PORADNIK

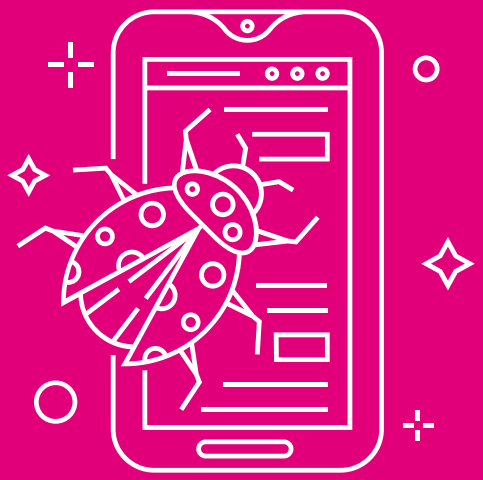
W internecie rób prezenty bliskim, nie oszustom!

Pobierz poradnik i dowiedz się:

- jak chronić swoje dane w internecie
- jak robić bezpieczne zakupy w sieci
- jak działają cyberoszuści i jak się przed ich działaniami chronić

tauron.pl/bezpieczenstwo

Spis treści



Czym jest phishing?

Phishing [czyt: *fiszing*] to oszustwo, którego celem jest wyłudzenie danych lub zainfekowanie urządzenia (komputera, telefonu czy tabletu) złośliwym oprogramowaniem.

Do ataku oszuści wykorzystują:

- e-maile
- SMS-y
- posty w mediach społecznościowych
- wiadomości w komunikatorach
- rozmowy telefoniczne

Przestępcy podszywają się pod firmy, osoby zaufania publicznego lub przedstawicieli znanych marek i instytucji. Najczęściej podają się za:

- funkcjonariuszy służb (policja, straż miejska, służba celna),
- pracowników urzędów (ZUS, Urząd Skarbowy),
- dostawców mediów (np. dostawcy prądu, gazu czy telefonii komórkowej),
- serwisantów IT,
- przedstawicieli firm kurierskich i znanych sieci handlowych.

Jak wyglądają przestępstwa phishingowe?

Oszust stara się zaintrygować ofiarę lub ją przestraszyć.

1. Oferuje „superpromocję", informuje o popełnionym przestępstwie albo o czyhającym zagrożeniu.

2. Tłumaczy, że można złapać okazję, uniknąć kary lub ochronić się przed niebezpieczeństwem.

3. Zanim zdołasz ochłonąć i uspokoić emocje, przestępca podsuwa proste rozwiązanie. Wmawia Ci, że musisz natychmiast kupić towar, przelać pieniądze na wskazane konto, zainstalować oprogramowanie lub wypełnić formularz.

4. Gdy dasz się skusić lub zastraszyć i klikniesz podany w wiadomości link, trafiasz na fałszywą stronę banku, sklepu lub instytucji. Jeżeli zalogujesz się albo zrobisz przelew, przestępca przejmie Twoje dane.

Niekiedy wystarczy samo kliknięcie podanego w wiadomości linka, aby ściągnąć oprogramowanie szpiegujące. Dzięki niemu przestępca uzyska dostęp do Twoich kont bankowych, pocztowych i społecznościowych, a także baz zdjęć i dokumentów.

Rodzaje danych, które możesz stracić w czasie ataku phishingowego:

1. loginy i hasła
2. numery telefonów
3. numer PESEL
4. data urodzenia
5. informacje o Twoich najbliższych
6. numery kart kredytowych
7. numery PIN

Rób prezenty bliskim, nie oszustom!

Jak rozpoznać oszustwo?

Cechy wiadomości tekstowej, które powinny Cię zaniepokoić:

- **presja na szybkie działanie** – przynaglenia w treści wiadomości, np. kliknij natychmiast, zrób przelew jeszcze dzisiaj, została tylko godzina,
- **błędy językowe** – zła ortografia, brak polskich znaków czy krzaczki zamiast polskich znaków,
- **fragmenty tekstu w obcym języku** – pojedyncze zdania lub całe akapity,
- **podejrzane linki** – po najechaniu na link kursorem (bez klikania) wyświetla się inny, nieznany adres,
- **nieład graficzny** – niestarannie wykonane grafiki, nieostre linie, za małe lub zbyt duże napisy,
- **nieoczekiwane załączniki** – do maila załączone są dokumenty, których nie zamawiałeś i nie znasz ich nadawcy, wyskakujące powiadomienia wymagające działania,
- **nietypowa kolorystyka** – niedoskonałości koloru grafiki, np. zmiany nasycenia barw w logotypie,
- **błędy w adresie strony** – podany w mailu adres ma zmienioną końcówkę (na przykład zamiast **.pl** oznaczenie innego kraju), niektórych liter brakuje, inne są podwojone, a niekiedy mają małą dolną kreskę lub kropkę (tzw. kropka bankructwa).

