CRÉDIT AGRICOLE

Bezpieczeństwo w sieci

Jak ochronić siebie i swoje pieniądze?

#NIEDAJSIĘZŁOWIĆ

Spis treści

Wiele mówi się o internetowych atakach i przestępstwach. Może nawet ktoś z Twoich bliskich lub znajomych stracił w taki sposób swoje dane lub pieniądze. A może taka sytuacja spotkała Ciebie?

Wszystko to jest bardzo prawdopodobne,

bo niemal 1/3 Polaków[1] twierdzi, że została oszukana w internecie.

Czy to jest powód, żeby wpadać w panikę? Nie. To zachęta do tego, żeby lepiej zadbać o swoje bezpieczeństwo w sieci. **Musisz wiedzieć, gdzie jest zagrożenie, na czym polega i jak się przed nim ustrzec... A jeśli już spotka Cię coś złego, dobrze wiedzieć, jak sobie z tym poradzić.**

W tym raporcie:

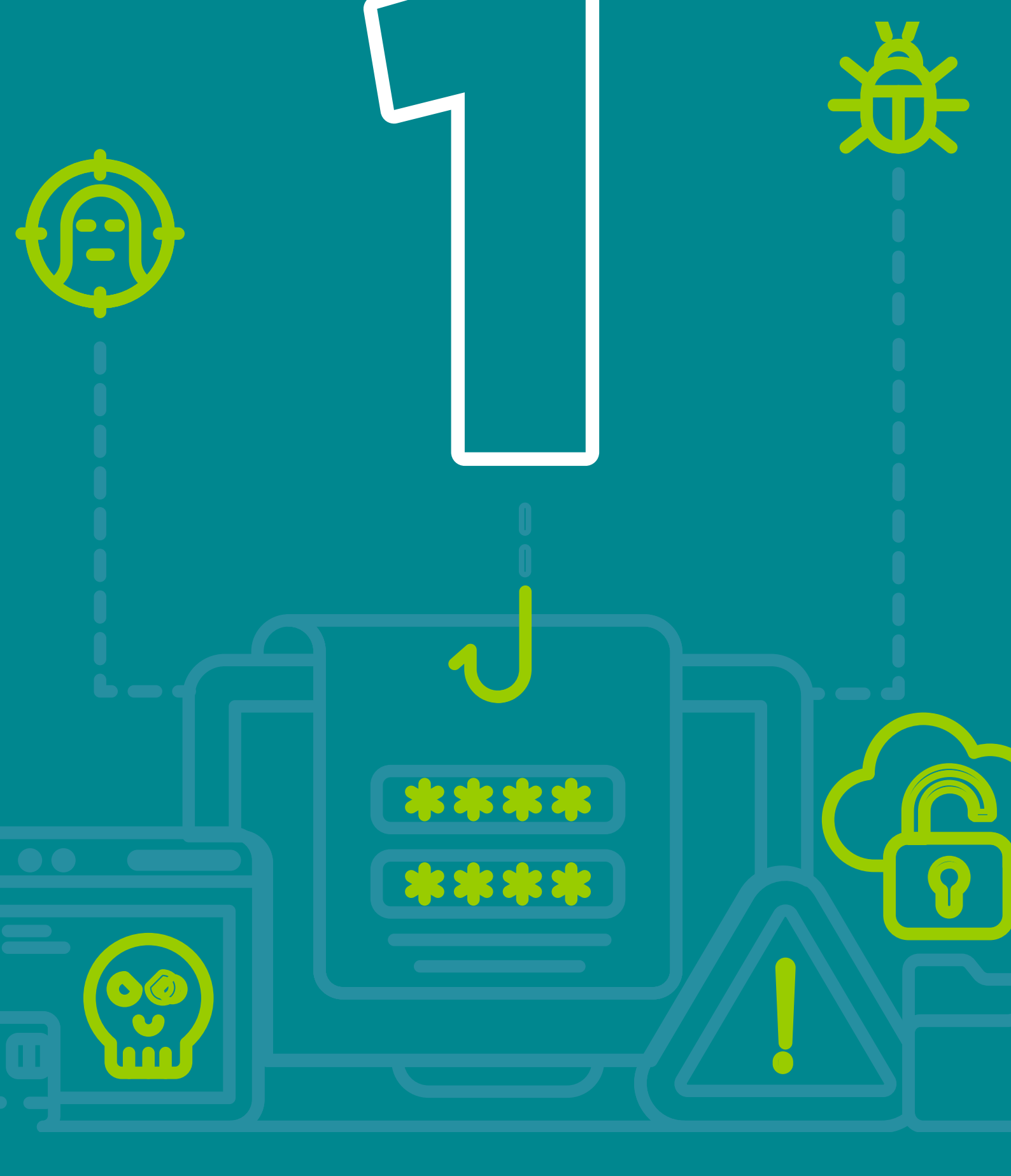
- **dostaniesz solidną dawkę wiedzy** o popularnych metodach oszustw internetowych, na czym polegają i co zrobić, kiedy coś takiego zdarzy się Tobie,
- przedstawiamy wnioski z **naszych badań o oszustwach internetowych.**

Miłej lektury! Zapraszamy 🙂

I miej ten raport zawsze pod ręką – zapisz go telefonie lub komputerze.
Tak na wszelki wypadek.

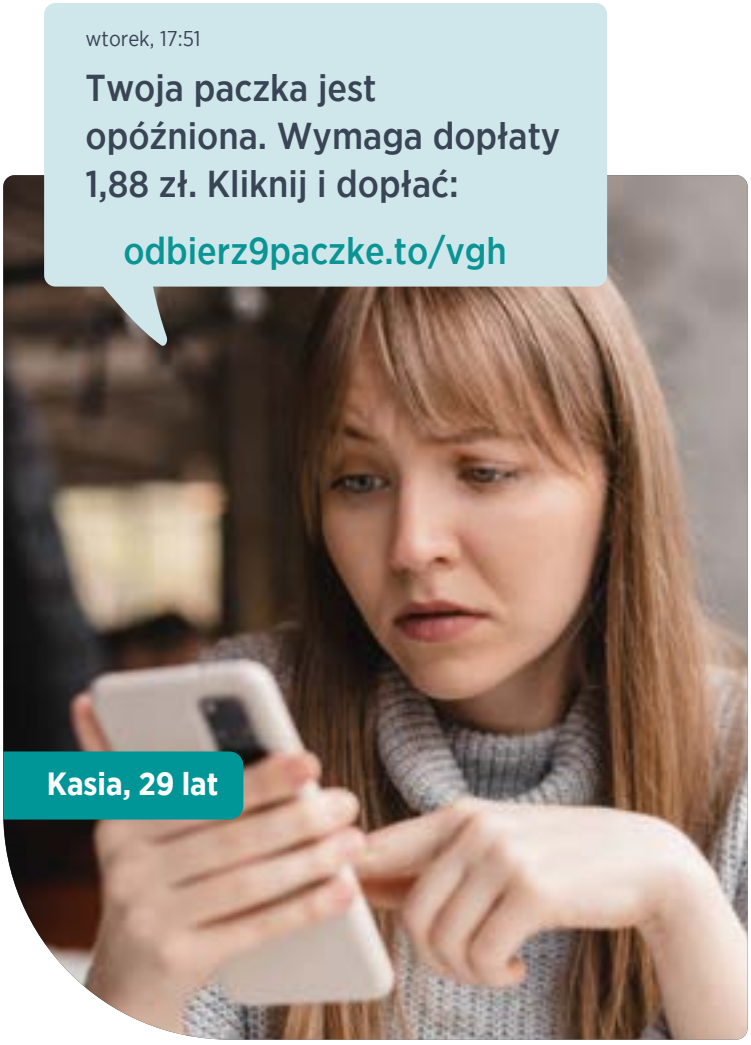
[1] Badanie CAWI realizowane na Panelu Internetowym Ariadna, N=1492 osób w wieku 16+, styczeń 2024

Część 1



SMS z fałszywym linkiem

Hej, jestem Kasia! Często kupuję przez internet. Pewnego dnia dostałam dziwnego SMS-a...



Co zrobiłam?

Nie zastanawiałam się długo, kliknęłam link i przeszłam na stronę, która wyglądała jak strona bankowości internetowej mojego banku. **Podałam swoje dane logowania (login, hasło) i kod autoryzacyjny z SMS-a od banku.**

Co się stało?

