



PORADNIK

Klikaj bezpiecznie!

Jak chronić siebie, swoje dane i pieniądze?

Z BEZPŁATNEGO PORADNIKA DOWIESZ SIĘ:

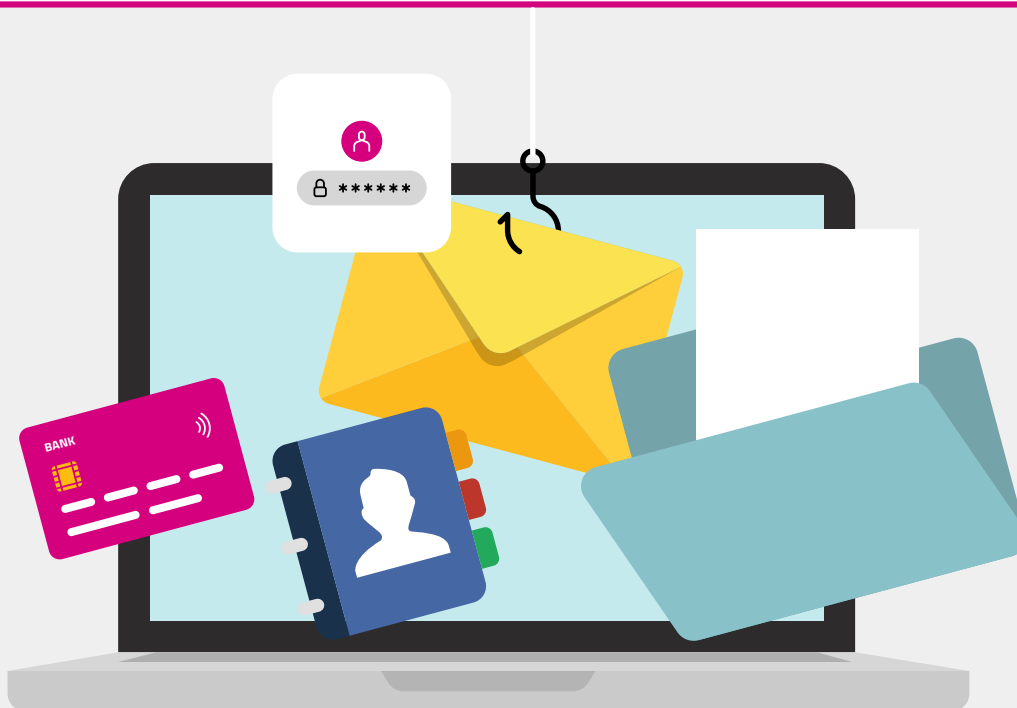
- jak chronić dane osobowe i bezpiecznie dokonywać transakcji w sieci
- na jakie oszustwa w internecie musisz uważać
- jak rozpoznać oszustwa z wykorzystaniem AI i jak się przed nimi zabezpieczyć

Spis treści

Czym jest phishing?	3
Jak wyglądają przestępstwa phishingowe?	4
Jak rozpoznać oszustwo?	6
Przykład phishingu	7
Na czym polega oszustwo na BLIKA?	8
Popularne rodzaje oszustw i wyłudzeń	9
Czym jest chargeback?	11
Oszustwa na platformach sprzedażowych	12
Sztuczna inteligencja w rękach cyberprzestępców	14
Chroń swoje dane w sieci	16

Czym jest phishing?

Phishing [czyt: fizing] 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

Najczęściej przestępcy 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?

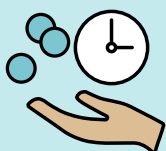
Oszust stara się zaintrygować ofiarę lub ją przestraszyć



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.

