INTERNETOWE LOVE

Jak zadbać o swoje cyberbezpieczeństwo w relacjach online

PORADNIK 2023/2024

NASK

NASK

INTERNETOWE LOVE

Jak zadbać o swoje cyberbezpieczeństwo
w relacjach online

Poradnik 2023/2024

AUTORZY:

Anna Kwaśnik

Anna Kwaśnik, absolwentka Instytutu Profilaktyki Społecznej i Resocjalizacji na Uniwersytecie Warszawskim, ekspertka w Dziale Budowania Świadomości Cyberbezpieczeństwa w Państwowym Instytucie Badawczym NASK. Autorka materiałów popularyzacyjno-edukacyjnych z zakresu cyberbezpieczeństwa, różnych zagrożeń internetowych, jak również trenerka z zakresu profilaktyki niebezpiecznych zachowań w internecie, nowoczesnych technologii oraz zagadnień związanych z cyberhigieną.

Marta Melka-Roszczyk

dr Marta Melka-Roszczyk, doktor nauk o zdrowiu, psycholog, psychoterapeuta oraz biegła sądowa. W swojej prywatnej praktyce zajmuje się psychoterapią indywidualną osób dorosłych, par i małżeństw. Nieustannie doskonali warsztat swojej pracy, uczęszczając na seminaria, konferencje naukowe oraz specjalistyczne kursy i szkolenia. Autorka różnych artykułów i prac naukowych. Kwalifikacje zdobyła m.in. na Uniwersytecie Wrocławskim, Pomorskim Uniwersytecie Medycznym oraz w Krakowskim Centrum Psychodynamicznym.

Redakcja:

Tomasz Kulas

Opracowanie graficzne:

Julia Zdancewicz

Wsparcie merytoryczne:

Zuzanna Polak

Katarzyna Koletyńska

Sebastian Kondraszuk

Korekta:

Marta Danowska-Kisiel

SPIS TREŚCI

WSTĘP

Czas spędzany online przez społeczeństwo wydłuża się każdego roku, a dostęp do sieci to nasza codzienność. Wykorzystujemy ją w wielu aspektach życia, zarówno prywatnego, jak i zawodowego. Internet to już nie tylko poczta e-mail, strony internetowe i szybki dostęp do informacji, ale przede wszystkim okno na świat i dla wielu miejsce, gdzie można wyrażać siebie, swoje poglądy, a także nawiązywać znajomości, budować i podtrzymywać relacje.

Niestety, popularność różnych aplikacji, mediów społecznościowych i usług internetowych powoduje, że cyberprzestępcy i inni oszuści chętnie je wykorzystują do nieuczciwych celów. Dzięki różnym metodom manipulacji, zwanymi także socjotechniką[1], najpierw wzbudzają zaufanie, oferują pomoc i wsparcie, a w niektórych przypadkach obiecują wielką miłość czy wygraną na loterii, by w kolejnych krokach namówić swoją ofiarę do podjęcia działań, które mogą posłużyć do wyłudzenia danych lub pieniędzy.

To właśnie ataki oparte na inżynierii społecznej są najpopularniejszą grupą oszustw komputerowych, na jakie narażeni są zwykli użytkownicy internetu. Bazują one przede wszystkim na ludzkich błędach, popełnianych najczęściej pod wpływem emocji – lęku, wstydu, poczucia zażenowania, ale również euforii lub ekscytacji. Zbyt duża ufność wobec usług internetowych, czasami lenistwo, ciekawość czy pośpiech mogą sprawić, że zapominamy o podstawowych zasadach bezpiecznego korzystania z sieci i dajemy się złapać. Również wysokie poczucie pewności siebie w stosunku do nowych technologii, swoboda w ich stosowaniu oraz pozorne poczucie bezpieczeństwa ułatwiają przestępcom ich działania i powodują, że jesteśmy podatni na mechanizmy i sztuczki, jakie wobec nas stosują.

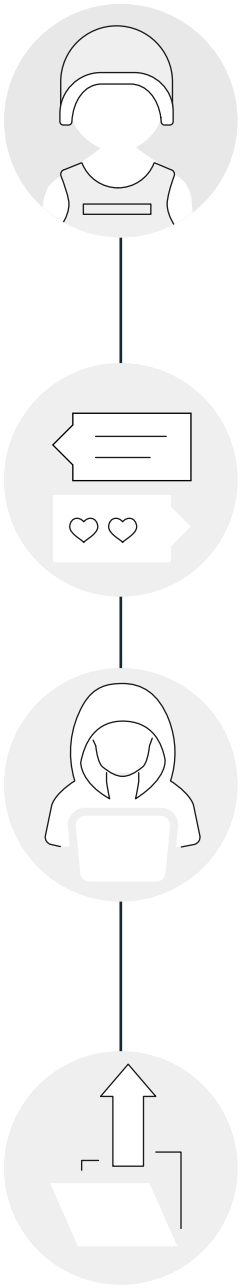
Eksperci z zespołu CERT Polska, a także z Centralnego Biura Zwalczania Przestępczości podkreślają, że zagrożenia i przestępstwa, które dotykają uczuciowej sfery użytkowników internetu i są związane ze znajomościami zawieranymi online, mogą spotkać każdego. Choć w wielu przypadkach takie zdarzenia mają znamiona czynów karalnych, to poszkodowani nie chcą powiadamiać o tym policji ani innych instytucji. Prawdopodobnie ofiary czują się nie tylko oszukane, ale również wykorzystane, a wstyd powodowany tym, że „dały się nabrać", niepotrzebnie hamuje je przed zgłoszeniem swojej krzywdy.

Konsekwencje oszustw internetowych, zwłaszcza tych związanych ze sferą intymną, to nie tylko straty finansowe czy zniszczenie wizerunku, ale przede wszystkim poczucie wykorzystania, które może prowadzić do utraty zaufania wobec innych ludzi, również bliskich. Dlatego w naszym poradniku poruszamy tematy, które dotyczą również sfery psychologicznej, związanej z naszymi emocjami.

1 Nicholson Ch., (2020), „Ataki socjotechniczne", tłum. Wnuk B., Węgrzynowicz A., „OUCH!" Biuletyn Bezpieczeństwa Internetowego nr 3 [online], dostęp 9.03.2023 r.

PRZED JAKIMI ZAGROŻENIAMI PRZESTRZEGAMY

Nasz poradnik szczegółowo omawia cztery najczęstsze odmiany przestępstw, które dotyczą relacji międzyludzkich, często w ich najbardziej intymnym wymiarze. Każde z tych zagrożeń opisane jest pod kątem technicznym, ale również wyjaśnione są pewne procesy psychologiczne, jakie mogą towarzyszyć ofierze.



OSZUSTWO NA „AMERYKAŃSKIEGO ŻOŁNIERZA”

– fałszywe historie przedstawiane przez przestępców, podszywających się pod kobiety lub mężczyzn szukających w internecie pogłębionej relacji lub miłości. Ofiary narażone są z reguły na znaczące straty finansowe.

OSZUSTWO NA PORTALU RANDKOWYM

– nastawione w pierwszej kolejności na finansowe wykorzystanie ofiary. Mechanizmy, jakie są stosowane w tego typu działaniach, mogą być bardzo różne, np. fałszywe tożsamości, szantaż, kradzież danych, obietnica szybkich zysków.

SZANTAŻ SEKSUALNY (*SEXTORTION*)

– rodzaj szantażu, podczas którego przestępcy próbują wymusić od ofiary zapłatę okupu pod groźbą ujawnienia materiałów o charakterze seksualnym.

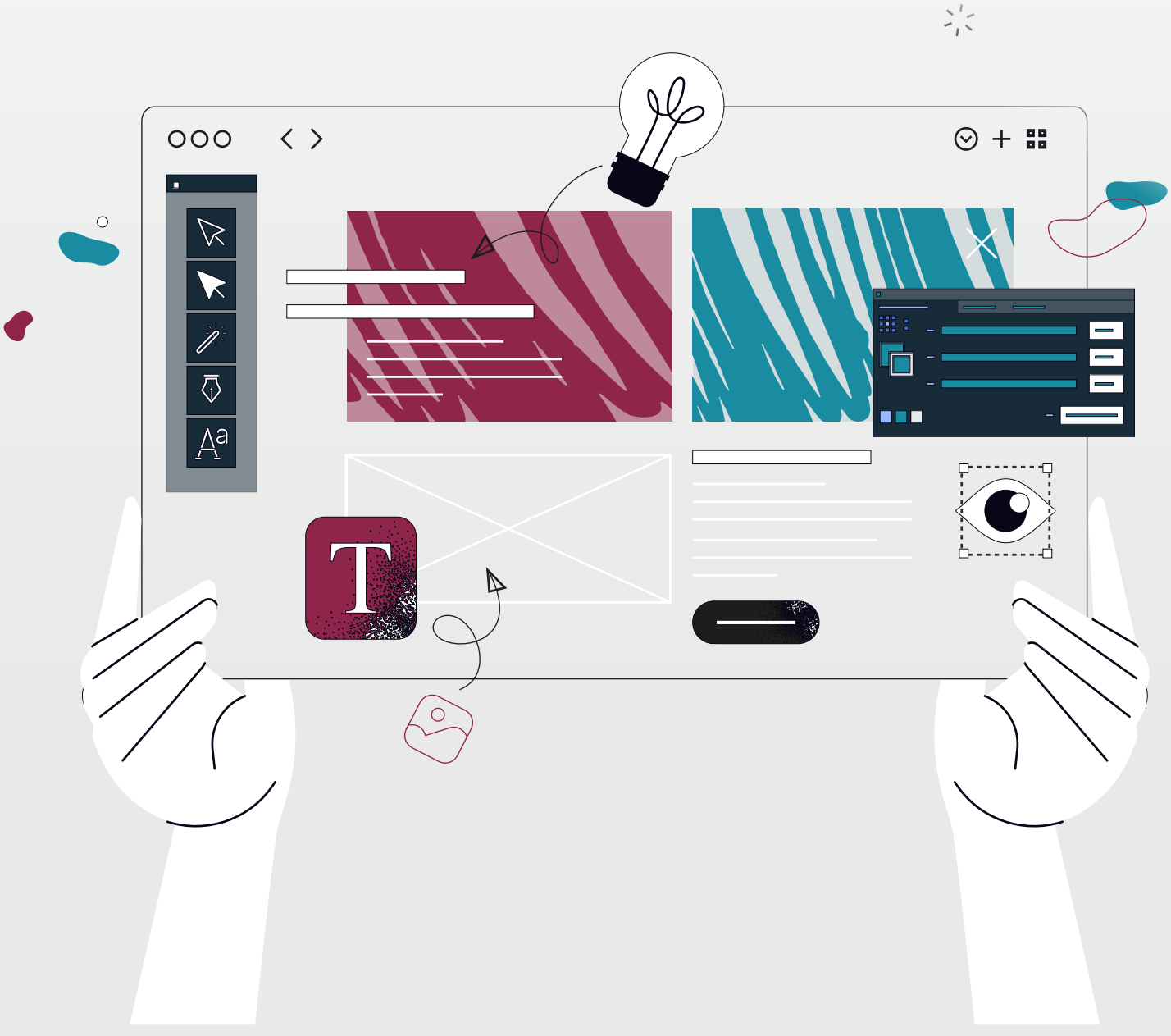
ZEMSTA PORNO *(REVENGE PORN)*

– przestępstwo polegające na ujawnieniu intymnych, seksualnych materiałów ofiary, ale w tym przypadku zazwyczaj motywacja sprawcy nie ma podłoża finansowego. Ten typ zagrożeń związany jest zwykle z działaniami bliskich osób, na przykład byłych partnerów czy osób z bliskiego otoczenia, a nie przestępców.

Rozwój współczesnych technologii sprawia, że zarówno w przypadku *sextortion*, jak i *revenge porn*, możliwe stało się wykorzystanie fałszywych materiałów o charakterze seksualnym, dlatego odrębnie omawiamy też zjawisko *deepfake porn*.

W poradniku znajdują się również wskazówki, jak się nie dać złapać na sztuczki cyberprzestępców, a także co zrobić, jeśli ktoś nas oszukał lub wykorzystał.

Podstawowym założeniem poradnika było wykorzystanie odrębnych kompetencji jego twórczyń, ekspertek w zakresie psychologii, seksuologii, ale także cyberbezpieczeństwa i internetowych przestępstw związanych chociażby z pornografią. Dzieląc się swoją wiedzą i doświadczeniem, autorki poradnika chcą ostrzec użytkowników sieci przed zagrożeniami, które wykorzystują wrażliwość związaną z potrzebą bliskości, intymności i budowania relacji.



OSZUSTWO
NA „AMERYKAŃSKIEGO ŻOŁNIERZA”
– PRZYKŁAD OSZUSTWA „ROMANCE SCAM”

Niezapłacona faktura, problemy z kontem bankowym lub dopłata do paczki to wybrane przykłady oszustw, w jakich przestępcy wykorzystują emocje, w tym strach i zaskoczenie, by zmanipulować swoją ofiarę do podjęcia aktywności, które umożliwią im przejęcie danych lub środków finansowych. Wprowadzanie w błąd, ponaglanie do podjęcia szybkich działań, presja czasu to najczęstsze narzędzia, jakimi posługują się w swoich postępowaniach. Również miłość, potrzeba bycia kochanym i inne aspekty związane ze sferą uczuciową są stale wykorzystywane przez oszustów, którzy bezustannie szukają sposobów, by zrealizować nieuczciwe zamiary.

Oszustwa oparte na różnych technikach manipulacji towarzyszą ludzkości od momentu, kiedy zaczęliśmy się komunikować. Także te o charakterze romantycznym (tzw. *romance scam*) nie są niczym nowym. Odkąd funkcjonowanie w świecie wirtualnym stało się codziennością, a duża część relacji przeszła właśnie tam, chociażby do portali społecznościowych czy randkowych, skala tego rodzaju oszustw jest znacznie większa, a wykrycie sprawców trudniejsze niż w świecie realnym.

Wchodząc w interakcję „na żywo”, człowiek zawsze ma do dyspozycji różne obszary obserwacji, takie jak np. komunikacja niewerbalna, mimika, relacje między poszczególnymi osobami, zachowanie. Jeśli któryś z tych elementów budzi zastrzeżenia i sprawia wrażenie niespójnego, człowiek nabiera podejrzeń.