Nie wiedziałam, że SMS pochodził od oszustów, a strona była podrobiona. **Dałam oszustom klucze do swojego finansowego domu, a oni ukradli moje pieniądze z konta.**

Oszuści mogą chcieć ukraść Twoje pieniądze – zrobić przelew, aktywować w Twoim imieniu aplikację mobilną, albo dodać Twoją kartę płatniczą do ich cyfrowego portfela. **Dlatego zawsze sprawdź, co zatwierdzasz kodem z SMS-a od banku**

Ten rodzaj oszustwa to smishing

Oszuści podszywają się pod firmy kurierskie, znane osoby lub instytucje. Wysyłają SMS-y z linkiem do podrobionej strony, którą sami zarządzają. **Wszystko po to, żeby dostać dane logowania klientów do bankowości internetowej, a potem ich okraść.**

Aż 39% osób badanych spotkało się z tą formą oszustwa.

Cechy charakterystyczne:

- **drobna suma,** którą musisz dopłacić,
- sytuacja jest bardzo prawdopodobna, bo oszuści mogą trafić z SMS-em od rzekomej firmy kurierskiej, **kiedy rzeczywiście czekasz na przesyłkę**,
- SMS zawiera **link**,
- z wiadomości wynika, że **musisz coś zrobić szybko i jest to koniecznie,** np. przesyłka nie jest w pełni opłacona,
- takie SMS-y mogą dotyczyć też **np. rachunku za prąd czy opłaty za mandat**.

Co robić, gdy spotka Cię podobna sytuacja?

- **Zadzwoń do firmy kurierskiej,** która rzekomo wysłała Ci SMS-a.
- Nie pamiętasz, czy czekasz na jakąś przesyłkę? **Sprawdź historie zamówień ze swoich ulubionych sklepów i skrzynkę mejlową.**
- Nie podawaj swoich danych logowania. **Sprawdź dokładnie adres strony internetowej.** Jest z pewnością inny niż adres strony logowania banku.
- Próbę oszustwa **zgłoś do CERT Polska** — to zespół NASK, który reaguje na oszustwa internetowe. Możesz to zrobić przez:

  1. funkcję **„przekaż SMS”** na numer **CERT Polska – 8080**, albo
  2. stronę **https://incydent.cert.pl.**

  Do zgłoszenia wystarczy podać numer telefonu, z którego przyszedł SMS z linkiem.

Firma kurierska nie może wymagać dodatkowych opłat za przesyłkę.

Oszustwa na portalach sprzedażowych

Jakiś czas temu chciałem sprzedać telefon na jednym z serwisów ogłoszeniowych. Wystawiłem sprzęt i czekałem na odzew. Parę dni później dostałem wiadomość na innej aplikacji, w której pewien pan twierdził, że kupił telefon. Byłem nieco zdziwiony, bo w serwisie ogłoszeniowym nie widziałem takiej informacji. Pomyślałem jednak, że może jest to jakiś błąd techniczny.

Robert, 60 lat

środka 11:51

Dzień dobry! Kupiłem u Pana telefon. Pieniądze może Pan odebrać pod tym linkiem olx.pl.oferta.pw/order?id=981

Co zrobiłem?

Kliknąłem link i trafiłem na stronę, która do złudzenia przypominała serwis ogłoszeniowy. Tam z łatwością znalazłem instrukcję co mam zrobić i działałem jak po sznurku... **Kliknąłem przycisk „Odbierz środki”**, potem „Zaloguj się do banku” i podałem swoje dane (login i hasło). Nie pomyślałem wtedy, dlaczego kupujący nie przesłał po prostu pieniędzy na moje konto. To przecież od początku było dziwne.

Co się stało?

Oszuści dostali moje dane do logowania do bankowości internetowej i ukradli mi pieniądze z konta.

Najpopularniejsze portale sprzedażowe, z których korzystamy to Allegro (84%), OLX (45%), Vinted (28%).

Ten rodzaj oszustwa to oszustwo przez portal sprzedażowy

W tym przypadku oszust pisze do Ciebie poza portalem sprzedażowym, na innym komunikatorze. W wiadomości **zapewnia Cię, że kupił wystawiony przedmiot i przesyła link.** Dzięki tej stronie rzekomo możesz odebrać swoje pieniądze za produkt.

Aż 59% badanych sprzedaje coś przez Internet. To dobra okazja dla oszustów internetowych.

Cechy charakterystyczne:

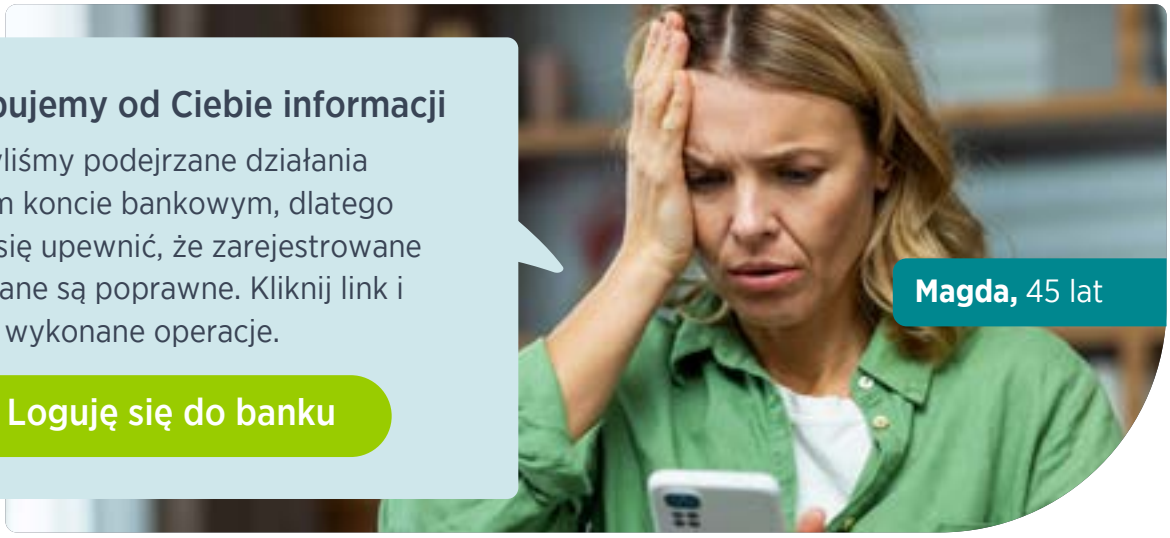
- „kupujący” kontaktuje się z Tobą **poza portalem sprzedażowym**,
- dostajesz link, przez który masz odebrać pieniądze,
- **nie widzisz informacji o zakupie na portalu sprzedażowym**,
- dla większej wiarygodności czasem „kupujący” może podać fałszywe dane do wysyłki produktu,
- gdy postanowisz się wycofać, **oszust może próbować Cię zastraszyć** (np. „Ja już zapłaciłem, poniosłem koszty. Pójdę z tym na policję”).

Co robić, gdy spotka Cię podobna sytuacja?

- Zignoruj wiadomość — **nie wdawaj się w rozmowę z oszustem.**
- Z kupującymi rozmawiaj wyłącznie w serwisie, w którym sprzedajesz.
- **Nie klikaj w linki, które dostajesz w wiadomościach.**
- Jeśli ktoś twierdzi, że kupił Twój towar, upewnij się na serwisie ogłoszeniowym. Jeśli nie widzisz tej transakcji — napisz do obsługi serwisu.
- **Próbę oszustwa zgłoś do CERT Polska** przez stronę **https://incydent.cert.pl.**

Wiadomości od oszustów, którzy podszywają się pod bank

Mam na imię Magda i opowiem Ci, jak oszuści ukradli moje pieniądze. Wszystko zaczęło się od z pozoru niewinnego mejla z mojego banku. To znaczy, tak na tamten moment myślałam.



Co zrobiłam?

Byłam przerażona. Tak dużo słyszy się teraz o kradzieży pieniędzy. **W pośpiechu kliknęłam link i weszłam na stronę „banku”**. Tak wtedy myślałam. Nawet nie sprawdziłam adresu tej strony... Wpisałam login, hasło i potwierdziłam kodem z SMS-a.

Co się stało?

Strona, na którą weszłam i podałam swoje dane — była fałszywa. Dałam oszustom dostęp do mojego konta i pieniędzy.

Bank nigdy nie wysyła wiadomości z linkiem do logowania. Nie prosi o zrobienie jakiejś operacji ani podanie kodu BLIK. Jeśli dostaniesz taką wiadomość — zgłoś to do banku.

Ten rodzaj oszustwa to phishing

Oszuści wysyłają wiadomości, w których podszywają się pod bank, serwisy płatności albo inne instytucje. Kierują z nich na fałszywą stronę i nakłaniają do logowania. Kiedy podasz tam swoje dane, wykorzystają je, żeby wejść na Twoje prawdziwe konto i ukraść Twoje pieniądze.

Aż 23% badanych doświadczyło phishingu.

