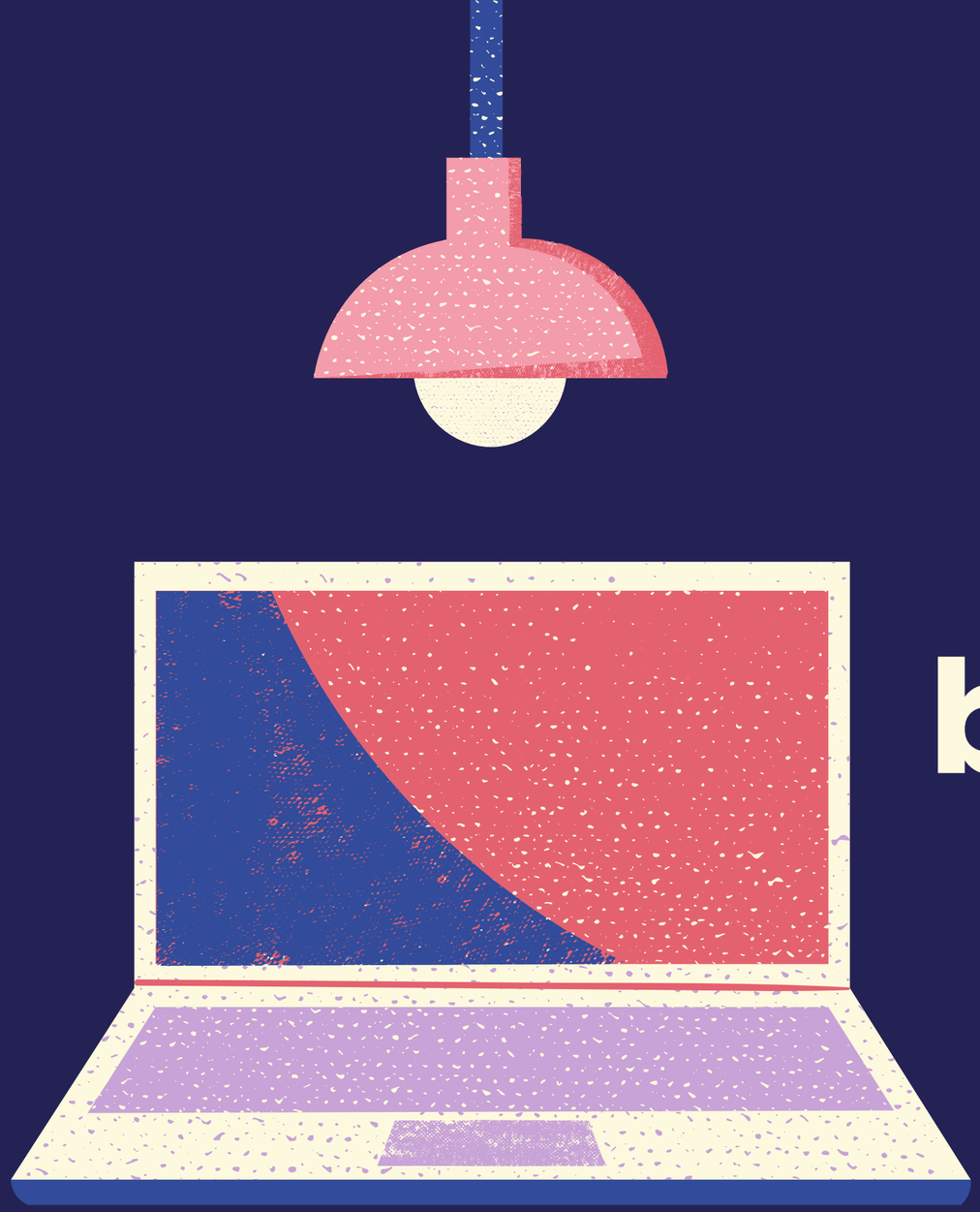


Wszystko o bezpieczeństwie w internecie.

Wskazówki, które pozwolą przeciwdziałać oszustwu w internecie.

Spis treści

Na czym polega Internetowe oszustwo?

Oszustwo internetowe to przestępstwo, które polega na wykorzystaniu Internetu do oszukiwania ludzi, zwykle w celu osiągnięcia korzyści finansowej. Oszustwa mogą przyjmować różne formy, od phishingu, aż po oszustwa aukcyjne, kradzież tożsamości i wiele innych.