W świecie internetu jego użytkownicy są pozbawieni tych możliwości, a każda narracja może być tak samo prawdziwa, jak i zakłamana. Świetnie zdają sobie sprawę z tych ograniczeń oszuści poszukujący w sieci swoich ofiar. Do jednego z najczęściej spotykanych mechanizmów oszustwa internetowego, w której przestępcy bazują na sferze uczuciowej (związanej przede wszystkim z budowaniem bliskich relacji, poszukiwaniem miłości w sieci), należy metoda na „amerykańskiego żołnierza”.

Poniżej obrazowo przedstawiamy schemat tego oszustwa, ale należy oczywiście pamiętać o tym, że liczba scenariuszy wykorzystujących zaprezentowany mechanizm może być nieograniczona. Zamiast żołnierza w sieci można spotkać „dysydenta z kraju ogarniętego wojną”, „dziennikarza walczącego z cenzurą” czy mężczyznę szukającego

„idealnej żony", a w przypadku kobiet „uciekinierkę z obozu pracy" czy po prostu „kobietę szukającą prawdziwego mężczyzny" – tę listę można rozwijać jeszcze długo, jednak wiele elementów schematu tego oszustwa jest bardzo podobnych[2].

„Amerykański żołnierz" lub „lekarka służąca na misji" – niezwykła osoba, która znalazła się w trudnej sytuacji, potrzebuje wsparcia i pocieszenia.

Ten sposób oszustwa charakteryzuje się następującym wzorcem relacyjnym: na portalu społecznościowym bądź randkowym pojawia się użytkownik, który wykazuje chęć nawiązania bliższej znajomości – opisywany tu „amerykański żołnierz".

Osoba ta, kontaktując się ze swoją ofiarą, przeważnie przedstawia siebie jako kogoś wyjątkowego, z niebywałym doświadczeniem życiowym i zawodowym, a jednocześnie niezwykle trudną sytuacją bytową. W swoim mniemaniu jest człowiekiem szlachetnym, dbającym przede wszystkim o innych, nie o siebie. To ktoś, kto mimo wielu poświęceń i służbie drugiemu człowiekowi, wskutek różnych wydarzeń (np. politycznych, katastrof naturalnych), jest samotny, potrzebuje kogoś bliskiego i znalazł się w beznadziejnym położeniu.

W kolejnych wiadomościach osoba ta przeważnie opisuje, co robi, gdzie się znajduje, z jakimi problemami się boryka oraz jak wygląda jej codzienność. Buduje wokół siebie tajemniczą, ale przyjazną atmosferę – w taki sposób, by zdobyć zainteresowanie swojej ofiary, a z czasem również jej zaufanie. Dzięki zmyślonej przez siebie historii wzbudza nie tylko chęć poznania jej bliżej, ale również współczucie.

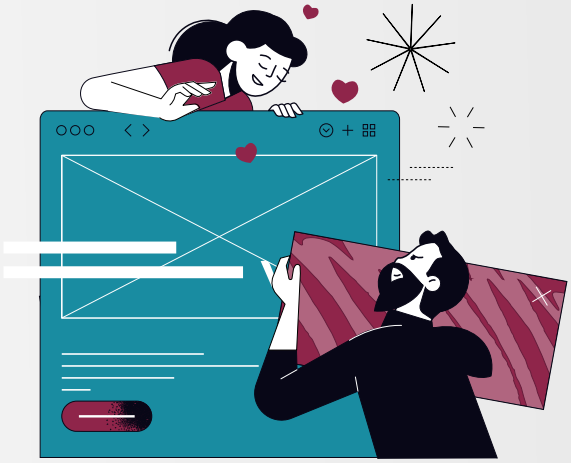
W ŚWIECIE WIRTUALNYM UDOWODNIENIE FAŁSZYWEJ TOŻSAMOŚCI JEST ŁATWIEJSZE

Kolejnym krokiem do rozkochania w sobie ofiary jest przesłanie przez oszusta zdjęć, które mają uwiarygodnić to, kim jest oraz czym się zajmuje. Nietrudno się domyśleć, że zdjęcia prezentują przystojnych, pociągających i dobrze zbudowanych mężczyzn lub piękne, atrakcyjne kobiety (w zależności od tego, za kogo podają się oszuści). Fotografie przeważnie nawiązują do historii, jaka została przedstawiona, np. osoba pokazana jest w otoczeniu sprzętu wojskowego czy poszkodowanych przez wojnę dzieci. Zdjęcia zazwyczaj pochodzą z internetu lub są przerobione na potrzeby zmyślonej opowieści. Oszust w trosce o swoje bezpieczeństwo prosi swoją ofiarę, żeby nie mówiła nikomu (przynajmniej na razie) o ich znajomości.

2 Coluccia A., Pozza A., Ferretti F., Carabellese F., Masti A., Gualtieri G., (2020), „Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review." Clinical Practice Epidemiology in Mental Health, v. 16, s. 24-35 [online], dostęp 7.03.2023 r.

TO WŁAŚNIE CIEBIE POTRZEBUJĘ, TYLKO TY MOŻESZ MI POMÓC...

Jeśli oszustowi udało się zbudować bliską relację ze swoją ofiarą, wzbudzić jej zaufanie, a także współczucie, w kolejnych wiadomościach pojawiają się obietnice wielkiej przygody i romantycznej miłości. Dla osób, które są samotne i szukają kogoś bliskiego, może się to wydawać niezwykłą szansą na piękny i długotrwały związek. Co więcej, potrzeba poczucia bycia kimś wyjątkowym, kogo wybrał „amerykański żołnierz" lub „lekarka służąca na misji", może całkowicie uśpić czujność ofiary. Wcześniej czy później, gdy oszust poczuje się pewnie, pojawią się prośby o pomoc finansową.

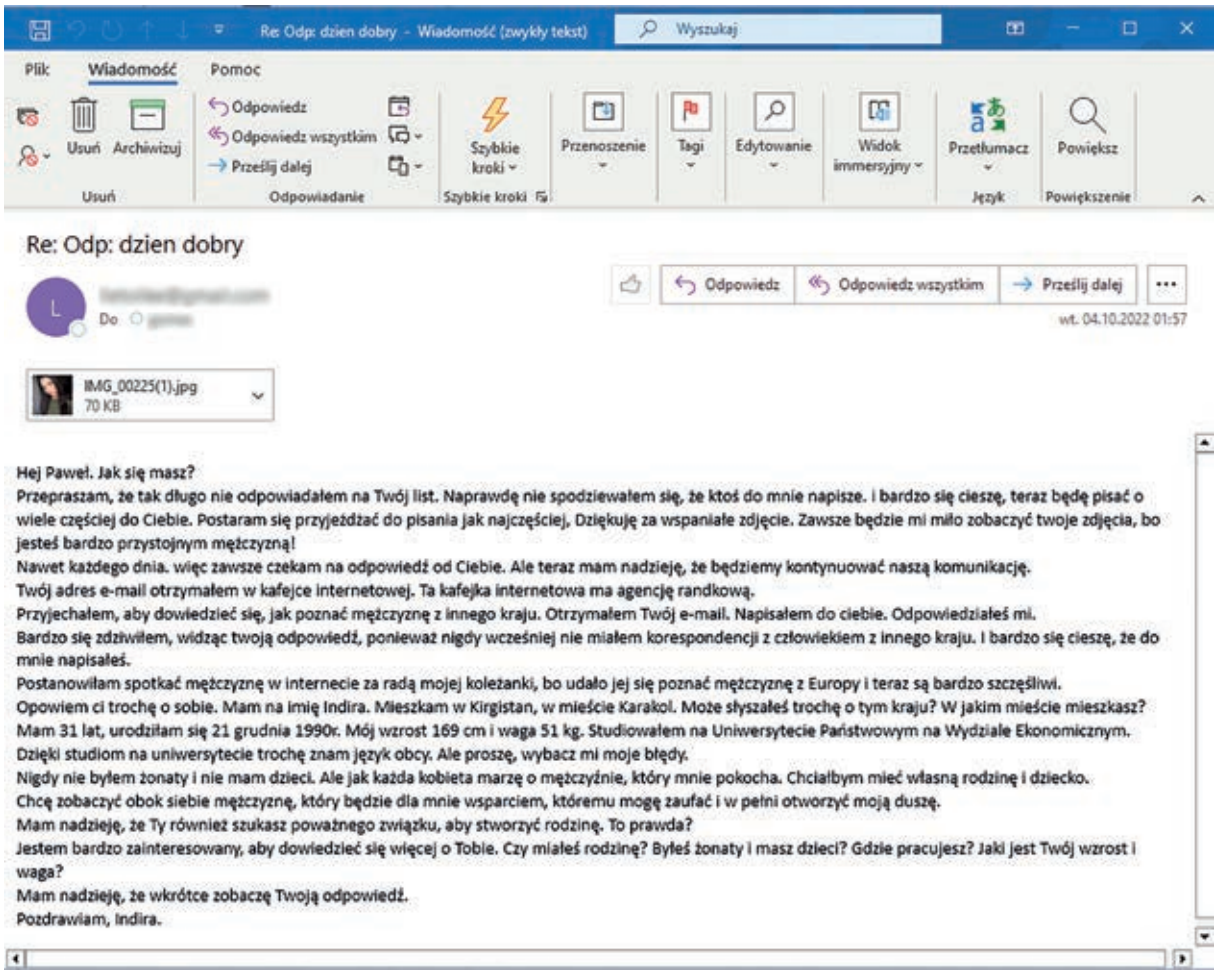


CEL OSZUSTWA

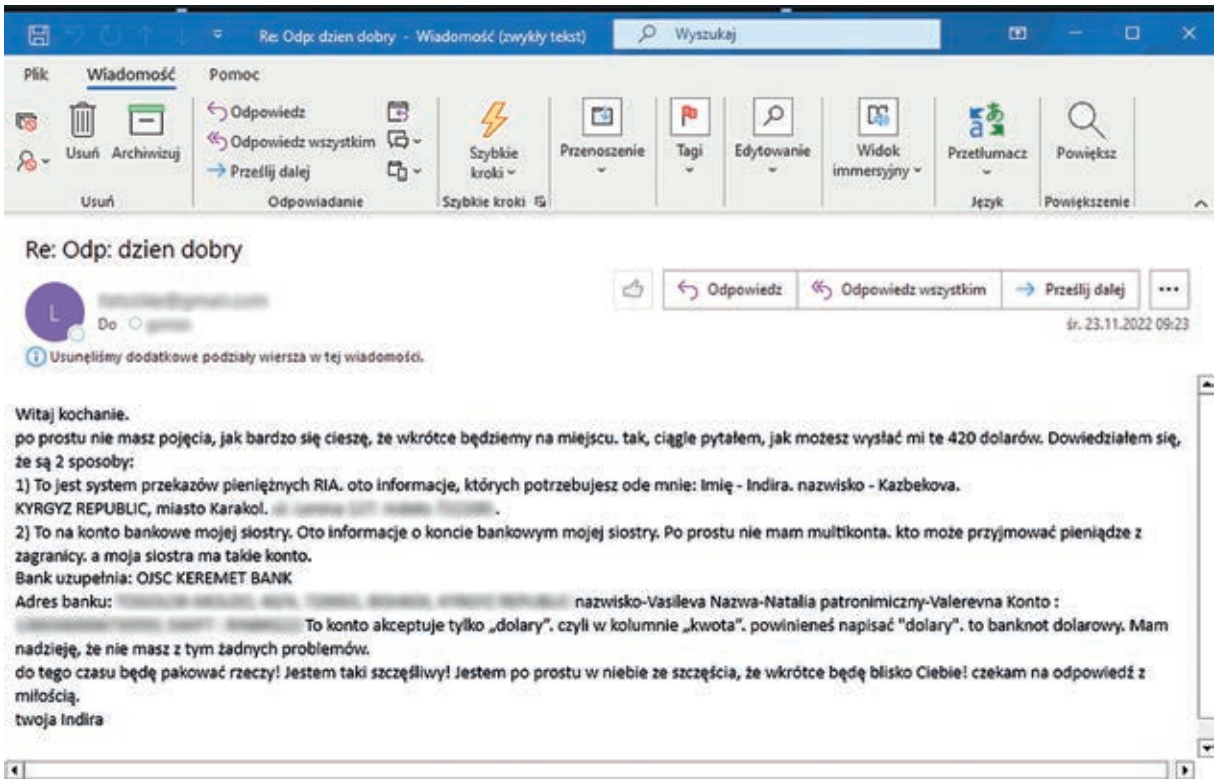
„To właśnie prośba o przesłanie pieniędzy jest punktem kulminacyjnym takiej znajomości. Oszuści wymyślają różne scenariusze, by wyłudzić od swoich ofiar pieniądze. Ich prośby często przedstawiane są jako tymczasowa pożyczka, którą zwrócą od razu, jak tylko spotkają się z ofiarą. Mogą to być środki niezbędne do przeżycia, na bilet do kraju, operację kogoś bliskiego lub inne, zmyślone cele. Schematy postępowania oszustów są bardzo różne" – mówi Anna Kwaśnik, ekspertka NASK-PIB.

Czasami oszuści znikają już po pierwszej wpłacie, ale bardzo często proceder wyłudzania pieniędzy trwa tygodniami. Niczego nieświadome, zakochane w bohaterze lub bohaterce z internetu ofiary, dokonują na wskazane konto wpłat, które czasami sięgają nawet kilkudziesięciu tysięcy złotych. Gdy kończą się oszczędności i brakuje pieniędzy na kolejne przelewy, oszuści przestają się odzywać, urywają kontakt i znikają.

Kolejnym sposobem, by wyłudzić pieniądze, jest proszenie przez oszustów swoich ofiar, by pomogły w odebraniu cennej przesyłki (zawierającej np. dokumenty), za którą najczęściej trzeba zapłacić kilka, a nawet kilkadziesiąt tysięcy złotych. Paczka przeważnie zostaje „zatrzymana na granicy" przez służby celne lub inne organy i, jeśli nie zostanie wniesiona opłata, odbiorca (ofiara oszustwa „na amerykańskiego żołnierza"), jak i rzekomy szczodry nadawca, zostaną ukarani. Zaangażowane osoby w obawie przed więzieniem lub inną karą, a także w poczuciu, że mogą zawieść swojego rozmówcę, wpłacają na wskazane konta pieniądze. W rezultacie zostają bez środków finansowych, jak i „wielkiej miłości"– która po przekazaniu pieniędzy urywa kontakt.