Cechy charakterystyczne:

- **dostajesz wiadomość z banku lub innej znanej firmy**,
- **ktoś oczekuje od Ciebie szybkiego działania** np. „Jeśli nie potwierdzisz operacji do końca dnia, Twoje konto zostanie zablokowane", „Pilne wezwanie do uregulowania zapłaty",
- **w wiadomości mogą być błędy językowe, literówki i adres może być dziwny**, albo podobny do adresu mejlowego banku lub instytucji, pod którą ktoś się podszywa,
- **adres strony do logowania jest inny** niż oryginalny banku.

Co robić, gdy spotka Cię podobna sytuacja?

- **Uważnie przeczytaj treść, przyjrzyj się grafice.** Porównaj z innymi wiadomościami, które masz od tej firmy.
- **Sprawdź nazwę i adres nadawcy** — czy są takie jak w innych wiadomościach od tej firmy?
- **Zwróć uwagę na błędy językowe, literówki** — mejle od oszustów często mają takie błędy.
- **Samodzielnie wpisz adres strony logowania do banku** albo wybierz go z listy adresów w swojej przeglądarce.
- **Zgłoś próbę oszustwa:**
  - do banku,
  - do CERT Polska na stronie **https://incydent.cert.pl**

  W ten sposób możesz uchronić innych.

Oferty fałszywych inwestycji

Kilka miesięcy temu trafiłam w internecie na reklamę bardzo atrakcyjnej inwestycji. Wyglądała obiecująco — wyjątkowa oferta z dużym zyskiem i niskim wkładem własnym. Propozycja była bardzo kusząca. Kliknęłam i wypełniłam formularz kontaktowy.

Anna, 56 lat

Po kilkunastu minutach zadzwonił do mnie doradca. Przedstawił ofertę, opowiedział o gwarantowanym zysku, potwierdził niską pierwszą wpłatę i zachęcił do szybkiej decyzji. **Oferta była limitowana i dostępna tylko dla pierwszych 15 osób.** Zostało tylko kilka miejsc. Jeśli chcę skorzystać, to muszę się szybko zdecydować.

Co zrobiłam?

Nie chciałam przegapić takiej okazji. Ta oferta naprawdę była atrakcyjna, nie było takich na rynku. I nie miałam dużo czasu na rozważania. **Zdecydowałam się i zrobiłam przelew zgodnie z instrukcją**, którą przekazał mi doradca.

Co się stało?

Oferta była oszustwem. **Pieniądze trafiły prosto na konto oszustów.** Nic nie zarobiłam, za to straciłam część oszczędności. To była droga lekcja.

Ten rodzaj oszustwa to oferty fałszywych inwestycji

Oszuści proponują wyjątkowo atrakcyjną ofertę szybkiego zysku, przy niedużym wkładzie początkowym. Wykorzystują naszą chęć szybkiego pomnażania oszczędności. **Oferta wygląda profesjonalnie, ale nie ma nic wspólnego z inwestowaniem. To tylko wyłudzenie pieniędzy.**

Z ofertą fałszywych inwestycji spotkało się aż 16% badanych.

Cechy charakterystyczne:

- w reklamie jest **gwarancja wysokiego zysku**,
- na start wystarczy zainwestować niską kwotę,
- **oferta wygląda profesjonalnie,** często zawiera np. formularz kontaktowy,
- **oszust dzwoni, dba o wysoki poziom rozmowy, wzbudza zaufanie,**
- oferta jest **ograniczona w czasie** albo dostępna dla **limitowanej liczby klientów**.

Co robić, gdy spotka Cię podobna sytuacja?

Nie klikaj w reklamy, które obiecują nierealnie wysokie zyski w krótkim czasie.

Ignoruj oferty, które zapewniają nierealnie wysoki zysk, bez ryzyka. Zgłoś taką reklamę:
- do serwisu, na którym jest publikowana, np. do Facebooka
- do CERT przez stronę https://incydent.cert.pl/

Telefon od pracownika banku — prośba o weryfikację przelewu

Cześć, jestem Bartek i dałem się nieźle wrobić! Odebrałem kiedyś telefon z banku z prośbą, żebym zweryfikował przelew na kwotę 1500 zł.

Zbladłem, gdy to usłyszałem, bo nie robiłem takiego przelewu. Konsultant – jeszcze wtedy myślałem, że naprawdę nim był - powiedział, że w takim razie prawdopodobnie oszuści próbowali ukraść pieniądze z mojego konta. Spanikowałem. **Konsultant zaproponował, że powie mi, co mam zrobić i jak mogę ochronić pieniądze na koncie.**

Bartek, 43 lata

Co zrobiłem?

Oczywiście, że się zgodziłem. Konsultant zapytał o **pewną aplikację,** dzięki której dział techniczny może sprawdzić mój telefon pod kątem wirusów. Twierdził, że powinienem mieć tę aplikację, bo tak wskazuje regulamin banku. Nie miałem jej, więc musiałem zainstalować.

Co się stało?

Niestety nie wiedziałem tego wcześniej, ale gdy odpaliłem tę aplikację, dałem oszustom wgląd do swojego telefonu. Od tej chwili widzieli dokładnie to samo co ja. Mogli zdalnie sterować moim telefonem i wykonywać różne działania. Zrobili sobie przelew na wysoką kwotę. Tak, chcąc ochronić swoje pieniądze, tylko je straciłem.

Jeśli w trakcie rozmowy konsultant poprosi Cię o dane do logowania, zainstalowanie jakiejś dodatkowej aplikacji, podanie kodu autoryzacyjnego lub kodu BLIK — **nie rób tego.**

Ten rodzaj oszustwa to vishing

Oszuści dzwonią i podszywają się m.in. pod banki, przedstawicieli różnych służb, np. policji, czy pracowników ochrony zdrowia. Mogą również podawać się za członków rodziny, np. wnuczka.

13% badanych spotkało się z vishingiem.

Cechy charakterystyczne:

- **oszust dzwoni do Ciebie,**
- **wyświetla Ci się numer,** taki sam jak numer danej instytucji,

i Spoofing

- **ktoś wzbudza w Tobie poczucie zagrożenia, niepokoju** (np. "prawdopodobnie" doszło do próby oszustwa, ktoś oferuje Ci pomoc),
- **oszust zachęca Cię do instalacji aplikacji lub podania poufnych danych,** takich jak dane do logowania lub kody autoryzacyjne operacji.

Co robić, gdy spotka Cię podobna sytuacja?

- **Rozłącz się i zadzwoń do banku** — wyjaśnij sytuację.
- **Nie podawaj nigdy swoich danych do logowania ani innych poufnych danych.**
- **Nie instaluj żadnych dodatkowych aplikacji** (innych niż oficjalne aplikacje banku).
- **Zgłoś próbę oszustwa do banku.**

Fałszywa strona logowania do banku

Wchodzisz na stronę bankowości internetowej z wyszukiwarki? Nie rób tego. Jestem Ewa i powiem Ci, jak w ten sposób straciłam pieniądze. Chciałam zalogować się na stronę swojego banku. Nie wiem, dlaczego tym razem skorzystałam z wyszukiwarki. Mogłam - jak zwykle - wejść z adresu, który mam zapisany w przeglądarce, albo po prostu wpisać adres banku. Wtedy jednak wpisałam nazwę banku w wyszukiwarce i kliknęłam pierwszy link.

Co zrobiłam?

Nie sprawdziłam adresu strony i nie zwróciłam uwagi na to, że link był oznaczony jako reklama. Kliknęłam, weszłam na stronę banku (niestety, nie zwróciłam uwagi na detale!). Zalogowałam się loginem i hasłem. Całość zatwierdziłam kodem z SMS-a z banku.

Co się stało?

Strona była sfałszowana. Gdy podałam swoje dane do logowania, trafiły one prosto w ręce oszustów. Tak straciłam pieniądze.

Oszuści czyhają w mediach społecznościowych. **Często fałszywe strony są ukryte pod szokującymi informacjami, zbiórkami, ankietami**, za które oferują nagrodę.

Ten rodzaj oszustwa to fałszywe reklamy

Oszuści wykorzystują naszą nieuwagę, pośpiech i przyzwyczajenie. Fałszywe strony wyglądają niemal identycznie jak oryginalne. **Czasem jedyną różnicę znajdziesz w adresie strony.** Przyjrzyj się dokładnie – fałszywa strona ma inny adres niż oficjalny adres strony logowania banku.

