Jak nie dać się złapać cyberprzestępcy?

Przykłady i praktyczne rozwiązania

Wstęp

Metody oszustw cyberprzestępców zmieniają się z miesiąca na miesiąc, dostosowując się do otaczającej nas rzeczywistości i bieżących wydarzeń jak pandemia, inflacja czy wojna. Oszuści wykorzystują ludzkie emocje, niewiedzę oraz błędy poznawcze. Wiedzą, że nasz pośpiech, nieuwaga lub błędy systemu są ich sprzymierzeńcami. Właśnie dlatego trzeba mieć świadomość, że my również możemy paść ich ofiarą. W internecie, jak na drodze, musimy kierować się zasadą ograniczonego zaufania.

Świadomość niebezpieczeństw czyhających na nas w internecie zwiększa się z roku na rok. Pomagają w tym akcje nagłaśniane szeroko w mediach. Dobre i silne hasło, programy antywirusowe, czy regularna aktualizacja oprogramowania to elementy, o które dba już większość z nas. Jednak życie pokazuje, że nadal zdarzają się przypadki ofiar, które zostały wykorzystane przez oszustów.

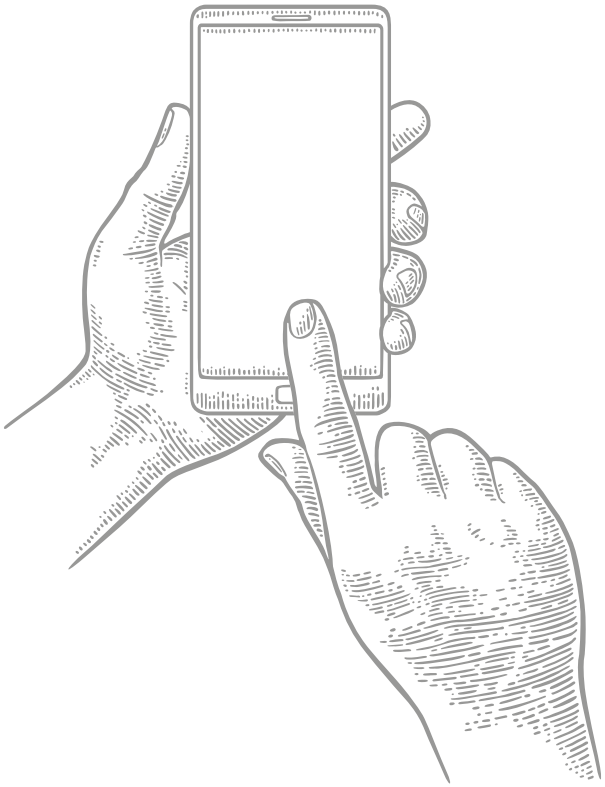
W tym e-booku przedstawiamy scenariusze popularnych oszustw internetowych, które mogły spotkać każdego. Dodatkowo do każdego scenariusza dołączony jest opis mechanizmu oszustwa oraz czytelne wskazówki, które powinny wzbudzić naszą czujność podczas codziennego surfowania w sieci.

01

Oszustwo w serwisie ogłoszeniowym

Oto Hania.

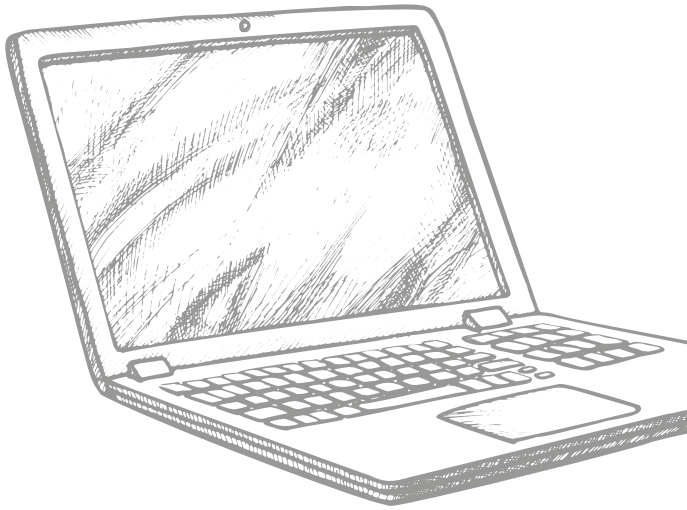
Hania postanowiła zrobić porządki w szafie i sprzedać niepotrzebną odzież i obuwie. Od koleżanki słyszała, że to łatwy sposób na pozbycie się rzeczy, a dodatkowo zarobienie kilku złotych. Hania przejrzała jak wyglądają inne ogłoszenia i zabrała się do akcji! Przygotowała rzeczy i wystawiła oferty w serwisie ogłoszeniowym. Po kilku minutach skontaktował się zainteresowany klient, który chciał kupić buty z ogłoszenia.

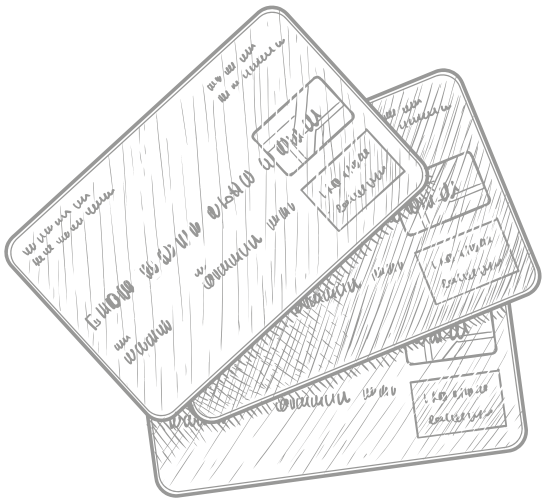


Otrzymała od niego wiadomość na komunikatorze internetowym. **Klient chciał szybko zapłacić przez opcję bramki płatności,** jednak w pierwszej kolejności prosił o podanie adresu e-mail Hani, aby serwis mógł wysłać potwierdzenie otrzymania środków za sprzedany przedmiot.

Dodatkowo, aby uwiarygodnić swoją prośbę, **wysłał screen z serwisu, gdzie wymagany jest adres e-mail sprzedawcy**. To świetna wiadomość – stwierdziła Hania, która nastawiała się na negocjacje i znacznie dłuższy proces sprzedaży.

Wysłała swój adres e-mail, a kupujący również ucieszył się z szybkiej odpowiedzi i zadeklarował złożenie zamówienia i natychmiastowe opłacenie. Hania otworzyła swoją skrzynkę e-mail i zobaczyła wiadomość od serwisu ogłoszeniowego – **nic nie wzbudziło jej podejrzeń,** ponieważ wiadomość wyglądała bardzo autentycznie. **Kliknęła w przycisk potwierdzający transakcję, aby otrzymać środki za sprzedany produkt.**

