Scamming Out!

ORGANIZATORZY

Puls Biznesu

Bankier.pl

Bezpieczne finanse

– jak rozpoznać i unikać scamu

ORGANIZATORZY

PATRONI HONOROWI

PARTNERZY

Wstęp

"321 mln zł - tyle pieniędzy oszuści ukradli Polakom za pomocą phishingu, vishingu, fałszywych ofert inwestycyjnych, oszukańczych relacji uczuciowych, stosując szantaż, grając na strachu, lęku, pożądaniu i chciwości.

Są to dane tylko za I półrocze. Nie wiemy, jak było w minionym roku i latach ubiegłych, ponieważ dopiero w I kwartale 2024 r. NBP po raz pierwszy podał statystyki dotyczące oszustw finansowych, w tym również ataków z wykorzystaniem chwytów socjotechnicznych. Wcześniej bank publikował zestawienia oszukańczych transakcji kartowych, które nie obejmowały strat z tytułu przelewów. A to one są od kilku lat głównym kanałem okradania klientów banków.

Jeśli wartość szkód z pierwszych sześciu miesięcy przemnożymy przez dwa, uzyskamy sumę ponad 600 mln zł strat rocznie spowodowanych przez przestępców. Dla porównania afera Amber Gold, która wstrząsnęła fundamentami państwa, kosztowała klientów piramidy finansowej 851 mln zł. Strata bolesna, ale jednorazowa. Scammerzy kradną Polakom co roku po kilkaset milionów złotych. O ofiary nikt się nie upomina, bo też one same, motywowane wstydem, że dały się podejść, często nie informują o przestępstwie nikogo. Statystycznie wartość pojedynczych strat jest mała. NBP podaje, że średnio jest to około 9 tys. zł na jednego okradzionego. Skala przestępstwa jest jednak bardzo duża. W I połowie roku okradzionych zostało aż 40 tys. osób. Znowu, dla porównania ofiarą Amber Gold padło 18 tys. klientów.

Oszustwa finansowe to w Polsce temat niszowy, znany głównie specjalistom od bezpieczeństwa. Nie ma debaty publicznej na temat coraz powszechniejszego zjawiska kradzieży internetowych, problem nie znajduje się na agendzie polityków. Inaczej jest w krajach takich jak Australia, Singapur, Wielka Brytania, gdzie skala oszustw jest podobna jak u nas, a poziom zaangażowania rządów jest bardzo duży.

Na szczęście jest szereg instytucji publicznych, firm i fundacji, które informują, edukują społeczeństwo w zakresie zagrożeń cyberoszustwami, a także opracowują rozwiązania technologiczne wspierające walkę ze scamem.

Jesteśmy dumni, że w gronie naszych partnerów i patronów mamy najznamienitszych przedstawicieli tego trendu, instytucje oraz firmy, których zasługi w szerzeniu wiedzy na temat bezpieczeństwa w sieci, monitorowania cyberprzestrzeni i zapobiegania niebezpieczeństwom są nie do przecenienia.

Na początku października Puls Biznesu i Bankier.pl rozpoczęły kampanię edukacyjną przeciw oszustwom finansowym **Scamming out!**, w ramach której zebraliśmy mnóstwo materiałów na temat finansowych oszustw w formie debat, podcastów, raportów i informacji.

Podsumowaniem naszych działań, esencją wiedzy o tym, czym są oszustwa finansowe, jak rujnujący mają wpływ na ofiary - nie tylko w wymiarze finansowym, jak się przed nimi chronić, jest ten e-book. Po więcej informacji zapraszamy na stronę scammingout.pl oraz na strony naszych partnerów i patronów akcji."

Eugeniusz Twaróg
- pomysłodawca i opiekun merytoryczny projektu Scamming out!

Spis treści

Rozdział 1:

Czym jest scam i dlaczego jest tak groźny?

Współczesny świat to arena nieustannej rywalizacji o uwagę. Reklama, media i technologie, które przez dekady stanowiły filary komunikacji masowej, przekształciły się w narzędzia o potężnej sile perswazji.

W ich cieniu rozwija się jednak groźne zjawisko – **oszustwa finansowe**, które zręcznie adaptują strategie marketingowe do swoich celów. Granica między autentycznym przekazem a manipulacją zaciera się, co czyni współczesnego człowieka wyjątkowo podatnym na wpływy.

Współczesne społeczeństwo coraz częściej podlega subtelnym mechanizmom wpływu, które działają w sposób niemal niezauważalny. Autonomia jednostki nie jest podważana otwartą siłą, lecz poprzez narrację i manipulacje, które stopniowo przenikają do codziennego życia. W tym kontekście scam staje się jednym z poważniejszych zagrożeń – przestępstwem opartym na manipulacji, które uderza nie tylko w nasze finanse, ale również w poczucie bezpieczeństwa i zdolność podejmowania świadomych decyzji

Czym jest scam i dlaczego z nim walczymy?

Scam to oszustwo mające na celu wyłudzenie Twoich pieniędzy lub danych, które przestępcy wykorzystują następnie, żeby Cię okraść.

Używają do tego manipulacji, metod socjotechnicznych, fałszywych obietnic, szantażu, gróźb, grają prostymi emocjami, jak strach lub chęć szybkich zysków.

Nadmiar bodźców i presja czasu

Codziennie jesteśmy bombardowani tysiącami komunikatów reklamowych – ich liczba może sięgać nawet 5000 dziennie. Reklamy, newslettery, powiadomienia w aplikacjach – wszystkie te elementy tworzą rzeczywistość, w której trudno znaleźć chwilę na refleksję. Nadmiar bodźców staje się sprzymierzeńcem manipulatorów.

Ofiary scamów często przyznają, że zostały oszukane w chwilach stresu, zmęczenia lub nadmiaru obowiązków. *„To był dzień pełen chaosu. Ledwo nadążałam z obowiązkami, gdy zadzwonił telefon. Głos w słuchawce był uspokajający, wręcz profesjonalny. W jednej chwili uwierzyłam, że to faktycznie bank. Zareagowałam odruchowo, tracąc czujność”* – wspomina jedna z ofiar, która swoimi doświadczeniami podzieliła się na stronie Scammingout.pl.

Oszuści wykorzystują mechanizm zmęczenia i przebodźcowania, które osłabiają zdolność do racjonalnej analizy. W takich warunkach człowiek staje się bardziej podatny na sugestie obiecujące szybkie i łatwe rozwiązania. Celowo kreują sytuacje wymagające natychmiastowego działania, co zwiększa presję i skłania do podejmowania impulsywnych decyzji.

Reklama jako narzędzie perswazji

Reklama przeszła długą ewolucję – od prostego przekazu informacyjnego do wyrafinowanych narracji, które odwołują się do emocji, budując relacje między marką a konsumentem. Wiele współczesnych reklam tworzy obrazy, które mają wpleść produkty w ważne momenty życia. Przykładem może być majonez, który w reklamach staje się symbolem świątecznej atmosfery.

Jednak rozwój reklamy wiąże się również z ryzykiem nadużyć. Reklama, która odpowiada na rzeczywiste potrzeby i buduje wartość społeczną oraz emocjonalną, może łatwo przekroczyć cienką granicę – od wspierającej użytkownika narracji do subtelnej manipulacji, wpływającej na jego wybory bez jego świadomości.

Scam – cień współczesnego marketingu

Mechanizmy, które w reklamie mają budować relacje, stają się inspiracją dla przestępców. Scammerzy, obserwując skuteczność klasycznych strategii marketingowych, wykorzystują je do swoich przestępczych celów.

„Dostałam SMS-a, który wyglądał jak wiadomość z mojego banku. Była tam informacja, że muszę szybko zweryfikować dane, bo moje konto zostanie zablokowane. Kliknęłam w link, który wyglądał jak prawdziwa strona banku. Dopiero po fakcie zrozumiałam, że straciłam pieniądze" – opowiada Anna.

Mechanizmy manipulacji opierają się na silnych emocjach. Oszuści wykorzystują strach przed stratą, obawy o bezpieczeństwo finansowe, kuszą wizją szybkiego i pewnego zysku lub grają na uczuciach, wciągając swoje ofiary w fałszywe relacje romantyczne. Wykorzystują techniki podobne do tych stosowanych w reklamie, jednak ich celem nie jest budowanie relacji, lecz wyłącznie wyzysk.

Vishing i smishing – oszustwa przez telefon i SMS

Vishing (Voice Phishing)

- Oszuści podszywają się pod pracowników banku, policji lub innych instytucji, aby zdobyć Twoje dane lub nakłonić Cię do przelania pieniędzy na „bezpieczne konto".

Przykładowe scenariusze:

- Informacja o nieautoryzowanym przelewie.
- Rzekoma konieczność zabezpieczenia środków przed hakerami.
- Prośba o podanie danych do logowania lub przelanie pieniędzy.

Smishing

- Wiadomości SMS zawierające linki prowadzące do fałszywych stron. Najczęściej podszywają się pod firmy kurierskie, operatorów telefonicznych czy banki.

Przykłady wiadomości:

- „Twoja paczka nie może zostać dostarczona. Kliknij tutaj, aby zapłacić brakującą kwotę."
- „Zablokowano Twoje konto bankowe. Zaloguj się tutaj, aby je odblokować."

Jak się chronić?

- Nie udostępniaj danych przez telefon. Zawsze rozłącz się i samodzielnie skontaktuj z bankiem.
- Nie klikaj linków w SMS-ach. Sprawdzaj komunikaty na oficjalnych stronach firm.

Granice między reklamą a manipulacją

Reklama w swojej etycznej formie spełnia ważną funkcję – umożliwia konsumentom dostęp do informacji o produktach i usługach. Problem pojawia się, gdy te same mechanizmy są wykorzystywane w sposób nieetyczny – zarówno w marketingu, jak i w oszustwach finansowych.

W obu przypadkach odbiorca poddawany jest presji czasu. Hasła typu **„Ostatnia szansa!"** czy **„Oferta ważna tylko dziś!"** wywołują efekt FOMO (Fear of Missing Out) – lęk przed przegapieniem okazji. Oszuści stosują ten mechanizm, tworząc fałszywe oferty czy wiadomości, które zmuszają odbiorców do szybkiego działania.

Kierunki na przyszłość

Człowiek współczesny musi nauczyć się poruszać w świecie pełnym subtelnych wpływów i jawnych manipulacji. Świadomość mechanizmów marketingowych, umiejętność krytycznej analizy komunikatów oraz edukacja w zakresie cyberbezpieczeństwa to kluczowe kroki w budowaniu odporności na scam.

Autonomia nie polega na całkowitym odcięciu się od zewnętrznych wpływów, ale na umiejętności ich świadomego analizowania i oceniania. Reklama i komunikacja mogą pełnić pozytywną rolę, jeśli postrzegamy je jako część dialogu, a nie jako narzędzie jednostronnego oddziaływania.

W ramach akcji **Scamming out!** chcemy rozpocząć dyskusję na temat sposobów ograniczenia działalności przestępczej w internecie. Wspólnie z mediami, platformami społecznościowymi i firmami technologicznymi możemy stworzyć świat, w którym konsument czuje się świadomy i bezpieczny – niezależnie od tego, czy spotyka reklamę, czy oszusta.