Cechy charakterystyczne:

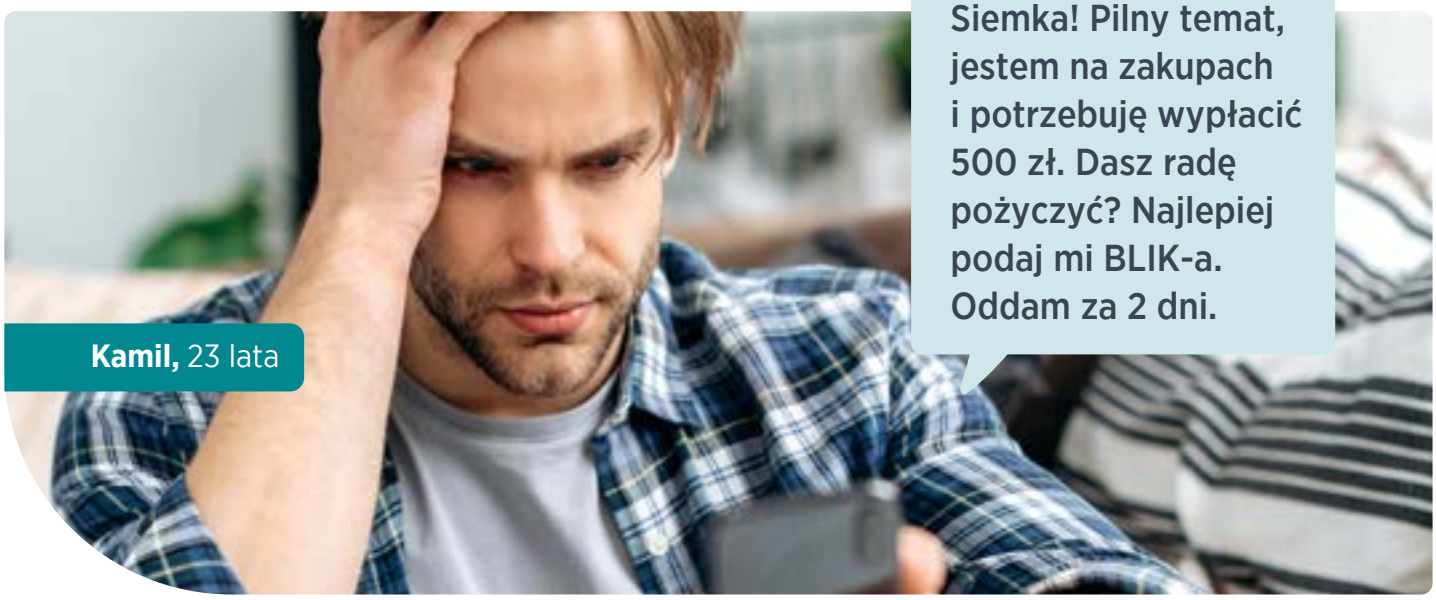
- strona **wyświetla się w wyszukiwarce jako „reklama”**,
- wygląda niemal identycznie jak oryginalna strona, różnicę możesz znaleźć jedynie w **adresie strony, czasem w błędach językowych w treści.**

Co robić, gdy spotka Cię podobna sytuacja?

- Nie wyszukuj strony logowania do banku w wyszukiwarce internetowej. **Oszuści często wykupują miejsca reklamowe**, aby wyświetlać się jak najwyżej w wynikach wyszukiwania.
- Wpisz ręcznie adres strony logowania swojego banku lub wybierz ją z zapamiętanych w przeglądarce stron.
- Na stronie logowania banku, zanim wpiszesz login i hasło, **upewnij się, że adres jest taki, jaki znasz. Bez literówek.**
- **Oszuści podrabiają też strony sklepów internetowych i innych firm.**
- **Jeśli trafisz na fałszywą stronę - zgłoś ją:**
  - do firmy, pod którą podszywają się oszuści,
  - do CERT Polska na stronie: **https://incydent.cert.pl/.**

Wiadomość od kolegi z prośbą o BLIK

Hej, jestem Kamil i dałem się oszukać. Myślałem, że na takie haczyki łapią się tylko starsi ludzie. Z pewnością nie ja. A jednak...
Dostałem wiadomość od znajomego.



Co zrobiłem?

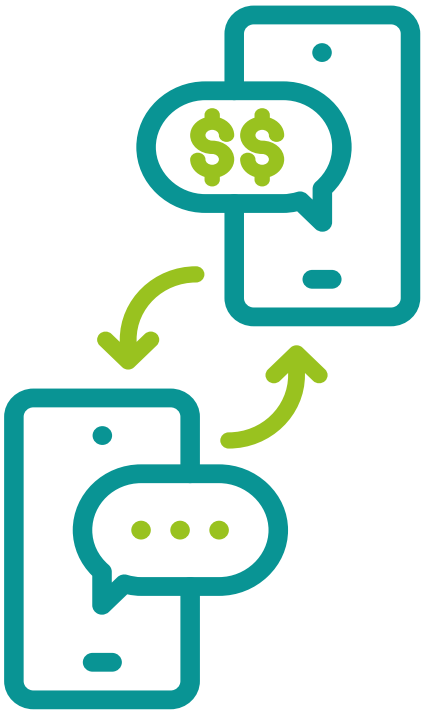
Znamy się, lubimy, więc **bez wahania wyklikałem kod BLIK**, podałem mu i zaakceptowałem wypłatę gotówki z bankomatu. Proste! Jak nie pomóc koledze w potrzebie?!

Co się stało?

Okazało się, że **wiadomość wysłali oszuści, którzy przejęli konto społecznościowe mojego kolegi**. To im przekazałem kod BLIK i oni przejęli kasę z bankomatu.

Ten rodzaj oszustwa to wyłudzenie przez BLIKA

Ta metoda oszustwa staje się dość popularna. **Oszuści potrafią kontynuować rozmowę, która już trwa.** Oszust zwykle prosi o niewielką pożyczkę i zapewnia, że odda jak najszybciej. Wskazuje na pilną potrzebę czy awaryjną sytuację, np. „Chyba coś mi w banku zablokowali".



Operacji z użyciem kodu BLIK nie możesz cofnąć.
Zawsze upewnij się, co dokładnie zatwierdzasz i czy faktycznie pomagasz znajomemu.

Cechy charakterystyczne:

- dostajesz wiadomość **na dowolnym komunikatorze,** może to być nawet kontynuacja jakiejś prawdziwej rozmowy,
- oszust podszywa się pod **osobę, którą znasz**,
- prosi o **niewielką pożyczkę**,
- **podkreśla pilność sytuacji** — np. „Jestem na zakupach i nie chce mi przejść płatność kartą. Pożyczysz? Oddam Ci później”,
- **rozmowa toczy się w naturalny sposób,** co nie wzbudza Twoich podejrzeń.

Co robić, gdy spotka Cię podobna sytuacja?

- **Zadzwoń do swojego znajomego** i upewnij się, że on faktycznie potrzebuje pożyczki.
- **Nie podawaj kodu BLIK** przez żaden komunikator.
- **Profil znajomego zgłoś** do portalu jako przejęty przez oszustów. Dokładne informacje jak to zrobić, znajdziesz w danym serwisie – poszukaj zakładki „Pomoc” lub „Kontakt”.

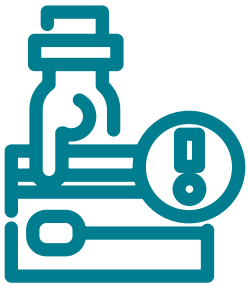
Chroń się w sieci — Twoja lista bezpieczeństwa

- **Sprawdź link, zanim w niego klikniesz** (np. w mejlu najedź kursorem myszki na podlinkowany element i sprawdź, czy adres wygląda poprawnie).
- Kiedy ktoś prosi Cię o pieniądze w wiadomości - **zawsze upewnij się, czy to Twój znajomy lub znajoma. Zadzwoń!**
- **Nie klikaj w linki w SMS-ach.**
- **Sprawdzaj dokładnie adresy stron i adresy mejlowe.**
- **Upewnij się, z kim rozmawiasz** — szczególnie kiedy ktoś prosi o Twoje poufne dane.
- Nie wierz w oferty, które obiecują **szybkie wzbogacenie się lub gwarantują zysk.**
- **Jeśli ktoś podaje się za pracownika banku albo innej instytucji — potwierdź to.** Rozłącz się i zadzwoń na infolinię tej firmy.
- Do swojego banku **loguj się zawsze z adresu, który masz zapisany w przeglądarce internetowej** albo po prostu wpisz adres samodzielnie (to najbardziej bezpieczne).
- **Chroń dostęp do swojego telefonu** — ustaw kod PIN, wzór, odcisk palca lub skan twarzy.
- Zanim potwierdzisz coś kodem z SMS-a albo w aplikacji bankowej, **dokładnie przeczytaj wiadomość. Upewnij się, co zatwierdzasz!**
- **Jeśli czegoś nie rozumiesz, nie wiesz, jak działa albo jakie mogą być skutki - to nie rób tego. Porozmawiaj z kimś bliskim i zaufanym.**
- **Czytaj komunikaty o bezpieczeństwie**, które wysyła Twój bank.