Jedna z pierwszych wiadomości e-mail, trafiła do mężczyzny mieszkającego w Polsce. Długotrwałe budowanie relacji (cała korespondencja obejmowała ponad 40 wiadomości e-mailowych) miało na celu zrealizowanie oszustwa na „amerykańskiego żołnierza", a w tym przypadku – na kobietę z Kirgistanu. Źródło: CERT Polska.



Jedna z końcowych wiadomości e-mail z tej samej próby oszustwa: prośba oszustów o pieniądze. Źródło: CERT Polska.

Po oszustwie

Osoby, które zostały oszukane w internecie, przeważnie zostają z ogromnym żalem, rozczarowaniem, a często też z zaciągniętym kredytem bądź zobowiązaniami finansowymi, np. wobec bliskich. Pojawiające się pretensje od otoczenia oszukana osoba przyjmuje bardzo osobiście – to ona czuje się winna, nie przypisuje sprawstwa przestępcy. „Jak można było tak dać się wykorzystać? Co trzeba mieć w głowie, żeby tak dać się zmanipulować?". Bardzo często ofiary obwiniają siebie za to, co się im przydarzyło, a ciąg negatywnych i błędnych myśli może prowadzić do niebezpiecznych dla ich zdrowia i życia zachowań.

„W tym momencie bardzo dużo zależy od nastawienia otoczenia. To najbliżsi powinni stać się źródłem wsparcia. Jeśli osoba poszkodowana nie radzi sobie z wyrzutami sumienia lub nie może sobie poradzić z faktem bycia oszukaną, a nawet wykorzystaną, warto zasugerować pomoc ze strony wykwalifikowanych specjalistów. Przede wszystkim jednak należy przezwyciężyć w niej dominujące poczucie wstydu i utratę zaufania do ludzi" – radzi dr Marta Melka-Roszczyk, psycholog, biegła sądowa.

Według danych przekazanych przez Centralne Biuro Zwalczania Cyberprzestępczości, w latach 2020-2022 polska policja otrzymała co najmniej 400 zgłoszeń w sprawie oszustw na „amerykańskiego żołnierza". Ich skala jest prawdopodobnie dużo większa, jednak ofiary, z różnych względów, nie zawsze zgłaszają się na policję.

28-latka z Gdańska straciła

75

tysięcy złotych,
bo uwierzyła w historię „żołnierza"[3].

72-letnia mieszkanka powiatu sokólskiego przelała oszustowi

350

tysięcy złotych,
który obiecywał jej wielką miłość[4].

49-letni mężczyzna z powiatu jarosławskiego wysłał blisko

95

tysięcy złotych
„amerykańskiej żołnierce" poznanej przez internet[5].

Przykłady tych i innych prawdziwych historii oszustw możesz znaleźć na stronie Komendy Głównej Policji[6].

3 Oszustwo na amerykańskiego żołnierza – nie daj się nabrać!, 7.04.2022 r. oficjalny serwis Polskiej Polcji, dostęp publikacja 9.03.2023 r.

4 James miał być amerykańskim żołnierzem – okazał się oszustwem. 31.10.2022 r. oficjalny serwis Polskiej Policji, dostęp publikacja 9.03.2023 r.

5 49-latek oszukany na "amerykańską żołnierkę" 12.10.2022 r. oficjalny serwisj Polskiej Policji, dostęp publikacja 9.03.2023 r.

6 https://policja.pl/pol/tagi/21978,oszustwo-quotna-amerykanskiego-zolnierzaquot.html, oficjalny serwis Polskiej Policji, dostęp publikacja 9.03.2023 r.

CO ZROBIĆ, ABY NIE PAŚĆ OFIARĄ OSZUSTWA NA „AMERYKAŃSKIEGO ŻOŁNIERZA"

- Korzystając z różnych serwisów randkowych i portali społecznościowych, musisz pamiętać o zasadzie ograniczonego zaufania.
- Jeśli poznajesz kogoś przez internet, nigdy nie masz pewności, kim jest ta osoba, ani jakie ma wobec Ciebie zamiary. **Zanim wejdziesz z kimś w relację, zastanów się, skąd ta osoba Cię zna i w jaki sposób trafiła na Twój profil.**
- Zweryfikuj, czy nowo poznana osoba jest tą, za którą się podaje. Sprawdź jej dane w internecie (np. imię, nazwisko, adres e-mail). Jeśli otrzymujesz od niej zdjęcia, **sprawdź, czy są one prawdziwe i czy nie pochodzą z przypadkowych stron internetowych.** Możesz to zrobić z wykorzystaniem wyszukiwarki, np. Google, Bing, korzystając z opcji „wyszukiwanie obrazem".
- Wymagaj bezpośredniego kontaktu – takiego jak rozmowa telefoniczna czy wideokonferencja w czasie rzeczywistym. **Jeśli Twój rozmówca będzie tego unikał, to prawdopodobnie jest oszustem. Większość z nich nie będzie się aż tak angażować, a także mogą pojawić się obawy przed zdemaskowaniem.**
- Jeśli osoba, z którą korespondujesz, poprosi Cię o pieniądze (nawet niewielką kwotę), zachowaj czujność. **Uważaj na zbyt szybkie wyznania miłosne, deklaracje spędzania wspólnie reszty życia.**
- Unikaj przesyłania pieniędzy osobom, **które znasz wyłącznie online.**
- Pod żadnym pozorem nie podawaj swoich wrażliwych danych, numerów kart płatniczych, danych do logowania. Nie wysyłaj skanów żadnych dokumentów (np. paszportu, dowodu osobistego). **Staraj się też nie podawać prywatnych informacji ze swojego życia osobom, których nie znasz – nigdy nie możesz mieć pewności, w jaki sposób je wykorzystają.**
- Zachowaj ostrożność, klikając podesłane linki, szczególnie jeśli prowadzą do panelu płatności albo strony wymagającej logowania – mogą być fałszywe! W większości przypadków samo kliknięcie zazwyczaj nie powoduje jeszcze problemów. **Dopiero działania, jakie wykonasz na stronie, np. wprowadzisz dane dostępowe lub ściągniesz plik, mogą mieć naprawdę groźne konsekwencje.**
- W celu zainicjowania oszustwa *romance scam* przestępcy używają również wiadomości e-mail. **Niechciane wiadomości oznaczaj jako SPAM, dzięki czemu nie będziesz ich otrzymywać na swoją skrzynkę.**
- Zawsze korzystaj z **programu antywirusowego** i aktualizuj swój sprzęt oraz oprogramowanie.
- Pamiętaj – w każdej chwili masz prawo **„wylogować się" i zakończyć znajomość.**

Jeśli padłaś/padłeś ofiarą oszustwa w sieci, **zgłoś sprawę do CERT Polska oraz na policję.** Być może uda się odzyskać Twoje pieniądze i powstrzymać oszusta.

OSZUSTWA NA PORTALACH I APLIKACJACH RANDKOWYCH

Portale randkowe zdobywają coraz większą popularność na całym świecie, a Polska nie jest tu wyjątkiem. Tylko z Tindera korzysta globalnie ponad 100 mln osób, natomiast w naszym kraju wyróżnić można ponad 80 internetowych społeczności randkowych! Korzystanie z nich związane jest jednak z wieloma rodzajami zagrożeń.

Rosnący stres, presja, natłok obowiązków, codzienny szum informacyjny – wszystko to sprawia, że wiele osób nie znajduje przysłowiowego „czasu na miłość" w świecie rzeczywistym, dlatego przenosi swoje oczekiwania do świata wirtualnego. Działanie w nim jest po prostu szybsze, wygodniejsze, bardziej dostępne, ale jednocześnie bardzo często iluzoryczne.

Problem kłamstw i oszustw pojawiających się w relacjach międzyludzkich istniał od zawsze, ale wyraźnie nasilił się w czasie pandemii COVID-19, gdy duża część naszych kontaktów przeniosła się do sieci. Niestety, równocześnie kilkukrotnie wzrosły też szkody społeczne, emocjonalne i relacyjne, ponieważ znacznie trudniej rozpoznać zwodnicze i manipulacyjne zamiary oszustów realizowane przez nich w świecie wirtualnym.

JAK (NIE) ZNALEŹĆ IDEALNEGO PARTNERA

Wysoka popularność portali i aplikacji randkowych może wiązać się z tym, że ich użytkownicy wykorzystują je do nawiązywania różnych typów relacji i kontaktów. Jak pokazują badania, ponad 64% użytkowników wyraża chęć poznania kogoś, z kim będzie mogła stworzyć stały związek[7].

Niestety, w wielu przypadkach znajomości online nie są tak trwałe, jak oczekują tego posiadacze kont na portalach i aplikacjach randkowych. Co więcej, presja otoczenia, silna chęć poznania kogoś i spotkania się w świecie realnym mogą przysłonić niebezpieczeństwa i zagrożenia, na jakie narażeni są ich użytkownicy.

7 Kacprzak-Wachniew K., Pilarska N., „Doświadczenia osób korzystających z aplikacji i portali randkowych", Uczuciowo Naukowo, publikacja 23.09. 2022 r., [online], dostęp 7.03.2023 r.

Decydując się na korzystanie z portali lub aplikacji randkowych, warto wziąć pod uwagę wykorzystywane w nich mechanizmy. Zasadę działania tego typu społeczności można scharakteryzować za pomocą znanej maksymy: „jeśli coś jest za darmo, to Ty jesteś produktem". To aktywność online jest towarem, który kupują od właścicieli portali randkowych reklamodawcy. Warto mieć świadomość tego, że z punktu widzenia właściciela platformy randkowej najistotniejsze nie jest to, aby jej użytkownicy znaleźli partnera, ale to, by jak najwięcej zarobić na tym, że użytkownicy z niej korzystają. Z dystansem należy traktować chwytliwe hasła o wielkiej miłości czy doskonale dopasowanych partnerze. Owszem, taki pozytywny scenariusz jest możliwy, ale nie ma pewności ani gwarancji, że tak się stanie.

Czy wiesz, że...

Korzystanie z aplikacji randkowych, zwłaszcza tych, które działają w oparciu o swipe'owanie (czyli funkcjonalność aplikacji pozwalającą na przeglądanie profili i za pomocą przesunięcia w lewo lub w prawo akceptację kontaktu lub jej brak) może powodować rozkojarzenie, a nawet i przytłoczenie liczbą potencjalnych partnerów. U niektórych użytkowników zmniejsza poczucie pewności siebie, a także zwiększa obawę przed pozostaniem singlem[8].

APLIKACJE RANDKOWE SĄ SUPER... RÓWNIEŻ DLA OSZUSTÓW

„Rosnącą popularność oraz zalety portali randkowych świetnie wykorzystują oszuści. Mimo różnych narzędzi i zabezpieczeń wprowadzanych przez właścicieli portali i aplikacji randkowych, dzięki różnym metodom wspomnianej już socjotechniki, oszuści stale znajdują nowe sposoby, by podstępnie uwieść swoją ofiarę" – mówi Anna Kwaśnik, ekspertka NASK-PIB.

Profile na portalach społecznościowych doskonale odsłaniają styl i poziom życia potencjalnych ofiar. Ułatwiają też oszustom tworzenie własnych fikcyjnych tożsamości. Wystarczy kilka informacji, parę wspólnych konwersacji, a osoba wyćwiczona w manipulacji będzie już doskonale wiedzieć, jakiego partnera poszukuje dany użytkownik. Czy ma prezentować się jako wyrozumiały, czuły, dobry chłopak albo jako delikatna, skromna dziewczyna? A może przybrać maskę buntownika, żeby zaimponować znudzonej rutyną codziennego życia ofierze?

Oszuści przekazują nietypowe informacje, które mają zszokować manipulowaną osobę, wywrzeć na niej wrażenie. Nasuwa się tu skojarzenie wręcz z psychopatycznym poziomem manipulacji i zdolnością do wyczuwania sytuacji społecznych oraz umiejętnością wchodzenia w nie, poprzez idealne dostosowywanie się do oczekiwań ofiary. Oszust działa niczym „społeczny kameleon", skłonny wyczekiwać na dogodny moment i obserwować swój cel, aby dobrać perfekcyjne kolory i wtopić się w jego tło życiowe.

8 Thomas M. F. Binder A., Stevic, A., & Matthes J. (2023). 99 + matches but a spark ain't one: Adverse psychological effects of excessive swiping on dating apps. Telematics and Informatics: An Interdisciplinary Journal on the Social Impacts of New Technologies, 78, [101949], [online], dostęp 8.03.2023 r.

Użytkownik/użytkowniczka portalu znajduje się pod wielkim wrażeniem nie tylko życia swojego rozmówcy, ale też jego cech charakteru bądź gestów. Nowy znajomy, a raczej jego wykreowany wizerunek, spełnia głębokie potrzeby swojej ofiary. Jest taki, jakim powinien być idealny partner: dostępny emocjonalnie, wrażliwy, spontaniczny, romantyczny, zdolny do poświęceń, zaangażowany. Otwiera wizję swojego życia: ciekawego, najpewniej związanego z wykonywaniem zawodu zaufania publicznego, ale też z elementem tragedii, smutku (np. chorą matką, uzależnionym synem).

CZAS NA OSZUSTWO

Gdy po kilku konwersacjach użytkownik lub użytkowniczka portalu nabiera zaufania do swojego rozmówcy, ten w podstępny sposób zaczyna prosić o pieniądze, np. poprzez dokonanie płatności na wskazane konto czy podanie kodu płatności mobilnych. Oszust przeważnie tłumaczy się ograniczeniami na koncie lub innymi problemami i obiecuje szybki zwrot pieniędzy.

W tym momencie powinna zapalić się czerwona lampka i mimo pozornie ugruntowanej już zażyłości, intymności i zaufania, nie należy ulegać presji. Mimo różnych argumentów, których używa osoba poznana w sieci, trzeba zachować zdrowy rozsądek i przemyśleć, czy przesłanie pieniędzy to na pewno dobre rozwiązanie... Niestety, bardzo często po wyłudzeniu od ofiary pieniędzy lub, co gorsza, danych logowania do banku albo numerów kart płatniczych, rozmówca znika.

Relacja się urywa. Ofiara zostaje z poczuciem wykorzystania, nie mogąc pojąć, co tak naprawdę się wydarzyło.