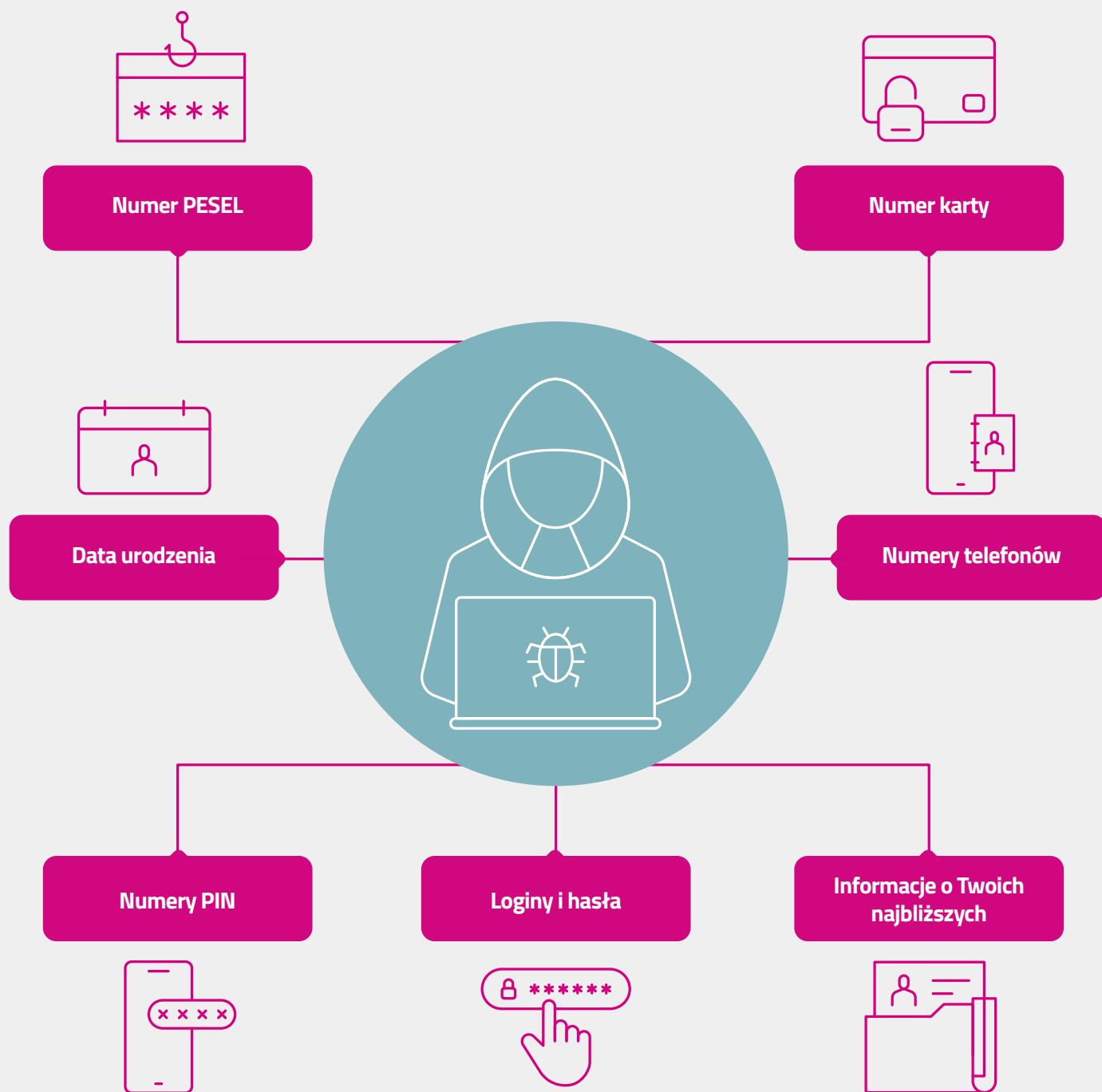


4 Gdy dasz się skusić lub zastraszyć i klikniesz podany w wiadomości link, trafiasz na fałszywą stronę banku, sklepu lub instytucji. Jeżeli zalogujesz się albo zrobisz przelew, przestępca przejmie Twoje dane.

Ważne!

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:



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 o przelew od znajomego, 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 energii elektrycznej 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.

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.

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

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 przejmując (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 znajomych rzekomej ofiary.

5

Wyłudzenie przelewu BLIK

Jeżeli przestępca przekonał ofiarę do wykonania przelewu BLIK, pieniądze natychmiast trafiają na jego konto.

6

Wyłudzenie pieniędzy na kod BLIK

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 znajomych rzekomej ofiary.



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.

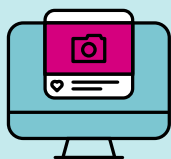
Popularne rodzaje oszustw i wyłudzeń

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.



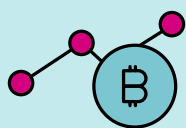
Oszustwa w mediach społecznościowych

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 zyskowej 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.



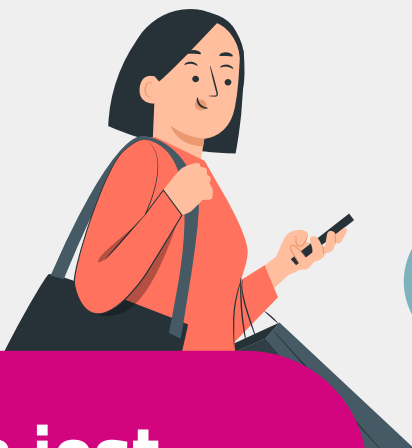
Gra na giełdzie kryptowalut

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.