Część 2

W dzisiejszym świecie technologia przenika wszystkie aspekty naszego życia. **Rośnie liczba przestępstw internetowych, dlatego cyberprzestępczość staje się coraz większym zagrożeniem.** Z roku na rok wzrasta również liczba użytkowników internetu oraz dynamicznie rozwija się działalność online.

Powstaje coraz więcej nowych e-commerce'ów oraz usług finansowych świadczonych przez internet. To wszystko daje większe możliwości cyberprzestępcom, których działania dotykają zarówno osoby prywatne, jak i przedsiębiorstwa.



Jak podaje Związek Banków Polskich zaledwie w I kwartale 2024 roku odnotowano aż **3 069 prób wyłudzeń danych** i zaciągnięcia kredytu na cudzą tożsamość. Łączna kwota, na którą próbowano zaciągnąć kredyt wyniosła **82,9 mln zł**[1].

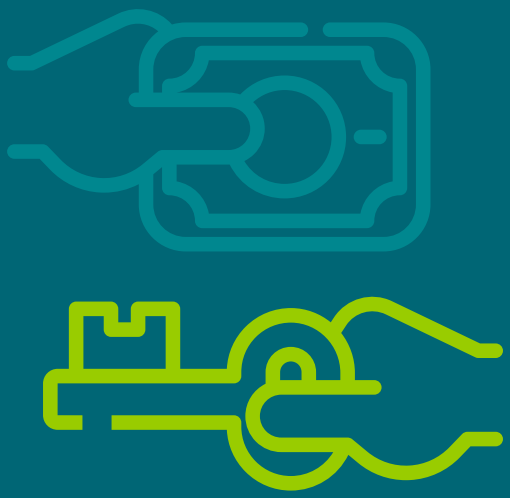
i

CERT Polska działa w ramach NASK od 1996 roku.
Jego zadaniem jest **monitorowanie zagrożeń oraz reagowania na zgłaszane incydenty**. CSIRT NASK pełni swoją funkcję w ramach Krajowego Systemu Cyberbezpieczeństwa.

[1] https://zbp.pl/Aktualnosci/Wydarzenia/Konferencja-prasowa-Raport-InfoDOK-I-kw-2024)

W 2024 liczba oszustw nadal rośnie. Oszuści coraz częściej wykorzystują sfałszowane nagrania audio i wideo, co może prowadzić do dezinformacji i manipulacji.

Wynika to m.in. z ciągłego rozwoju technik deepfake.



Poważne zagrożenie nadal stanowią ataki ransomware — nie tylko dla firm, ale także dla indywidualnych użytkowników. W wyniku takiego ataku cyberprzestępcy mogą przechwycić dane wrażliwe klientów firmy, co bezpośrednio przekłada się na bezpieczeństwo prywatnych użytkowników.

W Credit Agricole przeprowadziliśmy własne badanie o cyberbezpieczeństwie. **Zapytaliśmy 1 492 osoby**[2] o ich doświadczenia z oszustwami internetowymi i wiedzę o cyberzagrożeniach.

Na kolejnych stronach prezentujemy wyniki i wnioski z tego badania.

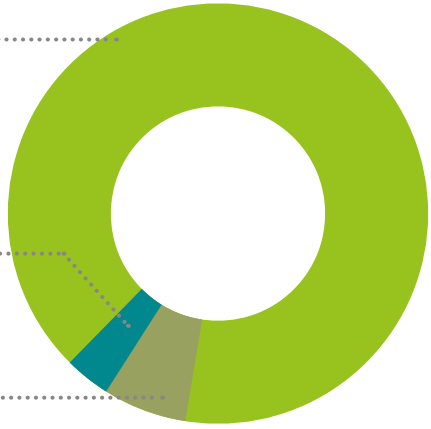
[2] Badanie CAWI realizowane na Panelu Internetowym Ariadna, N=1492 osób w wieku 16+, styczeń 2024

Załatwianie spraw przez internet

Co najczęściej załatwiasz przez internet (online):

94% badanych załatwia różne sprawy przez internet. Najczęściej korzysta z banku, robi zakupy (bilety, elektronika, odzież) i załatwia sprawy urzędowe.

Czy załatwianie spraw przez internet jest bezpieczne:

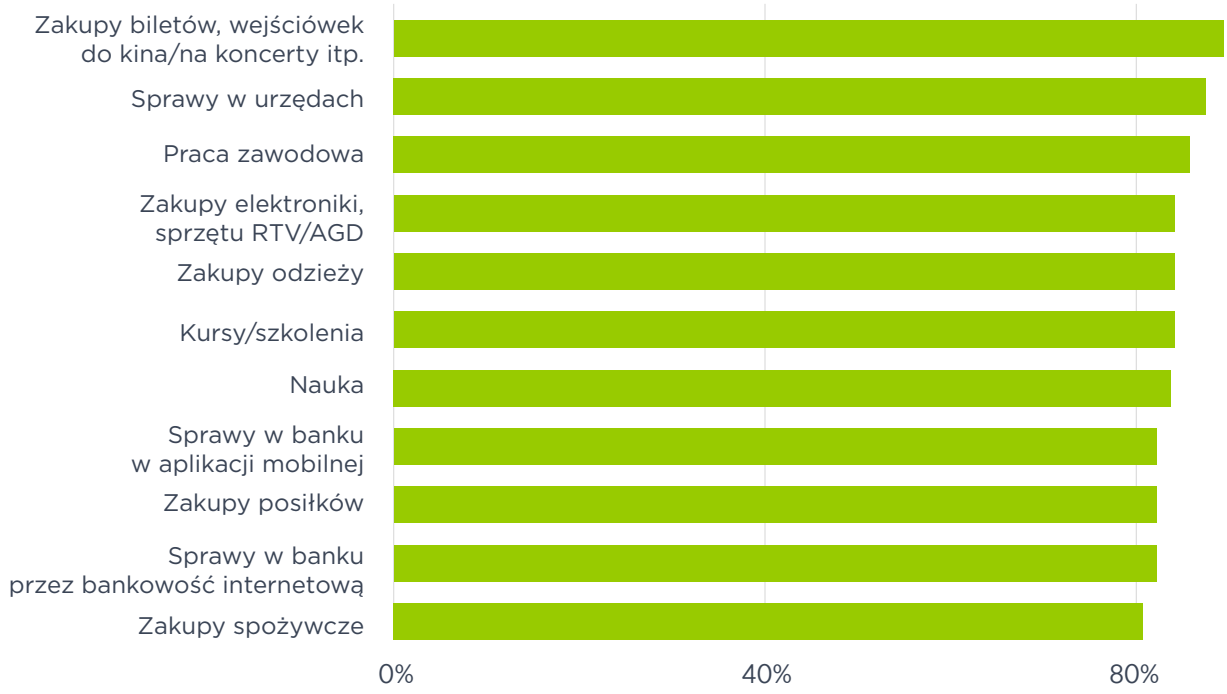


83%
Tak (zdecydowanie tak/raczej tak)

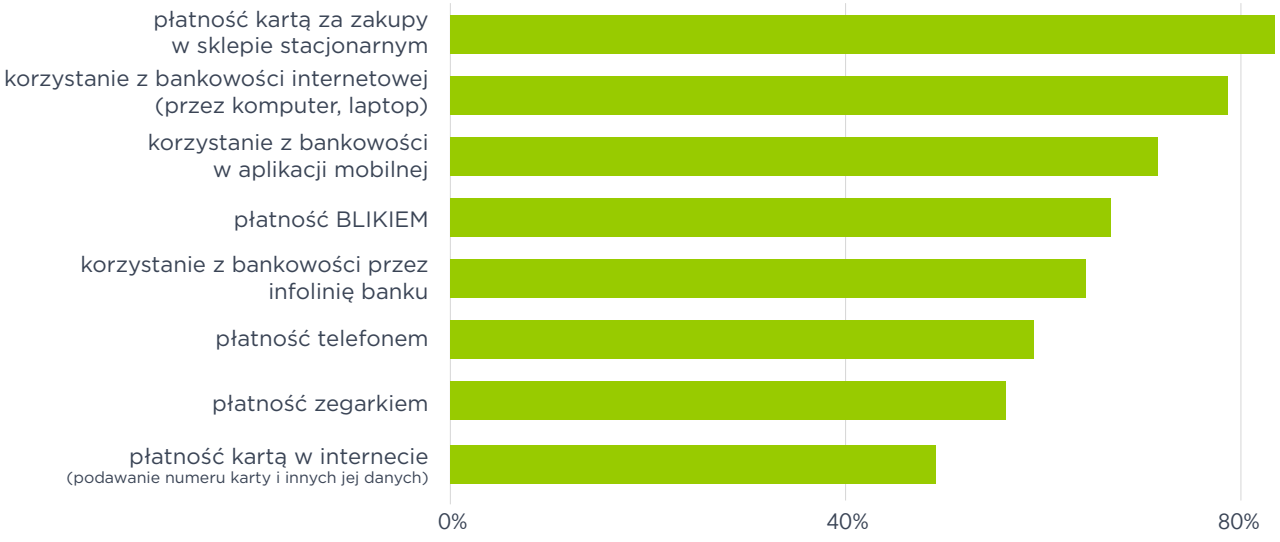
6%
nie

11%
Nie wiem/Trudno mi to ocenić

Czuję się bezpiecznie, załatwiając te sprawy przez internet (zdecydowanie/raczej bezpiecznie):



Uważam, że taka forma kontaktu z bankiem jest bezpieczna: (zdecydowanie/raczej bezpiecznie):



Badani oceniają, że załatwianie spraw przez internet jest bezpieczne. Najwięcej obaw budzi płatność kartą w internecie i płatność zegarkiem.