Jaki jest cel akcji Scamming out!

1. Opisanie skali przestępczości związanej z oszustwami finansowymi
2. Przedstawienie metod działania przestępców
3. Prezentacja sposobów radzenia sobie ze scamami w innych krajach
4. Szeroka akcja informacyjna z udziałem partnerów dotycząca oszustw w sieci
5. Edukacja, jak bronić się przed atakami oszustów
6. Angażowanie partnerów publicznych do wspólnego poszukiwania rozwiązań prawnych służących ograniczaniu przestępczości w cyberprzestrzeni

Rozdział 2:

Współczesny konsument – między nadmiarem a wyborem

Żyjemy w epoce nadmiaru. Codziennie mamy dostęp do tysięcy informacji, ofert, produktów i usług, które obiecują uczynić nasze życie lepszym, łatwiejszym lub bardziej satysfakcjonującym. Jednak ten zalew możliwości rodzi paradoks: im więcej mamy wyborów, tym trudniej nam podjąć decyzję. W tej przestrzeni pełnej bodźców współczesny konsument staje się łatwym celem dla manipulatorów – zarówno marek, jak i oszustów.

Nadmiar informacji sam w sobie nie stanowi problemu; wyzwanie pojawia się w sposobie zarządzania uwagą w tej rzeczywistości. Brak umiejętności selekcji prowadzi do chaosu w podejmowaniu decyzji, a ten chaos tworzy idealne warunki dla manipulacji i zewnętrznych wpływów.

Reklama, technologie, a nawet nasze własne pragnienia tworzą środowisko, w którym wybory rzadko są w pełni autonomiczne. Manipulacja staje się możliwa tam, gdzie ludzie tracą zdolność do świadomej refleksji. Scam – oszustwo, które przybiera formę ofert finansowych, fałszywych sklepów internetowych czy telefonów od „banków" – doskonale wpasowuje się w ten krajobraz.

Fałszywe sklepy

Oszustwa polegają na tworzeniu stron internetowych przypominających znane marki, oferujących produkty w niezwykle atrakcyjnych cenach.

Fałszywe oferty wakacyjne

- Ofiary wpłacają zaliczki na wynajem nieruchomości, które nie istnieją. Najczęściej pojawia się to w sezonie wakacyjnym.

Jak się chronić?

- Kupuj w znanych sklepach. Sprawdzaj opinie o sprzedawcy.
- Nie wpłacaj zaliczek za wynajem nieruchomości bez weryfikacji. Sprawdź adres i właściciela nieruchomości.

Człowiek wobec nadmiaru

Współczesny konsument stoi przed ogromnym wyzwaniem – jak wybrać w świecie, który oferuje tak wiele? Problem polega na tym, że nasza zdolność przetwarzania informacji jest ograniczona. Psychologowie zauważają, że przy zbyt dużej liczbie opcji pojawia się efekt „paraliżu decyzyjnego". Zamiast cieszyć się możliwością wyboru, odczuwamy stres, a nasze decyzje stają się mniej przemyślane.

> *„W tamtym momencie byłam przytłoczona ilością rzeczy do zrobienia. Nie miałam czasu na analizowanie każdego szczegółu, więc gdy zadzwonił ktoś z 'mojego banku', uwierzyłam. Zrobiłam, co kazali, bo chciałam szybko rozwiązać problem"* – mówi jedna z ofiar scamu.

Scammerzy doskonale rozumieją, jak działa ludzka psychika w sytuacjach stresu i zmęczenia, dlatego tworzą przekazy zaprojektowane, by natychmiast przyciągnąć uwagę i wymusić szybkie działanie. W takich momentach ludzie częściej ulegają sugestiom, które oferują pozorną ulgę i rozwiązanie problemów.

Psychologia współczesnego konsumenta

Aby zrozumieć, dlaczego współczesny konsument jest tak podatny na manipulacje, warto przyjrzeć się podstawowym mechanizmom psychologicznym. Po pierwsze, ludzie mają naturalną skłonność do poszukiwania prostych rozwiązań.

W świecie zdominowanym przez szybkość i efektywność wolimy skróty myślowe niż długotrwałe analizy. Po drugie, nasze decyzje są silnie uwarunkowane emocjami. Produkty, które obiecują poprawę samopoczucia lub spełnienie naszych marzeń, łatwiej zdobywają naszą uwagę.

W świecie pełnym ofert i komunikatów konsument nie kieruje się wyłącznie racjonalnością. Emocje i pragnienia często przejmują kontrolę nad procesem decyzyjnym, stając się głównymi czynnikami wpływającymi na dokonywane wybory.

Scammerzy doskonale rozumieją tę dynamikę. Ich strategie manipulacji często opierają się na wywoływaniu silnych emocji – od strachu i presji czasu po ekscytację i nadzieję na szybki zysk. Jedną z najczęściej stosowanych taktyk jest stworzenie sytuacji, w której ofiara czuje, że musi działać natychmiast.

> *„Dostałem SMS-a z informacją o podejrzanej transakcji na moim koncie. Serce zabiło mi szybciej. Kliknąłem w link, zanim pomyślałem, czy to ma sens”* – przyznaje Tomasz, który stracił pieniądze w wyniku oszustwa phishingowego*.

*Phishing – oszustwo przez e-mail, SMS lub fałszywe strony internetowe

Phishing to najpopularniejsza forma scamu, która według raportu Orange stanowiła w 2023 roku aż **44% wszystkich cyberzagrożeń**. Oszuści wykorzystują e-maile, SMS-y lub fałszywe strony internetowe do wyłudzania danych osobowych, takich jak loginy, hasła czy numery kart kredytowych.

Jak wygląda atak phishingowy?

- Ofiara otrzymuje wiadomość o konieczności:
  - aktualizacji danych w banku,
  - weryfikacji konta,
  - pobrania nowej wersji aplikacji bankowej.
- Wiadomość zawiera link prowadzący do fałszywej strony internetowej, która do złudzenia przypomina oryginalną witrynę banku. Na stronie ofiara podaje swoje dane logowania, które trafiają do oszustów.
- Często pod linkiem ukryte jest złośliwe oprogramowanie, które infekuje urządzenie i daje przestępcom pełny dostęp.

Jak się chronić?

- Nie klikaj linków w wiadomościach e-mail i SMS-ach. Banki nigdy nie wysyłają takich wiadomości.
- Sprawdzaj adres URL strony internetowej. Fałszywe strony często mają literówki w adresach (np. „bank.pl” zamiast „bank.com”).
- Zgłaszaj podejrzane wiadomości. Informując bank o phishingu, pomagasz w zwalczaniu oszustów.

Relacja między konsumpcją a tożsamością

Współczesna konsumpcja przestała być jedynie sposobem zaspokajania podstawowych potrzeb. Produkty i usługi, które wybieramy, często stają się częścią naszej tożsamości. Marki, których używamy, mają mówić coś o nas – o naszych aspiracjach, wartościach czy stylu życia. W efekcie konsumpcja nabiera wymiaru symbolicznego, a jej granice coraz bardziej się zacierają.

Ta zależność między konsumpcją a tożsamością jest często wykorzystywana zarówno przez reklamy, jak i przez oszustów. Scammerzy tworzą oferty, które odwołują się do pragnienia prestiżu, sukcesu czy bezpieczeństwa. Fałszywe platformy inwestycyjne obiecują szybkie zyski, a fałszywe sklepy internetowe oferują luksusowe produkty w niezwykle niskich cenach.

Presja czasu jako kluczowy element manipulacji

Jednym z najskuteczniejszych narzędzi manipulacji, zarówno w marketingu, jak i w scamie, jest presja czasu. Oferty typu **„Ostatnia szansa!”** czy **„Promocja kończy się za godzinę!”** sprawiają, że konsumenci czują, iż muszą działać natychmiast, aby nie przegapić okazji. Mechanizm ten bazuje na lęku przed stratą – emocji, która potrafi wyłączyć logiczne myślenie.

„Kliknęłam w link z informacją, że oferta wygasa za 10 minut. Myślałam, że to okazja życia. Dopiero później zorientowałam się, że straciłam pieniądze”
– wspomina Ewa, która padła ofiarą fałszywego sklepu internetowego.

Scammerzy celowo wywierają presję czasu, aby uniemożliwić ofiarom spokojną refleksję. W sytuacjach wymagających natychmiastowych decyzji zdolność do analizy maleje, co sprawia, że manipulacja staje się wyjątkowo skuteczna.

Odpowiedzialność konsumenta w erze nadmiaru

Choć nadmiar ofert i bodźców wydaje się nieuniknionym elementem współczesnego świata, konsument nie jest całkowicie bezradny. Świadomość mechanizmów manipulacji oraz umiejętność krytycznej analizy informacji to kluczowe narzędzia, które mogą pomóc w ochronie przed oszustwami.

Odpowiedzialność za podejmowane decyzje spoczywa zarówno na osobach wywierających wpływ, jak i na nas samych. Im bardziej jesteśmy świadomi mechanizmów manipulacji, tym trudniej na nas oddziaływać.

Aby zmniejszyć ryzyko stania się ofiarą scamu, warto nauczyć się odróżniać autentyczne oferty od tych, które budzą podejrzenia. Umiejętność zarządzania swoją uwagą i krytycznego podejścia do informacji to fundament odporności na manipulację.

Wnioski:

Współczesny konsument znajduje się w trudnej sytuacji – **między presją nadmiaru a potrzebą świadomego wyboru**. Nadmiar możliwości i złożoność ofert sprawiają, że podatność na manipulację rośnie. Jednak odpowiedzialność za swoje decyzje oraz umiejętność filtrowania informacji mogą pomóc w odzyskaniu kontroli nad własnym życiem. Konsumpcja nie musi być narzędziem manipulacji – może być aktem świadomego wyboru, jeśli tylko nauczymy się zarządzać własną uwagą.

Rozdział 3:

Mechanizmy manipulacji – jak działa scam?

W świecie przesyconym informacjami manipulacja staje się codziennym elementem naszego życia. Scammerzy, którzy opanowali sztukę wpływania na ludzkie emocje i decyzje, stosują wyrafinowane techniki oparte na psychologii, socjologii i najnowszych technologiach. Rozumiejąc, jak działają te mechanizmy, możemy lepiej chronić siebie i innych przed ich destrukcyjnymi skutkami.

Manipulacja polega na wykorzystywaniu nieświadomości jednej strony przez drugą w celu osiągnięcia własnych korzyści. Jej skuteczność opiera się na subtelności – umiejętności stworzenia iluzji, że podejmowane decyzje są nasze, podczas gdy w rzeczywistości zostały narzucone z zewnątrz.

W tym rozdziale przeanalizujemy kluczowe mechanizmy wykorzystywane przez oszustów finansowych oraz poznamy historie ofiar, które pokazują, jak łatwo wpaść w ich pułapkę.