KAŻDY MOŻE STAĆ SIĘ OFIARĄ

Wydawać by się mogło, że pokazany schemat oszustwa będzie dotyczył co najwyżej niedoświadczonych i młodych osób. W rzeczywistości tak nie jest. **Raporty pokazują, że oszuści zręcznie wyłudzają pieniądze na „księcia z bajki" w każdej grupie wiekowej, zarówno od kobiet, jak i od mężczyzn**[9]**.**

Ale nie chodzi tylko o straty materialne – negatywne następstwa takiego oszustwa są często druzgocące dla osoby pokrzywdzonej. Wstyd, nawet przed bliskimi, poniesione szkody finansowe, często bardzo poważne, mogą prowadzić do silnych, negatywnych emocji i poczucia bezradności. Wina za całe zdarzenie przypisywana jest często nie oszustowi, ale ofierze, nawet gdy popatrzymy na całe wydarzenie z perspektywy społecznej. Najczęstsze komentarze odnoszące się do pokrzywdzonych są takie, że „dały się nabrać". „Dał się! Dała się!" – to kluczowe stwierdzenie jest niesprawiedliwym obarczaniem winą ofiary, wmawianiem jej, że była naiwna, jest sama sobie winna i dostała to, na co zasłużyła.

Zadaniem świadka sytuacji czy osoby bliskiej nie jest ocena, a tym bardziej obwinianie osoby pokrzywdzonej. Również racjonalizowanie problemu czy obarczanie winą ofiary może powodować dalszą wiktymizację osoby oszukanej, dlatego ważne jest, aby unikać takich działań i zachowań.

9 Wnęk-Gozdek J., „Oszustwa romantyczne online – studium przypadku". Bliskie relacje w doświadczeniach życiowych człowieka, 2(17)/2019, Kraków, Exlibris. Biblioteka Gerontologii Społecznej, s.39-55, [online] dostęp 9.03.2023 r.

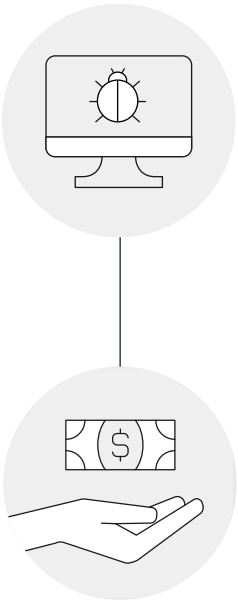
„W atmosferze uważnego zrozumienia starajmy się pomóc, dotrzeć do przyczyn tego zdarzenia, wyjaśnić i zrozumieć, dlaczego tak się stało. Najważniejsze to zwyczajne wsparcie, którego często brak, zwłaszcza ze strony najbliższych, a właśnie to mocno pogarsza i tak trudną sytuację" – radzi dr Marta Melka-Roszczyk, psycholog, biegła sądowa.

Czy wiesz, że...

Według najnowszego raportu amerykańskiej Federalnej Komisji ds. Handlu (FTC) aż 40% ofiar, które straciły pieniądze w wyniku oszustwa internetowego, to ofiary „oszustw romantycznych". FTC podaje, że w 2022 roku cyberprzestępcy wyłudzili od swoich ofiar ponad 1,3 miliarda dolarów[10]!

JAKIE NIEBEZPIECZEŃSTWA MOGĄ NIEŚĆ ZA SOBĄ ZNAJOMOŚCI ONLINE

Decydując się na nawiązywanie relacji online, musisz pamiętać, że nigdy nie możesz mieć pewności, kim jest osoba po drugiej stronie, jakie ma intencje i zamiary wobec Ciebie. Sprawdź, na jakie jeszcze zagrożenia możemy być narażeni i w jakich sytuacjach należy szczególnie uważać:



ZAINFEKOWANIE SPRZĘTU, UTRATA DANYCH

– aplikacje i portale randkowe mogą posłużyć cyberprzestępcom jako narzędzie do wysyłania fałszywych i szkodliwych linków, które mogą doprowadzić do zainfekowania naszego sprzętu, a także wycieku danych i informacji, które w nim przechowujemy. Jeśli korespondujesz z oszustem z portalu randkowego ze służbowego sprzętu, może to również prowadzić do strat w instytucji, w której pracujesz.

FAŁSZYWE FUNDUSZE INWESTYCYJNE I KRYPTOWALUTY

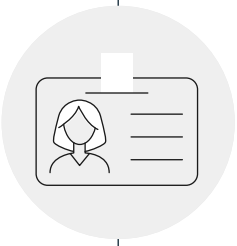
– to kolejne narzędzia, jakich mogą użyć przestępcy na portalach i aplikacjach randkowych, by pozyskać Twoje pieniądze lub prywatne dane. Po nawiązaniu bliższego kontaktu oszust wysyła propozycję szybkiego zarobienia pieniędzy poprzez inwestycję w fundusz lub kupno krytpowalut. Przesyła link do strony internetowej, gdzie można dokonać transakcji. Żeby uwiarygodnić sytuację, proponuje nawet wypłatę niewielkiej sumy pieniędzy. Następnie zachęca do zainwestowania kolejnej kwoty, najlepiej jak najszybciej. W momencie kiedy oszukiwana osoba chce dokonać wypłaty, przestępca wymyśla

10 Fletcher E., Romance scammers' favorite lies exposed, oficjalny serwis Amerykańskiej Komisji ds. Handlu (FTC), publikacja 9.02.2023 r., dostęp 9.03.2023 r.

powody, dla których nie jest to możliwe. Kiedy osoba przestaje wpłacać pieniądze, przestępca ucina z nią kontakt. W niektórych sytuacjach, gdy oszust zbuduje bliską relację, może prosić o pożyczkę, by „sam mógł zainwestować", a zysk, jaki otrzyma, przeznaczy na dalsze, wspólne życie.

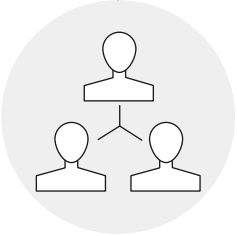
PRANIE BRUDNYCH PIENIĘDZY

– przestępstwo, w które można zostać wciągniętym, nawet zupełnie nieświadomie. Jeśli ktoś poprosi Cię o wykonanie kilku przelewów pomiędzy bankami, musisz zachować czujność. Z pozoru zwykła przysługa może okazać się niezgodnym z prawem procederem, który pozwala oszustom wyprać pieniądze pochodzące z nielegalnych źródeł.



KRADZIEŻ TOŻSAMOŚCI[11]

– portale randkowe i media społecznościowe to doskonałe miejsca, za pomocą których przestępcy mogą pozyskać prywatne informacje na temat swoich potencjalnych ofiar. Większość tych danych publikowana jest przez nieświadomych użytkowników, którzy chcą pochwalić się sobą, swoim życiem i zabłysnąć w mediach społecznościowych. Przestępcy, którzy pozyskają nasze prywatne informacje i dane, a także zdjęcia i filmy, mogą tym samym skraść naszą tożsamość i wykorzystać ją w różnych celach – np. przy oszustwach online, do zaciągnięcia na nas kredytu, szantażu, naruszenia naszego wizerunku i wielu innych.



TWOJE BEZPIECZEŃSTWO W ŻYCIU REALNYM

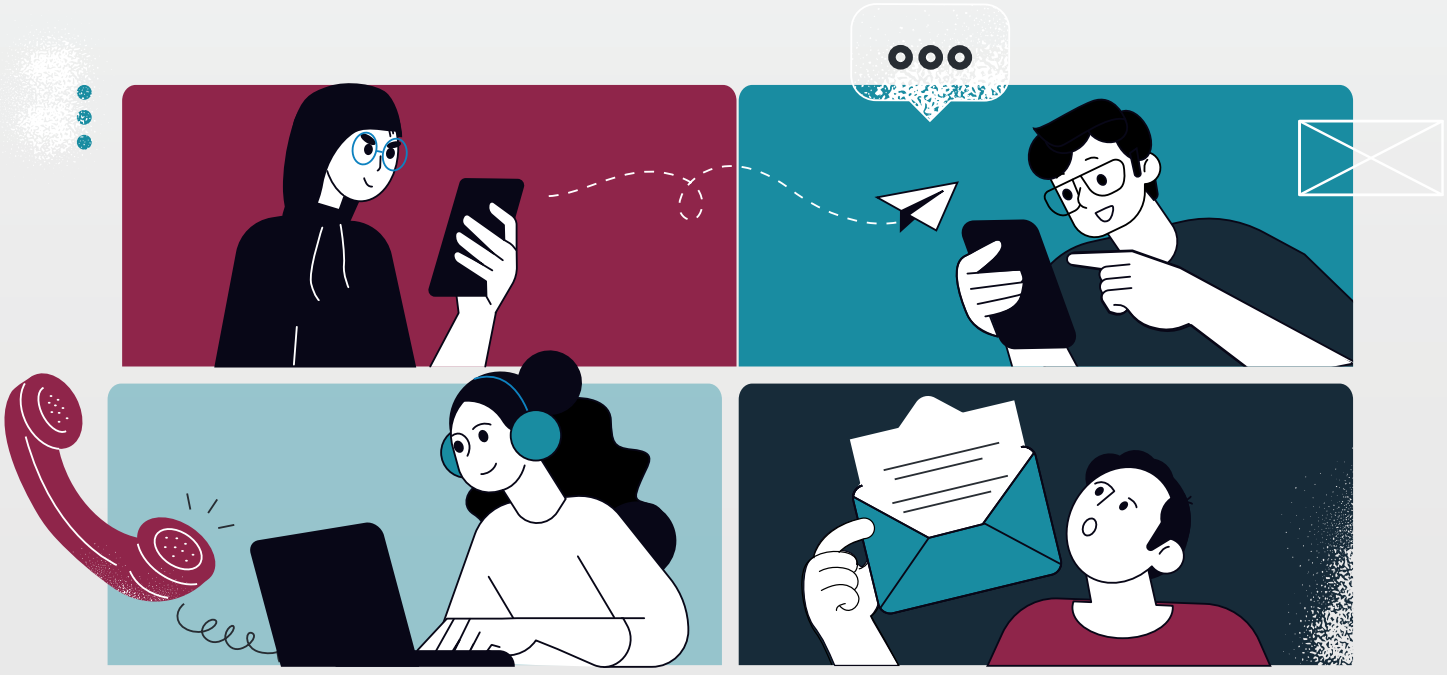
– znajomości internetowe dają pozorne wrażenie, że dobrze znamy naszego rozmówcę i wiemy o nim wszystko. Nic bardziej mylnego! Nigdy nie możesz mieć pewności, kim jest ta osoba i czy historia, którą przedstawiła, jest prawdziwa. Jeśli decydujesz się na spotkania w świecie realnym, musisz pamiętać o kilku podstawowych zasadach bezpieczeństwa. Przede wszystkim nigdy nie umawiaj się z kimś w miejscu, którego nie znasz i jest ono odosobnione. Wybieraj takie miejsca, gdzie w razie niebezpieczeństwa możesz poprosić o pomoc. Poinformuj kogoś ze swojego otoczenia, gdzie idziesz, z kim, o której planujesz wrócić. Jeśli podczas spotkania czujesz się niekomfortowo, zawsze masz prawo je zakończyć.

11 Zeltser L. (red.), (2021), „Kradzież tożsamości – ochroń się przed nią", tłum. Wnuk B., Węgrzynowicz A., „OUCH!" Biuletyn Bezpieczeństwa Komputerowego, nr 3 [online], dostęp 10.03.2023 r.

JAK SIĘ NIE DAĆ OSZUKAĆ PODCZAS ZNAJOMOŚCI ZAWIERANYCH PRZEZ INTERNET

- Zawsze weryfikuj osobę, z którą rozmawiasz. Sprawdź, czy ma konta w mediach społecznościowych, jak długo jej profile są aktywne, ilu ma znajomych. Jeśli poczujesz, że coś ukrywa lub próbuje Cię oszukać, zakończ relację.
- Uważaj na osoby, które szybko próbują zbudować z Tobą bliską relację, namawiają do spotkania w odosobnionym miejscu, zachęcają do wysyłania intymnych zdjęć czy filmów.
- Jeśli Twój rozmówca poprosi o pieniądze, nawet drobną kwotę, traktuj to co najmniej jako poważny sygnał ostrzegawczy.
- Nie klikaj linków przesłanych przez nieznajome osoby i nie pobieraj załączników, jeśli nie masz pewności, co w nich jest.
- Nie instaluj aplikacji, co do których nie masz pewności, że są bezpieczne.
- Nigdy nie podawaj innym haseł logowania ani innych prywatnych danych.
- Jeśli ktoś poprosi Cię o przesłanie skanu lub zdjęcia Twoich dokumentów (np. dowodu osobistego, paszportu), zakończ relację i zgłoś sprawę do administratorów serwisu.
- Pamiętaj, że zawsze masz prawo powiedzieć NIE, zakończyć rozmowę a nawet relację, w której będziesz się czuć niekomfortowo.

Jeśli padniesz ofiarą oszustwa na portalu randkowym lub w serwisie społecznościowym, jak najszybciej zgłoś sprawę do administratora serwisu, na policję, a także do swojego banku.



SEXTORTION – EROTYCZNE ZNAJOMOŚCI, WYMUSZENIA PIENIĘDZY

Określenie *sextortion* powstało z połączenia dwóch angielskich słów: *sex* oraz *extortion* (wymuszenie). To przestępstwa polegające na zdobyciu intymnych, często nagich zdjęć ofiary lub filmów z jej udziałem, a następnie wykorzystywaniu ich jako narzędzia nacisku i szantażu. Celem szantażu ofiary są zazwyczaj – choć nie zawsze – korzyści materialne.

Schemat szantażu wykorzystującego intymne materiały ofiary powtarza się w większości przypadków. Ofiara oszustwa zakłada konto na portalu randkowym bądź społecznościowym, na którym udostępnia wiele informacji na swój temat: opisuje swoje zainteresowania, preferencje, przemyślenia, typ idealnego partnera bądź partnerki. Ważna jest przy tym motywacja towarzysząca założeniu konta – wyraźna i ujawniana publicznie chęć poznania innych osób, a często wręcz tej wybranej, drugiej osoby, w celu zbudowania z nią naprawdę bliskich relacji.