Platformy zakupowe

Czy sprzedajesz rzeczy przez platformy zakupowe?

59% Tak

41% Nie

Jakie platformy?

39% OLX

30% Vinted

27% Allegro

5% AliExpress

2% Temu

1% Inne

Odpowiedź „Tak" według wieku badanych

74% 16 - 25 lat

73% 26 - 40 lat

58% 41 - 55 lat

32% 56 - 75 lat

Czy kupujesz rzeczy przez platformy zakupowe?

91% Tak

9% Nie

Jakie platformy?

84% Allegro

45% OLX

28% Vinted

26% AliExpress

14% Temu

3% Inne

Odpowiedź „Tak" według wieku badanych

92% 16 - 25 lat

96% 26 - 40 lat

93% 41 - 55 lat

83% 56 - 75 lat

Sprzedawanie rzeczy w internecie jest popularne wśród osób młodszych, ale kupują już wszystkie pokolenia. Najpopularniejsze platformy to OLX, Vinted i Allegro.

Oszustwo w internecie – własne doświadczenia

Czy kiedykolwiek byłeś/aś oszukany/a w internecie?

31% Tak

- **14%** ale nie straciłem/am pieniędzy
- **17%** straciłem/am pieniądze

Odpowiedź według wieku badanych:

- **17%** 16 - 25 lat
- **15%** 26 - 40 lat
- **20%** 41 - 55 lat
- **15%** 56 - 75 lat

Czy ktoś z Twojego otoczenia został oszukany w internecie?

(rodziny, przyjaciół, znajomych)

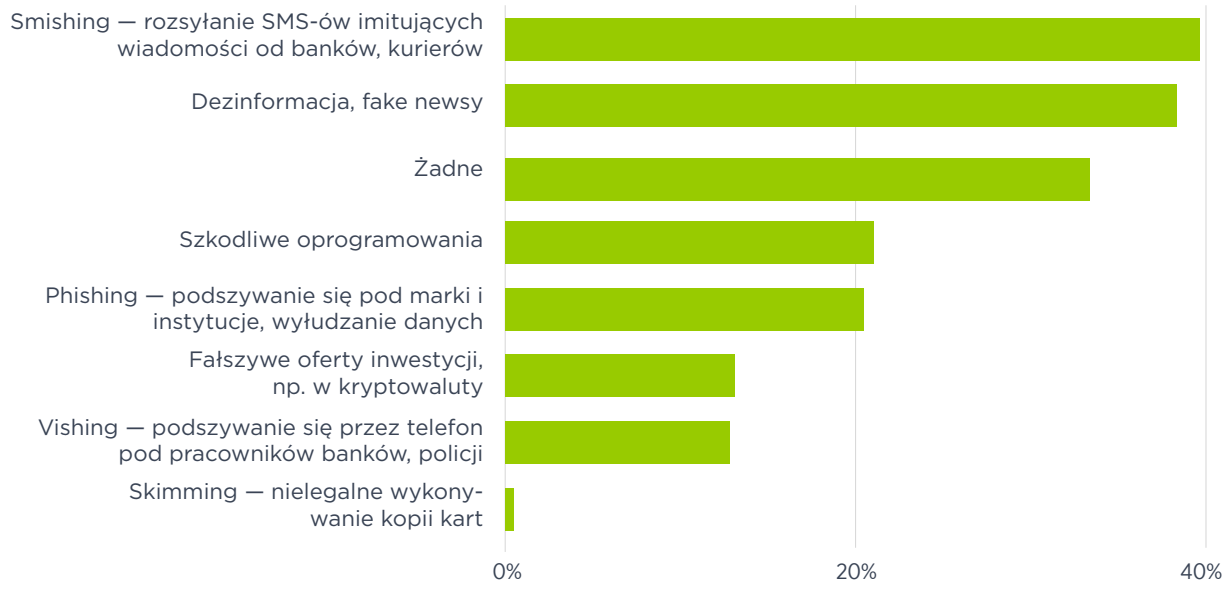
- **36%** Tak
- **32%** nie
- **32%** nie wiem

Odpowiedź według wieku badanych:

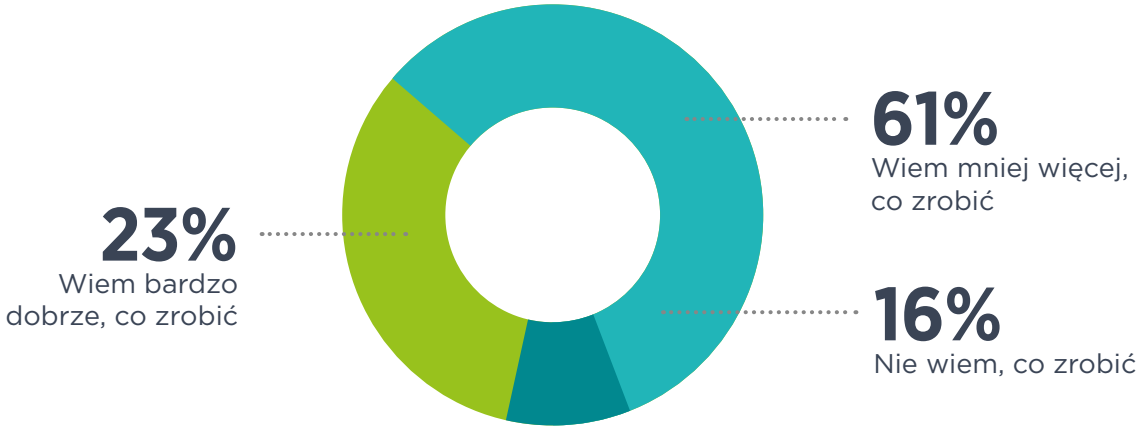
- **38%** 16 - 25 lat
- **40%** 26 - 40 lat
- **39%** 41 - 55 lat
- **27%** 56 - 75 lat

Niemal 1/3 badanych padła ofiarą oszustwa, cyberataku.
36% słyszało o tym, że ktoś z ich otoczenia padł ofiarą takich działań.
Ofiarą oszustwa były zarówno osoby starsze, jak i młodsze.

Którego z oszustw internetowych doświadczyłeś/ doświadczyłaś (także próby oszustwa)?



Czy wiesz, co zrobić, kiedy padniesz ofiarą oszustwa internetowego?



Tylko 33% badanych nie doświadczyło żadnej próby oszustwa czy cyberataku, co wskazuje na dużą styczność badanych z oszustwem lub jego próbą (67%). Najczęściej badani spotkali się ze smishingiem. Drugą najpopularniejszą formą były fake newsy i dezinformacja. Z kolei najrzadziej spotykanym przestępstwem wśród badanych był skimming (4%).

Opinia na temat zagrożenia cyberatakami

W dzisiejszych czasach zagrożenie oszustwami internetowymi, cyberatakami jest:

42%

Bardzo duże
(...jest to poważny problem)

Odpowiedź według wieku badanych:

- 39% 16 - 25 lat
- 45% 26 - 40 lat
- 40% 41 - 55 lat
- 43% 56 - 75 lat

46%

Raczej duże
(jest to problem)

Odpowiedź według wieku badanych:

- 45% 16 - 25 lat
- 41% 26 - 40 lat
- 52% 41 - 55 lat
- 46% 56 - 75 lat

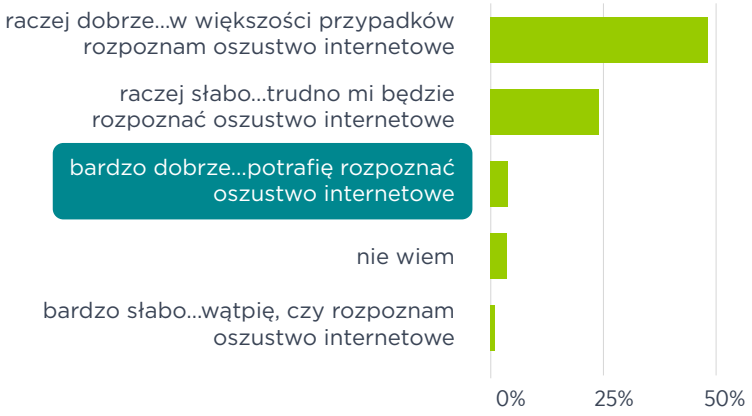
6% **Raczej małe**
(nie jest to poważny problem)

1% **Bardzo małe**
(nie jest to żaden problem)

Badani oceniają, że zagrożenie cyberatakami i oszustwami internetowymi jest duże lub bardzo duże.