Scamy finansowe: nowoczesne oszustwa, które mogą dotknąć każdego

Scamy finansowe to często wyrafinowane oszustwa, coraz częściej z wykorzystaniem technik deepfake. Jeśli myślisz, że przestępstwa finansowe z wykorzystaniem mediów społecznościowych, SMS-ów, poczty elektronicznej, połączeń telefonicznych czy aplikacji randkowych to trywialne historie w stylu „metody na wnuczka", jesteś w błędzie. Każdy może stać się ofiarą scammerów. Oszustwa i wyłudzenia to potężny biznes przestępczy, w który inwestowane są duże pieniądze, ponieważ stopa zwrotu jest wysoka.

Presja czasu – „Musisz działać teraz!"

Jednym z mechanizmów najczęściej stosowanych przez oszustów jest wywołanie poczucia pilności. Informacje takie jak: **„Twoje konto zostanie zablokowane w ciągu 15 minut"** lub **„Oferta ważna tylko dziś!"** budują presję, która wyłącza racjonalne myślenie. To moment, w którym działamy impulsywnie, z obawy przed utratą czegoś ważnego.

Historia Oli:
„Pracowałam nad ważnym projektem, gdy dostałam SMS-a, że na moim koncie bankowym zauważono podejrzaną transakcję. Było napisane, że muszę kliknąć w link i szybko zaktualizować dane, inaczej konto zostanie zablokowane. W panice zrobiłam to. Dopiero gdy zadzwoniłam do banku, zrozumiałam, że straciłam wszystkie oszczędności".

Historia Oli doskonale ilustruje, jak presja czasu może skłonić do błędnych decyzji. Brak możliwości spokojnej refleksji ogranicza zdolność do podejmowania świadomych wyborów, co sprawia, że manipulacja staje się wyjątkowo skuteczna w takich sytuacjach.

Budowanie zaufania – fałszywe autorytety

Wielu oszustów posługuje się techniką budowania zaufania poprzez podszywanie się pod znane instytucje, takie jak banki, urzędy czy renomowane

firmy. Scammerzy często wykorzystują także wizerunki celebrytów, by nadać swoim ofertom pozory wiarygodności.

Historia Andrzeja:
„Widziałem reklamę z Robertem Lewandowskim, który rzekomo inwestował w kryptowaluty. Wszedłem na stronę, gdzie było pełno pozytywnych opinii. Myślałem, że to świetna okazja, więc wpłaciłem 5000 zł. Następnego dnia strona zniknęła, a wraz z nią moje pieniądze".

Oszustwo na autorytet to często stosowana technika manipulacji, opierająca się na naturalnej skłonności ludzi do ufania osobom rozpoznawalnym. Autorytet działa jak skuteczny filtr, który zmniejsza wątpliwości i sprawia, że mniej chętnie kwestionujemy wiarygodność przekazu, szczególnie gdy pochodzi od kogoś, kogo podziwiamy.

Granice intymności – manipulacja emocjami

Oszustwa często opierają się na wykorzystaniu emocji, takich jak strach, współczucie czy nadzieja. Scammerzy celują w nasze najsłabsze punkty, by zdobyć przewagę.

Historia Magdy:
„Dostałam wiadomość na Messengerze od znajomej, że jest w szpitalu i potrzebuje pieniędzy na pilną operację. Byłam w szoku, bo to dobra koleżanka, więc od razu przelałam jej 1000 zł przez BLIK. Dopiero później zadzwoniłam do niej i dowiedziałam się, że jej konto zostało zhakowane".

Scammerzy doskonale wykorzystują mechanizmy ludzkiej psychiki, manipulując naturalnymi odruchami, takimi jak chęć niesienia pomocy, by realizować swoje cele. Manipulacja emocjami staje się szczególnie skuteczna, gdy odwołuje się do naszych najważniejszych wartości, takich jak rodzina, przyjaźń czy poczucie bezpieczeństwa.

Obietnica szybkiego zysku – „Zainwestuj teraz i zarób miliony"

Fałszywe platformy inwestycyjne to jeden z najbardziej dochodowych rodzajów scamu. Obietnice dużych zysków przy minimalnym ryzyku przyciągają ludzi, którzy marzą o poprawie swojej sytuacji finansowej.

Historia Piotra:
„Dostałem telefon od konsultanta, który zachwalał platformę inwestycyjną. Obiecał, że w ciągu tygodnia podwoję swoje pieniądze. Zainwestowałem 10 000 zł, a potem zaczęli prosić o kolejne wpłaty, by rzekomo zwiększyć zyski. Po miesiącu zorientowałem się, że zostałem oszukany".

Obietnice szybkiego zysku przyciągają, ponieważ odwołują się do naturalnej potrzeby poprawy sytuacji materialnej i pragnienia bogactwa. To uniwersalne marzenie często wykorzystywane jest przez oszustów, którzy manipulują naszymi aspiracjami. Kluczowe jest rozwijanie umiejętności odróżniania rzeczywistych możliwości od iluzji.

Personalizacja – „To oferta specjalnie dla ciebie"

Scammerzy coraz częściej stosują personalizację, aby ich oferty wyglądały bardziej wiarygodnie. Dzięki danym z mediów społecznościowych lub innych źródeł potrafią tworzyć komunikaty, które wydają się skrojone na miarę.

Historia Anny:
„Otrzymałam e-mail, który wyglądał jak spersonalizowana oferta mojego banku. Zawierał moje imię i szczegóły konta. Wydawało się, że wszystko jest w porządku, więc kliknęłam w link i podałam dane do logowania. Kilka godzin później moje konto zostało wyczyszczone".

Personalizacja skutecznie buduje wrażenie wyjątkowości, co sprawia, że ofiara chętniej obdarza oszusta zaufaniem. Tworzy iluzję, że komunikat został stworzony specjalnie dla nas, co znacząco obniża naszą czujność i zwiększa podatność na manipulację.

Nauka z doświadczeń ofiar

Historie ofiar scamu pokazują, że każdy może paść ofiarą manipulacji, niezależnie od wieku, wykształcenia czy świadomości zagrożeń. Mechanizmy stosowane przez oszustów są tak dopracowane, że potrafią oszukać nawet osoby uważane za ostrożne i doświadczone.

Najskuteczniejszą obroną przed manipulacją jest zrozumienie jej mechanizmów. Świadomość tego, jak działa manipulacja, pozwala lepiej rozpoznawać próby wpływu i znacząco zmniejsza naszą podatność na jej oddziaływanie.

Wnioski:

Manipulacja jest narzędziem, które w rękach oszustów może prowadzić do tragicznych konsekwencji. Rozumienie mechanizmów, takich jak presja czasu, emocje czy personalizacja, pozwala nam lepiej chronić siebie i innych. Historie ofiar są ostrzeżeniem, ale także lekcją – pokazują, jak ważne jest zachowanie czujności i umiejętność krytycznego myślenia.

Rozdział 4:

Emocjonalne, społeczne i systemowe skutki scamu

Scam to zjawisko, które pozostawia za sobą nie tylko straty finansowe, ale także głębokie rany emocjonalne i społeczne. Za każdym przypadkiem kryje się człowiek, który w jednej chwili traci nie tylko pieniądze, ale także poczucie bezpieczeństwa, zaufanie do innych i wiarę w siebie.

Scam to nie tylko kwestia strat finansowych; jest to również atak na fundamentalne wartości, takie jak zaufanie, autonomia i poczucie bezpieczeństwa, które stanowią podstawę naszej tożsamości. Jego konsekwencje sięgają znacznie głębiej niż aspekty materialne, wpływając na nasze życie emocjonalne i społeczne.

W tym rozdziale przyglądamy się, jak oszustwa finansowe wpływają na jednostki, rodziny i społeczeństwo, jakie mechanizmy społeczne są szczególnie narażone na destrukcyjne skutki scamu oraz co można zrobić, aby zapobiegać kolejnym tragediom.

Emocje ofiar – od zaufania do wstydu

Historie ofiar scamu pokazują, że oszuści umiejętnie manipulują emocjami, wykorzystując strach, presję czasu i zaufanie do instytucji.

Historia Marty:
„To był telefon, który wywrócił moje życie do góry nogami. Mężczyzna powiedział, że dzwoni z banku i że moje konto jest zagrożone. W tamtym momencie byłam tak zestresowana, że uwierzyłam w każde jego słowo. Kazał mi pobrać aplikację i podać kody SMS. Zanim się zorientowałam, co się dzieje, straciłam 20 tys. zł – wszystkie oszczędności na remont mieszkania. Do dziś czuję wstyd, że dałam się tak oszukać".

Wstyd jest jednym z najsilniejszych uczuć, które powstrzymuje ofiary scamu przed szukaniem pomocy. Zamykając się w sobie, często izolują się od otoczenia, co sprawia, że stają się bardziej podatne na kolejne próby oszustwa. Pokonanie tego wstydu jest kluczowe, by przerwać cykl manipulacji i uzyskać wsparcie.

Straty finansowe to nie wszystko

Historia Pawła:
„W internecie znalazłem ofertę inwestycji w kryptowaluty. Wyglądało to bardzo profesjonalnie – były rekomendacje ekspertów, historie sukcesu i gwarancje bezpieczeństwa. Zainwestowałem 50 tys. zł – oszczędności życia. Dwa dni później strona przestała działać. Straciłem wszystko. Dziś mam nie tylko problem finansowy, ale i ogromne poczucie winy wobec rodziny, która ufała, że podejmuję mądre decyzje".

Według danych NBP średnia strata finansowa ofiar oszustw w pierwszym półroczu wyniosła 9 tys. zł, choć niektóre osoby tracą całe oszczędności gromadzone przez lata. Konsekwencje takich oszustw są niezwykle dotkliwe – mogą prowadzić do zadłużenia, rozpadu relacji rodzinnych, a nawet problemów psychicznych. Straty materialne to tylko część problemu; prawdziwa tragedia scamu polega na zburzeniu poczucia stabilności i bezpieczeństwa, które często budujemy przez całe życie.

Rodziny na celowniku – konsekwencje finansowe i emocjonalne

Scam nie kończy się na jednostce. Straty finansowe i emocjonalne często odbijają się na bliskich, wpływając na relacje i stabilność rodzinną.

> **Historia Marii:**
> *„Mój mąż padł ofiarą oszustwa na fałszywe inwestycje. Straciliśmy pieniądze odkładane na studia dla naszego syna. To zrujnowało nasze plany i relację. Przez wiele miesięcy nie mogliśmy o tym rozmawiać bez kłótni".*

Scam można postrzegać jako formę przemocy społecznej, która atakuje fundamentalne struktury, takie jak rodzina. Niszczy poczucie stabilności i bezpieczeństwa, mając dalekosiężne konsekwencje zarówno dla jednostek, jak i ich otoczenia.

Zniszczone zaufanie – fundament relacji społecznych

Scam atakuje jeden z najważniejszych społecznych zasobów – zaufanie.

> **Historia Anny:**
> *„Kiedy odkryłam, że moja dobra znajoma była zamieszana w scam, straciłam zaufanie do niej i do ludzi w ogóle. Zaczęłam podejrzewać wszystkich o złe intencje".*

Zaufanie można porównać do delikatnej nici pajęczej, która opiera się na wielu punktach podparcia. Naruszenie choćby jednego z tych punktów osłabia całą strukturę, prowadząc do utraty stabilności i poczucia bezpieczeństwa.