Pamiętaj!

W przypadku tzw. oszustwa metodą na BLIKA prośbę o wykonanie przelewu możesz otrzymać od osób, które masz w gronie znajomych na swoim profilu w mediach społecznościowych. Taka wiadomość wygląda wiarygodnie – nie daj się jednak oszukać. W przypadku, gdy otrzymasz wiadomość z prośbą od znajomego o przelew, koniecznie skontaktuj się z nim w inny sposób, np. telefonicznie. W żadnym wypadku nie wykonuj przelewu!

Przykład phishingu:

zobacz reklamę, którą oszuści wykorzystywali, aby wyłudzić dane klientów TAURONA. Sprawdź, jakie elementy powinny zwrócić Twoją czujność i dlaczego. Przekonaj się, że wiadomości przygotowywane przez oszustów mogą być łudząco podobne do prawdziwych wiadomości.

Styl wskazuje na oszustwo. To dzieło automatycznego tłumacza. Podejrzana jest też treść: dlaczego sprzedawca prądu miałby płacić komukolwiek 200 zł za dzień? Wątpliwości budzi też wyjątkowo niedbałe ustawienie napisów na grafice: ledwie mieszczą się na zaznaczonym polu, co wygląda nieprofesjonalnie i nieestetycznie.

Zwróć uwagę na groteskową treść: patos charakterystyczny dla komunikatów propagandowych. Nienaturalnie wyglądają powiększone litery I oraz P.

Ktoś skopiował poprawne logo Towarzystwa Obrotu Energią, lecz zrobił to nieudolnie i niedbale. Grafika jest rozmazana, a tekst mało czytelny.

Te trzy frazy na pierwszy rzut oka nie budzą większych zastrzeżeń. Jednak wystarczy sprawdzić, jaką działalność prowadzi TAURON, aby nabrać podejrzeń. Bezpieczeństwo dochodów odnosi się do jakiejś formy zarobkowania, co ma się nijak do oferty TAURONA. Napisy wyglądają nienaturalnie: są zbyt mocno przysunięte do krawędzi pola wyznaczonego przez kolor.

Zaskakujący adres strony, który w żaden sposób nie kojarzy się z TAURONEM. Końcówka .cf to domena narodowa Republiki Środkowoafrykańskiej. Adres anvocoldunc.cf znajduje się na liście niebezpiecznych witryn CERT (Computer Emergency Response Team)

Informacja jest kopią tekstu zamieszczanego na oficjalnych materiałach TAURONA. Jednak także w tym przypadku bardzo niska jakość wskazuje na to, że jest to fałszerstwo.

Jak reagować na podejrzane reklamy?

Skontaktuj się z firmą, której logo lub nazwa znajdują się w mailu, SMS-ie, poście czy reklamie. To najskuteczniejszy sposób, aby ustalić, czy masz do czynienia z oszustwem. Nagłośnienie tego typu przypadków pozwala skutecznie chronić innych odbiorców przed zakusami przestępców.

Na czym polega oszustwo na BLIKA?

Kod BLIK zastępuje karty płatnicze i tradycyjne przelewy. Zapłacisz nim online i w sklepach stacjonarnych, prześlesz pieniądze na telefon i pobierzesz gotówkę z bankomatu. Niestety ta metoda płatności jest chętnie wybierana przez oszustów. Sprawdź, jak działają, i dowiedz się, jak rozpoznać próbę oszustwa.

Wyłudzenie pieniędzy przy użyciu kodu BLIK – krok po kroku:

1. **Włamanie** – przestępca włamuje się do czyjejś skrzynki e-mail, profilu na portalu internetowym, komunikatora internetowego albo przejmuje (kradnie lub hakuje zdalnie) smartfon;
2. **Kradzież tożsamości** – oszust działa w imieniu ofiary, np. wyraża opinie w mediach, zaciąga zobowiązania finansowe, utrzymuje kontakty towarzyskie;
3. **Prośba o przelew BLIK** – przestępca wysyła do wybranych osób z listy znajomych lub z książki telefonicznej prośbę o pilny przelew BLIK na telefon lub przesłanie kodu BLIK. Dlatego prośbę o taki przelew możesz otrzymać z konta Twojego znajomego w mediach społecznościowych;
4. **Dramatyczna argumentacja** – oszust uzasadnia prośbę nagłą potrzebą: pisze, że zgubił kartę płatniczą lub portfel, że zabrakło mu środków na wykupienie drogich lekarstw dla dziecka – stara się wykorzystać empatię i uczciwość Twoich znajomych;
5. **Wyłudzenie przelewu BLIK** – jeżeli przestępca przekonał ofiarę do wykonania przelewu BLIK, pieniądze natychmiast trafiają na jego konto;
6. **Wyłudzenie pieniędzy na kod BLIK** – przestępca, który dostał kod BLIK, natychmiast używa go do opłacenia zakupów lub wprowadza do bankomatu, a oszukiwana osoba otrzymuje z banku prośbę o potwierdzenie transakcji kodem PIN - jeśli to zrobi, bezpowrotnie traci pieniądze.

Jak chronić się przed oszustwem na BLIKA?

- **Stosuj silne hasła dostępu do portali społecznościowych, poczty e-mail i komunikatorów. Nigdy nie wysyłaj pocztą i nie pokazuj nikomu swoich danych dostępowych. Używaj dwustopniowych zabezpieczeń, np. hasłem i kodem przesyłanym na telefon.**
- **Zabezpiecz hasłem dostęp do smartfona i komputera.**
- **Jeżeli dostaniesz wiadomość tekstową z prośbą o przelew na telefon lub podanie kodu BLIK, zadzwoń do znajomego, aby potwierdzić jego tożsamość.**

Popularne rodzaje oszustw i wyłudzeń

Celem wszystkich oszustw jest bezpośrednie wyłudzenie pieniędzy lub danych. Oszust wykorzysta dane osobowe, hasła i kody dostępu, aby okraść Cię, zaciągnąć zobowiązania finansowe w Twoim imieniu lub wyłudzić pieniądze od rodziny i znajomych. Gdy przestępca ma dostęp do Twoich prywatnych plików (np. intymnych zdjęć czy ważnych dokumentów medycznych), często posuwa się do szantażu: żąda pieniędzy lub wymusza określone postępowanie.

Oszustwa przez telefon

Oszuści wykorzystują rozmowy głosowe (vishing) i wiadomości SMS (smishing). Pod różnymi pretekstami starają się wyłudzić dane osobowe lub pieniądze. Przestępca najczęściej podaje się za członka rodziny (metoda na wnuczka) lub funkcjonariusza publicznego (metoda na policjanta). Stara się pozyskać zaufanie ofiary i nakłonić ją do przekazania gotówki, biżuterii lub innych cennych przedmiotów. Z kolei wyłudzone dane służą najczęściej do zaciągania pożyczek i kredytów. Ofiara dowiaduje się o nich dopiero w momencie, gdy otrzyma ponaglenie do zapłacenia zaległych rat.

Oszustwa w mediach społecznościowych

W mediach społecznościowych przestępcy nakłaniają internetowych „znajomych" do udzielania pożyczek, płacenia za swoje rachunki czy do zakupu różnych towarów lub usług po mocno zawyżonych cenach. Częstym sposobem na wyłudzenie danych są fałszywe quizy i konkursy, oferty pracy oraz clickbaity (grafika i teksty zachęcające do natychmiastowego kliknięcia).

Oszustwa matrymonialne

Nie brakuje oszustów, którzy wykorzystują urodę i urok osobisty, aby wyłudzać pieniądze i drogie podarunki od osób poszukujących „drugiej połówki". Uwodzą swoje ofiary, uzależniają od siebie emocjonalnie, a następnie okradają i porzucają. Najczęściej polem działania dla oszustów matrymonialnych są portale randkowe i media społecznościowe.

Fikcyjne inwestycje

Oszust umieszcza w sieci ogłoszenie o wyjątkowo zyskownej inwestycji. Jeżeli dasz się skusić, trafiasz na zbudowaną przez przestępców stronę internetową. Dowiadujesz się, że aby zacząć inwestować, musisz zasilić swój wirtualny portfel. Gdy przelejesz pieniądze na podane konto, fałszywy doradca przestanie odpowiadać na maile i telefony.