Czym jest chargeback?



Chargeback, czyli inaczej obciążenie zwrotne, to mechanizm chroniący kupujących, którzy płacą za towar czy usługi kartą płatniczą, przed nieuczciwymi usługodawcami, nadużyciami czy błędami systemów płatniczych. Procedura zwrotu pieniędzy jest bezpłatna i możliwa dla płatności kartami Visa i MasterCard (debetowymi, kredytowymi i przedpłaconymi).

W jakich sytuacjach ma zastosowanie procedura chargeback?

Dzięki mechanizmowi chargeback odzyskasz swoje pieniądze w sytuacji, gdy:

- nie otrzymasz zamówionego towaru lub usługi;
- otrzymasz produkt uszkodzony lub niezgodny z opisem;
- transakcja nie była przez Ciebie autoryzowana (nastąpiła w wyniku kradzieży danych);
- sprzedawca nie zwrócił Ci pieniędzy mimo reklamacji;
- sklep pobrał opłatę za towar, którego nie zamówiłeś;
- opłata za towar lub usługę została pobrana dwukrotnie;
- bankomat wypłacił za mało pieniędzy.

Wówczas bank klienta po rozpatrzeniu zgłoszenia może cofnąć środki z konta sprzedawcy i zwrócić je klientowi.

Jak odzyskać środki? Instrukcja krok po kroku

- 1 Najpierw spróbuj wyjaśnić sprawę bezpośrednio ze sprzedawcą, co często jest wymagane przez bank jako początkowy krok.
- 2 Zbierz dowody potwierdzające zasadność reklamacji (np. potwierdzenie zwrotu towaru, brak usług, niezgodność kwoty).
- 3 Zgłoś reklamację do banku, podając dokładne dane transakcji, opisz problem i załącz dokumenty.
- 4 Bank rozpatruje zgłoszenie, kontaktuje się z agentem rozliczeniowym, a sprzedawca ma możliwość przedstawienia swoich dowodów.
- 5 W przypadku uznania reklamacji przez sprzedawcę lub braku jego odpowiedzi środki są zwracane na rachunek klienta.

Na zgłoszenie reklamacji masz zazwyczaj do 120 dni od daty transakcji, a proces rozpatrzenia 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 wyłudniają pieniądze, towary lub dane dostępne (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.

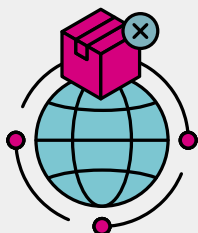
Przykładowe oszustwa na platformach sprzedażowych

Wyłudnianie poprzez aplikacje i komunikatory

Szczególnie popularne stały się oszustwa polegające na wyłudnianiu danych oraz płatności przez komunikatory i aplikacje, zarówno na platformach sprzedażowych, jak i rezerwacyjnych. Cyberprzestępcy kontaktują się poza oficjalnymi platformami (do publikowania ogłoszeń, rezerwacji noclegów), wykorzystując komunikatory czy SMS do przesyłania fałszywych linków i żądania płatności lub danych, narażając ofiary na ryzyko utraty pieniędzy i kradzieży danych osobowych. Ten typ oszustwa dynamicznie rośnie, bo wiadomości w komunikatorach trudniej wykryć i zablokować.



Oszustwo „nigeryjskie”



Nigeria jest krajem, w którym kwitnie cyberprzestępczość. Przymiotnik „nigeryjskie” przylgnął do oszustw, których autorzy posługują się łamaną polszczyzną z tłumacza 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.



Sztuczna inteligencja w rękach cyberprzestępców

Sztuczna inteligencja (AI) już teraz jest częścią Twojego codziennego życia i coraz częściej ułatwia Ci różne zadania. Korzystasz z niej, gdy rozmawiasz z wirtualnym asystentem na smartfonie, używasz automatycznych tłumaczeń w internecie, otrzymujesz spersonalizowane rekomendacje zakupowe czy kiedy oglądasz filmy i słuchasz muzyki dopasowanej do Twoich upodobań.

AI pomaga też firmom usprawniać obsługę klienta czy analizować wielkie ilości danych, co skraca czas pracy i podnosi efektywność. Niestety, te same technologie, które przynoszą korzyści, mogą być wykorzystywane przez cyberprzestępców. Dlatego musisz wiedzieć, jak się przed tym bronić.