Społeczne koszty scamu

Na poziomie społecznym skutki oszustw finansowych są dalekosiężne:

- **Straty finansowe na poziomie globalnym:** Oszustwa finansowe powodują straty liczone w setkach miliardów dolarów rocznie, które są często reinwestowane w działalność przestępczą.
- **Spadek zaufania do instytucji:** Ludzie tracą zaufanie do banków, rządów i systemów prawnych, co zagraża stabilności społecznej i politycznej.
- **Kryzys zaufania do technologii:** Scam wykorzystuje platformy cyfrowe, które miały służyć poprawie jakości życia. Brak zaufania do tych technologii może hamować innowacje i rozwój gospodarki.

Samotność i stygmatyzacja ofiar

Ofiary scamu często spotykają się z brakiem empatii ze strony otoczenia, co pogłębia ich izolację i poczucie wstydu.

> **Historia Krzysztofa:**
> *„Straciłem oszczędności życia na fałszywe inwestycje w kryptowaluty. Brat wyśmiał mnie, nazywając naiwnym. Od tamtej pory nikomu już o tym nie mówię".*

Empatia odgrywa kluczową rolę w udzielaniu wsparcia ofiarom oszustw. Bez niej osoby dotknięte traumą pozostają osamotnione w swoich przeżyciach, co zwiększa ich podatność na kolejne manipulacje i oszustwa.

Społeczna odporność – klucz do przyszłości

Budowanie ochrony przed scamem wymaga działań na wielu poziomach:

- **Edukacja i świadomość:** Powszechna edukacja o zagrożeniach musi stać się priorytetem.
- **Wzmacnianie więzi społecznych:** Silne relacje międzyludzkie zmniejszają podatność na manipulacje.
- **Odpowiedzialność instytucji:** Banki i firmy technologiczne powinny wprowadzać skuteczne systemy ochrony oraz wspierać ofiary scamu.
- **Budowanie zaufania:** Transparentność instytucji i kampanie społeczne mogą pomóc w odbudowie zaufania tam, gdzie zostało ono naruszone.

Scam to problem o charakterze systemowym, który wymaga skoordynowanych działań na globalną skalę. Budowanie odporności społecznej oznacza nie tylko ochronę przed zagrożeniami, ale również zdolność do odbudowy relacji i wartości, które oszustwa próbują zniszczyć.

Cyberprzestępczość od kuchni: zorganizowane grupy, wymuszenia i międzynarodowe powiązania

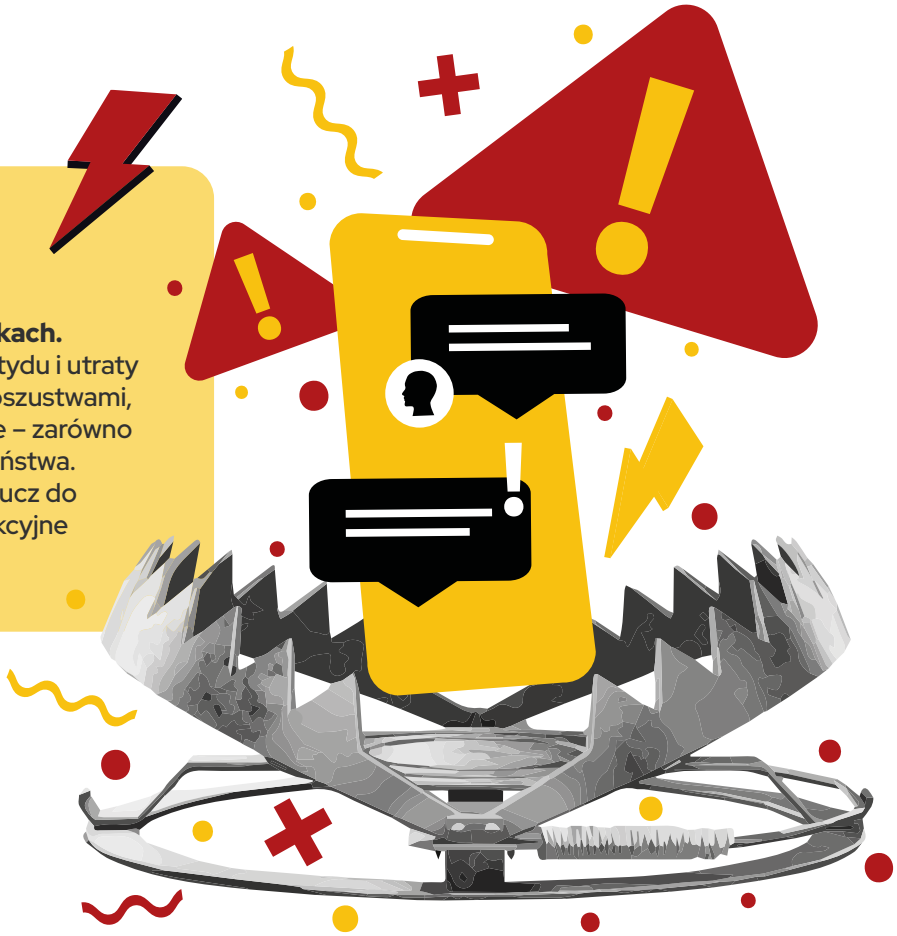
Postaraj się pomyśleć o przestępcach internetowych nie w kategoriach drobnych złodziejaszków, ale profesjonalnej, zorganizowanej grupy przestępczej z własnym call center, „marketingiem", specjalistami od IT, grafikami i zapleczem technologicznym. Korzystają z najnowocześniejszych rozwiązań technologicznych i wiedzy z zakresu technik manipulacyjnych. Mają zasięg międzynarodowy, a często ze sobą współpracują.

Z danych Interpolu wynika, że oszuści finansowi działają na przecięciu innych przestępczych biznesów, takich jak handel ludźmi, bronią i narkotykami. W Azji, Afryce, ale także, jak wiele na to wskazuje, w Europie do ataków scammerskich wykorzystywani są ludzie działający pod przymusem. Są to osoby zrekrutowane na fikcyjne oferty pracy lub ofiary handlu ludźmi.

Osoba, która dzwoni, próbując wyłudzić twoje pieniądze, niekoniecznie musi być cynikiem bez skrupułów, pozbawionym empatii socjopatą, ale osobą przymuszoną do określonych działań.

Wnioski

Scam to nie tylko **liczby w statystykach.** To ludzkie historie pełne strachu, wstydu i utraty zaufania. Aby skutecznie walczyć z oszustwami, musimy zrozumieć ich konsekwencje – zarówno na poziomie jednostki, jak i społeczeństwa. Edukacja, współpraca i empatia to klucz do budowania odporności na te destrukcyjne działania.



Rozdział 5:

Technologia w rękach oszustów – ewolucja scamu

Technologia, która miała ułatwiać nasze życie, stała się jednym z głównych narzędzi wykorzystywanych przez oszustów. Scam ewoluował wraz z rozwojem cyfrowych innowacji: od fałszywych e-maili po zaawansowane deep fake'i. Rozumiejąc, jak technologie są wykorzystywane przeciwko nam, możemy nauczyć się lepiej chronić siebie i swoje dane.

Technologia sama w sobie nie jest ani dobra, ani zła – jej wartość zależy od tego, jak zostanie wykorzystana przez ludzi. Wyzwaniem staje się sytuacja, gdy rozwój innowacji przewyższa nasze możliwości etycznego i odpowiedzialnego zarządzania nimi, co może prowadzić do ich niewłaściwego zastosowania.

Phishing i smishing – pierwsze kroki oszustów w cyberprzestrzeni

Pierwsze próby oszustw internetowych były proste, ale skuteczne. Phishing, czyli podszywanie się pod zaufane instytucje w celu wyłudzenia danych, był jednym z najwcześniejszych narzędzi stosowanych przez cyberprzestępców. Smishing (phishing za pomocą wiadomości SMS) szybko zyskał na popularności wraz z rozwojem telefonii komórkowej.

Historia Jakuba:
„Dostałem SMS-a od rzekomej firmy kurierskiej z informacją, że moja przesyłka czeka na opłacenie 2 zł. W linku podano szczegóły. Kliknąłem, wpisałem dane karty i nie minęło kilka godzin, a z mojego konta zniknęło 10 tys. zł. To był mój pierwszy kontakt z czymś takim – nigdy bym nie pomyślał, że można tak łatwo zostać oszukanym".

Phishing działa, ponieważ ludzie ufają instytucjom, które są znane i powszechnie używane. Oszuści często wykorzystują nazwiska popularnych firm kurierskich, banków czy platform zakupowych, aby ich przekazy wydawały się autentyczne.

Zaawansowane techniki – ransomware i ataki BEC

W miarę jak technologie stawały się bardziej zaawansowane, oszuści zaczęli korzystać z metod takich jak ransomware – oprogramowanie, które blokuje dostęp do danych i żąda okupu za ich odblokowanie. Innym przykładem jest BEC (Business Email Compromise), gdzie przestępcy podszywają się pod członków zarządu firm, by wymusić przelewy. W tym roku doszło do najsłynniejszego jak dotąd ataku typu BEC. Pracownik brytyjskiej firmy w Hong Kongu odbył telekonferencję z kilkoma przedstawicielami centrali, którzy zlecili mu przelanie 25 mln dol. na wskazane konto. Dopiero po zrealizowaniu transakcji wyszło na jaw, że uczestnicy narady zostali wygenerowani przez AI i całość była dobrze przeprowadzonym deep fake'owym atakiem scammerskim.

Historia Małgorzaty:
„Pracuję w firmie średniej wielkości. Dostałam e-mail od przełożonego z prośbą o pilny przelew na konto kontrahenta. Wszystko wyglądało jak zawsze – e-mail był identyczny, a ton wiadomości pasował do szefa. Dopiero później okazało się, że przelew trafił na konto przestępców. Straciliśmy 50 tys. zł".

BEC (Business Email Compromise) to forma manipulacji, która łączy wykorzystanie technologii z ludzką skłonnością do zaufania i posłuszeństwa wobec autorytetów. Technologia w takich przypadkach jest jedynie narzędziem, a to cechy naszej natury, takie jak ufność i respekt wobec autorytetów, sprawiają, że te oszustwa są tak skuteczne.

Deep fake – przyszłość manipulacji?

Jedną z najnowszych i najbardziej niepokojących technologii wykorzystywanych przez oszustów jest właśnie deep fake – cyfrowo zmanipulowane obrazy i filmy, które mogą wyglądać jak prawdziwe. Deep fake pozwala przestępcom tworzyć fałszywe reklamy, oszukańcze treści medialne, a nawet podrabiać głosy znanych osób.

Na stronie Scammingout.pl zamieściliśmy wideoklip będący kolażem fałszywych reklam, w których wykorzystano wizerunki znanych osób. Warto dodać, że CERT NASK doliczył się aż 121 polityków, sportowców, duchownych, lekarzy, dziennikarzy, celebrytów, których wizerunki zostały wykorzystane w fałszywych reklamach w tym roku.