Nie tylko młodzi

Panuje przekonanie, że zjawisko *sextortion* dotyczy naiwnych i niedoświadczonych nastolatków. To nieprawda. Istnieje wiele motywów skłaniających ludzi – i to niemal w każdym wieku – do podjęcia aktywności na portalach i aplikacjach randkowych. Czasem jest to chęć nawiązania kontaktu z innymi ludźmi i próba znalezienia „lepszej" grupy rówieśniczej, a czasem po prostu potrzeba poznania kogoś bliskiego, kogoś, „kto w końcu nas zrozumie". Niekiedy założone konto służy zaś wprost jednemu celowi – odnalezieniu swojego najbliższego partnera, osoby, z którą uda się zbudować szczęśliwy związek.

Mając dość samotności, nieprzyjemności i dyskomfortu wynikających z bycia singlem, ludzie są skłonni zrezygnować z ochrony swojej prywatności – zaufać i wpuścić do swojego świata kogoś nowego, innego.

Powolne budowanie relacji

Typowy, ale nie jedyny schemat oszustwa polega w tym przypadku na powolnym zdobywaniu zaufania przyszłej potencjalnej ofiary. Dociera do niej pierwsze zaproszenie od kogoś żywo zainteresowanego tym, co ma ona do powiedzenia, chcącego ją poznać. Oszust prezentuje się przy tym jako człowiek niezwykle wyrozumiały, nieoceniający, ofiarujący bezinteresowne wsparcie. Po prostu inny, nie „taki jak wszyscy".

Oszukiwana osoba zaczyna coraz bardziej polegać na nowej znajomej lub znajomym, radzić się, oczekiwać ciągłego kontaktu, który staje się dla niej niezbędny. Na początku jest nawet zaskoczona – „jak to możliwe, że ktoś rozmawia ze mną przez pół nocy i nie chce niczego w zamian?". Nowy znajomy/znajoma wydaje się ucieleśnieniem wielu z tych zalet, których właśnie poszukiwała oszukiwana osoba. Jest zawsze dostępny, zawsze gotowy pocieszyć dobrym słowem czy radą.

Zdobywanie zaufania, tematy intymne

W końcu oszust robi pierwszy krok. Rozmowy schodzą na tematy związane z cielesnością, bliskością, intymnością. W wersji ostrożniejszej scenariusza oszustwa, ofiara może zostać poproszona o opisywanie fantazji seksualnych, dotychczasowych doświadczeń, przemyśleń związanych ze związkami i relacjami romantycznymi – jeszcze bez dzielenia się intymnymi zdjęciami czy filmami. Tworzy się podłoże wzajemnego zaufania i kontrolowanej iluzji intymności. Oczywiście kontrolowanej przez sprawcę.

Obecnie panująca promocja nierzeczywistych norm piękna, powszechny dostęp do pornografii, zniesienie romantyczności na rzecz sprawności fizycznej oraz wyobrażeń dotyczących samego aktu seksualnego sprawia, że większość ludzi czuje się bardzo niepewnie w kwestiach związanych z seksualnością. Miejsce romantyczności zajęła sprawność seksualna, a seks stał się dyscypliną niemal sportową, gdzie rywalizacja (szczególnie ta wyobrażona) nie daje zdrowej przestrzeni na doświadczanie bliskości i szeregu doznań związanych z fizycznością. Powszechnie występuje zjawisko niezadowolenia, a wręcz wstydu ze względu na wygląd niektórych części ciała, które nie są wystarczająco piękne bądź kształtne. Wygląd często bywa porównywany do sylwetek i urody zawodowych modeli i modelek, którzy – czego czasem nie mamy świadomości – ze względu na pracę korzystają regularnie z usług profesjonalnych dietetyków, trenerów, a także makijażystów oraz specjalistów chirurgii estetycznej czy profesjonalnych fotografów i retuszerów.

Na tym właśnie bazują oszuści. Po zbudowaniu aury zaufania i intymności, okazują (być może jako pierwsi w życiu potencjalnej ofiary) tak oczekiwane wsparcie i akceptację. Komentarze typu: „ale przecież pięknie wyglądasz, nie masz się czego wstydzić", „czas porzucić kompleksy", „masz piękne ciało", „niedoskonałości masz tylko w swojej głowie" są na porządku dziennym. Nie zawsze muszą świadczyć o nieuczciwości, ale jeżeli jest ich zbyt dużo i uwaga odbiorcy jest skupiona wyłącznie na ciele, powinno to stanowić znak ostrzegawczy.

Wymiana intymnych materiałów i... finał

Spirala manipulacji nakręca się dalej. Przestępcy jako pierwsi wysyłają rzekomo swoje zdjęcia bądź filmiki, na których pozują nago. Zazwyczaj są to obrazy atrakcyjnych kobiet bądź mężczyzn – oczywiście nieprawdziwe. Sprawcy używają obrazów, które pobierają z dostępnych banków zdjęć bądź „zapożyczają" z innych kont. Ofiara, nie mając tej świadomości i podbudowana okazywanym jej dotychczas zrozumieniem, czuje chęć odwdzięczenia się – więc również wysyła materiały tego typu. Gorąca atmosfera nakręcana jest jeszcze bardziej przez kolejne śmiałe obrazki czy filmy. Aż do momentu, po którym następuje cisza.

Nagle „bliski znajomy" przestaje się odzywać. Pojawia się uczucie niepokoju: „Może coś się stało?". Następnie ofiara otrzymuje krótką, ale wstrząsającą informację: „Zapłać mi określoną kwotę, gdyż w innym przypadku udostępnię wszystko co mi wysłałeś. Twoi znajomi, przyjaciele, rodzice, wszyscy zobaczą Twoje nagie szpetne ciało i to, co z nim robisz, gdy nikt nie patrzy".

Zapłata okupu

Dlaczego tak wielu ludzi ulega tego typu szantażom i wysyła pieniądze? Ponieważ czują się przede wszystkim wykorzystani. To uczucie wstydu, zażenowania, pretensje kierowane do siebie: „Jak mogłem być tak głupi? Jak mogłam się dać tak wykorzystać?".

To właśnie wspomniane poczucie wstydu i obawa przed ujawnieniem materiałów działają na korzyść sprawców. Osoba, która została oszukana, często działa w panice i chcąc uniknąć upokorzenia, decyduje się spełnić oczekiwania szantażystów. Niestety, jeśli raz zapłaci okup, prawdopodobnie oszuści będą domagać się kolejnego, a zdjęcia lub filmy w końcu i tak mogą zostać opublikowane.

Oczywiście zdarzają się przypadki, gdy ktoś odmawia zapłaty okupu, a wyłudzone materiały nie zostają upublicznione. Ale czy na pewno? Zawsze zostaje jednak niepewność – co się z tymi treściami stało? Czy zostały usunięte? A może szantażyści czekają na bardziej dogodny moment?

„Każda relacja online może być dla nas niebezpieczna. Przestępcy stale szukają nowych sposobów, by wyłudzić nasze dane lub pieniądze. Technologia otwiera nowe możliwości na polu komunikowania się i nawiązywania znajomości. Niemniej zanim wejdziemy w ten świat, musimy opanować pewne zasady, które pozwolą nam skutecznie rozpoznać próbę oszustwa. Kluczowy jest zdrowy rozsądek i zasada ograniczonego zaufania" – podkreśla Sebastian Kondraszuk, kierownik Kierownik Działu CERT Polska, NASK-PIB.

Pozamaterialne konsekwencje oszustwa

Konsekwencje oszustwa i szantażu typu *sextortion* najczęściej wykraczają poza sferę materialną. Dotykają także sfery emocjonalnej, dobrostanu psychicznego. Czasami presja staje się nie do wytrzymania. Wyrzuty sumienia, stracone (czasem duże) pieniądze, wstyd. Objawami współtowarzyszącymi są dalsza izolacja społeczna, utrata zaufania do innych ludzi, skrytość i daleko posunięta zachowawczość w stosunku do bliskich. Mogą pojawiać się stany lękowe, depresyjne, rezygnacja z życia towarzyskiego czy zawodowego, a nawet myśli i próby samobójcze.

„W przypadku, gdy materiały rzeczywiście wyciekły do internetu, praca terapeutyczna będzie się skupiać wokół dominującego uczucia wstydu i lęku społecznego oraz mechanizmu samowykluczenia towarzyskiego. Jednakże zawsze należy pamiętać o tym, że to nie ofiara jest winna przestępstwa. To oszustowi grozi kara od 3 miesięcy do nawet 5 lat pozbawienia wolności" – podkreśla dr Marta Melka-Roszczyk, psycholog, biegła sądowa.

JAK CYBERPRZESTĘPCY WYKORZYSTUJĄ *SEXTORTION* DO WYŁUDZANIA PIENIĘDZY

Cyberprzestępcy wykorzystujący *sextortion* jako narzędzie do wyłudzania pieniędzy coraz częściej uderzają też w osoby, które chcą się w sieci „tylko zabawić" i szukają szybkiej, intymnej relacji. Najczęściej wykorzystują wizerunek atrakcyjnych osób i kontaktują się z potencjalnymi ofiarami przez popularne serwisy społecznościowe i komunikatory. Następnie zachęcają swoją ofiarę do kliknięcia przesłanego linku lub do pobrania aplikacji z funkcją wideo, za pomocą której będą mogli porozmawiać, widząc się wzajemnie. Wskazany przez nich link może prowadzić na niebezpieczną stronę internetową, a pobrany plik – ściągnąć na urządzenie złośliwe oprogramowanie, które nie tylko umożliwi dostęp do wrażliwych danych, ale także pozwoli przechwycić obraz z kamery, np. z wideorozmowy[12].

Pamiętaj!

- **Ostrożnie podchodź do linków, które otrzymasz od rozmówcy.**
- **Nie pobieraj i nie instaluj aplikacji, które proponuje Ci rozmówca.**
- **Korzystaj z programu antywirusowego i aktualizuj go zgodnie z zaleceniami producenta.**

12 Kumar A., Albrecht J., New Spyware Used by Sextortionists iOS/Android Blackmail, publikacja 16.12.2020 r., oficjalna strona firmy Lookout Mobile Security, dostęp 8.03.2023 r.

„W latach 2020-2022 zgłoszono ponad 2000 przestępstw, które dotyczą szantażu na tle seksualnym. Szacuje się, że liczba ofiar jest zdecydowanie większa. Jednak, ze względu na wrażliwy i intymny charakter sprawy, ofiary nie zgłaszają spraw na policję" – podaje Centralne Biura Zwalczania Cyberprzestępczości.

SEXTORTION SCAM

Na skrzynki e-mailowe użytkowników sieci trafiają wiadomości, które bardzo często są nie tylko niepotrzebne i zaśmiecają pocztę, ale w wielu przypadkach mogą być dla nas niebezpieczne, wzbudzać różne emocje, a czasami prowadzić do ryzykownych działań.

Jeśli otrzymasz wiadomość e-mail od nieznajomego, w której będzie Cię przekonywał, że przejął kontrolę nad Twoim sprzętem, ma dostęp do Twoich danych oraz wie, jakie treści oglądasz, a także dzięki kamerze podglądał Cię podczas sytuacji intymnych, to najlepiej zignoruj ją. To oszustwo.

W takich wiadomościach przestępcy bardzo często straszą potencjalną ofiarę, że mają kontakt do wszystkich znajomych (szefa, współpracowników, partnera lub partnerki) i jeśli nie otrzymają żądanej kwoty, kompromitujące, intymne materiały zostaną do tych osób wysłane lub upublicznione. Aby zwiększyć swoją wiarygodność, oszuści informują, jak przejęli kontrolę nad sprzętem (przeważnie powołują się na złośliwe oprogramowanie zainstalowane np. podczas korzystania z różnych stron pornograficznych) oraz podają hasło, które prawdopodobnie pochodzi z wycieku z jednej z baz danych, ale przeważnie jest już stare i nieaktywne.

Uwaga! Jeśli podawane przez oszustów hasło jest prawdziwe i aktualne, nie panikuj i zachowaj spokój. Nawet jeśli ktoś poznał dane dostępowe Twojego konta, to jest małe prawdopodobieństwo, że uzyskał dostęp do Twojego sprzętu (np. komputera, kamerki internetowej). Pamiętaj, aby od razu zmienić swoje hasło!

Czy wiesz, że...

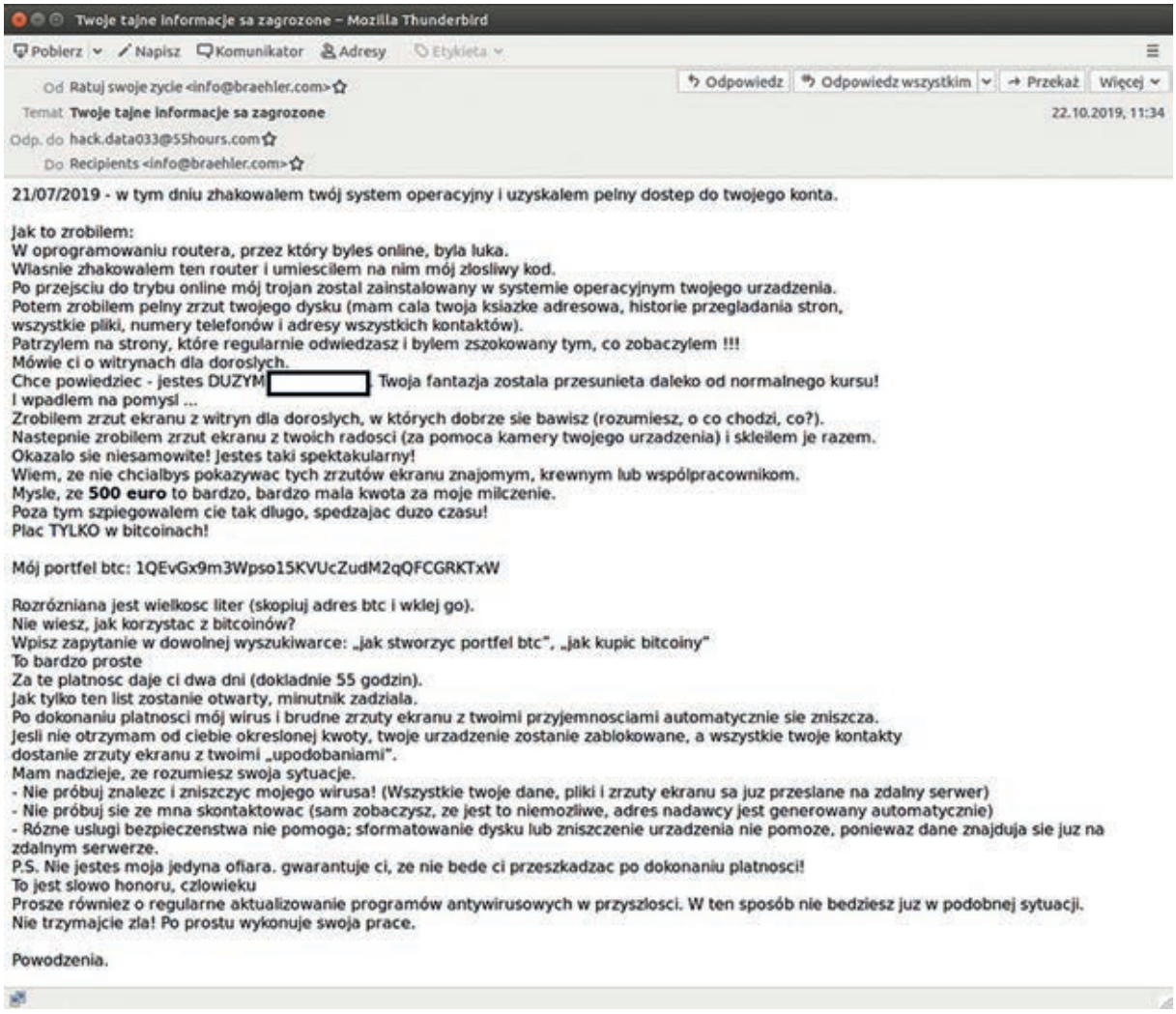
Jeśli chcesz się przekonać, czy doszło do wycieku Twoich danych lub hasła, możesz to sprawdzić za pomocą przeznaczonych do tego serwisów, np. Have I been Pwned.