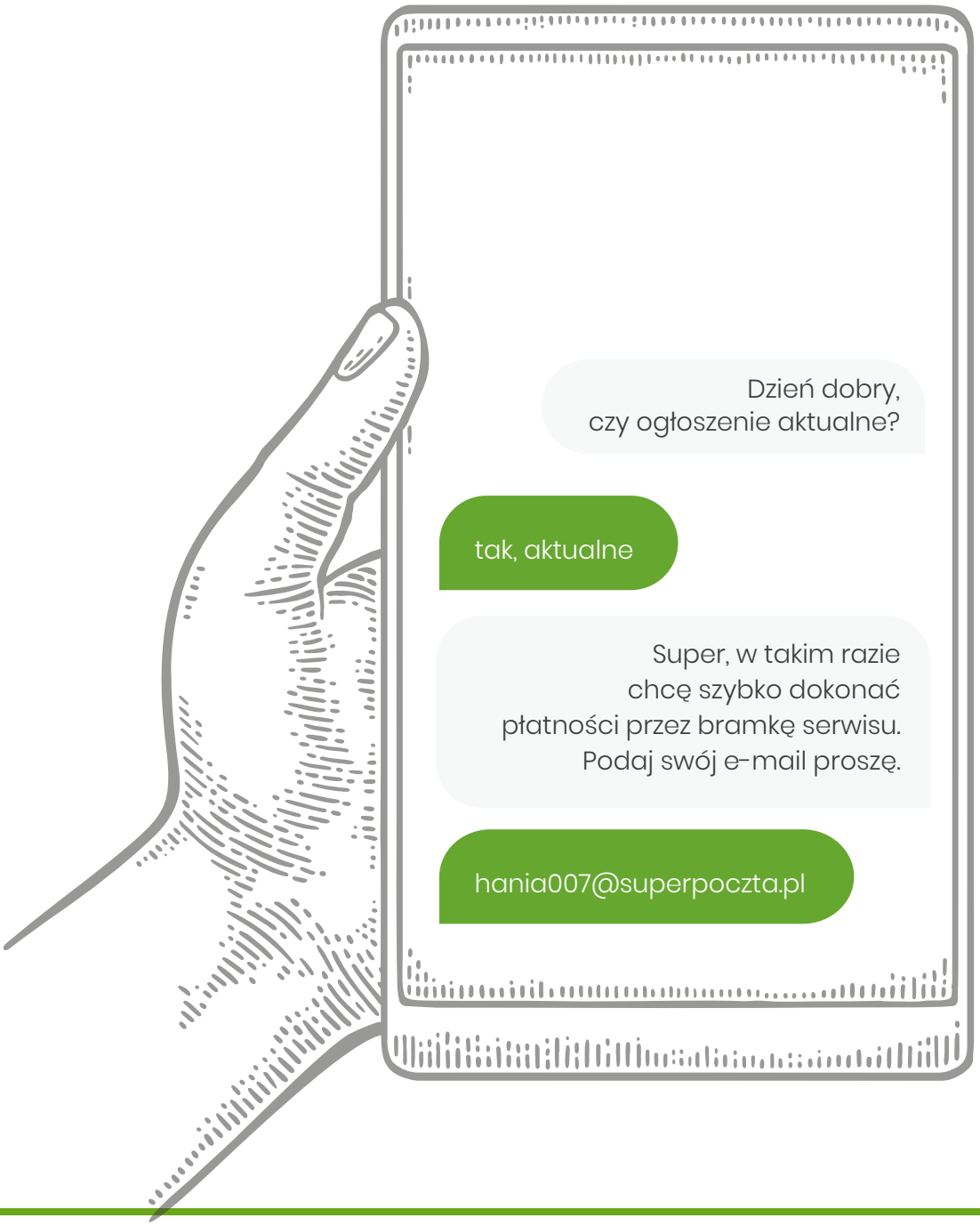




Została przekierowana do strony serwisu ogłoszeniowego, na której zobaczyła potwierdzenie sprzedaży produktu wraz z ceną oraz konieczność uzupełnienia danych do swojej karty płatniczej. **Wpisała numer karty, datę ważności oraz kod CVV,** a następnie zaakceptowała formularz, po chwili otrzymała screen z potwierdzeniem przelewu od kupującego. Hania zadowolona z szybkiej transakcji odłożyła telefon i poszła zrobić sobie kawę. Teraz pozostało tylko czekać na kontakt od kuriera, który odbierze paczkę – pomyślała Hania.

Po kilkunastu minutach siedząc wygodnie w fotelu z kawą, nasza bohaterka postanowiła wejść do swojej aplikacji bankowej i sprawdzić, czy pieniądze za sprzedane buty są już na jej koncie. Hania zalogowała się i serce jej stanęło... I to wcale nie z powodu dodatkowych środków, które miały wpłynąć. **Rachunek bankowy Hani był wyczyszczony do ZERA!**

Kubek z kawą wypadł jej z dłoni, a Hania czuła, że krew napływa jej do mózgu. Na myśl przychodziło jej tylko jedno pytanie: jak to się stało, że zostałam okradziona?



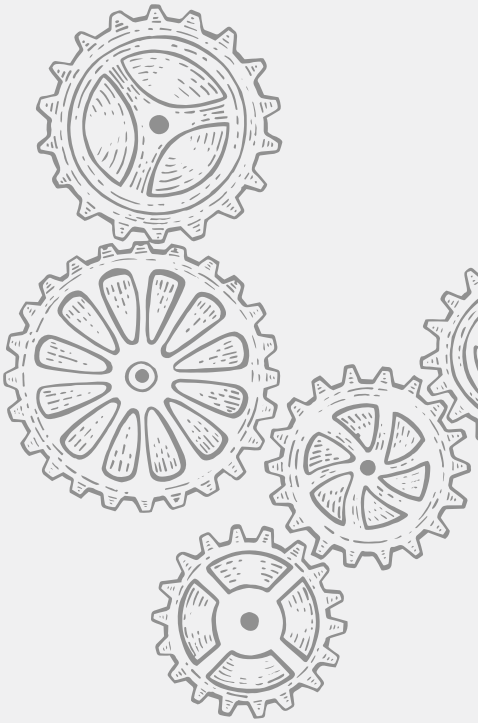
NO WŁAŚNIE, JAK TO SIĘ STAŁO, ŻE HANIA STRACIŁA WSZYSTKIE PIENIĄDZE?

Hania zaufała oszustowi i uwierzyła w jego dobre intencje. Nie pomyślała, że **ktoś może chcieć ją oszukać na transakcji za 25 zł.** Hania niby słyszała o **phishingu,** ale nie powiązała faktów, że może się to odbyć podczas sprzedaży.

Dla sprzedającej dowodami uwiarygodniającymi kupującego były screeny i e-mail, które graficznie były spójne z identyfikacją wizualną portalu ogłoszeniowego. Hania nie sprawdziła dodatkowych elementów, takich jak adres e-mail nadawcy, poprawność językowa treści czy adres URL strony, na której wpisywała dane do swojej karty bankowej. Co więcej, Hania nie miała wcześniej pojęcia, że **dane karty bankowej podajemy w przypadku kiedy chcemy w internecie za coś zapłacić, a nie otrzymać środki.**

MECHANIZM DZIAŁANIA OSZUSTÓW

Oszustwo **„na portal ogłoszeniowy”** ostatnio jest bardzo popularne. Minęły już czasy, gdy obawialiśmy się, że zakupy w internecie grożą otrzymaniem np. pustej paczki czy cegły, a nie zamawianego produktu. Chętnie kupujemy w serwisach ogłoszeniowych, ponieważ często są to transakcje szybkie oraz lokalne. Właśnie dlatego oszuści tak bardzo upodobali sobie ten sposób wyłudzania danych. To zjawisko nazywa się phishingiem.



Cyberprzestępcom zależy na danych dostępowych do konta bankowego lub innych istotnych informacji, jak np. PESEL, które umożliwiłyby im zaciągnięcie pożyczki lub kredytu w naszym imieniu. Często również tego typu oszustwo wiąże się z wyczyszczeniem konta za pomocą BLIKa. Metody cyberprzestępców w tym zakresie są bardzo „kreatywne”. Tworzone są strony, które podszywają się pod witryny serwisów sprzedażowych, czy też maile wyglądające bardzo podobnie do wiadomości, które mógłby nam wysłać portal, gdzie umieściliśmy ogłoszenie oraz potwierdzenia przelewu, a które trudno odróżnić od tych prawdziwych. Czasami **zdarza się, że oszust wysyła link do strony firmy kurierskiej,** co może uśpić czujność internauty, który słyszał o phishingu na portalach ogłoszeniowych. W ten sposób **wyłudzane są nie tylko dane do konta bankowego, ale również inne wrażliwe dane**, które dostaną się w niepowołane ręce i mogą być wykorzystane w późniejszym czasie.

CZERWONE FLAGI W TEJ SYTUACJI:

- **Szybki kontakt od kupującego i konieczność pilnej transakcji** - to powinno wzbudzić Twoją czujność, jednak nie zawsze jest to sygnał, że ktoś chce Cię oszukać. Sprawdź kolejne punkty, aby zweryfikować, czy transakcja na pewno będzie bezpieczna.

- **Przenoszenie konwersacji poza portal sprzedażowy** - tu powinna zapalić się czerwona lampka. Dlaczego komuś zależy, aby rozmawiać poza oficjalnym kanałem sprzedaży? Jednym z argumentów oszustów może być „szybsza wymiana wiadomości", jednak jeżeli komuś zależy na błyskawicznym sfinalizowaniu transakcji, to czy pozostanie chwile dłużej aktywnym w ramach portalu ogłoszeniowego jest aż takim dużym problemem? Przykładowo serwis OLX w ramach „przesyłek OLX" ostrzega, aby nie przenosić komunikacji poza ich aplikację.

- **Kliknięcie w linki do zewnętrznej płatności wysłane przez nieznajomego** - po wejściu na tego typu stronę zwykle widzimy bardzo dobrze przygotowaną witrynę, np. ścianki płatności, która ma uśpić czujność ofiary swoją autentycznością i profesjonalnym designem.

- **Podejrzany link** - oczywista zasada bezpieczeństwa w internecie to nieklikanie w linki od obcych. Jednak gdyby nic wcześniej nie wzbudziło naszych podejrzeń i wierzylibyśmy, że nie mamy do czynienia z oszustwem, warto zweryfikować adres URL strony wysłanej przez nieznajomego – czy nie posiada literówek oraz, czy jest w odpowiedniej domenie, która pasuje do oficjalnej witryny firmy. Pamiętajmy przy tym, że nawet gdy adres wydaje się w pełni poprawny, w dalszym ciągu możemy zostać oszukani. W innych alfabetach funkcjonują znaki do złudzenia przypominające znane nam litery, których użycie pozwoli przestępcy uzyskać zamierzony efekt wizualny, jednocześnie kierując internautę w zupełnie inne miejsce, niż sugerowałby to odnośnik.

- **Podejrzany adres e-mail** - podobnie jak wyżej, adres e-mail nadawcy może pomóc nam w weryfikacji, czy mamy do czynienia z oszustwem. Warto zwrócić uwagę na nietypowe znaki oraz domenę, z której została wysłana wiadomość.