Historia Sylwii:
„Widziałam reklamę wideo, w której znany ekonomista zachwalał platformę inwestycyjną. Wyglądało to tak wiarygodnie, że nie miałam wątpliwości, że to prawdziwe. Zainwestowałam 20 tys. zł, a potem odkryłam, że cały materiał był fałszywy".

Deep fake rewolucjonizuje świat oszustw, zmieniając fundamentalne zasady weryfikacji rzeczywistości. Kiedy obraz czy głos przestają być wiarygodnymi dowodami, tracimy jedno z podstawowych narzędzi do oceny prawdziwości informacji, co otwiera szerokie pole do manipulacji.

Zbieranie danych – jak oszuści zdobywają informacje?

Jednym z kluczowych elementów sukcesu cyberprzestępców jest dostęp do danych. Współczesne technologie pozwalają na zbieranie informacji o użytkownikach na niespotykaną dotąd skalę. Media społecznościowe, pliki cookies czy publiczne rejestry to tylko niektóre z narzędzi wykorzystywane przez oszustów do tworzenia spersonalizowanych ataków.

Sami również ułatwiamy zadanie przestępcom w niefrasobliwy sposób, dzieląc się informacjami na swój temat w mediach społecznościowych czy podając wrażliwe dane, które pomagają określić adres zamieszkania, zawód, miejsce pracy. Takie szczegóły znakomicie pomagają oszustom w zwodzeniu ofiar podczas celowanego w konkretną osobę ataku scammerskiego.

Historia Michała:
„Zorientowałem się, że oszuści musieli wiedzieć coś o mnie. Wiedzieli, że ostatnio szukałem kredytu, więc zadzwonili z ofertą ‚specjalnie dla mnie'. Byłem przekonany, że rozmawiam z prawdziwym konsultantem".

Personalizacja zwiększa podatność ofiar na oszustwa, ponieważ ludzie mają większą skłonność do zaufania informacjom, które wydają się dostosowane specjalnie do nich. W rzeczywistości takie treści często wynikają z analizy danych udostępnianych w internecie, co pozwala oszustom precyzyjnie dopasować swoje przekazy.

Wnioski: Edukacja jako fundament ochrony

Choć technologie wykorzystywane przez oszustów stają się coraz bardziej zaawansowane, edukacja pozostaje najskuteczniejszym narzędziem ochrony. Zrozumienie, jak działają scammerzy i jakie techniki stosują, pozwala zmniejszyć ryzyko stania się ofiarą.

NASK podaje, że podczas piłkarskich Mistrzostw Europy kilkakrotnie wzrosła liczba powiadomień o fałszywych stronach, reklamach zgłaszanych przez użytkowników. Powód był jeden: przed meczami pojawiała się reklama społecznościowa przestrzegająca przed scamami.

Historia Alicji:
„Kiedyś kliknęłabym w link bez zastanowienia. Ale po tym, jak wzięłam udział w szkoleniu o cyberbezpieczeństwie, zaczęłam podchodzić do takich rzeczy z większą ostrożnością. Dziś wiem, jak rozpoznać fałszywą wiadomość i nie dać się oszukać".

Technologia, choć stanowi wyzwanie, może także stać się narzędziem budowania odporności na manipulację. Kluczem jest współpraca między użytkownikami, instytucjami i ekspertami, którzy muszą wspólnie działać, aby minimalizować zagrożenia.

Rozdział 6:

Systemy i regulacje – jak prawo walczy ze scamem?

Scam jest nie tylko problemem jednostek, ale także wyzwaniem dla systemów prawnych, które próbują nadążyć za dynamicznie rozwijającymi się technologiami i metodami oszustów. W tym rozdziale przyjrzymy się, jakie regulacje i mechanizmy ochronne funkcjonują obecnie w Polsce i na świecie, oraz ocenimy ich skuteczność w walce z oszustwami finansowymi.

Prawo stanowi fundament wyznaczający granice moralne w społeczeństwie. W kontekście scamu problemem nie jest brak regulacji, lecz ich niedostosowanie do dynamicznie zmieniającej się rzeczywistości technologicznej, co utrudnia skuteczne przeciwdziałanie oszustwom.

Prawo a oszustwa – obecne ramy prawne

W Polsce walka ze scamem opiera się głównie na przepisach kodeksu karnego, w tym art. 286 dotyczącego oszustwa oraz art. 287 regulującego kwestie przestępstw komputerowych. W praktyce oznacza to, że każda osoba, która wyłudza pieniądze, dane lub usługi, podlega odpowiedzialności karnej.

> **Historia Jana:**
> *„Zgłosiłem sprawę na policję, gdy straciłem 5 tys. zł po fałszywym telefonie od ‚pracownika banku'. Funkcjonariusze powiedzieli mi, że takie sprawy są trudne do rozwiązania, bo oszuści często działają z zagranicy. Czułem się bezradny".*

Zwalczanie skutków scamów jest sprawą niełatwą z kilku przyczyn. Główna to ograniczone zasoby policji. Od kilku lat działa **Centralne Biuro Zwalczania Cyberzagrożeń**, ale z ogromnym zakresem odpowiedzialności: od walki z hakerami, przez pornografię dziecięcą, pedofilię, aż po oszustwa finansowe. Nieźle działa system wymiany informacji między organami ścigania w ramach Interpolu, co skutkuje udanymi próbami rozbijania międzynarodowych gangów oszustów. Problem w tym, że bardzo trudno jest odzyskać pieniądze z przestępstw i zwrócić je ofiarom.

Nieco lepiej jest z przestępczością na krajowym podwórku. Bardzo dobrą pracę wykonują krajowe CERTy i CSiRTy oraz wyspecjalizowane komórki bezpieczeństwa w bankach, które uważnie monitorują internet i generalnie rynek pod kątem oszustw, wspierając policję w namierzaniu przestępców.

Technologie w służbie prawa

W odpowiedzi na rosnące zagrożenie oszustwami coraz więcej instytucji finansowych i firm technologicznych inwestuje w zaawansowane systemy zabezpieczeń. Przykłady to:

- **Sztuczna inteligencja:** algorytmy analizujące transakcje w czasie rzeczywistym i wykrywające podejrzane operacje.
- **Blokady phishingu:** mechanizmy w przeglądarkach i aplikacjach mobilnych, które ostrzegają użytkowników przed potencjalnie niebezpiecznymi stronami.
- **Systemy dwuskładnikowego uwierzytelniania (2FA):** zwiększające bezpieczeństwo kont użytkowników.

Historia Tomasza:
„Kiedy oszuści próbowali zalogować się na moje konto, bank natychmiast zablokował dostęp dzięki systemowi wykrywającemu nietypowe logowania. To uratowało moje pieniądze. Bez nowoczesnych technologii straciłbym wszystko."

Technologia może być zarówno narzędziem w rękach oszustów, jak i skuteczną bronią przeciwko nim. Kluczem do ograniczenia zagrożeń jest nieustanny rozwój systemów zabezpieczeń, które potrafią przewidywać i reagować na coraz bardziej zaawansowane metody przestępców.

Edukacja jako element regulacji

Prawo i technologie nie wystarczą, jeśli społeczeństwo nie będzie świadome zagrożeń. Dlatego coraz więcej krajów wprowadza programy edukacyjne skierowane zarówno do młodzieży, jak i dorosłych.

Przykład Finlandii:

Finlandia wprowadziła obowiązkowe lekcje cyberbezpieczeństwa w szkołach średnich. Dzięki temu młodzi ludzie uczą się, jak rozpoznawać oszustwa i chronić swoje dane w internecie.

W Polsce nie ma takich przepisów, tym niemniej należy zauważyć, że prywatne firmy, instytucje, jak UOKiK, KNF, NASK, mnóstwo organizacji i fundacji prowadzi wiele wartościowych kampanii edukacyjnych uświadamiających społeczeństwo, jak groźne są oszustwa finansowe, uczących, jak się przed nimi bronić.

Wady i wyzwania systemowe

Mimo licznych regulacji i technologii walka ze scamem wciąż napotyka poważne przeszkody:

1. **Międzynarodowy charakter oszustw.**
   Przestępcy często działają z krajów, gdzie ściganie ich jest trudniejsze.

2. **Brak jednolitych regulacji.**
   Nawet w ramach Unii Europejskiej różnice w prawie utrudniają współpracę.

3. **Niska świadomość społeczna.**
   Wielu ludzi nadal nie wie, jak rozpoznać scam lub gdzie zgłaszać przypadki oszustw.

Historia Anny:
„Kiedy zgłosiłam scam na policję, usłyszałam, że kwota jest za mała, by wszczynać dochodzenie. Czułam się, jakby nikogo to nie obchodziło. Dopiero po zgłoszeniu do mediów sprawa została zauważona".

Systemy prawne często nie nadążają za potrzebami związanymi z przeciwdziałaniem oszustwom. Skuteczna reakcja wymaga nie tylko dostosowania przepisów, ale również silniejszej woli politycznej i społecznej, by zmierzyć się z tym rosnącym problemem.

Wnioski

Walka ze scamem wymaga kompleksowego podejścia, które łączy prawo, technologię i edukację. Musimy dążyć do:

1. Harmonizacji przepisów międzynarodowych, aby ułatwić ściganie przestępców działających transgranicznie.
2. Inwestycji w technologie, które pozwolą na szybsze wykrywanie i neutralizowanie zagrożeń.
3. Zaangażowania platform internetowych w realną walkę z oszustwami finansowymi, fałszywymi reklamami i ofertami.
4. Wspierania ofiar scamu, które często czują się osamotnione i bezradne.

Prawo pełni funkcję tarczy, chroniąc przed zagrożeniami, ale aby było skuteczne, musi być stale doskonalone, by sprostać nowym wyzwaniom. Walka ze scamem to długotrwały proces, który wymaga współpracy i zaangażowania wszystkich stron.

Rozdział 7:

Wiedza kontra praktyka – jak nauczyć się rozpoznawać scam?

Edukacja na temat scamu i oszustw finansowych jest dzisiaj ważniejsza niż kiedykolwiek. Jednak wiedza teoretyczna to jedno, a umiejętność zastosowania jej w praktyce to zupełnie inna sprawa. Badania pokazują, że nawet osoby świadome zagrożeń często nie potrafią rozpoznać oszustwa w codziennych sytuacjach. W tym rozdziale zastanowimy się, dlaczego tak się dzieje i jak możemy zwiększyć naszą zdolność do identyfikowania scamu.

Edukacja a rzeczywistość – wyniki badań

Z przeprowadzonej na stronie www.scammingout.pl ankiety wynika, że 100% badanych zadeklarowało, iż padło ofiarą scamu. Jednak wnikliwsza analiza wykazała, że tylko 30% z nich potrafiło rozpoznać oszustwo w praktyce. Oznacza to, że większość ludzi nie zdaje sobie sprawy, że została zmanipulowana, co wskazuje na ogromną lukę między świadomością a zdolnością do rozpoznania oszustwa.

