wellcome
home

# JAK NIE DAĆ SIĘ OSZUKAĆ?

PRZEWODNIK PO INTERNECIE (I NIE TYLKO)

**Każdy z nas może paść ofiarą oszustwa i wyłudzenia.**
**Tak, Ty też (niestety)!**

Nieważne, czy korzystasz ze smartfona, komputera, setek aplikacji i codziennie logujesz się do banku, korzystasz ze starego telefonu i odbierasz jedynie telefony i SMSy, czy tylko otworzysz drzwi nieznajomemu.
Sposoby złodziei i hakerów są coraz bardziej wyszukane. Potrafią zadzwonić do nas z numeru banku, wysłać SMS jako kurier lub podszyć się pod pracownika urzędu.

Zobacz, w jakich sytuacjach najczęściej grozi Ci niebezpieczeństwo, jakie metody stosują oszuści i jak nie dać się nabrać.

## W świecie wirtualnym

Internet (i nieostrożne z niego korzystanie) to oczywiście najbardziej prawdopodobna sytuacja, że ktoś Cię oszuka. Możliwości jest nieskończenie wiele. W momencie, gdy Ty czytasz ten przewodnik, ktoś prawdopodobnie pada ofiarą zupełnie nowego ataku. Wszystkiego nie przewidzimy, ale możemy obudzić Twoją czujność na poniższe sytuacje.

### 1. E-MAIL OD ZNAJOMEGO

Niebezpieczne maile wcale nie muszą przychodzić z nieznanych nam adresów i mieć podejrzanie nazwanych linków. Zdarza się, że cyberprzestępca podszywa się pod znaną nam osobę, a jego adres jest łudząco podobny do tego, który znamy.

#### Jaki jest scenariusz?

Dostajesz wiadomość z teoretycznie sprawdzonego źródła: firmy, banku, operatora. Jesteś proszony o pobranie załącznika (instalujesz w komputerze wirusa) lub o zrobienie przelewu (który oczywiście nie trafia do nadawcy).
Inny popularny scenariusz: dostajesz e-mail od samego siebie, ze swojego adresu mailowego. „Haker” straszy, że obserwuje, co robisz w sieci, grozi upublicznieniem nagrań video, żąda przelewu na swoje konto, najczęściej w kryptowalucie.

#### Co robić?

- nie daj się nabrać i nie płać. Podszywanie się pod Twojego maila jest popularne i nie oznacza, że ktoś ma dostęp do Twoich materiałów. Płacenie pokazuje, że takie wyłudzenia są skuteczne;
- nie pobieraj nieznanych załączników, nie klikaj w podejrzane linki. Przelew weryfikuj osobiście na dwóch ekranach (zawsze przychodzi np. też SMS z potwierdzeniem numeru konta i kwoty);

- korzystaj z opcji przelewów zdefiniowanych. Podmioty, z którymi regularnie się rozliczasz, stosują najczęściej MPT (masowe przetwarzanie transakcji), dzięki któremu masz nadany swój indywidualny i niezmienny numer konta;
- jeśli numer konta nagle się zmienił, napisz lub zadzwoń do firmy. Być może pomożesz wykryć kampanię mającą na celu okradanie ludzi;
- nie przepisuj numeru konta z faktury, a użyj właśnie opcji przelewu zdefiniowanego;
- weryfikuj zgodność numeru konta w SMSie weryfikacyjnym z tym podanym na fakturze;
- korzystaj z programów pocztowych, które mają wbudowane mechanizmy ograniczające ryzyko ataku. Popularnymi serwisami, który aktywnie przeciwdziałają spamowi i rozsyłaniu wirusów są np. Gmail i outlook.com.

## 2. NIEBEZPIECZNA STRONA WWW, CZYLI JAKA?

Czy wchodząc na stronę internetową zwracasz uwagę na to, jaki link Ci się wyświetla? To szczególnie istotne w przypadku dostępu do banku, gdzie wymagane jest zalogowanie, podanie wrażliwych danych, wykonywanie transakcji finansowych. A oszuści potrafią podszyć się pod autentyczną stronę i uśpić naszą czujność.

### Jaki jest scenariusz?

Dostajesz maila lub wiadomość z linkiem do banku, w który klikasz. Wygląd strony nie budzi podejrzeń, adres też wydaje się znajomy, ale… no właśnie. Hakerzy mogą Cię zmylić, podstawiając w miejsce litery inną, np. z obcym znakiem specjalnym (amażon.com zamiast amazon.com) albo zarejestrować domenę z celową literówką.