- **Logowanie na stronach do rzekomych płatności, czy usług kurierskich** - sprzedając przez portale ogłoszeniowe nie musisz podawać swoich wrażliwych danych, a tym bardziej numeru do karty płatniczej. Pamiętaj, że jeżeli podasz dane do karty, to pieniądze zostaną z niej pobrane, a nie wpłacone. Transakcje kartą realizuj tylko w zweryfikowanych i zaufanych sklepach internetowych, a nie na przypadkowych stronach.

- **Zwracaj uwagę na język komunikacji** - oczywiście w internecie nieczęsto trafimy na purystów językowych w codziennych, szybkich konwersacjach. Jednak w przypadku pisania z potencjalnym kupującym na portalu ogłoszeniowym zwróć uwagę, kiedy osoba zainteresowana używa dziwnej polszczyzny, gdzie jest bardzo mało bezokoliczników oraz pojawiają się wyrazy wyłącznie w mianowniku. Według obserwacji serwisu Niebezpiecznik za wieloma tego typu atakami stoją się osoby rekrutowane zza granicy, które często nie są oszustami, a tylko pionkami w machinie prawdziwej siatki cyberprzestępczej.

- **Sprzedawca/kupujący z krótkim stażem** - oszustwo może dotyczyć obu stron, ale warto pamiętać, że cyberoszuści często mają krótki staż konta w danym serwisie.

CO ZROBIĆ W SYTUACJI, GDY PADLIŚMY OFIARĄ CYBERPRZESTĘPCY?

Przede wszystkim zachowaj spokój, chaotyczne działanie w nerwach w tej chwili nie pomoże. Bycie ofiarą oszusta to ogromny stres, natomiast trzeba zacząć działać szybko, aby zminimalizować straty. Wszystko zależy od tego, kiedy zidentyfikowaliśmy oszustwo.

01 **Jeżeli nabierzesz podejrzeń na pierwszych etapach transakcji** i uda Ci się zidentyfikować phishing, zanim przekażesz swoje dane, możesz zgłosić naruszenie na portalu ogłoszeniowym. Dzięki temu serwis będzie mógł szybko zareagować i zapobiec przyszłym kradzieżom przez tego użytkownika.

02 **W sytuacji, gdy przekazaliśmy swoje dane cyberprzestępcy,** trzeba jak najszybciej skontaktować się ze swoim bankiem i wydać dyspozycję blokady dostępu do pieniędzy na koncie. Jeżeli pieniądze nie zostały jeszcze przelane lub wykorzystane przez oszusta, to jest duża szansa, że procedury bankowe utrudnią mu działania. Dodatkowo każdą transakcję oszustów należy reklamować.

03 **W przypadku gdy nasz rachunek został już okradziony** ze środków, trzeba również zastrzec nasz dowód osobisty oraz wykupić usługę „Alerty BIK", dzięki której uniemożliwimy zaciąganie zobowiązań na nasze dane.

04 W następnej kolejności trzeba napisać **wiadomość do serwisu ogłoszeniowego,** że padliśmy ofiarą cyberprzestępcy.

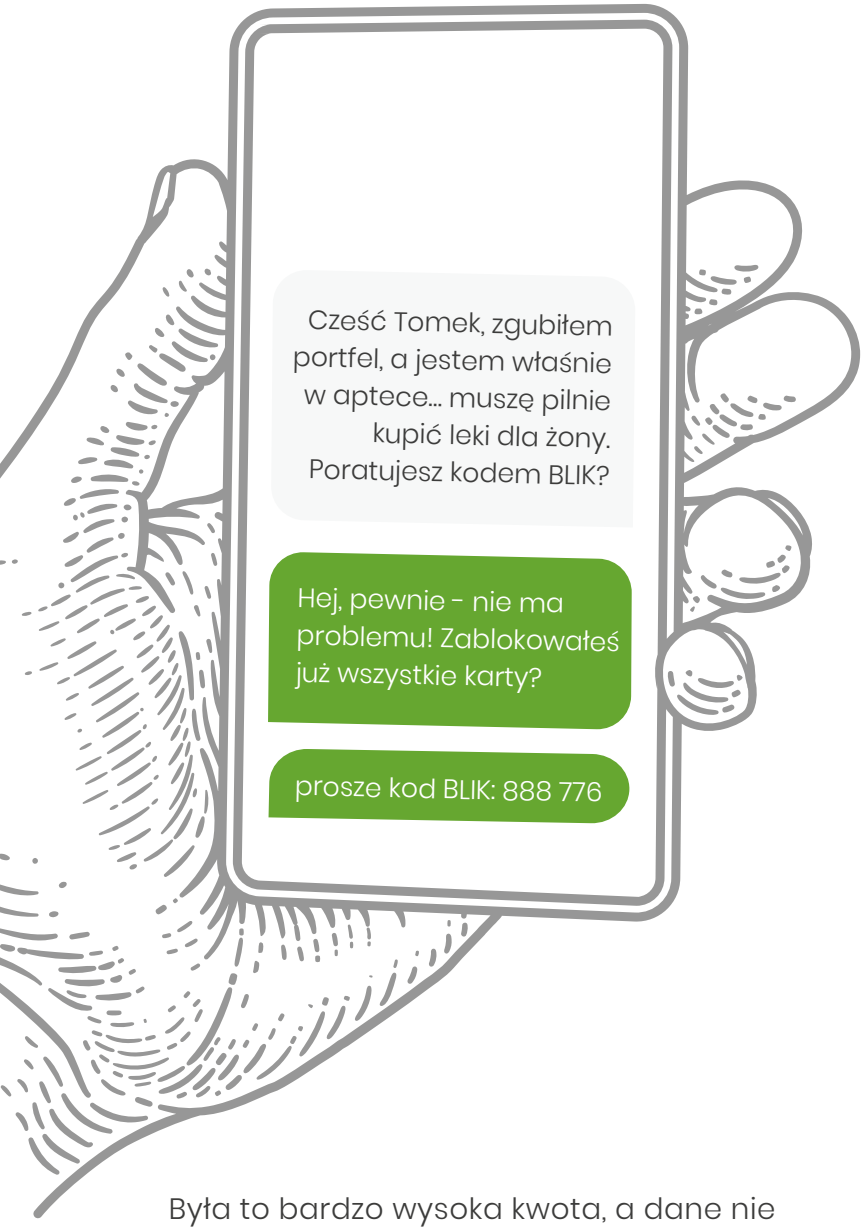
05 **Zgłoszenie na policję** będzie również obowiązkowe, w tej sytuacji konieczne jest natychmiastowe działanie. Praktycznie w całej Polsce policjanci znają tę metodę oszustwa.

02

Oszustwo na BLIK

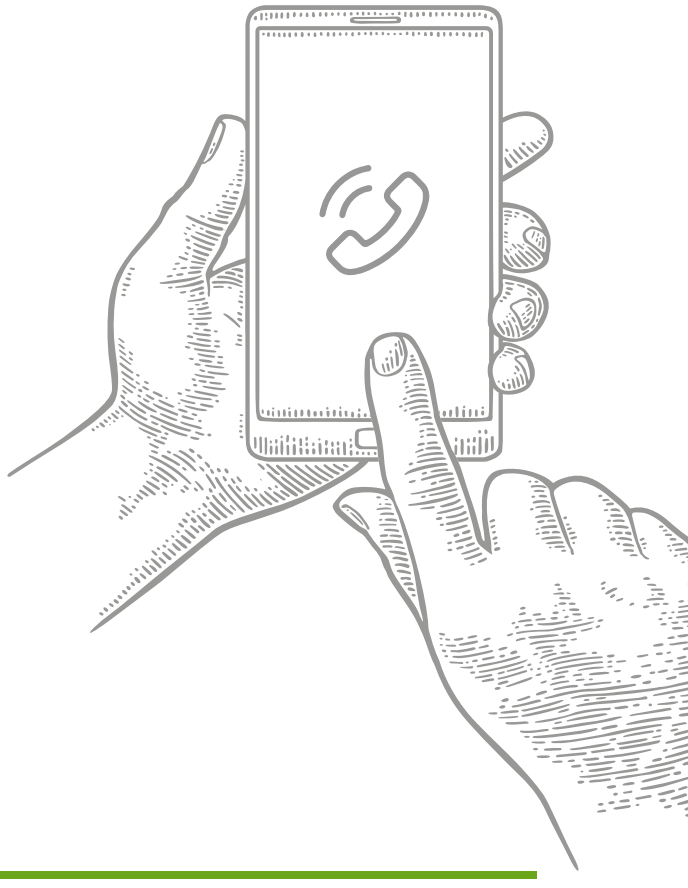
To jest Tomek.

Jest aktywnym internautą i użytkownikiem mediów społecznościowych. Ma dużą sieć znajomych i chętnie spędza wolny czas, scrollując na telefonie aplikacje popularnych platform. Tego typu serwisy są dla niego również kanałem kontaktu ze znajomymi, bardzo rzadko do nich dzwoni, a dzięki komunikatorom online będzie widział, czy odczytali wiadomość. żal znajomego i chętnie zaoferował swoją pomoc.