Świadomość zagrożeń to zaledwie pierwszy krok. Kluczowe jest praktyczne zastosowanie tej wiedzy w codziennych sytuacjach, co wymaga systematycznego ćwiczenia i budowania nawyków pozwalających skutecznie reagować na potencjalne zagrożenia.

Dlaczego nie potrafimy rozpoznać scamu?

1. **Przeciążenie informacyjne**
   W dzisiejszym świecie bombardowani jesteśmy setkami informacji każdego dnia. W takim chaosie trudno odróżnić prawdziwe wiadomości od fałszywych.

> **Historia Agnieszki:**
> *„Codziennie dostaję dziesiątki e-maili i SMS-ów. Nie zawsze mam czas, by je dokładnie czytać, więc klikam w to, co wygląda znajomo. Tak właśnie dałam się nabrać na fałszywą wiadomość od mojego banku".*

2. **Zbyt duże zaufanie do technologii**
   Wiele osób uważa, że technologia zawsze działa w ich najlepszym interesie. Tymczasem oszuści celowo tworzą strony, aplikacje i wiadomości, które wyglądają na autentyczne.

> **Historia Piotra:**
> *„Myślałem, że mój bank ma świetne zabezpieczenia i nie da się podszyć pod jego stronę. Gdy zobaczyłem fałszywą stronę, nawet się nie zorientowałem, że coś jest nie tak".*

Jak poprawić zdolność rozpoznawania scamu?

1. **Edukacja praktyczna zamiast teoretycznej**
   Zamiast jedynie mówić o zagrożeniach, warto ćwiczyć realne scenariusze. Szkoły, organizacje i firmy mogą organizować symulacje oszustw, które pomogą ludziom nauczyć się identyfikować zagrożenia.

2. **Technologie wspierające rozpoznawanie oszustw**
   Korzystanie z narzędzi takich jak menedżery haseł, filtry antyphishingowe czy aplikacje edukacyjne może pomóc w identyfikowaniu fałszywych stron i wiadomości.

3. **Kultura otwartej komunikacji**
   Ludzie często wstydzą się przyznać, że zostali oszukani, co utrudnia dzielenie się wiedzą i doświadczeniami. Promowanie otwartej komunikacji o scamach może zwiększyć świadomość i zdolność do rozpoznawania oszustw.

Historia Elżbiety:
„Po tym, jak oszukano mnie na fałszywej zbiórce charytatywnej, byłam zbyt zawstydzona, by powiedzieć o tym znajomym. Teraz wiem, że mogłam ostrzec innych i zapobiec kolejnym oszustwom".

Najczęstsze błędy w rozpoznawaniu scamów

1. **Ufność w wygląd stron internetowych**
   Oszuści inwestują w profesjonalne grafiki i layouty, które wyglądają niemal identycznie jak strony oficjalne.

2. **Klikanie w linki bez weryfikacji**
   Brak dokładnego sprawdzenia adresu URL to jeden z najczęstszych błędów.

3. **Podawanie danych osobowych i finansowych na niesprawdzonych platformach**
   Często ofiary nie zastanawiają się, dlaczego dana strona prosi o ich dane.

Oszuści wykorzystują nasze nawyki i brak uwagi, co sprawia, że jesteśmy bardziej podatni na ich manipulacje. Rozpoznanie oszustwa wymaga świadomego zatrzymania się i dokładnej analizy każdej sytuacji, zamiast automatycznego reagowania.

Jak edukować społeczeństwo?

1. **Kampanie społeczne**
   Duże instytucje, takie jak banki czy rządy, powinny inwestować w kampanie uświadamiające zagrożenia związane z oszustwami.

2. **Programy szkolne i firmowe**
   Szkoły powinny wprowadzać zajęcia z cyberbezpieczeństwa, a firmy organizować regularne szkolenia dla pracowników.

3. **Aplikacje i quizy edukacyjne**
   Interaktywne narzędzia, które symulują różne rodzaje oszustw, mogą pomóc ludziom lepiej rozpoznawać zagrożenia.

Wnioski: Droga do skutecznej obrony

Walka ze scamem to proces, który wymaga ciągłego doskonalenia naszych umiejętności i świadomości. Choć badania pokazują, że większość ludzi miała styczność z oszustwami, niewielu potrafi je skutecznie rozpoznawać. To wyzwanie, ale także szansa na zbudowanie społeczeństwa bardziej świadomego i odpornego na manipulację.

Rozpoznawanie scamu to umiejętność, którą można i należy rozwijać. Wymaga to edukacji, regularnej praktyki oraz refleksji nad otaczającymi nas sytuacjami i naszymi własnymi reakcjami, by zwiększyć odporność na manipulację.

Ostatecznie walka z oszustwami to kwestia nie tylko ochrony finansów, ale także budowania zaufania, bezpieczeństwa i poczucia kontroli nad własnym życiem. Jeśli wyciągniemy wnioski i zaczniemy działać teraz, możemy stworzyć świat, w którym scam stanie się zjawiskiem marginalnym, a nie codzienną rzeczywistością.

Wnioski końcowe:

6 kluczowych wniosków na temat walki ze scamem

1. Współpraca

W 2025 r. Polska obejmie prezydencję w Unii Europejskiej. To dobra okazja, żeby problem oszustw finansowych poruszyć na szerokim forum państw członkowskich. Scamy finansowe są wspólnym problemem i doświadczeniem każdego z krajów. Walka w pojedynkę jest o wiele mniej skuteczna niż w ramach wspólnego frontu. Chodzi w szczególności o jedno stanowisko wobec platform internetowych, bez udziału których wciąż będziemy zwalczać skutki scamów, a nie jedną z głównych przyczyn.

2. Regulacje

System regulacji wspierających walkę z oszustwami finansowymi w Polsce jest nieźle zorganizowany. Dobrym przykładem pozytywnych działań regulacyjnych jest ustawa mocno ograniczająca możliwość spoofowania numerów telefonów. Brakuje natomiast przepisów umożliwiających wymianę informacji między kluczowymi uczestnikami rynku: bankami, telekomami, KIR-em. Każdy z sektorów jest obwarowany tajemnicami danych klienta, co mocno ogranicza skuteczność walki ze złodziejami. Przykładowo banki muszą korzystać z pośredników, żeby pozyskać wiedzę o połączeniach realizowanych ze spoofowanych numerów telefonów.

3. Odpowiedzialność

Do walki z oszustwami finansowymi należy koniecznie w większym stopniu zaangażować platformy internetowe. Pomimo deklaracji z ich strony, że dokładają wszelkich starań w tym zakresie, przestępczość internetowa rozwija się w zastraszającym tempie. Niezbędne są działania regulatorów i instytucji nadzorczych na poziomie krajowym i unijnym, które zmuszą platformy do wzięcia odpowiedzialności za scam.

4. Edukacja

Zdecydowanie najważniejsze narzędzie w walce z oszustwami. Najsłabszym ogniwem w schemacie scammerskim jest człowiek. Na nic się zdadzą zabezpieczenia i technologia, jeśli ludzie nie będą świadomi swojej odpowiedzialności za własne bezpieczeństwo. Nic tak nie podnosi świadomości jak akcje edukacyjne, kampanie promocyjne. Na szczęście w Polsce jest ich bardzo dużo w przestrzeni publicznej i - coraz częściej - medialnej. Rzeczą bardzo wartościową byłoby wprowadzenie edukacji dotyczącej fałszerstw i oszustw internetowych do programu nauczania w polskich szkołach.

5. **Centralizacja**
W Polsce podejmowanych jest wiele akcji, kampanii, inicjatyw związanych z edukacją w zakresie cyberprzestępczości. Monitorowaniem cyberzagrożeń zajmuje się kilka wyspecjalizowanych ośrodków. Jest potrzeba centralizacji i koordynacji wszystkich działań, które mają na celu przeciwdziałanie oszustwom, informowanie o zagrożeniach, edukację i ochronę ludności. Ośrodek mógłby powstać w NASK, który już dzisiaj w dużym stopniu pełni taką funkcję, lub być podporządkowany UOKiK-owi. Dobrym przykładem skutecznej centralizacji działań wymierzonych w scamerów jest National Anty-Scam Center w Australii.

6. **Wsparcie psychologiczne**
Powinien powstać ośrodek udzielający wsparcia psychologicznego ofiarom oszustw finansowych. Oszukani pozostawieni są sami sobie z gigantycznym problemem finansowym i emocjonalnym, z którym często sobie nie radzą. Wskazane byłoby utworzenie telefonu zaufania dla poszkodowanych przez przestępców cybernetycznych.

Najpopularniejsze rodzaje scamu

Scam to przestępstwo, które ewoluuje w miarę postępu technologicznego. Różnorodność i poziom wyrafinowania scamów sprawiają, że mogą one dotknąć każdego – zarówno osoby prywatne, jak i firmy. Poniżej przedstawiamy najpopularniejsze rodzaje scamu, które zyskały na znaczeniu w ostatnich latach.

Phishing – oszustwo przez e-mail, SMS lub fałszywe strony internetowe

Phishing to najpopularniejsza forma scamu, która według raportu Orange stanowiła w 2023 r. aż 44% wszystkich cyberzagrożeń. Oszuści wykorzystują e-maile, SMS-y lub fałszywe strony internetowe do wyłudzania danych osobowych, takich jak loginy, hasła czy numery kart kredytowych.

Jak wygląda atak phishingowy?

- Ofiara otrzymuje wiadomość o konieczności:
  - aktualizacji danych w banku,
  - weryfikacji konta,
  - pobrania nowej wersji aplikacji bankowej.
- Wiadomość zawiera link prowadzący do fałszywej strony internetowej, która do złudzenia przypomina oryginalną witrynę banku. Na stronie ofiara podaje swoje dane logowania, które trafiają do oszustów.
- Często pod linkiem ukryte jest złośliwe oprogramowanie, które infekuje urządzenie i daje przestępcom pełny dostęp.

Jak się chronić?

- **Nie klikaj w linki w wiadomościach e-mail i SMS-ach.** Banki nigdy nie wysyłają takich powiadomień.
- **Sprawdzaj adres URL strony internetowej.** Fałszywe strony często mają literówki w adresach (np. „bank.pl" zamiast „bank.com").
- **Zgłaszaj podejrzane wiadomości.** Informując bank o phishingu, pomagasz w zwalczaniu oszustów.

Vishing i smishing – oszustwa przez telefon i SMS

Vishing (voice phishing)

Oszuści podszywają się pod pracowników banku, policji lub innych instytucji, aby zdobyć Twoje dane lub nakłonić Cię do przelania pieniędzy na „bezpieczne konto".

Przykładowe scenariusze:

- Informacja o nieautoryzowanym przelewie.
- Rzekoma konieczność zabezpieczenia środków przed hakerami.
- Prośba o podanie danych do logowania lub przelanie pieniędzy.

Smishing

Wiadomości SMS zawierające linki prowadzące do fałszywych stron. Najczęściej podszywają się one pod firmy kurierskie, operatorów telefonicznych czy banki.

Przykłady wiadomości:

- „Twoja paczka nie może zostać dostarczona. Kliknij tutaj, aby zapłacić brakującą kwotę."
- „Zablokowano Twoje konto bankowe. Zaloguj się tutaj, aby je odblokować."