### Co robić?

- korzystaj z zakładki „Ulubione strony”;
- logując się do banku, adres najlepiej wpisuj ręcznie. Uważaj, aby nie zrobić literówki. Przeglądarka sama zasugeruje stronę, na którą wchodziłeś już wcześniej;
- nigdy nie loguj się do banku, klikając w wątpliwego pochodzenia link.
- dla bardziej wnikliwych: klikając w kłódeczkę przed linkiem możesz sprawdzić, dla kogo został wystawiony certyfikat. Nazwa powinna zgadzać się z nazwą banku.

## 3. O! FAJNA APKA!

Ilość aplikacji, jakie mamy do dyspozycji na naszych smartfonach, potrafi zawrócić w głowie. Problematyczne są szczególnie nowe aplikacje, mogące posiadać szkodliwe oprogramowanie albo uzyskujące uprawnienia dostępu do Twoich danych.

### Gdzie tkwi niebezpieczeństwo?

W niezweryfikowanych aplikacjach, w grach masowo ściąganych na telefon przez nasze dziecko, w aplikacjach, gdzie podajemy nasze dane. Najbardziej narażone na niebezpieczeństwo są starsze telefony, w których system operacyjny nie jest aktualizowany regularnie.

### Co robić?

- na telefonie, z którego masz dostęp do bankowości, nie instaluj nieznanych aplikacji;
- dziecku, które masowo ściąga gierki, daj drugi telefon, bez dostępu do wrażliwych danych;
- zastanów się dwa razy, zanim ściągniesz nieznaną aplikację;

- aktualizuj swój system i aplikacje regularnie. To naprawdę ważne!

## 4. JUŻ ROBIĘ PRZELEW

Czy wiesz, że zawirusowany komputer potrafi „podmienić" numer konta i podstawić na stronie przelewu inny, błędny? A najgorsze jest to, że wirus wciąż wyświetla nam ten poprawny, abyśmy nie mogli wyłapać błędu.

### Jaki jest scenariusz?

Numer konta, na jaki musisz wykonać przelew, przychodzi mailem, jest podany na stronie, ktoś podsyła Ci go na chacie. Kopiujesz go i wklejasz w odpowiednią rubrykę na stronie banku. Autoryzujesz przelew SMS-em i odhaczasz zadanie. Tymczasem odbiorca raczej nie doczeka się swoich pieniędzy, bo wyszły one na zupełnie inne konto…

### Co robić?

- po pierwsze: wiedza! Każdy numer konta w UE składa się z 26 cyfr. 2 pierwsze to suma kontrolna, 8 kolejnych to bank, 16 kolejnych to numer konta. Jeśli nie zgadzają się 2 pierwsze, już powinna zapalić Ci się lampka kontrolna!
- akceptując przelew w aplikacji czy poprzez SMS, zweryfikuj dwie pierwsze i 6 ostatnich cyfr numeru. Tylko w tym momencie może być możliwe wyłapanie różnicy. Ostatnio banki automatycznie usuwają te cyfry i wymagają, by wpisać je ręcznie. To rozwiązanie dobre, ale nie idealne. Jeśli nie masz przelewów zdefiniowanych, lepszym pomysłem będzie przepisanie numeru konta ręcznie.

## 5. MODNE KRYPTOWALUTY

Inwestowanie w kryptowanuty stało się w ostatnim czasie bardzo popularne. Coraz częściej zdarza się, że ktoś odbiera telefon z propozycją inwestycji i zostaje skuszony łatwym i szybkim zarobkiem

### Jaki jest scenariusz?

Dzwoni do Ciebie „specjalista", oferuje duże pieniądze. Zaczynasz wierzyć, że naprawdę możesz zarobić. Oszust prosi Cię o zainstalowanie oprogramowania, które da mu zdalny dostęp, dzięki któremu będzie mógł robić to za Ciebie. Oczywiście tym sposobem dajesz mu zdalny dostęp do informacji na Twoim komputerze.

### Co robić?

- po pierwsze - nie wierz w magiczne sposoby zarobienia czegokolwiek;
- nigdy nie instaluj nieznanych programów na swoim komputerze. Jeśli ktoś prosi Cię o zainstalowanie AnyDesk, TeamViewer czy jakiegokolwiek innego programu, to brzmi już jak próba wyłudzenia.