Znajomy o imieniu **Marek poprosił naszego bohatera o wygenerowanie kodu BLIK** w jego aplikacji bankowej i wysłanie mu go za pomocą komunikatora. Tomek bez wahania ruszył na pomoc! **Wysłał kod BLIK i bez zagłębiania się w szczegóły autoryzował transakcję.** Jednak Marek odpisał, że transakcja została odrzucona i potrzebuje kolejnego kodu. Tym razem po podaniu kodu Markowi podczas potwierdzania płatności w aplikacji, **Tomek zwrócił uwagę na kwotę i miejsce realizacji płatności.**

Była to bardzo wysoka kwota, a dane nie wskazywały na aptekę, tylko na bankomat w innym mieście... **Sprawa wydała się bardzo podejrzana.** Tomek postanowił zadzwonić do Marka i sprawdzić, czy na pewno to on potrzebuje tych pieniędzy. Okazało się, że **Marek jest w pracy i wcale nie zgubił portfela** ani nie pisał do kolegi w sprawie pieniędzy. Po odłożeniu słuchawki nasz główny bohater, który już czuł, że padł ofiarą przestępstwa, postanowił sprawdzić stan swojego rachunku bankowego. Podczas logowania do banku jego ręce drżały, wiedział już czego się spodziewać.
Z jego konta zniknęło 400 zł... Jak mogłem dać się tak wrobić - myślał Tomek i zastanawiał się, jak bardzo czujnym trzeba być w internecie.

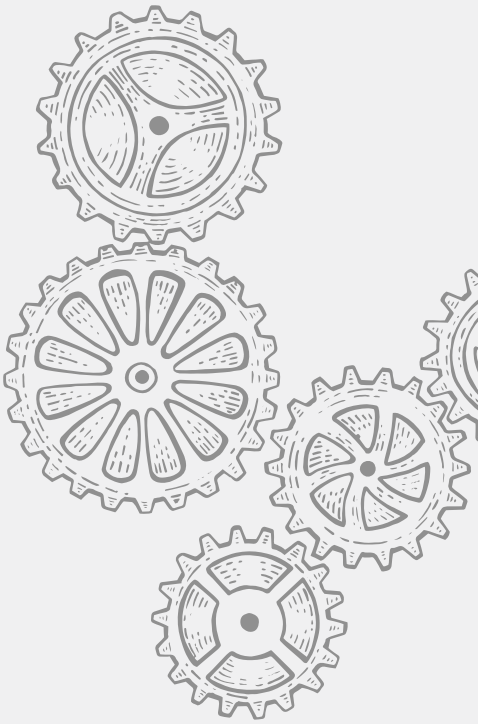


JAK TO SIĘ STAŁO, ŻE Z KONTA TOMKA ZNIKNĘŁO 400 ZŁ?

Tomek wierzył, że pisze do niego jego prawdziwy znajomy, wyszedł z założenia, że skoro wcześniej w komunikatorze widział historię ich poprzednich rozmów, to najpewniej niemożliwe jest, aby ktoś się pod niego podszywał. Nic bardziej mylnego. **Ofiara nie przewidziała, że oszust może uzyskać dostęp do profili w mediach społecznościowych poprzez ataki hakerskie lub wyciek danych**. Tomek nie kierował się zasadą ograniczonego zaufania w internecie i nie wzbudziła w nim podejrzeń niecodzienna prośba kolegi. Dodatkowo nasz bohater nie zweryfikował szczegółów transakcji w aplikacji bankowej podczas akceptowania płatności.

MECHANIZM DZIAŁANIA OSZUSTÓW

Cyberprzestępcy korzystają z wycieków haseł oraz posiłkują się atakami hakerskimi, aby uzyskiwać dostępy do różnych profili w mediach społecznościowych, które posiadają funkcje komunikatora. **Za pomocą wykradzionych danych oszust loguje się na konto i dzięki temu może się kontaktować ze znajomymi ofiary**. Co więcej, cyberprzestępcy bardzo często wcześniej przygotowują się do takiego ataku starając się poznać nawyki i język komunikacji osób, pod które się podszywają, aby być jak najbardziej wiarygodnym. Kiedy oszust uzyska już kod BLIK, najczęściej natychmiastowo wypłaca w bankomacie pieniądze z konta ofiary.



Powodów, których oszust podszywający się pod Twoją rodzinę lub znajomego, może wykorzystywać jest milion, m.in. **zgubiony portfel, szybka pożyczka, opłata zakupów w internecie itp.** Warto wiedzieć, że Ty, a właściwie Twój profil w mediach społecznościowych może być wykorzystany przez oszustów do wyłudzania kodów BLIK. Dlatego tak istotne jest odpowiednie zabezpieczenie swoich kont w internecie, np. poprzez włączenie dwuskładnikowego uwierzytelnienia, oraz kierowanie się zasadą ograniczonego zaufania.

Wyłudzenie kodu BLIK może przebiec również wg innego scenariusza. **Oszuści równie często podszywają się pod pracowników banku** i dzwonią do ofiary z informacją, że została wykryta próba zaciągnięcia pożyczki na rachunek danej osoby. Cyberprzestępca pod płaszczykiem pracownika banku prosi o weryfikację tożsamości poprzez podanie danych szczegółowych o rachunku bankowym, a następnie wygenerowanie kodu BLIK, który miałby pomóc w weryfikacji oszustwa, do którego miało dojść.

CZERWONE FLAGI W TEJ SYTUACJI:

- **Niecodzienna prośba o pożyczkę od znajomego** - oczywiście może się zdarzyć tak, że znajomy będzie w pilnej potrzebie, ale z pewnością w takiej sytuacji wybierze inny kanał kontaktu z Tobą. Zawsze warto zweryfikować, z kim rozmawiamy.

- **Podejrzana kwota i lokalizacja transakcji** - jeżeli dasz się namówić na podanie kodu BLIK, ponieważ bezgranicznie ufasz i jesteś pewien, że napisał do Ciebie ktoś bliski, sprawdź kwotę transakcji oraz miejsce jej realizacji. Potwierdź je z potencjalnym odbiorcą środków, któremu ufasz. Jeżeli jej nie rozpoznajesz, to nie potwierdzaj niczego w aplikacji bankowej.

- **Chroń swoje konta w mediach społecznościowych** - stosuj weryfikację dwuskładnikową, która utrudni cyberprzestępcom przejęcie Twojego konta i wykorzystywanie go do wyłudzania danych.

- **Pracownik banku nigdy nie poprosi Cię o kod BLIK** - podobnie nigdy ze strony banku nie otrzymasz prośby o dane do logowania, które mają służyć np. weryfikacji transakcji. Jeżeli coś wzbudzi Twoje podejrzenia, jak najszybciej skontaktuj się z bankiem.

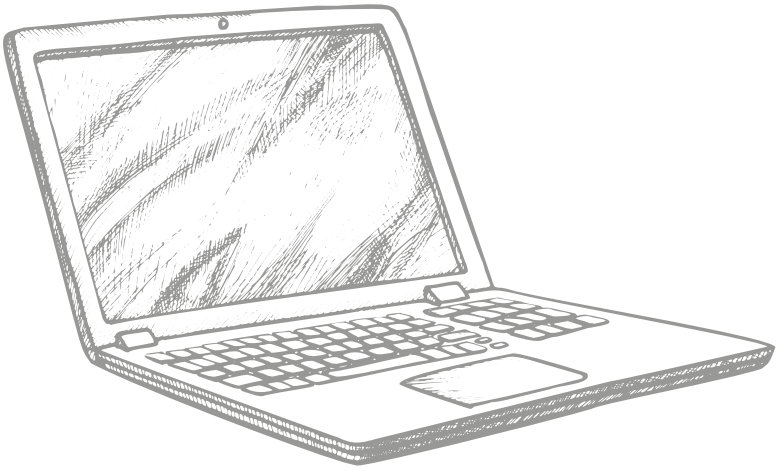
- **BLIK jest bezpieczny**, źródłem niebezpieczeństwa jest oszust podszywający się pod znajomego lub bank, wyłudzający go pod fałszywym powodem.

03

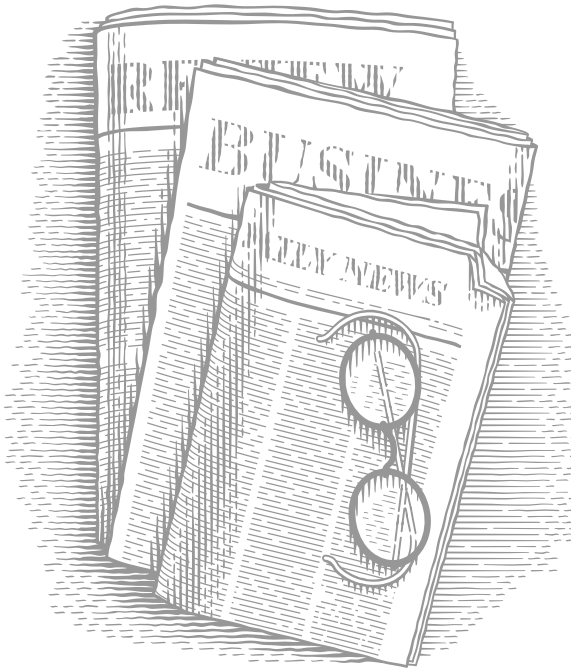
Oszustwo na inwestycje

Oto Daria.