Jak się chronić?

- **Nie udostępniaj danych przez telefon.** Zawsze rozłącz się i samodzielnie skontaktuj z bankiem.
- **Nie klikaj w linki w SMS-ach.** Sprawdzaj komunikaty na oficjalnych stronach firm.

Scam inwestycyjny – fałszywe reklamy i doradcy inwestycyjni

Oszustwa inwestycyjne to jeden z najbardziej wyrafinowanych rodzajów scamu. Oszuści podszywają się pod znane osoby, np. celebrytów, i zachęcają do inwestycji w nieistniejące produkty finansowe.

Jak działa scam inwestycyjny?

1. Ofiara widzi w mediach społecznościowych reklamę z obietnicą wysokich zysków.
2. Reklama prowadzi na stronę przypominającą platformę inwestycyjną.
3. Z ofiarą kontaktuje się „doradca", który nakłania ją do zainstalowania oprogramowania umożliwiającego zdalny dostęp do komputera.
4. Przestępcy przejmują kontrolę nad kontem ofiary i kradną jej środki.

Jak się chronić?

- Nie ufaj ofertom „złotych inwestycji". Zyski rzędu 300% w krótkim czasie to nierealne obietnice.
- Weryfikuj reklamy. Sprawdzaj, czy osoba reklamująca produkt faktycznie jest z nim związana.
- Nie instaluj podejrzanego oprogramowania.

Oszustwa w mediach społecznościowych

Scam na przelew (np. metoda „na BLIK")

Oszuści włamują się na konto społecznościowe ofiary i wysyłają do jej znajomych wiadomości z prośbą o szybki przelew, np. za pomocą kodu BLIK.

Romance scam

Przestępcy podszywają się pod atrakcyjne osoby w aplikacjach randkowych, budując relacje z ofiarami, aby wyłudzić pieniądze. Typowe scenariusze to prośby o opłacenie operacji, podróży czy rozwiązanie nagłych problemów finansowych.

Jak się chronić?

- Nie przesyłaj pieniędzy osobom poznanym online.
- Zabezpiecz swoje konta w mediach społecznościowych. Używaj silnych haseł i włącz uwierzytelnianie dwuetapowe.

Fałszywe sklepy internetowe i oferty wakacyjne

Fałszywe sklepy

Oszustwa polegają na tworzeniu stron internetowych

przypominających znane marki, które oferują produkty w niezwykle atrakcyjnych cenach.

Fałszywe oferty wakacyjne

Ofiary wpłacają zaliczki na wynajem nieruchomości, które nie istnieją. Najczęściej zdarza się to w sezonie wakacyjnym.

Jak się chronić?

- Kupuj w znanych sklepach. Sprawdzaj opinie o sprzedawcy.
- Nie wpłacaj zaliczek za wynajem nieruchomości bez weryfikacji. Sprawdź adres i właściciela nieruchomości.

Ransomware – ataki na firmy

Ransomware to złośliwe oprogramowanie, które blokuje dostęp do danych ofiary i żąda okupu za ich odblokowanie. Najczęściej celem są firmy, ale również osoby prywatne mogą stać się ofiarami.

Jak się chronić?

- Regularnie twórz kopie zapasowe.
- Aktualizuj oprogramowanie.
- Nie otwieraj podejrzanych załączników.

Fałszywe zbiórki charytatywne

Oszustwa bazujące na empatii i chęci niesienia pomocy. Przestępcy tworzą fałszywe kampanie na rzecz chorych dzieci, ofiar katastrof czy zwierząt, wyłudzając pieniądze od darczyńców.

Jak się chronić?

- **Weryfikuj zbiórki.**
  Sprawdzaj ich rejestr na stronie zbiorki.gov.pl.
- **Przekazuj datki za pośrednictwem znanych platform crowdfundingowych.**

Podsumowanie

Scam to narzędzie przestępców, które nieustannie się rozwija. Kluczem do ochrony przed nim jest edukacja, czujność i stosowanie podstawowych zasad bezpieczeństwa. Niezależnie od rodzaju scamu pamiętaj, że przestępcy bazują na emocjach, nieostrożności i braku wiedzy. Pozostawanie czujnym to Twoja najlepsza obrona.

Partnerzy „Scamming Out!". Wspólne działania na rzecz bezpieczeństwa finansowego.

mBank

Szczepionka na cyberoszustów

Magdalena Korona, inżynierka bezpieczeństwa ds. strategii i technologii antyfraudowych w mBanku

Metody stosowane przez cyberprzestępców ewoluują w szybkim tempie. Niemniej jednak bardzo często mają wspólny mianownik – opierają się na manipulacji oraz podszywaniu się pod konkretne instytucje czy pracowników banku. Wprowadziliśmy już szereg rozwiązań, które mają na celu ochronę klientów przed tego typu atakami.

Jednym z nich jest mobilna autoryzacja rozmowy z pracownikiem banku. Dzięki temu klienci mogą być pewni, że rozmawiają z autentycznym przedstawicielem banku. Kolejnym przykładem naszych działań jest wizualna identyfikacja nadawcy wiadomości e-mail. Identyfikator nadawcy jest widoczny w oficjalnych aplikacjach mobilnych danego serwisu lub po zalogowaniu do niego w przeglądarce internetowej. Dzięki temu klienci mogą łatwo rozpoznać, czy wiadomość pochodzi od mBanku, ponieważ jest oznaczona logotypem organizacji.

Jednakże technologia to nie wszystko. Niezwykle ważne jest również budowanie świadomości użytkowników o zagrożeniach, jakie na nich czyhają w sieci. W mBanku doskonale zdajemy sobie z tego sprawę i od lat prowadzimy kampanie edukacyjne w zakresie cyberbezpieczeństwa. Byliśmy pierwszym bankiem, który prowadzi takie działania regularnie.

Od ubiegłego roku w ramach kampanii „Samoobrona w sieci" edukujemy klientów na temat metod stosowanych przez cyberprzestępców oraz sposobów ochrony przed nimi.

Ponadto, by jeszcze lepiej przedstawić, w jaki sposób oszuści manipulują swoimi ofiarami, naciągając je na fałszywe inwestycje, wyprodukowaliśmy we współpracy z firmą Voice House 6-odcinkowy kryminalny serial audio „Jazgot". Scenariusz do słuchowiska, przy wsparciu ekspertów ds. bezpieczeństwa mBanku, napisał Łukasz Orbitowski. Narratorem serii jest Jarosław Kuźniar. W tym roku poszliśmy o krok dalej i do współpracy przy drugim sezonie „Jazgotu" zaprosiliśmy aż czworo autorów poczytnych powieści. Oprócz Łukasza Orbitowskiego - Katarzynę Puzyńską, Igora Brejdyganta oraz Marcela Woźniaka. Każda z osób przygotowała scenariusz, w którym przedstawiona jest inna metoda oszustwa. A jakie są to historie? Zachęcam do posłuchania na najpopularniejszych platformach podcastów. Wszystkie są dostępne na www.mbank.pl/jazgot.

Nasze kampanie to jednak nie wszystko. By budować świadomość klientów, regularnie informujemy o najnowszych zagrożeniach poprzez aplikację mobilną, serwis transakcyjny, stronę internetową czy strony w mediach społecznościowych.

Świadomość zagrożeń oraz wiedza o tym, jak się przed nimi chronić, m.in. stosując rozwiązania wprowadzane przez mBank, to swoista **„szczepionka na cyberoszustów".**

kryminalny serial audio Jazgot Historie

Czworo autorów. Cztery historie. Cztery oszustwa.
Posłuchaj serialu i nie daj się oszukać.

Katarzyna **Puzyńska** | Igor **Brejdygant** | Łukasz **Orbitowski** | Marcel **Woźniak**

Serial dostępny na najpopularniejszych platformach podcastowych.

Do wysłuchania zaprasza:

mBank

Wiedza i rozwaga w walce z zagrożeniami

Marta Strzyżewvska, dyrektor zarządzająca ds. marketingu i zaangażowań społecznych PZU

Szeroko pojęte oszustwa finansowe – *podszywanie się przez mail, SMS lub rozmowę telefoniczną, fałszywe konkursy, zbiórki, oferty inwestycyjne albo metoda „na wnuczka"* – są dziś prawdziwą plagą. Na celowniku scammerów są dosłownie wszyscy, od pojedynczych osób po największe korporacje i instytucje publiczne, a liczba dokonywanych każdego dnia na świecie, także w naszym kraju, prób cyberataków i innych oszustw jest trudna do wyobrażenia. Z naszych badań wynika, **że tylko 4 proc.** Polaków czuje się całkowicie bezpiecznie podczas korzystania z internetu, a rosnącej świadomości zagrożeń niekoniecznie towarzyszy praktyczna wiedza, jak w praktyce ich unikać lub przynajmniej minimalizować ryzyko. Dlatego przykładamy ogromną wagę do działań edukacyjnych i prewencyjnych, by wzmacniać zbiorową odporność na dezinformację. Jest to jeden z naszych celów w obszarze zaangażowania społecznego, wskazanych w nowej trzyletniej strategii Grupy PZU **„Z pewnością przyszłość".**

Chcemy szczególnie uczulić Polaków na socjotechniki stosowane przez oszustów, którzy grają na naszych emocjach, wykorzystują chwile słabości lub nieuważności. Niezależnie od coraz bardziej zaawansowanych i wyrafinowanych narzędzi technologicznych, jakimi dysponują przestępcy, ostatecznie otwartą dla nich furtką albo skuteczną barierą jest nasz umysł. Zasada ograniczonego zaufania musi stać się naszą rutyną. To ważny aspekt niedawnej kampanii edukacyjno-informacyjnej PZU na temat cyberbezpieczeństwa **„A kto tu się podszywa?"** i naszych przyszłych działań w tym obszarze. Angażujemy się też w cenne zewnętrzne inicjatywy, jak kampania „Scamming out!", które współgrają z naszym podejściem, czyli edukowaniem o bezpieczeństwie finansowym i w sieci w sposób, jakiego Polacy oczekują, czyli nie strasząc, lecz dostarczając im konkretnych porad i rozwiązań.

Jesteśmy w tych działaniach wiarygodni, bo sama Grupa PZU jest przykładem poważnego traktowania współczesnych zagrożeń i dbałości o bezpieczeństwo własnego biznesu oraz danych i pieniędzy naszych klientów. Jako lider rynku ubezpieczeniowego i największa grupa w sektorze finansowym jesteśmy także celem wielu prób ataków hakerskich czy wykorzystywania marki PZU przez podszywających twórców oszukańczych ofert finansowych. Wielowarstwowe, stale aktualizowane systemy bezpieczeństwa, odpowiednie procedury, szybkość reakcji na zagrożenia, współpraca z rynkiem i regulatorami, a przede wszystkim budowana konsekwentnie poprzez szkolenia i inne działania edukacyjne kultura cyberbezpieczeństwa wśród pracowników pozwalają nam skutecznie mierzyć się z tymi wyzwaniami.

A kto tu się **podszywa**?