## 6. ADMIN ADMIN, CZYLI ZMIEŃ WRESZCIE TO HASŁO

Kiedy ostatni raz zmieniałeś hasło do swojego banku? Gdzie zapisujesz dostępy do stron? Jak tworzysz nowe hasło i do ilu stron logujesz się tym samym systemem?

### W czym tkwi zagrożenie?

Czasami zdarza się, że z dużej bazy wyciekają dane klientów, w tym Twoje. Jeśli używasz wszędzie takiego samego hasła, zostawiasz oszustom otwartą furtkę. Z kolei używanie zbyt łatwych haseł naraża się Cię kradzież danych. Nawet te pozornie niewinne - jak konto na Facebooku - jest cennym łupem dla oszustów.

### Co robić?

- nie stosuj jednego hasła do wszystkich stron logowania;
- twórz hasła pozornie niekojarzące się z Tobą, np. ciągi łatwych do zapamiętania słów typu: Lawka1Krzeslo.Parasol;
- hasła przetrzymuj w chronionym menedżerze haseł (polecamy BitWarden), nigdy w otwartej notatce (czy tym bardziej na kartce!);
- jeśli nie korzystasz z managera haseł, to przynajmniej hasło do banku miej unikatowe (czyli takie, z którego nie korzystasz w innych serwisach);
- korzystaj z podwójnego uwierzytelniania jeżeli tylko masz taką możliwość (logowanie dodatkowo potwierdzane tokenem: SMSem lub kodem z aplikacji). Polecamy aplikacje 2FAS.

## W świecie rzeczywistym

Nie masz smartfona, nie korzystasz z maila, a rachunki płacisz na poczcie? To wcale nie znaczy, że jesteś bezpieczny. Oszuści nie mają litości, a ich pomysły granic. Miej świadomość niebezpieczeństwa nawet wtedy, gdy wylogowałeś się ze wszystkich aplikacji albo po prostu idziesz w miasto.

### 7. CO TO ZA NUMER?

Każdemu z nas zdarzyło się już chyba, że dziwił do niego nie tylko nieznany, ale też dziwnie wyglądający numer. Ostatnio sytuacje takie są rzadziej spotykane, a oszuści przerzucili się na bardziej wyrafinowane metody, ale warto przypomnieć popularny kiedyś (i wciąż możliwy) scenariusz.

### Jak to wygląda?

Dzwoni nieznany telefon, o egzotycznym numerze kierunkowym. Oddzwaniając, zostają nam naliczone koszty za połączenie, które mogą być niebotycznie wysokie.

### Co zrobić?

- NIC. Nie odbieraj, absolutnie nie oddzwaniaj;
- zwracaj uwagę na numery kierunkowe: plusy i zera na początku numeru. O ile polski numer telefonu łatwo rozpoznać (kierunkowy +48 raczej nigdy nie zostanie wyświetlony), o tyle na te wskazujące na zagraniczne pochodzenie lepiej w ogóle nie reagować. W efekcie przestępcy zarabiają na połączeniach przychodzących, gdyż numer, który wygląda znajomo jest tak naprawdę płatną infolinią zagraniczną.

wellcome
home

## 8. DZWONIĄ Z MOJEGO BANKU…

Tego rodzaju telefony są ostatnio coraz częstsze, znacznie bardziej wyrafinowane i trudniejsze do wyłapania.
Czy wiesz, że każdy może zadzwonić do Ciebie z dowolnego numeru telefonu? W konsekwencji oszust może zadzwonić z prawdziwego numeru Twojego banku. Mało tego, na telefonie wyświetli się nawet nazwa tego banku. Potem jest już tylko gorzej…

### Jaki jest scenariusz?

Osoba w telefonie przedstawia się jako pracownik twojego banku. Weryfikuje, czy robiłeś właśnie przelew na kwotę X. Po zaprzeczeniu (oczywiście, że nie robiłeś, masz się przecież zmartwić) ostrzega Cię o próbie włamania na konto i prosi o zainstalowanie programu na komputer czy telefon, który ma zatrzymać nielegalną transakcję. Pobierając wskazany program nie zabezpieczasz się, tylko dajesz oszustowi zdalny dostęp do swojego sprzętu i wszystkich informacji.