Jak działają oszustwa z użyciem sztucznej inteligencji?

AI Phishing

AI Phishing wygląda dziś inaczej niż tradycyjne próby wyłudzenia danych. Wyobraź sobie, że dostajesz e-mail lub SMS, który wydaje się pochodzić z Twojego banku, urzędu skarbowego albo firmy kurierskiej. Wiadomość jest napisana bardzo naturalnym językiem, używa Twojego imienia i zawiera szczegóły, które normalnie możesz znać tylko Ty – jak na przykład numer przesyłki czy część Twojego adresu. To nie przypadek – za tym stoi AI, która potrafi analizować Twoje publiczne profile w mediach społecznościowych, stronę firmy i styl komunikacji, żeby tworzyć spersonalizowane wiadomości. Co więcej, może ich wysłać tysiące jednocześnie, zwiększając ryzyko, że ktoś się złapie na haczyk.

Przykład

Otrzymujesz SMS-a „Twoja paczka od XYZ jest w drodze, kliknij tutaj, aby potwierdzić odbiór” i link, który wygląda niemal identycznie jak oficjalna strona firmy kurierskiej. Jeśli klikniesz i podasz dane swojej karty, oszuści natychmiast wyczyszczą Twoje konto.

Inny przykład to wiadomości na portalach społecznościowych, gdzie ktoś podszywa się pod Twojego znajomego, prosząc o pożyczkę lub link do pilnej płatności – to również może być AI generująca komunikat na podstawie stylu pisanie tej osoby.

Deepfake

Deepfake to z kolei technologia, która potrafi tworzyć fałszywe, ale bardzo przekonujące zdjęcia, filmy i nagrania głosu. Wyobraź sobie, że dzwoni do Ciebie ktoś, kto brzmi dokładnie jak członek Twojej rodziny i mówi, że ma problem oraz potrzebuje pilnej pomocy finansowej. To może być klon głosu stworzonego przez AI. Innym przykładem jest wideo znanej osoby publicznej, która przekazuje fałszywe informacje, często zachęcając przy tym do inwestowania, wpłacenia pieniędzy lub rejestracji na wybranej stronie. *Deepfake* może też posłużyć do kradzieży tożsamości, tworząc fałszywe dokumenty czy profile

Jak rozpoznać oszustwa z AI i jak się przed nimi zabezpieczyć?



1

Bądź czujny wobec niespodziewanych wiadomości, zwłaszcza takich, które proszą o podanie danych osobowych, hasła czy kodów z SMS. Prawdziwe instytucje nigdy nie proszą o takie informacje przez e-mail lub SMS.



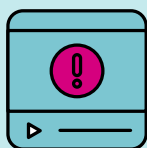
2

Sprawdzaj dokładnie linki i adresy stron, które klikniesz. Jeśli adres wygląda dziwnie lub jest inny niż oficjalny, nie ryzykuj.



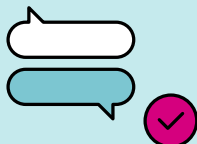
3

Zwracaj uwagę na drobne nieścisłości w treści wiadomości – literówki, dziwne zwroty, nadmierną presję na szybkie działanie. AI może tworzyć naturalne teksty, ale wciąż zdarzają się błędy lub nienaturalne elementy.



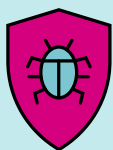
4

W przypadku podejrzanych nagrań video lub audio zwróć uwagę na nienaturalne ruchy ust, opóźnienia w dźwięku, dziwne tło lub „szumy”. Możesz też poprosić nadawcę o potwierdzenie ważnej informacji przez inny kanał, np. telefonicznie.



5

Zawsze weryfikuj informacje bezpośrednio u źródła – jeśli otrzymasz wiadomość rzekomo z banku, zadzwoń na oficjalną infolinię, zamiast odpowiadać na e-mail czy SMS.



6

Używaj dobrego antywirusa i aktualizuj regularnie oprogramowanie na swoich urządzeniach.



7

Nie przenoś rozmów poza oficjalne platformy – jeśli ktoś chce rozmawiać przez inne aplikacje czy wysyłać linki spoza platformy zakupowej czy rezerwacyjnej, zachowaj szczególną ostrożność.



8

Włącz uwierzytelnianie dwuskładnikowe (2FA) tam, gdzie to możliwe – to dodatkowa warstwa ochrony Twoich kont.

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? Rozwiąż 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.





Pamiętaj

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.



Więcej praktycznych porad znajdziesz na
lepiej.tauron.pl