Wiedza badanych na temat oszustw

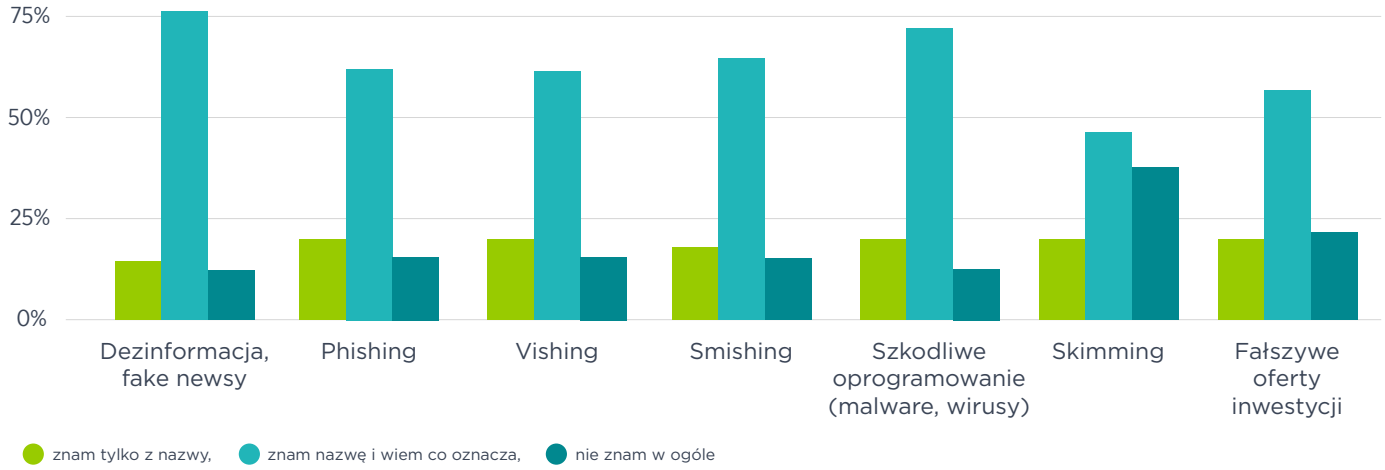
Jak oceniasz swoją wiedzę na temat oszustw internetowych:



Odpowiedź na pytanie „bardzo dobrze, potrafię”

- **20%** 16 - 25 lat
- **13%** 26 - 40 lat
- **10%** 41 - 55 lat
- **4%** 56 - 75 lat

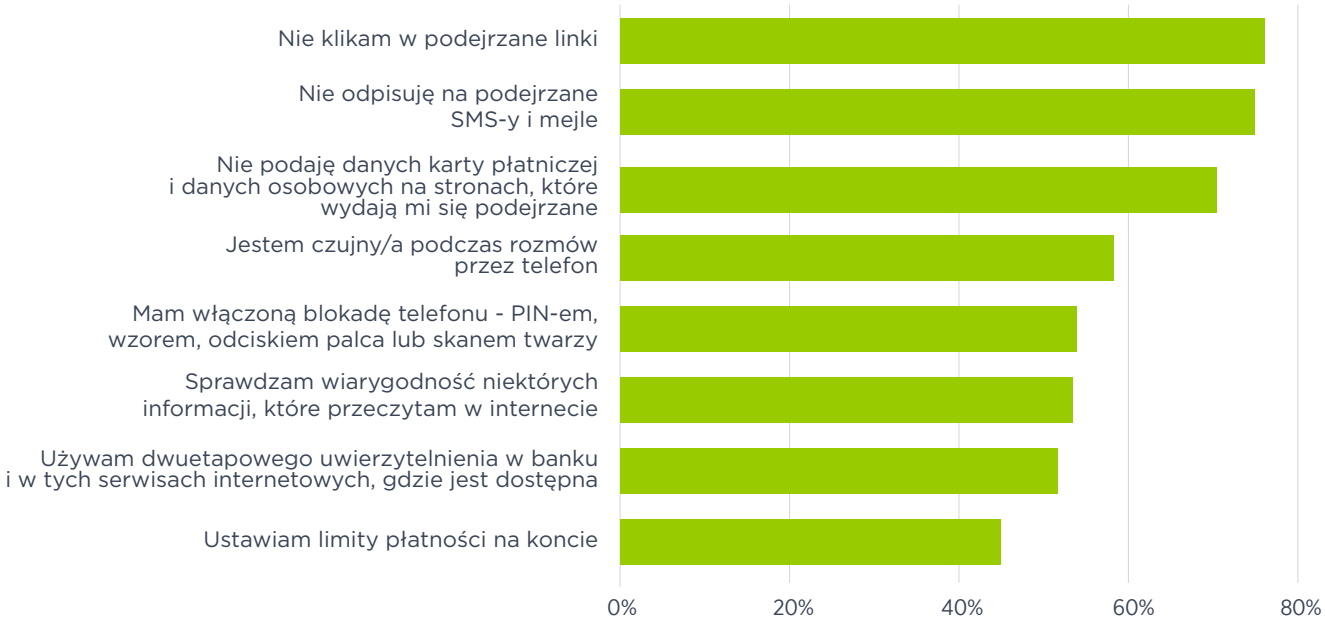
Jakie znasz oszustwa internetowe?



Badani całkiem dobrze oceniają swoją wiedzę na temat oszustw internetowych.

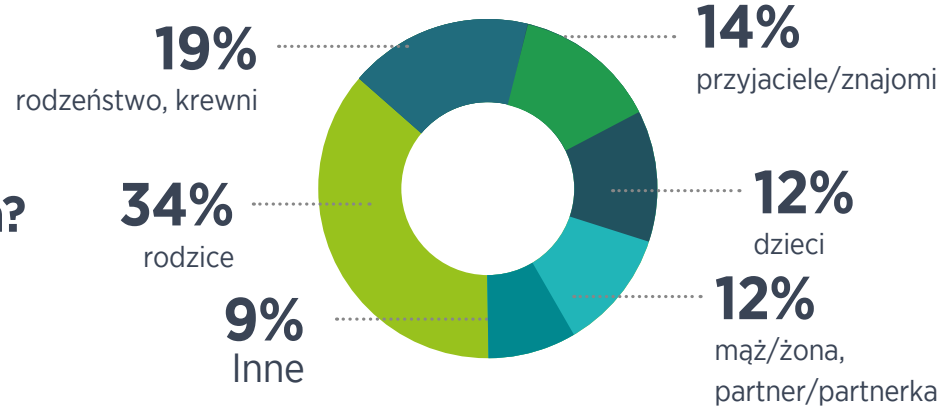
Bezpieczeństwo w internecie

W jaki sposób dbasz o bezpieczeństwo w internecie?

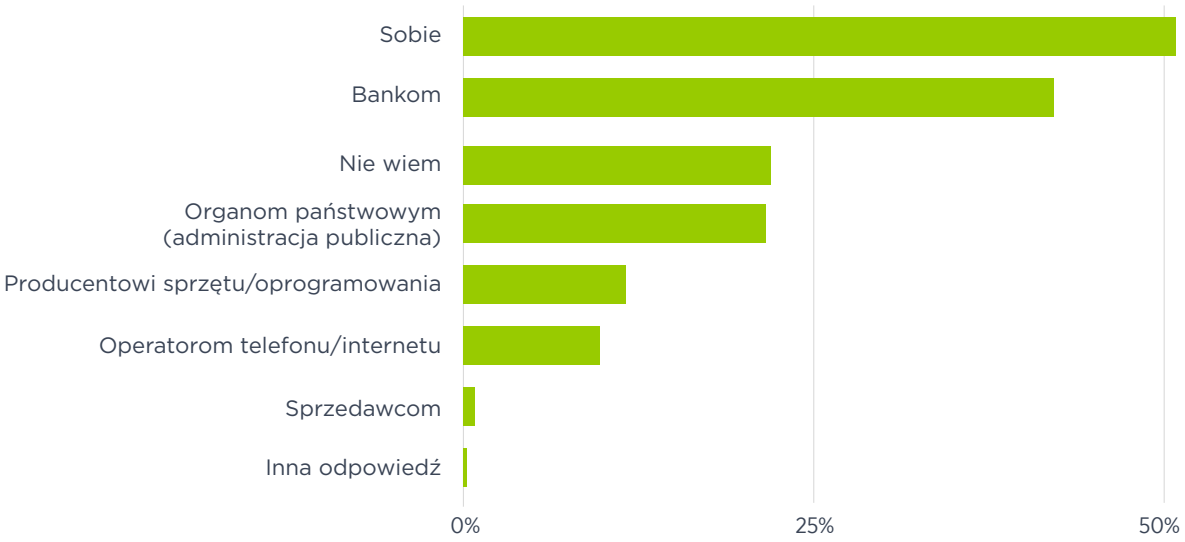


Najczęściej stosowaną metodą obrony przed oszustwami internetowymi jest unikanie klikania w podejrzane linki. Badani nie odpisują również na podejrzane SMS-y i mejle (74%) oraz nie podają danych karty płatniczej i danych osobowych na tych stronach, które wydają im się podejrzane.