W kolejnych akapitach wiadomości przestępcy informują, w jaki sposób należy wysłać im pieniądze (przeważnie są to kryptowaluty, przelew w Western Union lub inna płatność na wirtualny portfel) oraz w jakim czasie należy to zrobić – zazwyczaj około kilku dni.

„Przestępcy wykorzystują strach i obawę przed ujawnieniem prywatnych materiałów, a określając ramy czasowe, kiedy należy wpłacić pieniądze, nakładają na potencjalną ofiarę presję czasu. To kolejny przykład oszustwa, które opiera się na socjotechnice" – wyjaśnia Anna Kwaśnik, ekspertka NASK-PIB.

Takie wiadomości bardzo często napisane są w języku angielskim, a jeśli są przetłumaczone – zawierają błędy stylistyczne, gramatyczne i językowe. Może to ułatwić weryfikację, że dana wiadomość to SPAM. Przestępcy wysyłają je masowo do adresatów na całym świecie, a adresy mailowe nadawców najczęściej zarejestrowane są na mało popularnych domenach.

> Coraz częściej filtry antyspamowe blokują wiadomości zawierające adresy portfeli BitCoin, dzięki czemu zmniejsza się liczba wiadomości SPAM, które trafiają do użytkowników. Jeśli otrzymasz wiadomość typu *sextortion scam* lub inną – nakłaniającą Cię do wpłaty – oznacz ją jako SPAM i usuń. Dzięki temu ograniczysz liczbę tego typu wiadomości.


Twoje tajne informacje sa zagrozone – Mozilla Thunderbird

Pobierz | Napisz | Komunikator | Adresy | Etykieta

Od Ratuj swoje zycie <info@braehler.com>
Temat Twoje tajne informacje sa zagrozone
Odp. do hack.data033@55hours.com
Do Recipients <info@braehler.com>

Odpowiedz | Odpowiedz wszystkim | Przekaż | Więcej
22.10.2019, 11:34

21/07/2019 - w tym dniu zhakowalem twój system operacyjny i uzyskalem pelny dostep do twojego konta.

Jak to zrobilem:
W oprogramowaniu routera, przez który byles online, byla luka.
Wlasnie zhakowalem ten router i umiescilem na nim mój zlosliwy kod.
Po przejsciu do trybu online mój trojan zostal zainstalowany w systemie operacyjnym twojego urzadzenia.
Potem zrobilem pelny zrzut twojego dysku (mam cala twoja ksiazke adresowa, historie przegladania stron, wszystkie pliki, numery telefonów i adresy wszystkich kontaktów).
Patrzylem na strony, które regularnie odwiedzasz i bylem zszokowany tym, co zobaczylem !!!
Mówie ci o witrynach dla doroslych.
Chce powiedziec - jestes DUZYM [redacted]. Twoja fantazja zostala przesunieta daleko od normalnego kursu!
I wpadlem na pomysl ...
Zrobilem zrzut ekranu z witryn dla doroslych, w których dobrze sie bawisz (rozumiesz, o co chodzi, co?).
Nastepnie zrobilem zrzut ekranu z twoich radosci (za pomoca kamery twojego urzadzenia) i skleilem je razem.
Okazalo sie niesamowite! Jestes taki spektakularny!
Wiem, ze nie chcialbys pokazywac tych zrzutów ekranu znajomym, krewnym lub wspólpracownikom.
Mysle, ze **500 euro** to bardzo, bardzo mala kwota za moje milczenie.
Poza tym szpiegowalem cie tak dlugo, spedzajac duzo czasu!
Plac TYLKO w bitcoinach!

Mój portfel btc: 1QEvGx9m3Wpso15KVUcZudM2qQFCGRKTxW

Rozrózniana jest wielkosc liter (skopiuj adres btc i wklej go).
Nie wiesz, jak korzystac z bitcoinów?
Wpisz zapytanie w dowolnej wyszukiwarce: „jak stworzyc portfel btc", „jak kupic bitcoiny"
To bardzo proste
Za te platnosc daje ci dwa dni (dokladnie 55 godzin).
Jak tylko ten list zostanie otwarty, minutnik zadziala.
Po dokonaniu platnosci mój wirus i brudne zrzuty ekranu z twoimi przyjemnosciami automatycznie sie zniszcza.
Jesli nie otrzymam od ciebie okreslonej kwoty, twoje urzadzenie zostanie zablokowane, a wszystkie twoje kontakty dostanie zrzuty ekranu z twoimi „upodobaniami".
Mam nadzieje, ze rozumiesz swoja sytuacje.
- Nie próbuj znalezc i zniszczyc mojego wirusa! (Wszystkie twoje dane, pliki i zrzuty ekranu sa juz przeslane na zdalny serwer)
- Nie próbuj sie ze mna skontaktowac (sam zobaczysz, ze jest to niemozliwe, adres nadawcy jest generowany automatycznie)
- Rózne uslugi bezpieczenstwa nie pomoga; sformatowanie dysku lub zniszczenie urzadzenia nie pomoze, ponieważ dane znajduja sie juz na zdalnym serwerze.
P.S. Nie jestes moja jedyna ofiara. gwarantuje ci, ze nie bede ci przeszkadzac po dokonaniu platnosci!
To jest slowo honoru, czlowieku
Prosze równiez o regularne aktualizowanie programów antywirusowych w przyszlosci. W ten sposób nie bedziesz juz w podobnej sytuacji.
Nie trzymajcie zla! Po prostu wykonuje swoja prace.

Powodzenia.

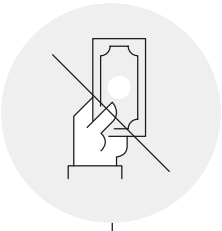
Źródło: CERT Polska

SEXTORTION – JAK SIĘ NIE DAĆ OSZUKAĆ I O CZYM NALEŻY PAMIĘTAĆ

Ofiarą przestępstwa typu *sextortion* może zostać każdy. Czasami chwila zapomnienia, chęć przeżycia czegoś wyjątkowego może wiązać się z wieloma nieprzyjemnymi dla nas konsekwencjami. Zachęcamy do zapoznania się z kilkoma wskazówkami, dzięki którym dowiesz się, co zrobić, aby nie dać się oszukać.

- **Przede wszystkim zasada ograniczonego zaufania.** Jeśli poznajesz kogoś w sieci, nigdy nie masz pewności, kim jest ta osoba, jakie ma intencje ani w jaki sposób może Cię wykorzystać. Zanim wejdziesz z nią w relację (zwłaszcza intymną), zastanów się i pomyśl, z jakimi konsekwencjami możesz się później mierzyć.
- **Ostrożnie podchodź do wiadomości, które otrzymujesz, zwłaszcza od nieznajomych.** Nie klikaj przesłanych linków, nie otwieraj załączników, nie daj się namówić na zainstalowanie aplikacji, której nie znasz.
- **Staraj się weryfikować tożsamość osób, z którymi kontaktujesz się za pośrednictwem portali randkowych.** Sprawdź, czy mają inne profile w mediach społecznościowych, nie daj się zwieść atrakcyjnym zdjęciom i miłym wiadomościom.
- **Nigdy nie podawaj swoich wrażliwych danych (np. do logowania, haseł, numerów kart płatniczych i innych wrażliwych informacji).** Osoba, która je pozyska, może Cię okraść.
- *Sextortion* jest przestępstwem! Jeśli ktoś pozyskał Twoje nagie zdjęcia i Cię szantażuje, zgłoś sprawę na policję.

Co możesz zrobić, jeśli padniesz ofiarą *sextortion*?



Przede wszystkim nie płać okupu – nigdy nie masz pewności, czy sprawca usunie materiały z Twoim udziałem, a także czy nie zażąda kolejnej wpłaty.

Zgłoś sprawę na policję – w tym celu zbierz i zabezpiecz dowody (zrób zrzuty ekranu wiadomości, które otrzymałaś/otrzymałeś, informacje na temat profilu osoby, która się z Tobą kontaktowała, a także dane konta do wpłaty pieniędzy).

Zablokuj swojego rozmówcę i zakończ z nim kontakt.

Porozmawiaj z kimś bliskim o tym, co Cię spotkało. Jeśli nie masz wokół siebie przyjaznej osoby, skorzystaj np. z telefonów zaufania dla osób dorosłych. Znajdziesz je w rozdziale: Gdzie szukać pomocy.

Jeśli sytuacja Cię przerasta, nie potrafisz sobie z nią poradzić, skontaktuj się ze specjalistą, który Cię wysłucha i udzieli potrzebnego wsparcia.

Ważne!

Jeśli ofiarą *sextortion* jest osoba poniżej 18. roku życia, sprawę należy bezzwłocznie zgłosić na policję oraz do zespołu Dyżurnet.pl, ponieważ ofiara mogła doświadczyć wykorzystywania seksualnego online.

Więcej na ten temat dowiesz się ze strony Dyżurnet.pl.

ZAGROŻENIE REVENGE PORN – ROZPOWSZECHNIANIE INTYMNYCH MATERIAŁÓW W CELU ZEMSTY

> **Określenie *revenge porn*, czyli zemsta porno, to niebezpieczne, stosunkowo nowe zagrożenie cyfrowe, polegające na szantażu z wykorzystaniem intymnych materiałów z udziałem pokrzywdzonej osoby.**

Zagrożenie *revenge porn*, podobnie jak *sextortion* (str. 21) polega na opublikowaniu intymnych materiałów bez zgody osoby, która na nich występuje. Podstawowa różnica polega na tym, że działania typu *sextortion* opierają się na szantażu i wymuszeniu w zamian za niepublikowanie treści, natomiast w przypadku *revenge porn*, motywem jest chęć zemsty i upokorzenia. Działania związane z *sextortion* dokonywane są zazwyczaj przez osoby obce ofierze, czyli specjalizujących się w tym przestępców działających w sieci, wyłudzających lub kradnących nagie zdjęcia czy filmy ofiary – i służą głównie do szantażowania w celu wymuszenia finansowego okupu. Natomiast za zemstę porno odpowiedzialne są przede wszystkim osoby, które już wcześniej znane były ofierze, czyli najczęściej były partner lub partnerka.

Czy wiesz, że...

Zjawisko ***revenge porn*** dotyka wiele osób, bez względu na wiek czy kraj zamieszkania. Jego szkodliwość jest bardzo wysoka, a ofiary często borykają się z wieloma trudnymi dla nich konsekwencjami przez wiele lat. Dlatego coraz więcej krajów dostrzega potrzebę uregulowania prawnego przestępstwa *revenge porn*, dzięki czemu sprawcy nie będą czuć się bezkarni[13].

13 Miliańska A., Szczygieł A., (2021) „Prawo kontra revenge porn", Wydawnictwo szczecińskich środowisk prawniczych, nr 151, [online] dostęp 10.03.2023 r.

TYPOWY SCENARIUSZ PRZESTĘPSTWA *REVENGE PORN*

Bywa tak, że związek dwojga ludzi z jakichś powodów przechodzi kryzys i rozpada się. Przyczyny mogą być różne: zdrada, niezgodność charakterów, znudzenie. Typowe jest przy tym jedno – partnerzy rozchodzą się w atmosferze konfliktu, a przynajmniej dużego żalu jednej ze stron. Taka osoba dokonuje później „tytułowej" zemsty, wykorzystując intymne materiały byłego partnera lub partnerki, które są w jej posiadaniu.

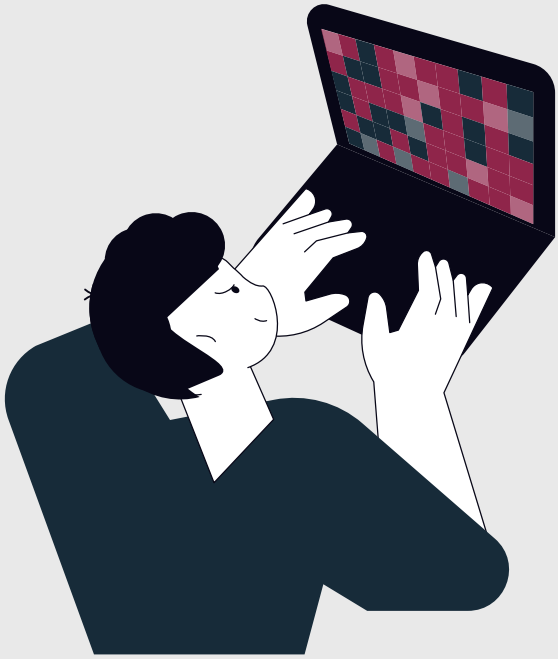
„Wysyłanie swoich intymnych zdjęć, filmów lub samo nagrywanie lub prezentowanie online takich treści może być dla nas niebezpieczne. Zawsze musimy liczyć się z tym, że mogą one zostać upublicznione lub – na przykład wskutek kradzieży lub utarty sprzętu – wypłynąć do sieci" – przestrzega Anna Kwaśnik, ekspertka NASK-PIB.