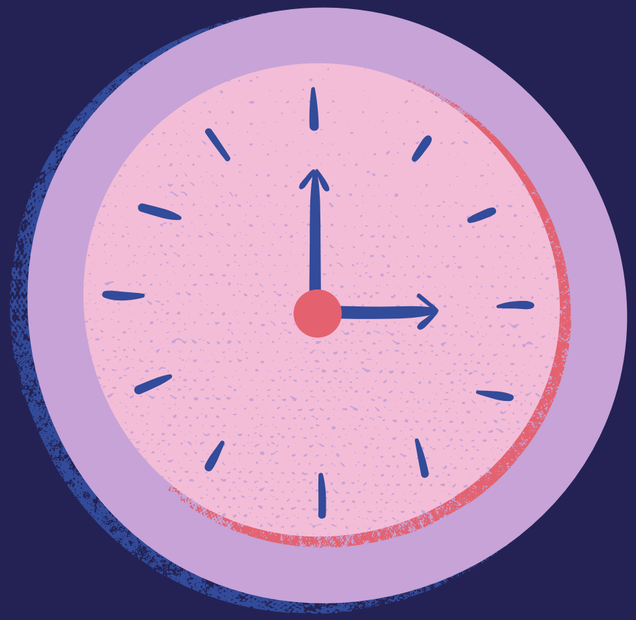
Przykłady oszustw i wyłudzeń w internecie:

- **scam – to różnego rodzaju nieprawdziwe informacje (przekazywane w mailach, postach, reklamach i rozmowach telefonicznych), których zadaniem jest przyciągnięcie uwagi, zaangażowanie emocjonalne i zmanipulowanie ofiary;**
- **phishing – aby pozyskać zaufanie ofiary i wyłudzić jej dane, przestępca podszywa się pod funkcjonariuszy służb mundurowych, konsultantów znanych firm, urzędników, serwisantów, pracowników zakładów energetycznych, banków i biur obsługi klienta;**
- **spoofing – polega na fałszowaniu danych identyfikacyjnych (numerów telefonów, adresów mailowych, adresów stron) w celu uśpienia podejrzeń osoby, która jest celem oszusta;**
- **spam – duże ilości niechcianych maili lub postów, wśród których łatwo ukryć wiadomości zawierające phishing i scam.**

Jak przeciwdziałać oszustwu w internecie?

Nie ma jednoznacznej odpowiedzi na pytanie: „Jak uchronić się przed oszustami w Internecie?” Oszustwa internetowe to łatwy sposób na kradzież pieniędzy innych ludzi i zawsze znajdzie się ktoś chętny do skorzystania z tej metody.
Metody zapobiegania oszustwom internetowym:

1.Kierowanie się zdrowym rozsądkiem;
2.Brak zaufania do kogoś, kto oferuje nieoczekiwanie duże kwoty;
3.Nie płacenie kartą, kierując się niezrozumiałymi linkami przesłanymi pocztą elektroniczną lub za pośrednictwem komunikatorów internetowych. Do płatności należy używać tylko tych witryn, do których ma się zaufanie. Można także ręcznie wpisać nazwę witryny w wyszukiwarce, by nie trafić na stronę stworzoną przez oszustów;
4.Nie należy wysyłać nikomu pieniędzy, aby później w zamian otrzymać coś za darmo.



Będąc oszukiwanym należy działać szybko.

Osoba, która padła ofiarą oszustwa w Internecie powinna jak najszybciej działać. Szczególnie ważne do wykonania są trzy kroki:

Krok 1- zawiadomienie policji

Kiedy tylko dowiesz się, że padłeś ofiara oszustwa internetowego natychmiast **złóż zawiadomienie o możliwości popełnienia przestępstwa**. Zrobisz to w najbliższej jednostce Policji albo Prokuratury. Wobec tego, że cyberoszuści świetnie się maskują i anonimizują swoje ruchy to w dużej liczbie spraw nie udaje się ustalić sprawcy przestępstwa. To nie szkodzi. Jest to jednak ruch konieczny dla powodzenia w sprawie.

Krok 2 – reklamacja do banku

Powiadom o całej sytuacji bank prowadzący Twój rachunek bankowy, z którego dokonano kradzieży pieniędzy. Złóż jednocześnie reklamację bankową. Z naszego doświadczenia wynika, że ponad 99% przypadków kończy się negatywnym rozpatrzeniem reklamacji. Nie martw się, to standardowa procedura bankowa. Złożenie reklamacji jest warunkiem koniecznym do podjęcia dalszych działań i odzyskania zabranych Ci pieniędzy.

Krok 3 – raport BIK

Natychmiast złóż wniosek o raport BIK. W ten sposób dowiesz się, czy cyberoszuści nie zaciągnęli na Twoje dane osobowe zobowiązań finansowych. Włamanie na konto bankowe, a w konsekwencji wyłudzenie kredytu to niestety często spotykane zjawisko. Przy okazji warto wykupić taką usługę jak Alert BIK. Dzięki niej w czasie rzeczywistym dowiesz się czy ktoś nie próbuje zaciągać kredytów i pożyczek na Twoje dane.