Oszuści mogą podszywać się pod Twoich bliskich lub znane Ci instytucje.
Poznaj ich sztuczki i bądź sprytniejszy.

Sprawdź na niedajsiepodszyc.pl.

PZU

Materiał wygenerowany przy użyciu sztucznej inteligencji.
Kampania sfinansowana z funduszu prewencyjnego PZU.


ORLEN
Uważaj
na oszustów
w sieci
www.orlen.pl

Nest! BANK

Bezpieczeństwo finansowe to nasz priorytet

Dariusz Włodarczyk, dyrektor Departamentu Cyberbezpieczeństwa w Nest Banku

W Nest Banku wiemy, że najlepsza ochrona to czujność i wiedza. Dlatego w działaniach na rzecz bezpieczeństwa finansowego skupiamy się na pokazywaniu realnych zagrożeń, z którymi mogą spotkać się nasi klienci. Nie mówimy skomplikowanym językiem – stawiamy na proste komunikaty i konkretne przykłady, które uczą, jak rozpoznać oszustwo i skutecznie się przed nim bronić.

Codziennie słyszymy o nowych technikach stosowanych przez cyberprzestępców, którzy próbują przejąć dostęp do naszych danych i pieniędzy. Kreatywność oszustów nie ma granic. Fałszywe SMS-y z linkami do „dopłat", podrobione strony logowania, telefony „od pracownika banku" czy atrakcyjne „oferty inwestycyjne" to tylko nieliczne z metod, z którymi możesz mieć do czynienia.

Warto wiedzieć, jak rozpoznać te zagrożenia i skutecznie się przed nimi bronić. Oszuści często wykorzystują presję czasu, sugerując, że natychmiastowa reakcja jest konieczna – to ich sposób na wywołanie stresu i ograniczenie naszej czujności. Podszywają się pod znane instytucje, korzystając z fałszywych numerów telefonów lub adresów e-mail, które na pierwszy rzut oka wyglądają wiarygodnie. Coraz częściej wykorzystują również nowe technologie, takie jak deep fake, aby jeszcze bardziej uwiarygodnić swoje działania. Kluczowe jest, aby zawsze weryfikować podejrzane wiadomości i nie podejmować pochopnych decyzji – szczególnie jeśli w grę wchodzi kliknięcie w link czy przekazanie swoich danych. Edukacja i działania zapobiegawcze to najskuteczniejsze sposoby ochrony przed negatywnymi skutkami tych zagrożeń.

Dlatego co roku aktywnie włączamy się w obchody Europejskiego Miesiąca Cyberbezpieczeństwa, promując świadome i bezpieczne korzystanie z usług cyfrowych. Pokazujemy, w jakich sytuacjach oszuści potrafią nas zaskoczyć i jak skutecznie się przed nimi chronić. Nasze kampanie opieramy na przykładach z życia, które są zrozumiałe i przystępne dla każdego. Prezentujemy konkretne metody oszustw, krok po kroku wyjaśniamy mechanizmy działania przestępców oraz podpowiadamy, jak się nie dać nabrać.

Nieustannie przypominamy, że bezpieczeństwo zaczyna się od czujności. Każdy powinien wiedzieć, jak rozpoznać zagrożenie. Oszuści nieustannie doskonalą swoje metody, wykorzystując najnowsze technologie. Według raportu Związku Przedsiębiorstw Finansowych w Polsce (ZPF) oraz EY Polska 37,5 proc. przedstawicieli branży finansowej uważa, że skala zagrożeń związanych z nadużyciami zwiększyła się w ciągu ostatnich 12 miesięcy[1] . Wskazuje to na potrzebę intensyfikacji działań prewencyjnych i edukacyjnych.

1[1] Nadużycia w sektorze finansowym 2024. Nowy raport ZPF i EY | EY - Polska

Bank Polski

Jak nie dać się oszustom w sieci

Piotr Kalbarczyk, dyrektor Departamentu Cyberbezpieczeństwa w PKO Banku Polskim

PKO Bank Polski regularnie prowadzi działania edukacyjne i informacyjne w zakresie cyberbezpieczeństwa i dostosowuje je do aktualnych zagrożeń oraz „sezonowych" działań oszustów. Takim sezonowym działaniem są np. oszustwa na fałszywe sklepy internetowe, a przestępcy tworzą tu coraz lepiej przygotowane „reklamy" skierowane do internautów. Wzmożona aktywność cyberoszustów jest szczególnie widoczna w okresie Black Friday i w czasie przedświątecznym oraz w trakcie „gorączki" noworocznych wyprzedaży i właśnie wtedy bank ostrzega przed tymi zagrożeniami.

Oczywiście działania, które zbroją klientów w wiedzę nt. cyberbezpieczeństwa, prowadzone są cały rok. Dostarczamy konkretne informacje i przykłady, jak działają oszuści i jak manipulują odbiorcami. Bank dzięki temu stara się „wyprzedzić" swoimi działaniami edukacyjnymi zbliżające się kampanie phishingowe. W tym roku uwrażliwialiśmy klientów hasłem: „Znamy ofertę oszustów! Sprawdź, jak nie skorzystać!", aby zwrócić uwagę na wszechobecne fałszywe reklamy i fałszywe sklepy internetowe będące często lustrzanym odbiciem tych prawdziwych.

W 2024 r. bank przybliżał też klientom rolę dwuetapowego logowania, zachęcając do aktywacji tej funkcji. Zwracaliśmy m.in. szczególną uwagę na fałszywe inwestycje, opisując modus operandi oszustów, obrazując rolę reklam stworzonych przy pomocy technologii deep fake i wskazując, jak ustrzec się przed oszustwami tego rodzaju. W innej kampanii opisywaliśmy oszustwa skierowane do użytkowników portali ogłoszeniowych, bo serwisy tego typu są i będą obszarem działalności przestępców z powodu ich popularności oraz możliwości zmanipulowania użytkowników, nie zawsze świadomych tego, jak dokładnie działa dany portal.

Wszechstronne materiały edukacyjne na temat zagrożeń w sieci można znaleźć na specjalnej stronie PKO Banku Polskiego poświęconej cyberbezpieczeństwu https://www.pkobp.pl/lp/w/cyberbezpieczenstwo, na której m.in. opisujemy 5 rodzajów oszustw: podszywanie się telefoniczne pod pracownika banku, wyłudzanie kodów BLIK, fałszywe linki w SMS, nabieranie na tzw. fałszywe inwestycje oraz podszywanie się pod publiczne sieci Wi-Fi.

Eksperci PKO Banku Polskiego zdają sobie sprawę, że zmieniające się działania oszustów wymagają dynamicznych środków bezpieczeństwa i systematycznych działań podnoszących świadomość na temat zagrożeń w sieci. Dlatego spotykają się stacjonarnie z klientami, aby skuteczniej promować wiedzę dotyczącą cyberbezpieczeństwa wśród osób mniej zaznajomionych z cyfrowych światem, np. seniorów. PKO Bank Polski stara się dotrzeć do różnych kategorii klientów, by możliwie jak największą grupę wyposażyć w wiedzę, jak świadomie poruszać się w internecie i eliminować ryzyko stania się ofiarą oszustów. Na takich spotkaniach eksperci banku informują też o aktualnych zagrożeniach i spodziewanych trendach w cyberprzestępczości. Spotkania odbywają się w miastach w całej Polsce kilka razy w miesiącu. Także na stronie internetowej banku i na bankowych profilach w mediach społecznościowych systematycznie informujemy na temat zagrożeń czyhających na klientów banku i zasad cyberbezpieczeństwa. Dzięki takiemu podejściu PKO Bank Polski rozmaitymi sposobami wzmacnia świadomość klientów na temat zagrożeń w sieci.

Razem przeciw oszustom: jak budować cyfrową odporność

Robert Grabowski, szef CERT Orange Polska

Wspólnym mianownikiem większości internetowych oszustw jest to, że to my sami **„otwieramy drzwi"** przestępcom. Sposobów na wykradanie danych czy pieniędzy jest mnóstwo, często wpisują się one w bieżącą sytuację, kontekst aktualnych wydarzeń czy tematykę interesującą konkretną grupę osób. Zwykle mają wspólną cechę: link do podstawionej strony, graficznie przypominającej witrynę znanego nam banku czy firmy obsługującej płatności online, pod którą podszywają się oszuści, albo też rozmowa telefoniczna z „bankowym konsultantem". Wpisanie na tej stronie lub podanie podczas rozmowy danych logowania do konta czy danych karty płatniczej grozi utratą wszystkich pieniędzy. A wystarczy odpowiednia świadomość, by chronić się przed tego rodzaju oszustwami.

W Orange Polska przywiązujemy ogromną wagę nie tylko do rozwijania odpowiednich mechanizmów zabezpieczeń i ochrony naszych klientów, ale też do edukacji w zakresie cyberbezpieczeństwa. Dlatego stale szukamy nowych kanałów dotarcia do społeczeństwa. Chodzi o wyrobienie **„cyberodporności stadnej".** Od niemal 30 lat budujemy nasze doświadczenie, co pozwala nam na coraz większą skuteczność. Tylko w ubiegłym roku nasze autorskie rozwiązanie – **CyberTarcza** – zablokowało ponad 360 tys. domen z fałszywymi stronami wyłudzającymi dane i ochroniła 5,5 mln użytkowników przed utratą pieniędzy. Internauci zawsze mogą liczyć na wsparcie z naszej strony. Wiadomości, które budzą wątpliwość, można przesłać na adres **cert.opl@orange.com lub SMS-em na nr 508 700 900**. To tylko chwila, a może przyspieszyć blokadę potwierdzonych stron phishingowych i pomóc ochronić także innych użytkowników internetu. Warto śledzić bieżące ostrzeżenia na stronie cert.orange.pl, a także na Twitterze @CERT_OPL.

Budowanie świadomości, ostrzeganie internautów to odpowiedzialna praca, która przynosi największe efekty, gdy działamy razem z innymi. Dlatego bardzo cenię wymianę myśli i współpracę z instytucjami, dla których zapewnienie bezpieczeństwa internautów jest najwyższą wartością.

Krzysztof Szczepański, dyrektor Departamentu Bezpieczeństwa i Ryzyka w KIR

Przestępcy są już o krok przed nami, bo nie mają ograniczeń prawnych. Tworzą struktury charakterystyczne dla korporacji, używają metod naukowych i działają globalnie. My musimy skonsolidować wysiłki, działać razem i szybko, inaczej zawsze będziemy krok z tyłu.

Źródła danych:

1. CERT Polska – Raport o cyberzagrożeniach w Polsce (2022 i 2023).

2. CSIRT KNF – Statystyki fałszywych reklam i incydentów (2023–2024).

3. Komisja Nadzoru Finansowego (KNF) – Ostrzeżenia dotyczące oszustw internetowych.

4. Raporty z kampanii edukacyjnych na temat cyberbezpieczeństwa w Polsce.

ORGANIZATORZY

PATRONI HONOROWI

PARTNERZY

Dziękujemy za udział w akcji!

Scamming Out!

ORGANIZATORZY

Puls Biznesu

Bankier.pl