DLACZEGO LUDZIE PUBLIKUJĄ INTYMNE MATERIAŁY BLISKICH IM OSÓB

Nie bez powodu się mówi, że „emocje są złym doradcą". Trudne i silne emocje, które towarzyszą człowiekowi w związku ze złamanym sercem lub rozstaniem, mogą stać się motorem napędowym do tego, by skrzywdzić osobę, która go odrzuciła. Czasami chęć skompromitowania kogoś, zranienia go, jest silniejsza niż zdrowy rozsądek.

ZEMSTA

Jednym z najpopularniejszych motywów, który popycha ludzi do upublicznienia intymnych materiałów osób trzecich (najczęściej im znanych, a nawet bliskich), jest chęć zemsty i upokorzenia kogoś. W przypływie trudnych, silnych emocji nie zawsze myśli się racjonalnie, a chęć skrzywdzenia kogoś, czyli wzięcia odwetu za to, czego teraz się doświadcza, jest tak silna, że nie myśli się o konsekwencjach swojego czynu. A mogą one być nie tylko krzywdzące dla drugiej osoby, ale również niebezpieczne dla osób publikujących materiały.



SZANTAŻ

Kolejnym motywem, dla którego ludzie są gotowi upublicznić czyjeś prywatne materiały, jest szantaż. Rozpaczliwa chęć utrzymania związku i zatrzymania drugiej osoby przy sobie może sprawić, że człowiek szuka różnych, często nieracjonalnych sposobów, by nie doszło do rozstania. Targany silnymi emocjami próbuje wykorzystać materiały, które otrzymał od swojej drugiej połówki, i grozi ich upublicznieniem, jeśli ta zdecyduje się odejść.

W niektórych przypadkach *revenge porn* może być rozpatrywane również jako *sextortion* – gdzie sprawcą jest osoba bliska. Formą zapłaty za niepublikowanie materiałów mogą być zarówno korzyści materialne, jak i te związane np. z pozostaniem w związku. Osoba, która doświadcza tego rodzaju przemocy, może czuć się bezsilna i bezradna, dlatego zgadza się na stawiane jej warunki.

ZNISZCZENIE DOBREGO WIZERUNKU

Upublicznienie intymnych materiałów niesie za sobą konsekwencje dla osoby, która na nich występuje – przede wszystkim to upokorzenie i utrata dobrego wizerunku. Wyciek prywatnych materiałów bardzo często wiąże się z trudnościami w pracy lub jej utratą, ośmieszeniem w oczach innych i utratą pozycji, na którą pracowało się wiele lat. Niezdrowa, chorobliwa wręcz zazdrość osób z bliskiego otoczenia, ich poczucie niesprawiedliwości i zawiść mogą sprawić, że jeśli wejdą w posiadanie naszych intymnych materiałów (np. poprzez kradzież danych z telefonu lub ich samodzielną rejestrację bez naszej zgody), mogą udostępnić je innym. Dlatego niezwykle ważne jest, aby dbać o swoją prywatność, a także bezpieczeństwo swoich danych na urządzeniach mobilnych czy w chmurze.

PSYCHICZNE KONSEKWENCJE *REVENGE PORN*

Jeśli ktoś z bliskiego otoczenia zrealizuje swój plan i intymne zdjęcia czy filmy rzeczywiście staną się powszechnie dostępne, osoba pokrzywdzona musi nie tylko pogodzić się z tym, że ktoś z jej bliskich ją skrzywdził, ale również z konsekwencjami upublicznienia materiałów. Wiąże się to z całym szeregiem przykrych stanów: od lęku społecznego, poprzez depresję aż do myśli samobójczych.

Po pierwsze, dominującym stanem jest poczucie bycia wykorzystanym i zdradzonym. Pokrzywdzona osoba często udostępniała intymne materiały dobrowolnie w trakcie trwającego jeszcze, szczęśliwego związku (lub udostępniła je zaufanej osobie), a po jego ustaniu (bez względu na powód), ktoś, przy kim czuła się bezpiecznie i darzyła zaufaniem, wyrządził jej krzywdę i upokorzył. Podobne uczucia towarzyszą również w sytuacji, gdy ktoś ze znajomych jest sprawcą.

Konsekwencją jest też lęk przed oceną społeczną, zwłaszcza ze strony osób bliskich. Każdy, kto obejrzy udostępnione materiały, zobaczy ofiarę w bardzo intymnej sytuacji i przekroczy granice jej prywatności. Takie wydarzenie jest traumatyczne zarówno dla pokrzywdzonego, jak i najbliższych, którzy w pewnym sensie stają się naocznymi świadkami np. aktów miłosnych. Co gorsza, takich świadków może być znacznie więcej.

„Ofiara revenge porn nie ma już poczucia tej ochronnej bariery intymności – między sobą a resztą społeczeństwa. Odbudowanie jej zajmuje całe lata" – mówi ekspertka Marta Melk-Roszczyk, psycholog, biegła sądowa.

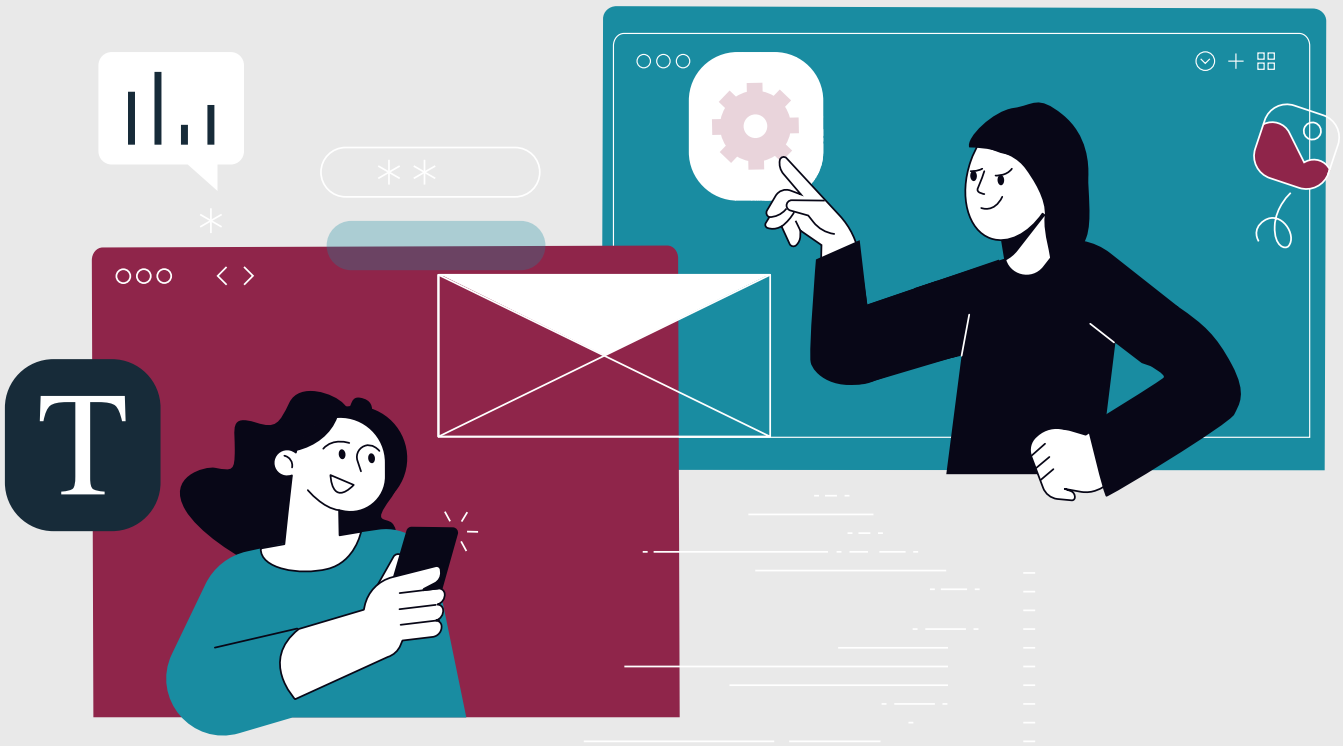
Pamiętaj!

Publikowanie i utrwalanie materiałów (zwłaszcza intymnych), które przedstawiają Twój wizerunek bez Twojej zgody, jest niezgodne z prawem!

CO ZROBIĆ, JEŚLI KTOŚ OPUBLIKUJE TWOJE NAGIE ZDJĘCIA W SIECI

To zrozumiałe, że jeśli ktoś opublikuje intymne materiały z Twoim udziałem, możesz czuć się bezsilny. W tej trudnej sytuacji warto mieć obok siebie bliską osobę, która nie tylko Cię wesprze i podniesie na duchu, ale również pomoże w skutecznym usuwaniu kompromitujących materiałów.

- Pamiętaj, że zawsze, gdy ktoś opublikuje zdjęcia lub filmy bez Twojej zgody, możesz zwrócić się do administratora serwisu lub portalu z żądaniem ich usunięcia.
- Jeśli materiały wypłyną do sieci, musisz się liczyć z tym, że prędzej czy później trafią one do Twoich znajomych, rodziny, pracodawcy. Porozmawiaj o tym z nimi.
- Zadbaj o swoją prywatność w sieci i skorzystaj z prawa do bycia zapomnianym, dzięki któremu możesz usunąć wyniki wyszukiwania powiązane z Twoimi danymi. Jak to zrobić: https://support.google.com/legal/answer/10769224
- Jeśli materiały z Twoim udziałem można wyszukać za pomocą wyszukiwarki Google, zgłoś się do osób zarządzających tą wyszukiwarką z prośbą o usunięcie materiałów. Jak to zrobić: https://support.google.com/websearch/answer/6302812
- Jeżeli po opublikowaniu zdjęć lub filmów z Twoim udziałem, otrzymujesz niechciane wiadomości lub połączenia telefoniczne, rozważ zmianę numeru.
- Sprawdź swoje ustawienia na portalach społecznościowych. Zmień je w taki sposób, aby nikt poza Twoimi znajomymi nie mógł się z Tobą skontaktować.
- Poszukaj wsparcia wśród swoich znajomych, powiedz im, co Cię spotkało. Jeśli nie radzisz sobie z emocjami, jakie Ci towarzyszą, poszukaj pomocy u specjalisty.
- Publikowanie takich materiałów to przestępstwo. Zgłoś sprawę na policję.



DEEPFAKE PORN – ZAGROŻENIE Z WYKORZYSTANIEM TECHNOLOGII

Wystarczy obraz twarzy, utrwalony i udostępniony na zdjęciu lub filmie, by stworzyć realistycznie wyglądające materiały pornograficzne z wizerunkiem niewinnej osoby. Zagrożenie określane jako *deepfake porn* to przykład wykorzystania dobrej i pożytecznej technologii w zdecydowanie złym celu.

Zjawisko *deepfake*[14] to w uproszczeniu technika obróbki obrazu, wykorzystująca rozwiązania sztucznej inteligencji. Termin powstał z połączenia dwóch angielskich słów: *deep*, odnoszącego się do *deep learning* – systemów głębokiego uczenia maszynowego oraz *fake*, oznaczającego fałsz. Materiały typu *deepfake* wytwarzane są przez algorytmy na podstawie prawdziwych próbek głosu, dźwięku, filmów lub zdjęć. W założeniu pozwala to na stworzenie materiałów, które są trudne do odróżnienia od filmów lub zdjęć zrealizowanych w tradycyjny sposób – z udziałem żywych, konkretnych osób.

Czym jest *deepfake porn*?

Mimo wielu imponujących rozwiązań technologia *deepfake* znalazła również zastosowanie przy produkcji fałszywych materiałów pornograficznych, których celem jest najczęściej wyrządzenie krzywdy drugiej osobie, np. poprzez jej ośmieszenie. W materiałach typu *deepfake porn* twarz aktora lub aktorki występującej w materiałach pornograficznych zostaje zastąpiona wizerunkiem innej osoby, oczywiście bez jej zgody.

Na czym polega zagrożenie?

Zagrożenia wynikające z produkcji materiałów *deepfake porn* są tak samo niebezpieczne i szkodliwe, jak te omawiane przy *sextortion* czy *revenge porn*. Da się je wykorzystać jako narzędzie szantażu – zarówno finansowego, jak i społecznego. Motywem sprawcy może też być chęć skrzywdzenia danej osoby lub ośmieszenia jej. Ofiarą *deepfake porn* może stać się każdy, choć szczególnie narażone są osoby publiczne czy celebryci.

Podstawowe różnice między materiałami *revenge porn* a *deepfake porn* to sposób pozyskania i wytworzenia materiałów, ich autentyczność oraz dostępność. Te pierwsze najczęściej wytwarzane są samodzielnie, za zgodą osób w nich występujących, a dostęp do nich mają tylko wybrani – najczęściej partner lub partnerka. To niestety oni są też ewentualnymi sprawcami *revenge porn*.

14 Tomlinson K., (2022), „Naucz się nowej umiejętności: wykrywanie Deepfake", tłum. Wnuk B., Węgrzynowicz A., „OUCH!" Biuletyn Bezpieczeństwa Komputerowego, nr 3 [online] dostęp 10.03.2023 r.

W przypadku materiałów *deepfake porn* ich autorem może być każdy, ponieważ do ich stworzenia wystarczy dostęp do zwyczajnych zdjęć czy filmów, które potencjalna ofiara udostępniła np. w mediach społecznościowych, i podłożenie ich do wybranego materiału pornograficznego. Liczba osób, które mogą wyrządzić krzywdę, jest zatem wielokrotnie większa.

Twórcom materiałów *deepfake porn* bardzo często towarzyszy wrażenie pozornej anonimowości, a co za tym idzie bezkarności. Ujawnienie prawdziwych materiałów intymnych z reguły dość szybko pozwala wskazać osobę, która się tego dopuściła, natomiast przy fałszywych materiałach autorem może być każdy. Niestety, sprawcy często nie czują się w żaden sposób winni, a swoje działania traktują wyłącznie jako żarty.

Warto jednak przypomnieć, że anonimowość jest w wielu internetowych działaniach tylko złudzeniem i zwykle istnieje możliwość wykrycia sprawcy tego typu aktywności.

Czy da się obronić przed *deepfake porn*?

Wykorzystanie technologii *deepfake* zarówno w przypadku filmów pornograficznych, jak i innych materiałów, których celem jest ośmieszenie lub upokorzenie innej osoby, jest niestety powszechne, i może dotknąć każdego z nas.