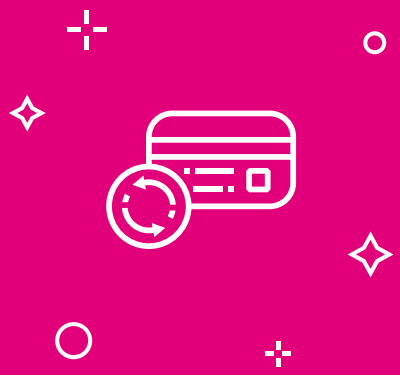
Gra na giełdzie kryptowalut

Ponad 70% osób handlujących kryptowalutami traci pieniądze. To bardzo ryzykowny rynek, który wymaga dużej wiedzy. Oszuści oferują „sprawdzone" i „pewne" sposoby zarabiania na giełdzie kryptowalut. Sprzedają kompletnie nieprzydatne kursy i aplikacje, które „handlują za Ciebie". Płacisz za oprogramowanie, które jest zupełnie nieskuteczne.

Fałszywe sklepy i sprzedawcy

Mechanizm oszustwa jest banalnie prosty: przestępcy oferują markowe produkty w bardzo atrakcyjnej cenie, inkasują pieniądze i urywają kontakt. Nigdy nie otrzymasz zamówionych przedmiotów. Oszustwo w wersji soft polega na tym, że zamiast markowych perfum, ubrań czy butów dostajesz tanie podróbki.

Jak działa procedura chargeback?



Chargeback to zwrot pieniędzy za towar lub usługę opłacone kartą. Usługa działa z każdą kartą debetową, kredytową i przedpłaconą. Jest bezpłatna i nie musisz jej aktywować.

Dzięki chargeback odzyskasz pieniądze, gdy:

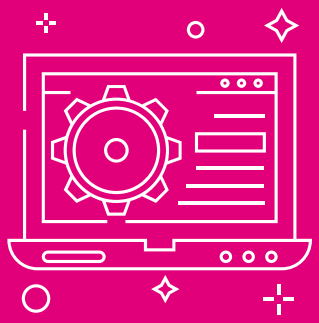
- sprzedawca nie dostarczył produktu lub usługi,
- towar jest niezgodny z zamówieniem,
- sprzedawca lub wykonawca usługi zbankrutował,
- opłata za towar lub usługę została pobrana dwukrotnie,
- bankomat wypłacił za mało pieniędzy.

Jak odzyskać środki za transakcje dokonane kartą płatniczą?

Najpierw spróbuj nawiązać kontakt ze sprzedawcą. Jeżeli nie odpowiada, unika kontaktu lub odmawia współpracy, zareklamuj transakcję w swoim banku. Od tego momentu to bank prowadzi negocjacje. Zwrot pieniędzy na konto otrzymasz natychmiast po złożeniu reklamacji lub po jej rozpatrzeniu. Procedura może trwać od kilku dni do kilku tygodni.

Oszustwa na platformach sprzedażowych

Oszustw na platformach sprzedażowych (marketplace) dopuszczają się zarówno sprzedawcy, jak i kupujący. Cyberprzestępcy wyłudzają pieniądze, towary lub dane dostępowe (login, hasło) do bankowości internetowej. Ofiarami manipulacji padają zazwyczaj niedoświadczeni sprzedawcy i osoby, które pierwszy raz lub sporadycznie robią zakupy. Złodzieje wykorzystują ufność, niewiedzę i brak czujności swoich ofiar.



Przykładowe oszustwa na platformach sprzedażowych

Oszustwo „nigeryjskie"

Nigeria jest krajem, w którym kwitnie cyberprzestępczość. Przymiotnik „nigeryjskie" przylgnął do oszustw, których autorzy posługują się łamaną polszczyzną z translatora Google. Przestępcy oferują zakup bez negocjacji ceny lub nawet podbijają stawkę. Stawiają tylko jeden warunek: masz wysłać zamówienie poza granice Polski. Zaraz potem przesyłają podrobione zaświadczenie przelewu. Jeżeli zdecydujesz się nadać przesyłkę, stracisz towar i dodatkowo zapłacisz za jego dostarczenie. Na Twoje konto nigdy nie wpłyną żadne pieniądze.

Fałszywe konto na platformie sprzedażowej

Przestępcy kradną dane osobowe, dzięki czemu mogą zakładać fałszywe konta na platformach sprzedażowych. Wystawiają towary, których nie mają, aby wyłudzać pieniądze. Często przechwytują także dane osobowe i hasła do bankowości elektronicznej.

Fałszywy pracownik marketplace

Popularnym sposobem oszustwa jest podszywanie się pod pracownika marketplace. Przestępca informuje np. o grożącej blokadzie konta na platformie i prosi o podanie w mailu lub poście hasła i loginu.

Fałszywy konkurs, ankieta lub oferta pracy

Banalnie prostym sposobem wyłudzenia danych jest fałszywy konkurs. Pod pozorem rejestracji uczestnika lub odbioru nagrody przestępcy nakłaniają swoje ofiary do ujawnienia danych osobowych, przekazania danych do konta na platformie sprzedażowej lub w bankowości elektronicznej. Podobny schemat ma oszustwo na badania ankietowe, agencje pośrednictwa pracy czy szkolenia.