Kiedy wykonasz wszystkie te czynności musisz zacząć realną walkę o sprawiedliwość. W końcu z twojego konta zniknęły pieniądze. Możliwe też, że oszuści dodatkowo wzbogacili się twoim kosztem zaciągając na Ciebie kredyty i pożyczki.

Jakie są sposoby oszustw w Internecie?

1.Phishing to jedna z najpopularniejszych metod działania oszustów internetowych. Ma ona na celu przede wszystkiem “łowienie haseł”. Standardowa wersja tej metody polega na rozsyłaniu fałszywych maili, podszywając się w nich pod instytucje takie jak banki, ZUS, czy US.

2. Carding to jedna z wielu metod wykorzystania cudzej karty kredytowej dla własnych korzyści. Polega ona przede wszystkim na uzyskaniu danych karty, jak numer, data ważności, kod CVV, w celu wykorzystania ich, najczęściej do dokonywania zakupów online.

3. Złodzieje w swych metodach są coraz bardziej kreatywni, czego dowodem jest oszustwo na BLIKa. Zaczynało się od prób wyłudzania różnymi kanałami i różnymi scenariuszami, udostępnienia kodu BLIK jako ratunku w jakiejś kryzysowej sytuacji. Pod naszych znajomych i rodzinę, na różnych komunikatorach, podszywali się złodzieje. Teraz doszły do tego fałszywe strony do płatności BLIK. Za ich pośrednictwem, złodziej może przechwycić kod i wykorzystać go w innym serwisie transakcyjnym, lub aby dokonać wypłaty z bankomatu.

4. Kolejna metoda działania oszustów, którą można podciągnąć pod rodzaj Phishingu. Oszustwo na Allegro to ostatnimi czasy prawdziwa plaga. Skrzynki mailowe Allegrowiczów zalewane są masą wiadomości email wymagających aktualizacji danych w serwisie. To samo tyczy się Allegro Lokalnie, choć maile dotyczą blokady konta. Oszuści preparują niemalże identyczne wiadomości z tymi, które faktycznie rozsyła Allegro. W tej metodzie chodzi przede wszystkim o to, by ofiara kliknęła link i przeszła do formularza, za pomocą którego oszuści wyłudzają nasze dane.

5. Bardzo popularna metoda wprowadzania ludzi w błąd to właśnie Spoofing. Metoda ta polega na podszywaniu się, a nawet wykorzystaniu osób trzecich czy instytucji, do uzyskania podstępem danych ofiar. W Spoofingu nie chodzi o imitowanie, ale wykorzystywanie faktycznie istniejących witryn internetowych, zarejestrowanych numerów telefonów, czy adresów email. Dla wprawnego hakera nie ma trudności, by przechwycić dane z niezaszyfrowanych stron internetowych, czy wykorzystać cudze ID Dzwoniącego i połączyć się z cudzego numeru telefonu, czy nawet wysłać email ze skrzynki należącej do realnej osoby.

Największe ataki hakerskie:

Nigeryjski szwindel

Nigeryjski szwindel to jeden z najbardziej znanych przekrętów internetowych typu scam phishing. Na kontach e-mailowych milionów osób pojawiły się wiadomości sugerujące, że ma się przed sobą niepowtarzalną okazję na uzyskanie nagrody wysokości co najmniej kilkuset tysięcy dolarów. Warunek? Trzeba uiścić początkową opłatę, która pomoże oszustowi odzyskać władzę nad majątkiem, którym jest gotów się podzielić. Na przełomie lat 90. i w roku 2000 w ten sposób na samym terenie USA wyłudzono około 100 milionów dolarów. Ciekawostką jest, że ten sposób oszustwa istniał już wcześniej, ale w formie analogowych listów.

Atak na PlayStation Network

Systemy zostały zamknięte z powodu konserwacji – z takim komunikatem spotkali się w kwietniu 2011 roku gracze chcący skorzystać ze swojej konsoli PlayStation. Okazało się jednak, że wiadomość ta została upubliczniona przez hakerów z grupy LulzSec. Platforma była niedostępna przez ponad miesiąc. Ciekawostka: hakerom udało się wykraść dostęp do kont 77 milionów użytkowników, w tym zdobyć cenne informacje dot. kart płatniczych i kredytowych.

Robak Sasser

Sven Jaschan, czyli 18-letni przestępca, stworzył robaka (szkodliwe oprogramowanie) o nazwie Sasser, który odpowiadał za 70% wszystkich infekcji komputerowych w 2004 roku. Program był zdolny do automatycznej replikacji, co powodowało, że skuteczna walka z nim była niemożliwa.
Ciekawostka: Sasser był tak skuteczny, że nie dało się przed nim uchronić nawet Komisji Europejskiej, ani kilku dużym bankom.