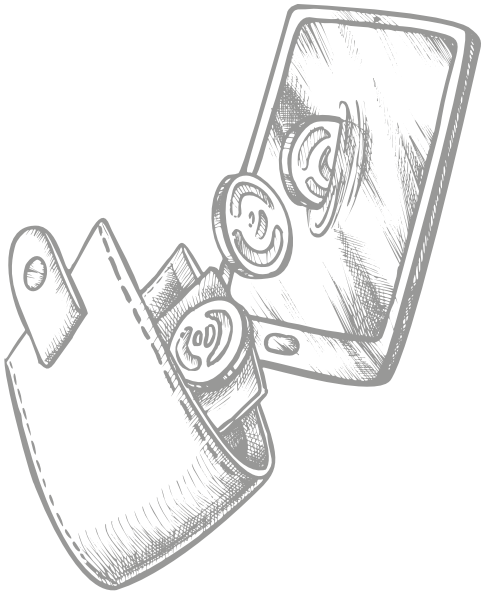
W ostatnim czasie zainteresowała się tematyką inwestycji i kryptowalut. Jak to się stało? Przeglądając różne kanały na YouTube, natknęła się na bardzo profesjonalnego pana w garniturze, który opowiadał, że od czasu gdy został inwestorem, nie musi wcale pracować na etacie, a w życiu zajmuje się głównie wydawaniem pieniędzy.



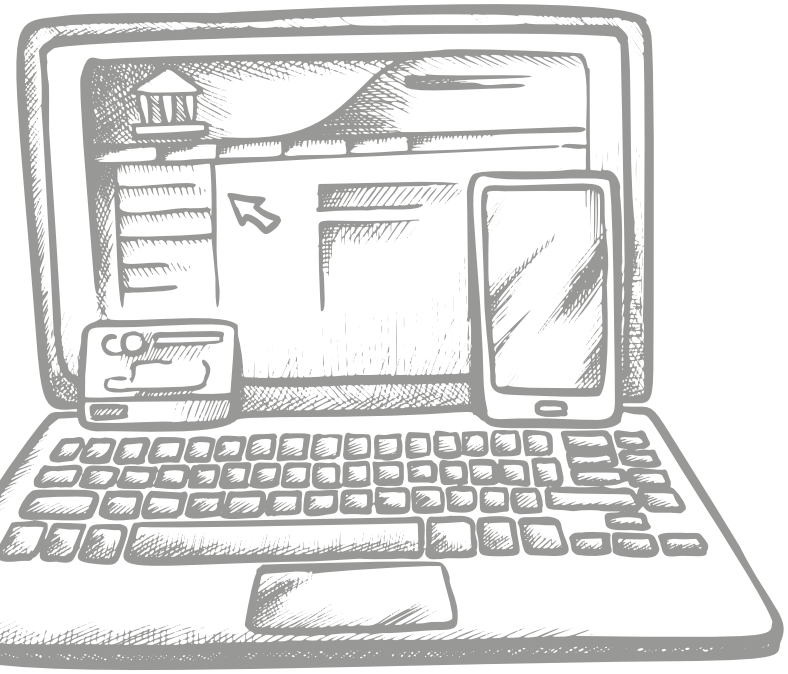
Podekscytowana Daria zaczęła oglądać filmy inwestora, w których przekonywał, że każdy może żyć jak on, tylko trzeba poznać kilka przepisów na inwestowanie i odważyć się zrobić pierwszy krok. **Brzmi kusząco, dzięki dodatkowym środkom mogłabym szybciej spłacić kredyt na mieszkanie** - pomyślała Daria, ale jeszcze się nie czuła przekonana do podejmowania spontanicznej decyzji o inwestycji, która wiąże się z ryzykiem



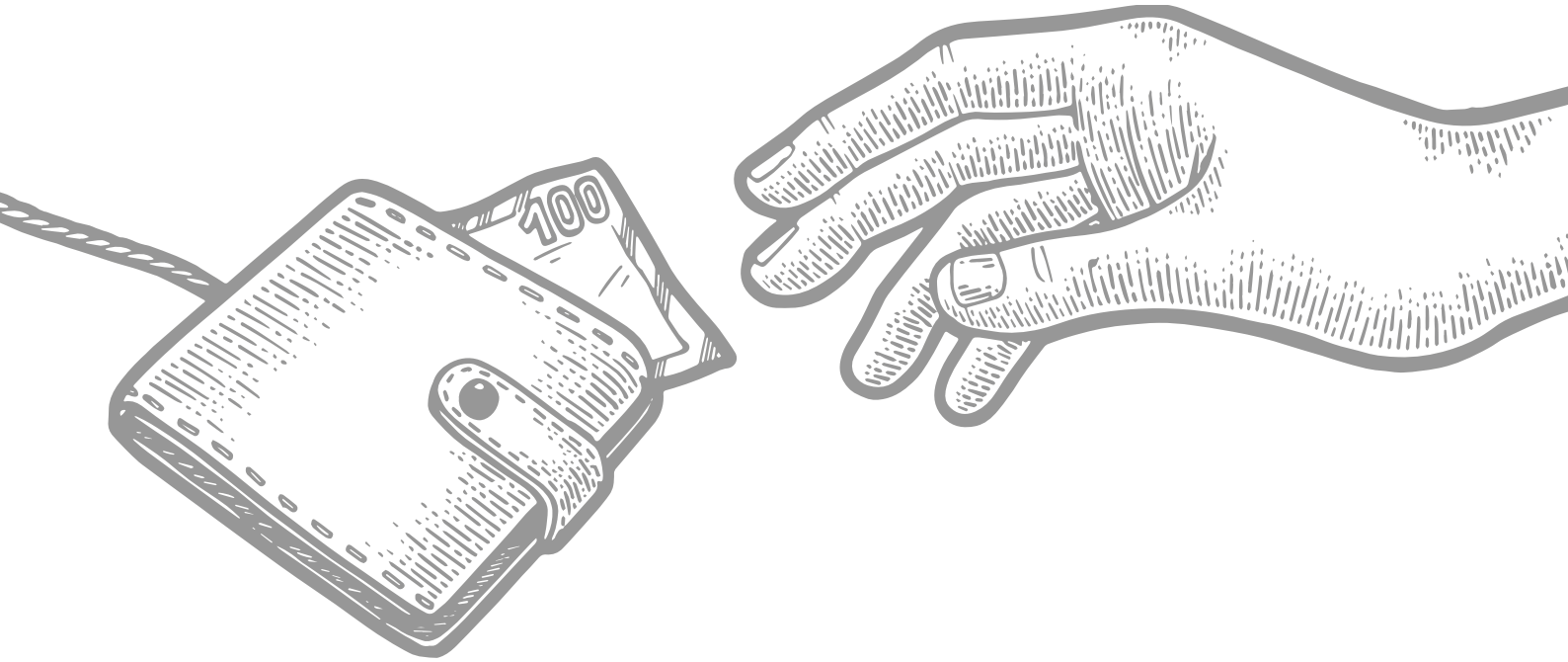
Postanowiła najpierw poobserwować rynek i zobaczyć, czy będzie to dla niej interesujące. **Czytała artykuły i oglądała na ten temat filmy**. Zaczęły jej się wyświetlać reklamy atrakcyjnych inwestycji w kryptowaluty, gdzie twarzą firmy był słynny aktor z jej ulubionego serialu. **Obiecują szybki zysk - przeczytała zainteresowana Daria** i bez wahania kliknęła w reklamę – w końcu jej ulubiony aktor nie zostałby twarzą nieuczciwej firmy. Zadzwoniła pod podany numer telefonu
i odbyła rozmowę z maklerem, który zapewnił, że **Daria może dużo zyskać, a inwestycja nie niesie ze sobą praktycznie żadnego ryzyka, bo są sprawdzoną firmą.**



Jedyne co zastanowiło naszą bohaterkę to **zagraniczny akcent rozmówcy**, który mimo że był bardzo profesjonalny i miał dużą wiedzę, to u **Darii zapaliła się lampka ostrzegawcza. Jednak makler zapewnił ją o swojej uczciwości.** Jeżeli tak, to możemy zacząć działać! - odrzekła uspokojona Daria. Makler **wytłumaczył całą procedurę** oraz zaoferował instalację programu, za pomocą którego będzie można wyświetlać bieżące zyski
i wyniki z inwestycji.