### Co robić?

- nigdy nie instaluj żadnego programu na prośbę nieznajomej osoby, nawet gdy dzwoni z banku. Nie masz takiego obowiązku;
- poproś o tożsamość pracownika, który do Ciebie dzwoni. Rozłącz się i sam zadzwoń do banku. Numer uprzednio sprawdź na jego stronie internetowej. Połączenie z bankiem na pewno zajmie trochę czasu, ale oszczędzi Ci nieprzyjemnej sytuacji; Zapytaj, czy taka i taka osoba mogła dzwonić z tego telefonu. Jeżeli nie, to pomogą Ci wyprowadzić złodzieja w pole;
- pamiętaj, że czasem nawet pracownicy banku mogą nie mieć świadomości zagrożenia, a Twoje zachowanie i przezorność mogą się spotkać z ich brakiem zrozumienia. To nic, bądź uparty i dbaj o swoje bezpieczeństwo.

## 9. …ALBO Z URZĘDU (WYKORZYSTANIE SYTUACJI W CZASIE RZECZYWISTYM)

Wiesz już, że oszust może zadzwonić do Ciebie z dowolnego telefonu, podając się nie tylko za pracownika banku, ale też urzędnika, policjanta, pracownika służb publicznych. Wykorzystanie sytuacji w czasie rzeczywistym usypia czujność i jest świetnym polem do popisu dla wszelkiej maści oszustów.

### Możliwy scenariusz nr 1

Dzwoni ktoś pod pretekstem przeprowadzenia Spisu Powszechnego. Sytuacja pozornie jest naturalna - rząd informował o tym, że rachmistrzowie będą się z nami kontaktować telefonicznie. Oszust pyta nas najpierw o podstawowe dane, później o te coraz bardziej szczegółowe.

### Możliwy scenariusz nr 2

Dzwoni pracownik urzędu pod pretekstem wykonania ankiety. Wypytuje o newralgiczne dane, które podane obcej osobie mogą być dla Ciebie katastrofalne w skutkach.

### Co robić?

- rozłącz się i samodzielnie oddzwoń do urzędu. Miej świadomość, że urzędnik może nie rozumieć Twojego zachowania;

- zwiększ czujność, gdy ktoś zapyta Cię o dane takie jak: numer PESEL*, nazwisko panieńskie matki, numer karty kredytowej, informacje o produktach bankowych, kredycie. Absolutnie nie udzielaj takich informacji.

*Warto mieć na uwadze, że jeśli jesteś udziałowcem spółki, Twój numer PESEL jest publicznie dostępny. Niewiele możesz w tej sytuacji zrobić, ale na pewno nieco pomoże ostatni punkt tej listy.

## 10. TO TYLKO SMS

Czy na pewno? Tak samo jak połączenie telefoniczne, SMS też może przyjść do nas z dowolnego numeru. Podejrzane są wszelkiego rodzaju wiadomości z linkiem, w którym mamy kliknąć, albo SMSy typu łańcuszki straszące śmiercią czy inną klątwą

### Możliwe scenariusze:

- SMS z firmy przewozowej, niedopłata do przesyłki i prośba o przelew niewielkiej kwoty;
- SMS od Twojego operatora, przepraszający za awarię i oferujący bonus pieniężny za niedogodności;
- SMS z platformy aukcyjnej z linkiem do płatności i prośba o podanie numeru karty (zamiast dostać pieniądze, tracimy je).

### Co robić?

- absolutnie nie reaguj na żadne SMSy. Odpisanie spowoduje dodanie Cię do bazy i dalsze nękanie wiadomościami, a sam SMS może Cię słono kosztować. Szczególnie podejrzane są krótkie numery zaczynające się od 7-ki;
- zwróć uwagę na podejrzane linki, szczególnie takie z końcówką typu: hxxp://jakislink.com/sdSFAD8.

## 11. METODA NA WNUCZKA (TAK, TO NADAL DZIAŁA!)

Bardzo popularna swego czasu metoda okazuje się nadal skuteczna. Świadomość tego typu zagrożenia nie sprawia, że stajemy się na nie odporni. A metody oszustów nie ograniczają się tylko do starszych ludzi i ich rzekomego wnuczka. Ostatnio mogą się nawet podszywać za Twojego znajomego na chacie i prosić o niewielki przelew.