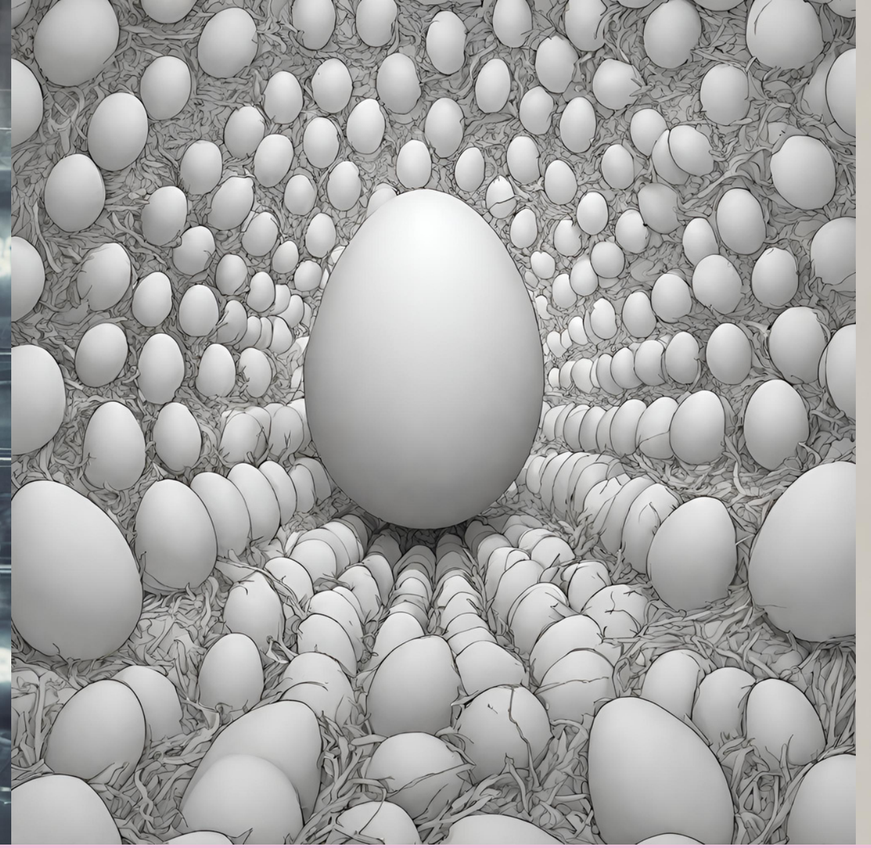
Gumisie

Za pierwszy atak cybernetyczny w Polsce uznaje się akcję przeprowadzoną przez tzw. Gumisiów. W drugiej połowie lat 90. udało im się zyskać dostęp do serwera Naukowej i Akademickiej Sieci Internetowej. Zmienili jej nazwę na ‚Niezwykle Aktywna Siatka Kretynów”.
Co było celem popełnienia przestępstwa? Grupa miała jedno żądanie: nie dopuścić do uznania podwyżek cen za użytkowanie internetu. Odpowiedzią NASK było ulepszenie ubezpieczeń, aby sytuacja nigdy się nie powtórzyła. Gumisiom się to nie spodobało i przeprowadzili drugi atak, ponownie skuteczny.

Centrum Hakerów w Indiach

Kim był Hamza Bendelladj ?

Urodzony w 1988 r. w Tizi Ouzou, to algierski cyberprzestępca i carder występujący pod pseudonimem BX1 i nazywany ‚Uśmiechniętym Hakerem”. Bendelladj jest poliglotą, władającym 5 językami, często używanymi w celach zarobkowych ze względu na swoją wiedzę językową, aby wyłudzić pieniądze niemal wszędzie na świecie. Skutkowało to poszukiwaniami, które trwały 5 lat. Znalazł się na liście 10 najbardziej poszukiwanych hakerów przez Interpol i FBI za rzekomą defraudację dziesiątek milionów dolarów z ponad dwustu amerykańskich i europejskich instytucji finansowych za pośrednictwem wirusa komputerowego ‚SpyEYE Botnet”, który zainfekował ponad 60 milionów komputerów na całym świecie, głównie w Stanach Zjednoczonych, i został opracowany wspólnie z jego rosyjskim wspólnikiem Aleksandrem Andriejewiczem Paninem, znanym również jako ‚Gribodemon”, w celu kradzieży informacji bankowych przechowywanych na zainfekowanych komputerach.
Wszystkie ukradzione pieniądze przeznaczył na ubogich w Afryce i Palestynie dlatego wiele osób nazywa go “Dobrym Hakerem”.


Dziękujemy za uwagę!