Z racji, że Daria czuła się niezbyt pewnie w instalacji programów **poprosiła od razu o pomoc techniczną**, rozmówca zgodził się bez problemu. Dokładnie poinstruował Darię, jakie kroki ma wykonywać po kolei oraz jaki program pobrać. W następnym kroku **makler zapewnił, że możemy od razu przejść do wykonania pierwszej inwestycji.** Daria postępowała zgodnie z instrukcją rozmówcy, a następnie zalogowała się na swoje konto bankowe i **przelała środki na podany rachunek**



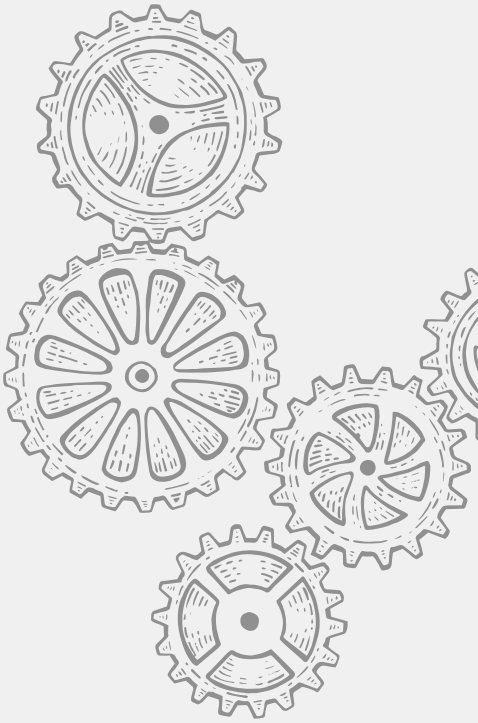
Teraz tylko pozostaje Pani czekać na zyski, które można śledzić w zainstalowanym programie - powiedział makler i rozłączył się. Daria poszła do kuchni zrobić sobie kawę, a w tym czasie zadzwonił do niej telefon... **Po odebraniu okazało się, że dzwoni do niej bank z informacją o podejrzanych transakcjach** na jej rachunku bankowym. Podchodząc do komputera, zobaczyła w oknie logowania banku, jak pieniądze znikają na jej oczach... **Jak to możliwe, że ktoś steruje moim komputerem?** - zapytała samą siebie nasza bohaterka.

JAK TO SIĘ STAŁO, ŻE Z KONTA DARII ZACZĘŁY ZNIKAĆ PIENIĄDZE?

Daria szukała **szybkiej inwestycji w kryptowaluty** bez ryzyka. Zaufała reklamom, ponieważ zobaczyła na nich znaną twarz, a na dodatek była przekonana, że po szybkim internetowym kursie sporo już wie o inwestowaniu i nic jej nie zaskoczy. Nasza bohaterka **nie przewidziała, że wizerunek celebryty lub aktora może być skradziony przez oszustów na potrzeby uwiarygodnienia reklamy.** Zaufała cyberprzestępcy podszywającemu się pod maklera, mimo że jego obcy akcent wzbudził jej podejrzenia, jednak wyparła tę myśl z głowy poprzez to, że wpadła w pułapkę wiedzy i przekonanie, że wie już wystarczająco dużo. **Daria nie sprawdziła jakiego rodzaju oprogramowanie kazał jej zainstalować oszust** podający się za maklera. Na dodatek zalogowała się na swoje konto bankowe bez świadomości, że udzieliła oszustowi dostępu do swojego komputera za pomocą zdalnego pulpitu.

MECHANIZM DZIAŁANIA OSZUSTÓW

Cyberprzestępcy tworzą strony i reklamy, które obiecują szybki i łatwy zysk bez ryzyka. Najczęściej są to obietnice atrakcyjnych inwestycji w kryptowaluty, waluty obce, czy obligacje spółek energetycznych lub paliwowych. Sylwetki znanych osobowości mają je uwiarygadniać, jednak **żadna z osób wykorzystanych w reklamie nie wyrażała nigdy zgody na wykorzystanie swojego wizerunku** - najczęściej jest to kradzież zdjęć.



W oszustwie na inwestycje cyberprzestępcy **oferują pomoc w instalacji odpowiedniego oprogramowania,** co jest kuszące dla osób, które niekoniecznie posiadają odpowiednie umiejętności techniczne. Dochodzi wtedy do instalacji programu, który działa na zasadzie zdalnego pulpitu, co skutkuje całkowitym przejęciem kontroli nad urządzeniem. Oszuści mogą wówczas sami zalogować się do banku ofiary za pomocą wyłudzonych danych lub zmanipulować ją, pod pozorem konieczności dostępu do rachunku bankowego, w celu potwierdzenia transakcji. W momencie uzyskania dostępu do rachunku bankowego oszuści wykradają z niego dostępne środki. **Zdarza się również, że oszuści nie muszą sięgać po dodatkowe oprogramowanie**. Nierzadko bywa, że są na tyle przekonujący, by **nakłonić ofiarę do samodzielnego zlecania przelewów**
i to na przestrzeni nawet kilku tygodni.

CZERWONE FLAGI W TEJ SYTUACJI:

- **Szybki i łatwy zysk bez ryzyka** - niestety coś takiego nie istnieje. Nie da się małym kosztem pomnożyć kilkukrotnie naszych oszczędności. Każda inwestycja to ryzyko, a przymiotniki jak „szybko i łatwo" bezdyskusyjnie powinny wzbudzić naszą czujność.

- **Natrętne reklamy rentownych inwestycji** - przed kliknięciem zawsze stosuj zasadę ograniczonego zaufania.

- **Powierzanie środków nieznanym osobom czy instytucjom** - podmioty oszustów są zwykle rejestrowane w egzotycznych krajach. Według rzecznika finansowego oszukańcze platformy mają najczęściej siedzibę w krajach typu Dominikana, czy Saint Vincent i Grenadyny. Jednak nasza czujność nie powinna być uśpiona w sytuacji natknięcia się na platformę zarejestrowaną w krajach europejskich

- **Pobieranie aplikacji lub oprogramowania z niezweryfikowanych źródeł** - właśnie w ten sposób oszust może przejąć kontrolę nad naszym komputerem lub telefonem. Programy typu AnyDesk, TeamViewer, czy Splashtop pozwalają na swobodny dostęp do jednego urządzenia za pośrednictwem innego.

CO ZROBIĆ JEŻELI PADLIŚMY OFIARĄ OSZUSTÓW?

01 **Skontaktuj się z bankiem i zablokuj wszystkie dostępy do swojej bankowości** na wypadek nieuprawnionego logowania - nawet jeżeli Twoje konto zostało wyczyszczone, to ten krok jest konieczny.

02 **Natychmiast zgłoś sprawę na policję** - być może uda się ustalić oszustów.

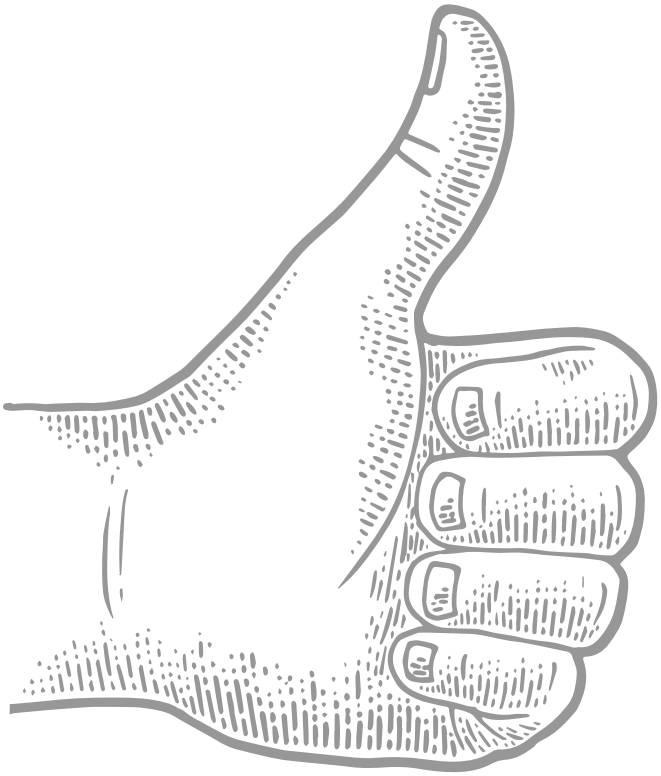
03 **Powinieneś udzielić kompletu informacji o oszustach policji oraz pracownikowi banku** - takie dane mogą pomóc zidentyfikować oszukańczy podmiot.