### Jaki jest scenariusz?

Oszust najczęściej odwołuje się do naszych emocji. Czasami potrafi wręcz podłożyć głos kogoś bliskiego, bezpośrednio prosząc Cię o pomoc.
Znane są też sytuacje, gdy dzwoni do nas Policja, informuje o udziale w tajnej akcji łapania przestępców i prosi o przekazanie tajnym służbom pieniędzy.
To, że dzwoni do nas numer 112 lub na telefonie wyświetla się ktoś bliski, nie jest przecież problemem. Ale to już wiesz, prawda?

### Co robić?

- absolutnie i pod żadnym pozorem nigdy nie przekazuj żadnych pieniędzy; to wcale nie musi być wysoka kwota. Te niższe jeszcze bardziej usypiają czujność;

- skontaktuj się bezpośrednio z osobą, która rzekomo potrzebuje pomocy i zweryfikuj ten fakt. Jeżeli to niemożliwe, skonsultuj to z kimś zaufanym, kto pomoże Ci ocenić sytuację i podjąć decyzję;
- nie poprzestawaj na jednym środku komunikacji. Jeśli pisze do Ciebie ktoś na chacie, zadzwoń do niego i potwierdź ten fakt.

## 12. POZORNIE NIEWINNE SPOTKANIE

Towarzyskie wyjście z domu wcale nie musi się skończyć grubą imprezą, żebyśmy padli ofiarą przestępstwa. W komfortowej sytuacji spotkania towarzyskiego i w tłumie ludzi tracimy czujność, a wtedy łatwo nas nie tylko okraść klasycznie, ale też wirtualnie.

### Jaki jest scenariusz?

W gwarnym miejscu, spuszczając na chwilę z oczu swoją szklankę, zostajesz „poczęstowany" środkiem odurzającym. Kolejnego dnia odzyskujesz przytomność i okazuje się, że przez całą noc wykonywałeś przelew z mobilnej aplikacji. Prawdopodobnie miałeś otwarte oczy i zatwierdzałeś przelewy poprzez biometrię (skanowanie twarzy lub odcisk palca), ale tego nie pamiętasz.

### Co robić?

- aplikację do banku zabezpiecz kodem PIN. Nie jest to metoda stuprocentowa (w stanie odurzenia możesz nieświadomie go podać), ale trudniejsza do sforsowania niż biometria;
- sprawdź, czy w Twoim banku jest możliwość wprowadzenia limitów na transakcje autoryzowane telefonem, płatności BLIKiem, przelewy. Ustaw je z komputera przed wyjściem na imprezę;
- jeśli Twój telefon ma opcję folderu chronionego, przenieś do niego wszystkie wrażliwe aplikacje i pliki - będą chronione dodatkowym hasłem lub biometrią.

## 13. ALE JA NIE BRAŁEM KREDYTU!

Jeśli Twój pesel jest publicznie dostępny (jesteś udziałowcem spółki) lub obawiasz się, że mogą znać go osoby niepowołane (np. skradziono Ci dokumenty), zabezpiecz się się przed możliwością wzięcia na Ciebie kredytu lub podpisania umowy na Twoje dane.

### Jak to działa?

- na stronie https://www.bik.pl/klienci-indywidualni/alerty-bik aktywujesz usługę Alerty w BIK;
- dzięki usłudze dostaniesz powiadomienie e-mail i SMS za każdym razem, gdy ktoś będzie chciał wziąć na Ciebie kredyt lub podpisać na Twoje dane umowę;
- dostając alert możesz od razu skontaktować się z BIK i zablokować możliwość zaciągnięcia fałszywego kredytu. Możesz też skorzystać z dodatkowej opcji zastrzeżenia kredytowego - wtedy wniosek o kredyt będzie automatycznie odrzucony;
- koszt to 24 zł/rok dla jednej osoby lub 99 zł/rok dla 4 osób (w ten sposób możesz chronić też członków swojej rodziny), a usługa działa 24/7.

### Troszczysz się o swoich bliskich? Podaj dalej!

Przekaż ten dokument znajomym, poślij go dalej w świat.
Bądźmy wszyscy świadomi zagrożeń, jakie mogą nas spotkać we współczesnym świecie.

Życzymy Ci bezpieczeństwa i cierpliwości!
Zespół Wellcome Home