącz się i sam zadzwoń na numer infolinii Twojego banku.** Zapytaj, czy faktycznie pracownik banku chciał się z Tobą skontaktować. Jeśli tak, konsultant infolinii przekaże Ci szczegóły sprawy. Pamiętaj, że pracownicy banku nigdy nie proszą rozmówców, by podali kody autoryzacyjne, hasła, numery kart płatniczych albo wysokość salda ani wykonali jakąkolwiek operację finansową.
- **Nie reaguj na wiadomości e-mail lub SMS od banku**, które proszą o kliknięcie w link. Banki w oficjalnej komunikacji nigdy o to nie proszą.
- **Nie reaguj na wiadomości dotyczące zatrzymania przesyłki ze względu na błędny adres czy prośby o dodatkową opłatę związaną z przesyłką, na którą czekasz. Jeśli otrzymasz taką wiadomość**, po prostu zadzwoń na infolinię firmy kurierskiej i wyjaśnij sprawę telefonicznie.

ZŁOTA ZASADA
mówi, że w razie jakichkolwiek podejrzeń co do prawdziwości wiadomości, najlepiej jest po prostu **zadzwonić do nadawcy**. Jeśli to bliska osoba, to pewnie znasz jej numer. A jeśli nadawcą jest firma lub instytucja, wyszukaj jej numer telefonu w internecie i zadzwoń z pytaniem, czy jej pracownik wysłał do Ciebie wiadomość.

- Staraj się, nigdy nie klikać w linki przesyłane Ci w wiadomościach od różnych firm lub instytucji. Zawsze, gdy masz zamiar kliknąć w taki link, upewnij się, że adres faktycznie jest powiązany z nadawcą wiadomości. **Szczególną uwagę zwróć na sprytne literówki w domenach. PoziomkaBank.pl i PoziornkaBank.pl to nie jest ta sama domena.**
- Dokładnie przyjrzyj się adresowi e-mail nadawcy. Czy wiadomość na pewno pochodzi z domeny powiązanej ze znaną Ci firmą lub instytucją?

Błędy językowe

Chociaż znaczna część komunikacji ze strony atakujących zawiera błędy stylistyczne lub literówki, niektórzy oszuści posługują się **idealną polszczyzną**. Zwracaj uwagę na błędy w treściach wiadomości, ale pamiętaj, że **jeśli ich nie ma, to nie przesądza o jej prawdziwości**.