04

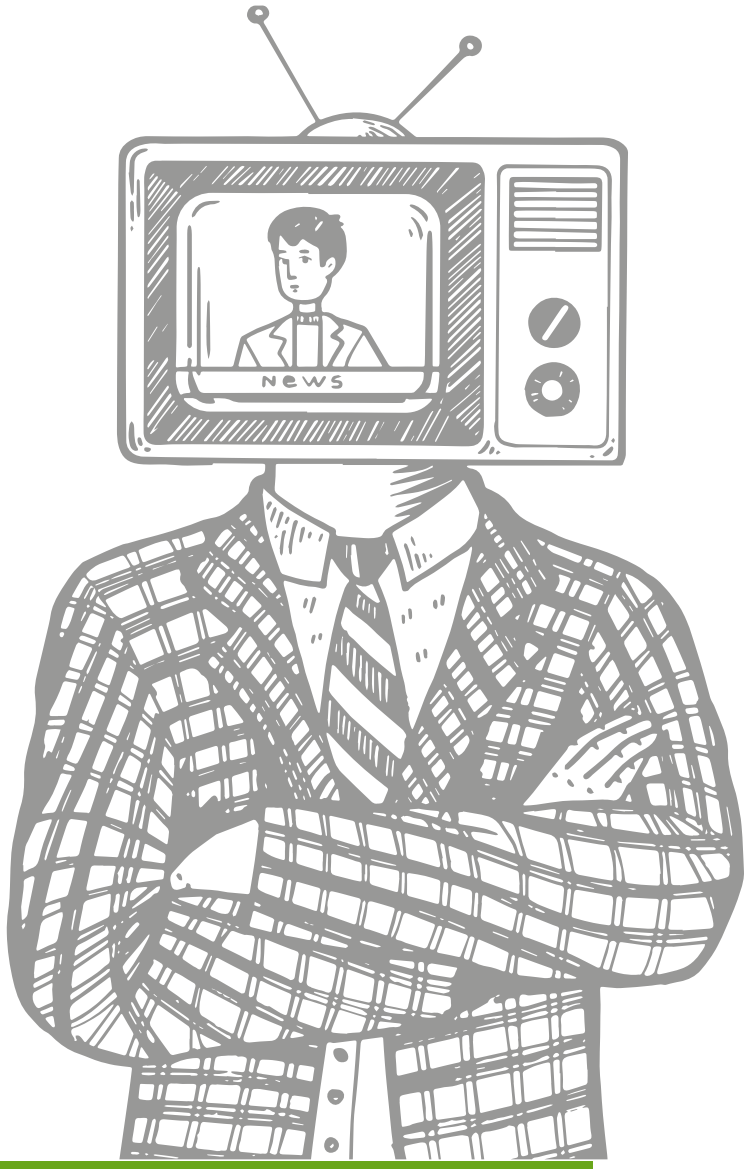
Fake newsy i dezinformacja w sieci

Oto Darek,

który interesuje się polityką oraz otaczającym go światem. Chętnie udostępnia w mediach społecznościowych interesujące newsy o wydarzeniach na świecie. Śledzi profile portali informacyjnych oraz opiniotwórczych osób i chętnie czyta ich publikacje, a także retwittuje te ciekawsze. Ostatnio natknął się na informację na temat tego, że w ciągu najbliższych dni może zabraknąć gotówki w bankomatach.



Darka bardzo poruszyła ta informacja, więc **przeczytał artykuł, polubił wpis na Twitterze (jak 500 innych użytkowników)** oraz udostępnił go dalej, aby jego znajomi również nie byli zaskoczeni, że już wkrótce nie będą mogli wypłacić środków z bankomatu. **Dobrze, że dowiedziałem się o tym wcześniej** - pomyślał Darek ubierając kurtkę i czym prędzej biegnąc wypłacić gotówkę.



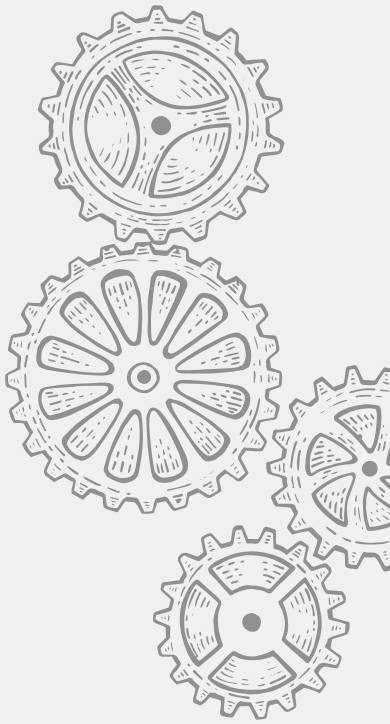
Jednak pod bankomatem okazało się, że nie tylko on postanowił się zabezpieczyć. **Stanął w długiej kolejce...** Po około 30 minutach oczekiwania na jego telefonie pojawiło się powiadomienie **„Darek, opanuj się! To fake news..."** - to była wiadomość od jego cioci, która z racji pracy w banku postanowiła zweryfikować prawdziwość informacji. Zaskoczony mężczyzna zaczął w głowie łączyć fakty i doszedł do wniosku, że może faktycznie dał się zmanipulować... Akurat po długim oczekiwaniu nadeszła jego kolej na wypłacanie pieniędzy z bankomatu, jednak **Darek wrócił zrezygnowany do domu zadając sobie pytanie: jakim cudem mogłem uwierzyć w taką nieprawdopodobną informację..?**

DLACZEGO DAREK
UWIERZYŁ W FAKE NEWSA?

Fake newsy i dezinformacja udają prawdę. Publikowane są w formie, która ma szybko rozejść się po internecie. Darek zobaczył **chwytliwy nagłówek, a informacja, którą przeczytał, wydawała się sensacyjna. Nie zweryfikował rzetelności portalu, na którym pojawił się artykuł, ani jego autora.** Uwierzył, że informacja jest wysoce prawdopodobna, ponieważ liczba polubień wpisu na Twitterze oraz retwittów była bardzo wysoka. W końcu tyle osób nie może się mylić reagując na dany wpis. Dodatkowo Darek **wpadł w typową pułapkę myślenia**, która polega na tym, że przeceniamy swoją zdolność do subiektywnej oceny - „ja się nie dam zmanipulować, ale każdy inny internauta już z pewnością tak". Reagując na wpis, a w dodatku podając go dalej, nasz bohater stał się narzędziem w machinie dezinformacji.

MECHANIZM DZIAŁANIA DEZINFORMACJI:

Dzisiaj sieć jest **zalewana potokiem informacji**, a same media często walczą o uwagę użytkownika. Publikacje mogą powstawać bardzo szybko, bez weryfikowania faktów. Osoby, które celowo wypuszczają fake newsy wiedzą, że najlepiej klikają się **chwytliwe nagłówki i niewiarygodne historie budzące emocje**. W całej machinie dezinformacji warto wiedzieć, że my jako odbiorcy treści nie jesteśmy tylko celem, ale także narzędziem. **Jeżeli podajemy dalej informacje, które są fake newsami pomagamy rozszerzyć zasięg dezinformacji** i dokładamy cegiełkę do samonapędzającej się kuli śnieżnej.



Dodatkowo **fake news może być połączony z dowolną inną formą oszustwa**, która ma już przynieść wymierne korzyści osobie za nim stojącej. Np. emocjonalny wpis zakończony linkiem do strony służącej phishingowi albo stanowiącej fałszywą zbiórkę.

Czasami fake news powstaje przez przypadek. Może wynikać z błędów w tłumaczeniu lub zasugerowaniu się opinią czy komentarzem do sytuacji, a nie faktem. Czasami zdjęcia lub filmy nie dotyczą sytuacji, która została przedstawiona w kontekście publikacji. Publikowane są materiały, które mają zakłamać faktyczny obraz wydarzenia, np. stare zdjęcie zestawione z komentarzem do aktualnej sytuacji. Widzimy wtedy prawdziwy film lub zdjęcie ze zmanipulowaną opinią.

Dezinformacja może również wynikać z nierzetelnej oceny materiałów, które np. dotarły do redakcji w formie informacji prasowej. **Dziennikarze również mogą wpaść w pułapki informacyjne** poprzez nieznajomość szerszego kontekstu. Wszyscy jesteśmy tylko ludźmi.

CZERWONE FLAGI W TEJ SYTUACJI:

- **Miej wątpliwości** - zastanów się, czy publikacja jest udostępniona przez rzetelny portal oraz, czy autor publikuje pod własnym nazwiskiem. Jeżeli ktoś nie był gotowy się podpisać pod artykułem, to możesz od razu założyć, że treść jest mniej wartościowa. Sprawdź, czy publikacja powołuje się na źródła - jeżeli nie, jest to wyraźny sygnał, aby jej nie ufać.

- **Chwytliwy nagłówek i sensacyjna informacja** - tego typu elementy powinny sprawić, że w naszej głowie zapali się czerwona lampka. Jeżeli informacja jest napisana emocjonalnym językiem, może to świadczyć, że publikacja jest opinią, a nie faktami.

- **Zweryfikuj i przeanalizuj treść** - pomyłki stylistyczne lub błędy w faktach historycznych to mogą być znaki, że publikacja została napisana przez trolli, których celem jest sianie zamętu za pomocą fake newsów.

- **Sprawdź wiarygodność grafiki lub filmu** - możesz sprawdzić, czy dane zdjęcie nie pojawiało się w artykułach w przeszłości. Zweryfikuj to za pomocą wyszukiwarki grafik w Google, być może stare zdjęcie z emocjonalnym komentarzem zostało dopasowane do aktualnej sytuacji.