Jeśli decydujesz się na korzystanie z różnych technologii, narzędzi oraz portali i serwisów społecznościowych, musisz pamiętać, że narażasz swój wizerunek na niebezpieczeństwo wykorzystania go przez inne osoby w niewłaściwy sposób.

- Po pierwsze, staraj się rozsądnie zarządzać udostępnianiem swojego wizerunku, zwłaszcza w mediach społecznościowych. Jeśli decydujesz się na prowadzenie profili w mediach społecznościowych, zadbaj o ustawienia prywatności.
- Pomyśl, zanim udostępnisz swoje zdjęcia lub filmy np. w stroju kąpielowym – kto ma do nich dostęp i w jakich sposób może je wykorzystać.
- Z rozwagą korzystaj z programów i aplikacji, które przetwarzają Twoje zdjęcia lub filmy pozornie wyłącznie w celach rozrywkowych (np. pokazują Twój wygląd za trzydzieści lat lub z inną fryzurą), a także rejestrują Twój głos.

ZAGROŻENIA INTERNETOWE A OCHRONA UŻYTKOWNIKÓW

Przytoczone w publikacji zagrożenia mogą pojawiać się w wielu miejscach w sieci – portalach społecznościowych, aplikacjach randkowych, komunikatorach czy innych platformach i w usługach internetowych. Narażony na nie jest każdy użytkownik, a w szczególności te osoby, które są samotne i szukają drugiej połówki. Niektóre przytoczone przez nas zjawiska przypominają, jak niebezpieczne jest dzielenie się swoimi prywatnymi, intymnymi zdjęciami, nawet z osobami, z którymi jesteśmy w związku.

Przedstawione w poradniku zagrożenia to w większości przypadków przestępstwa, a ich sprawcom grozi za nie odpowiedzialność karna.

Mimo że w polskim prawie nie mamy wprost określonych przestępstw typu *romance scam, sextortion, revenge porn* i innych opisywanych przez nas zagrożeń, to osoby, które padły ich ofiarą, powinny zgłosić sprawę na policję i domagać się od oszustów odszkodowania i poniesienia kary.

Każdy przypadek jest inny i należy go rozpatrywać indywidualnie. Poniżej przedstawiamy artykuły prawne, na jakie możesz się powoływać, jeśli ktoś Cię oszuka w sieci lub rozpowszechni intymne materiały bez Twojej zgody.

BEZPRAWNE WYKORZYSTANIE WIZERUNKU (ZWŁASZCZA INTYMNE MATERIAŁY)

Art. 81 Ustawy o prawie autorskim i prawach pokrewnych

1. *Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W przypadku braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie.*
2. *Zezwolenia nie wymaga rozpowszechnianie wizerunku:*
   - *osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;*
   - *osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.*

Art. 191 a Kodeksu karnego [Naruszenie Intymności Seksualnej]

§ 1. Kto utrwala wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej, używając w tym celu wobec niej przemocy, groźby bezprawnej lub podstępu, albo wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody rozpowszechnia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Ściganie następuje na wniosek pokrzywdzonego.

SZANTAŻ I WYMUSZENIA FINANSOWE

Art. 190. Kodeksu karnego [Groźba karalna]

§ 1. Kto grozi innej osobie popełnieniem przestępstwa na jej szkodę lub szkodę osoby najbliższej, jeżeli groźba wzbudza w zagrożonym uzasadnioną obawę, że będzie spełniona, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Ściganie następuje na wniosek pokrzywdzonego.

OSZUSTWO I OSZUSTWO KOMPUTEROWE

Art. 286 Kodeksu karnego [Oszustwo]

§ 1. Kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 3. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Art. 287. Kodeksu karnego [Oszustwo komputerowe]

§ 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Jeśli padłaś/eś ofiarą oszustwa, masz prawo zgłosić tę sprawę na policję. Nie pozwól, by sprawca czuł się bezkarny! Skonsultuj sprawę z prawnikiem i sprawdź, co możesz zrobić.

W przypadku oszustw internetowych zgłoś sprawę również do zespołu CERT Polska.

W JAKI SPOSÓB MOŻESZ SIĘ UCHRONIĆ PRZED INNYMI RODZAJAMI OSZUSTW INTERNETOWYCH

Zasada ograniczonego zaufania

- Z ostrożnością podchodź do linków i nie otwieraj załączników, co do których masz wątpliwości albo które otrzymałaś(-łeś) od nieznanych osób. Cyberprzestępcy wysyłają do nas różne wiadomości (poprzez e-mail, SMS-y, komunikatory, serwisy społecznościowe i inne), w których namawiają do kliknięcia przesłanego linku lub otwarcia załącznika. Mogą one prowadzić na szkodliwe i fałszywe strony internetowe lub zawierać złośliwe oprogramowanie.
- Zwracaj uwagę na adresy stron internetowych, z których korzystasz. Przestępcy bardzo często przygotowują fałszywe strony, które wyglądają jak prawdziwe portale internetowe, pod które się podszywają. Jeśli strona, na której jesteś, ma nieco inny adres niż zwykle (np. różni się choćby jedną literą), to prawdopodobnie jest fałszywa. W takiej sytuacji pod żadnym pozorem nie wprowadzaj danych logowania i zamknij stronę.
- Uważaj na wiadomości, które wymagają od Ciebie podjęcia albo szybkich, albo natychmiastowych działań.
- Jeśli decydujesz się na zawieranie znajomości online (np. poprzez aplikacje randkowe) zawsze weryfikuj, z kim rozmawiasz. Sprawdź, czy dane, jakimi się posługuje rozmówca (imię, nazwisko, e-mail), są prawdziwe. Zwróć uwagę na konto tej osoby w mediach społecznościowych – ilu ma znajomych, od kiedy to konto istnieje. Jeśli decydujesz się na bliższą znajomość, poproś o rozmowę wideo. Niestety, nigdy nie możesz mieć pewności, kto jest po drugiej stronie, jakie ma intencje i zamiary wobec Ciebie.
- Staraj się zachować czujność i zdrowy rozsądek – zwłaszcza jeśli nowo poznana osoba szybko wyznaje miłość, a w kolejnych wiadomościach prosi o pieniądze.

Bezpieczeństwo Twoich danych

- Pod żadnym pozorem nikomu nie podawaj swoich haseł ani danych logowania. Nigdy nie możesz mieć pewności, kto i w jaki sposób je wykorzysta.
- Stosuj długie i silne hasła, które są trudne do złamania – Twoje hasło powinno mieć co najmniej 12 znaków, nie może zawierać informacji o Tobie lub Twojej rodzinie (nie używaj dat urodzenia, imienia swojego pupila, tytułu ulubionej książki itp.). O tym, jak tworzyć silne hasła, dowiesz się z poradnika CERT Polska.
- Postaraj się, aby Twoje hasła były oryginalne, unikaj popularnych słów, zwrotów, fraz i kombinacji klawiszy.
- Zadbaj o to, aby Twoje hasła były unikatowe – każdy portal, serwis, z którego korzystasz, powinien mieć inne hasło.
- Używaj uwierzytelnienia dwuskładnikowego, zwłaszcza przy korzystaniu z poczty elektronicznej, serwisów społecznościowych, komunikatorów. Możesz do tego wykorzystać token sprzętowy, np. U2F lub aplikację (np. Google Authenticator); unikaj usług, które nie pozwalają na dwuskładnikowe uwierzytelnianie.
- Jeśli masz podejrzenia, że ktoś włamał się na Twoje konto lub że Twoje hasło wyciekło, zmień je natychmiast. Zakończ wszystkie aktywne sesje i wyloguj się z innych urządzeń. Jeśli nie możesz zalogować się na swoje konto ani zresetować hasła, zgłoś sprawę do administratora serwisu.

Chroń swoją prywatność

- Portale społecznościowe i serwisy randkowe zachęcają nas do tego, aby dzielić się w sieci prywatnymi informacjami z naszego życia. Udostępniamy tam nie tylko zdjęcia i filmy z naszym udziałem, ale chętnie też opowiadamy o sobie. Zanim podzielisz się szczegółami ze swojego życia w sieci, przemyśl to. Takie dane mogą zostać wykorzystane przez cyberprzestępców i różnych oszustów, którzy będą chcieli np. wymusić od Ciebie poufne dane lub wyłudzić pieniądze.
- Zadbaj o ustawienia prywatności w serwisach i portalach społecznościowych – dzięki temu ograniczasz swoją widoczność dla nieznajomych, którzy mogą mieć wobec Ciebie różne zamiary, nie zawsze uczciwe.
- Zanim udostępnisz komuś swoje prywatne, intymne zdjęcia lub filmy, przemyśl to. Nigdy nie masz pewności, kto i w jaki sposób je wykorzysta.

Bezpieczeństwo Twojego sprzętu

- Aktualizuj oprogramowanie swojego sprzętu i aplikacje, z których korzystasz. Dzięki temu są one mniej podatne na różnego rodzaje niebezpieczeństwa i zagrożenia online. Zalecamy włączenie automatycznych aktualizacji.
- Korzystaj z programu antywirusowego, aktualizuj go na bieżąco.
- Nie podawaj nikomu hasła dostępu do Twojego sprzętu (np. smartfona, komputera). Nigdy nie masz pewności, w jaki sposób osoba trzecia może wykorzystać dane, jakie na nich przechowujesz i przetwarzasz.
- Nie instaluj aplikacji, które sugerowane Ci są w rozmowie telefonicznej lub komunikatach e-mail/SMS przez osoby podające się za „konsultantów", „serwis", „pomoc techniczną" czy innego rodzaju przedstawicieli instytucji (np. banku), z której usług korzystasz.

GDZIE SZUKAĆ POMOCY

Incydenty związane z Twoim bezpieczeństwem online i oszystwami internetowymi zgłoś do zespołu CERT Polska, w wygodny dla Ciebie sposób:

przez formularz na stronie: incydent.cert.pl

wysyłając email na adres: incydent@cert.pl

wysyłając wiadomość SMS na numer: 799-448-084
(w przypadku podejrzanych wiadomości SMS zawierających link)

Gdzie szukać pomocy

- Kryzysowy Telefon Zaufania: 116 123
- Antydepresyjny Telefon Zaufania Fundacji Itaka: 22 484 88 01
- Całodobowy Telefon dla Osób Dorosłych w Kryzysie Psychicznym 800 70 22 22
- Fundacja dla Kobiet Doświadczających Przemocy
- Telefon Zaufania dla Mężczyzn 608 271 402
- Platforma 116sos.pl – bezpłatne wsparcie dla osób dorosłych w kryzysie emocjonalnym

Baza wiedzy – jak dbać o swoje cyberbezpieczeństwo

- https://bezpiecznymiesiac.pl/bm/baza-wiedzy
- https://cert.pl/ouch/
- https://cert.pl/hasla/
- https://cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf
- https://www.gov.pl/web/baza-wiedzy/aktualnosci
- https://cbzc.policja.gov.pl/bzc/zagrozenia-w-sieci

BILBLIOGRAFIA:

1. 49-latek oszukany na "amerykańską żołnierkę", publikacja 12.10.2022 r., oficjalny serwis Polskiej Policji, dostęp 9.03.2023 r.
2. Coluccia A., Pozza A., Ferretti F., Carabellese F., Masti A., Gualtieri G., (2020), „Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review." Clinical Practice Epidemiology in Mental Health, v. 16, s. 24-35 [online], dostęp 7.03.2023 r.
3. Fletcher E., Romance scammers' favorite lies exposed, oficjalny serwis Amerykańskiej Komisji ds. Handlu (FTC), publikacja 9.02.2023r., dostęp 9.03.2023 r.
4. https://policja.pl/pol/tagi/21978,oszustwo-quotna-amerykanskiego-zolnierzaquot.html, oficjalny serwis Polskiej Policji, dostęp 9.03.2023 r.
5. James miał być amerykańskim żołnierzem – okazał się oszustwem., publikacja 31.10.2022 r., oficjalny serwis Polskiej Policji, dostęp 9.03.2023 r.
6. Kacprzak-Wachniew K., Pilarska N., „Doświadczenia osób korzystających z aplikacji i portali randkowych", Uczuciowo Naukowo, 23.09.2022 r., [online], dostęp 7.03.2023r.
7. Kumar A., Albrecht J., New Spyware Used by Sextortionists iOS/Android Blackmail, publikacja 16.12.2020 r., oficjalna strona firmy Lookout Mobile Security, dostęp 8.03.2023 r.
8. Miliańska A., Szczygieł A., (2021) „Prawo kontra revenge porn", Wydawnictwo szczecińskich środowisk prawniczych, nr 151, [online], dostęp 10.03.2023 r.
9. Nicholson Ch., (2020), „Ataki socjotechniczne", tłum. Wnuk B., Węgrzynowicz, „OUCH"! Biuletyn Bezpieczeństwa Internetowego nr 3 [online], dostęp 9.03.2023 r.
10. Oszustwo na amerykańskiego żołnierza – nie daj się nabrać!, publikacja 7.04.2022 r. oficjalny serwis Polskiej Polcji, dostęp 9.03.2023 r.

11. Thomas M. F., Binder A., Stevic A., & Matthes J. (2023), 99 + matches but a spark ain't one: Adverse psychological effects of excessive swiping on dating apps. Telematics and Informatics: An Interdisciplinary Journal on the Social Impacts of New Technologies, 78, [101949]. [online], dostęp 8.03.2023 r.
12. Tomlinson K., (2022), „Naucz się nowej umiejętności: wykrywanie Deepfake", tłum. Wnuk B., Węgrzynowicz A., „OUCH!" Biuletyn Bezpieczeństwa Komputerowego, nr 3 [online], dostęp 10.03.2023 r.
13. Wnęk – Gozdek J. „Oszustwa romantyczne online – studium przypadku". Bliskie relacje w doświadczeniach życiowych człowieka, 2(17)/2019, Kraków, Exlibris. Biblioteka Gerontologii Społecznej, s.39-55, [online], dostęp 9.03.2023 r.
14. Zeltser L. (red.), (2021), „Kradzież tożsamości – ochroń się przed nią", tłum. Wnuk B., Węgrzynowicz A., „ OUCH!" Biuletyn Bezpieczeństwa Komputerowego"nr 3 [online], dostęp 8.02.2023 r.

Akty prawne:

- Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego(Dz.U.2022.0.1138 t.j)
- Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U.2022.0.2509 t.j. -)