Jak uniknąć oszustwa na platformie handlowej?

1. Korzystaj z komunikatorów i bezpiecznych procedur zakupowych oferowanych przez platformę sprzedażową.

2. Nigdy nie zgadzaj się na przelewy natychmiastowe na numer telefonu podawany przez sprzedającego, np. z użyciem kodu BLIK.

3. Nigdy nie podawaj obcym osobom swoich danych, w tym szczególnie danych kart kredytowych, haseł do bankowości elektronicznej, konta na platformach handlowych i w social mediach.

4. Nie klikaj linków wysyłanych przez sprzedawcę lub kupującego w zewnętrznych komunikatorach (np. WhatsApp) lub w prywatnej poczcie e-mail.

5. Zwróć uwagę na błędy językowe w korespondencji i dziwne adresy stron.

6. Spróbuj zweryfikować sprzedawcę – sprawdź jego dane kontaktowe lub dane jego firmy w internecie.

7. Jeżeli padniesz ofiarą oszustwa, zgłoś nieuczciwego sprzedawcę lub klienta – ochronisz w ten sposób innych użytkowników platformy.

Chroń swoje dane w sieci

Nie działaj pod wpływem emocji i nie daj się złowić! Przestępcy chcą wyprowadzić Cię z równowagi oraz zmusić do niezwłocznego działania. Ich kreatywność jest w tym zakresie niemal nieograniczona. Dlatego zachowanie zdrowego rozsądku jest kluczowe dla Twojego bezpieczeństwa w sieci.

Pamiętaj!

Żadna instytucja (ani bank, ani policja, ani jakikolwiek urząd) nie żąda i nie zmusza do podawania poufnych informacji za pomocą poczty elektronicznej lub telefonu. Żadne z nich nie potrzebuje też Twoich haseł dostępu do wszelkiego rodzaju kont. Nikt z nich nie prosi o uiszczenie opłat i należności na wskazane w wiadomościach dane.

Masz wątpliwości co do autentyczności otrzymanego maila lub wiadomości SMS i zawartej w nich treści? Rozwiej je, kontaktując się z instytucją, od której rzekomo pochodzi wiadomość. Możesz na przykład samodzielnie zadzwonić na infolinię, której numer znajdziesz na oficjalnej stronie lub w swoich dokumentach.

Co zrobić, gdy podejrzewasz, że wiadomość jest fałszywa?

Do czasu, aż nie upewnisz się, że wiadomość jest prawdziwa:

- **nie klikaj w żadne linki,**
- **nie odpowiadaj na wiadomości,**
- **nie otwieraj załączników,**
- **oznacz wiadomość jako spam.**

Aby zweryfikować, czy wiadomość jest prawdziwa, skontaktuj się z instytucją, pod którą podszywa się nadawca wiadomości.

Przykład

Otrzymałeś informację o tym, że zalegasz z płatnościami za prąd. W wiadomości tej jest link do szybkiej płatności.

Co powinieneś zrobić?
Skontaktuj się ze swoim sprzedawcą prądu, zweryfikuj saldo konta i prawdziwość wiadomości.

Ktoś Cię oszukał? Co zrobić w takim przypadku

Pomimo zachowania ostrożności i środków bezpieczeństwa może się zdarzyć, że padniesz ofiarą oszustwa. Co wtedy? Musisz skupić się na dwóch kwestiach:

1

Ograniczenie szkód

Zmień hasła na kontach, z których korzystasz, zaktualizuj oprogramowanie, które ma zabezpieczać sprzęt i sieć. Jeśli sprawa dotyczy kradzieży danych bankowych, skontaktuj się z bankiem, aby zablokować konta oraz karty płatnicze.

2

Zgłoszenie oszustwa odpowiednim organom i instytucjom

Złóż na policji doniesienie o popełnieniu przestępstwa. Phishing, jak każde inne oszustwo, jest karany. Zachowaj dowody, mogą nimi być np. screeny ekranu czy wiadomości.

- **Zgłoś oszustwo do CERT Polska** – to instytucja, która zajmuje się tematem bezpieczeństwa w internecie. Dzięki przekazaniu jej informacji o oszustwach przyczyniasz się do ograniczenia tego szkodliwego procederu w sieci.
- **Zgłoś oszustwo instytucji/firmie, pod którą podszywa się oszust.**

tauron.pl/bezpieczenstwo