- **Czy to prawdziwy serwis informacyjny** - podobnie jak w przypadku innych oszustw tworzenie stron podszywających się pod prawdziwe portale newsowe, które mają wprowadzać czytelnika w błąd, nie stanowi żadnego problemu. Sprawdź adres URL strony internetowej, a także przyjrzyj się szacie graficznej serwisu.

- **Ignoruj liczbę reakcji i udostępnień** - dla niektórych duża liczba reakcji uwiarygadnia informację, bo poleciło ją wiele osób. Jednak polubienia pod postami w mediach społecznościowych można kupić bądź wywoływać silnymi emocjami. Na to właśnie liczą osoby tworzące fake newsy.

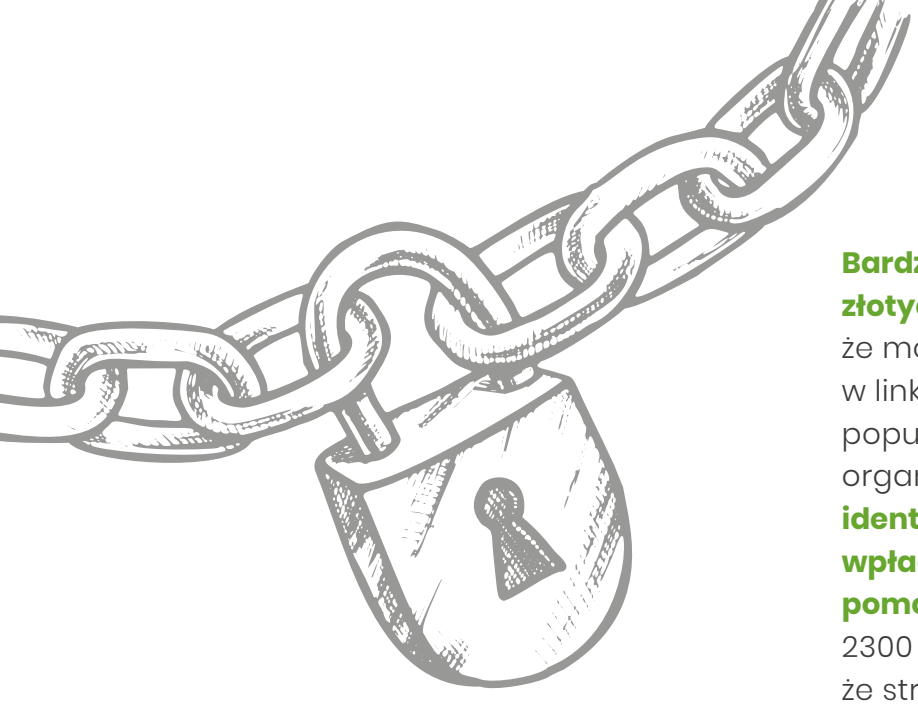
- **Obiektywizm i krytycyzm** - nie ulegaj błędom poznawczym! Często odrzucamy informacje, które nie pasują do naszego światopoglądu. Interesujemy się tym, co pasuje do naszej bańki zainteresowań. Dlatego właśnie nie można ulegać pierwszemu wrażeniu, bo możemy zostać zmanipulowani.

05

Oszustwa na zbiórki

Poznajcie Kamilę,

która bardzo przejęła się wojną za naszą wschodnią granicą i postanowiła aktywnie pomóc, na tyle ile może. Przekazała rzeczy na lokalną zbiórkę w swoim mieście, ale wiedziała, że może zrobić więcej. Pewnego dnia przeglądając media społecznościowe zauważyła, że ktoś zorganizował internetową zbiórkę pieniędzy na pomoc humanitarną.



Bardzo chętnie wpłacę kilkanaście złotych - stwierdziła Kamila, która liczyła, że może realnie pomóc. Kliknęła w link i została przekierowana na stronę popularnego serwisu, który umożliwia organizację zbiórek. **Witryna wyglądała identycznie jak portal, gdzie już kiedyś wpłacała pieniądze dla organizacji pomocowej**, a zbiórkę wsparło już 2300 osób. Kamila mając świadomość, że strona może być dziełem oszustów **sprawdziła, czy przed adresem URL widoczna jest kłódka**, w której upatrywała gwarancji bezpieczeństwa witryny.

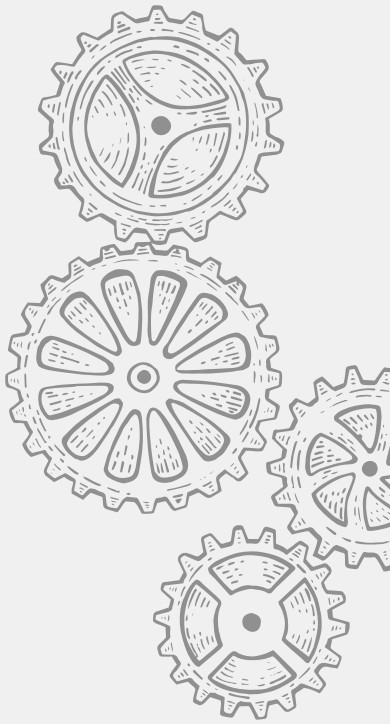
Owszem, była i tutaj. **Wszystko wygląda bezpiecznie** - pomyślała nasza bohaterka i kliknęła „Wpłacam teraz". Wpisała swoje imię i nazwisko oraz adres mailowy, a chwilę później na jej adres e-mail dotarły dane do przelewu. **Kamila zgodnie z instrukcją wykonała przelew** na podane konto. Zadowolona zamknęła komputer z nadzieją, że jej pieniądze komuś realnie pomogą. **Jednak w tym przypadku tak się niestety nie stanie...**

DLACZEGO DATEK KAMILI NIE TRAFI DO POTRZEBUJĄCYCH?

Nasza bohaterka **starała się zachować czujność**, jednak nie pomyślała, że oszuści są tak **perfidni i mogą chcieć wykorzystać taką sytuację jak kryzys humanitarny i wojna**. Kamila uwierzyła, że wpłaca pieniądze na prawdziwą zbiórkę, ponieważ strona wyglądała jak oryginalny serwis umożliwiający założenie zbiórki. **Nie sprawdziła adresu URL strony oraz wykonała przelew na konto nieznajomego. Nie zweryfikowała również, czy organizacja zbierająca pieniądze znajduje się na liście wiarygodnych zbiórek.**

MECHANIZM DZIAŁANIA OSZUSTÓW:

Oszuści **wykupują domeny związane z aktualną akcją pomocową** i tworzą strony łudząco podobne do witryn organizacji lub serwisów umożliwiających zakładanie zbiórek. Aby uwiarygodnić akcję, tego typu strony często posiadają certyfikaty SSL, więc warto pamiętać, że **kłódka przed adresem URL nie świadczy o wiarygodności witryny**.
Na podrabianych stronach pomocowych jedynym aktywnym przyciskiem jest „wpłać teraz”, który nie przekierowuje do płatności online, tylko strona wymaga wypełnienia danych typu imię i nazwisko oraz adres e-mail. Użytkownik nie musi również akceptować regulaminu zbiórki. Po wypełnieniu danych **ofiara otrzymuje na skrzynkę e-mail dane do wykonania przelewu.** Tego typu oszustwo może dotyczyć także wpłat w kryptowalutach lub NFT, czego lepiej unikać, jeżeli nie mieliśmy do czynienia z tego typu inwestycjami.



CZERWONE FLAGI W TEJ SYTUACJI:

- **Pomagaj finansowo tylko w ramach akcji organizowanych przez sprawdzone podmioty** - najlepszym rozwiązaniem jest weryfikacja zbiórki w zaufanych źródłach. W przypadku zbiórek pomocowych dla Ukrainy warto skorzystać ze stron rządowych lub samorządów lokalnych, które gromadzą w jednym miejscu autentyczne zbiórki, z których wiadomo, gdzie konkretnie trafi pomoc.

- **W przypadku chęci wpłaty na zbiórkę spoza zweryfikowanych źródeł** sprawdź dokładnie, kto jest organizatorem i czy już wcześniej tworzył akcje pomocowe.

- **Nie kieruj się emocjami, tylko zasadą ograniczonego zaufania** - sprawdzaj adresy URL stron pomocowych, czytaj dokładnie treści oraz język, w jaki sposób jest opisana zbiórka. Jeżeli pojawia się w nim dużo błędów i widać niedbałość powinien to być dla Ciebie sygnał ostrzegawczy.

- **Wspieraj tylko legalne zbiórki** - nawet jeżeli akcja pomocowa pojawi się na oficjalnej stronie umożliwiającej tworzenie zbiórek, warto zweryfikować podstawowe dane. Kto prowadzi akcję, na czym polega pomoc oraz daty rozpoczęcia i zakończenia zbiórki.

- **Nie otwieraj podejrzanych linków oraz załączników** - podstawowa zasada bezpieczeństwa w internecie ma również zastosowanie w sytuacjach tego typu. Oszuści niekoniecznie będą chcieli okraść Cię z pieniędzy, może im również zależeć na wyłudzeniu Twoich danych.

Internetowy Kantor.pl