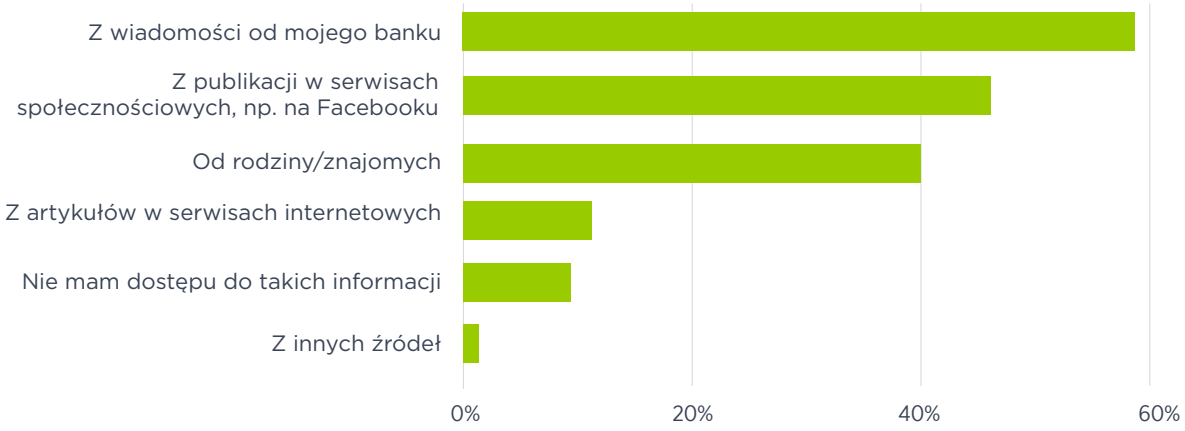
Z kim rozmawiasz na temat bezpieczeństwa?



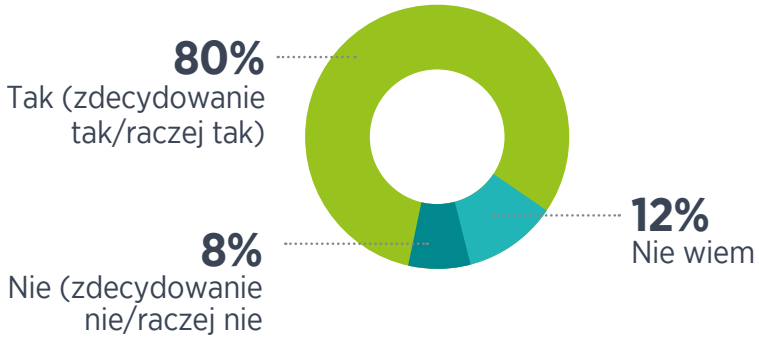
Kto według Ciebie najlepiej dba o cyberbezpieczeństwo? Komu najbardziej ufasz w tym zakresie?



Skąd czerpiesz informacje na temat bezpieczeństwa w internecie, cyberzagrożeń, sposobów ochrony przed nimi itd.?



Czy chcesz, żeby Twój bank dostarczał Ci informacji o cyberbezpieczeństwie?



Podsumowanie i wnioski z badań

Użytkownicy często załatwiają sprawy przez internet (94%), także bankowe — zwłaszcza pokolenia Y, X i Silver. Dlatego cyberbezpieczeństwo w bankowości jest kluczowe dla osób badanych.

Większość osób, które korzysta z internetu uważa, że **załatwianie spraw online jest raczej lub bardzo bezpieczne**, podobnie jak zdalny dostęp do bankowości. Większość niebezpośrednich form kontaktu z bankiem również oceniana jest jako bezpieczna.

Najwięcej wątpliwości budzi płacenie telefonem lub zegarkiem, a **największe obawy dotyczą podawania danych karty w internecie.**

Blisko 1/3 badanych została oszukana w internecie, a 36% zna kogoś, kto doświadczył takiego cyberataku. Jest to dużo, biorąc pod uwagę deklaracje badanych o bezpieczeństwie załatwiania spraw online (83%), co może wskazywać na większą potrzebę edukacji w temacie oszustw internetowych.

Ponad 80% internautów uważa, że zagrożenie cyberatakami jest duże lub bardzo duże.

Badani wierzą, że potrafią sami obronić się przed cyberatakami. Ponad połowa ocenia swoją wiedzę na temat oszustw internetowych jako dobrą, a młodsze pokolenia są bardziej pewne swoich umiejętności. Znają typy oszustw i twierdzą, że potrafią je rozpoznać.

Badani traktują oszustwa internetowe jako część rzeczywistości, z którą muszą się zmierzyć i przed którą muszą się nauczyć bronić, zamiast jej unikać. **Największe zaufanie w kwestii bezpieczeństwa w sieci mamy do siebie samych, na drugim miejscu plasują się banki.**

Banki są uważane za bezpieczne w kontekście cyberzagrożeń – **78% badanych uważa, że ich bank dobrze dba o ich bezpieczeństwo** i chroni przed oszustwami.

Jedynie **35% osób rozmawia o zagrożeniach i oszustwach internetowych** z rodziną lub przyjaciółmi, mimo że wiele osób ocenia te zagrożenia jako duże.

Ufanie sobie w kwestii cyberbezpieczeństwa to pozytywny znak, ale **użytkownicy mimo wszystko liczą na wsparcie od banków**. Oczekują pomocy, która obejmuje dostarczanie informacji, porad i wsparcia w sytuacjach awaryjnych.

Zakończenie

Mimo że większość użytkowników ma pozytywne zdanie o bezpieczeństwie w sieci, niemal jedna trzecia z nich doświadczyła oszustwa lub cyberataku. Wskazuje to na realne zagrożenia. Jednocześnie **cyberprzestępcy stale udoskonalają swoje techniki i dążą do tego, aby oszustwa jak najbardziej przypominały realne sytuacje.**

Wykorzystują coraz to nowsze technologie (m.in. AI, deepfake), co może nasilać zagrożenia i utrudniać ich rozpoznawanie. Z drugiej strony rozwój technologii może być również sprzymierzeńcem w walce z cyberprzestępcami.

Kluczowa w tym wszystkim jest edukacja siebie i innych na temat zagrożeń oraz sposobów ochrony. Niezwykle pomocnym źródłem mogą być rozmowy – z rodziną i przyjaciółmi – aby wzajemnie edukować się o różnych doświadczeniach i zdobytych informacjach.

Nie bez znaczenia jest także ścisła współpraca między bankami, organami ścigania i dostawcami z zakresu bezpieczeństwa.

Dbaj o swoje bezpieczeństwo online – zachowaj świadomość i czujność. Mamy nadzieję, że dzięki podanym wskazówkom unikniesz pułapek zastawionych przez oszustów internetowych!

Źródła

https://zbp.pl/Aktualnosci/Wydarzenia/Konferencja-prasowa-Raport-InfoDOK-I-kw-2024)

https://www.nask.pl/pl/aktualnosci/5379,CERT-Polska-krzyzuje-szyki-rosyjskim-szpiegom-a-przestepcom-psuje-biznes-Roczny-.html

https://www.nask.pl/pl/aktualnosci/5368,CERT-Polska-Liczba-oszustw-finansowych-w-internecie-alarmujaco-rosnie-Na-co-uwaz.html)

Bezpieczeństwo cyfrowe Polaków, Raport SMSAPI 2024

Badanie CAWI realizowane na Panelu Internetowym Ariadna, N=1492 osób w wieku 16+, styczeń 2024

CRÉDIT AGRICOLE

www.credit-agricole.pl/bezpieczenstwo