PORADNIK NIEROMANTYCZNY

NA CO UWAŻAĆ W CYBERMIŁOŚCI

UKE | Urząd Komunikacji Elektronicznej

SPIS TREŚCI

W czasach, kiedy znaczna część naszego życia przeniosła się do internetu, w sieci szukamy znajomych, przyjaźni, ale również partnerów. Już za pośrednictwem pierwszych czatów, forów dyskusyjnych czy tablic z ogłoszeniami użytkownicy sieci nawiązywali znajomości, które niekiedy przeradzały się w związki. W miarę jak ewoluował internet, ewoluowały również narzędzia komunikacji. Coraz większą popularnością cieszą się m.in. aplikacje randkowe. Jako początek branży randek online niektórzy wskazują rok 1959 r., kiedy studenci Uniwersytetu Stanforda, dopasowali prawie 50 par za pomocą kwestionariusza przetworzonego przez komputer mainframe IBM 650. Pierwsze portale randkowe zostały zarejestrowane w Stanach Zjednoczonych w 1994 i 1995 r. (kiss.com i match.com). W 1996 r. istniało już 16 portali randkowych.

W ślad za powstaniem nowej formy zawierania znajomości pojawiły się również cyberzagrożenia.

W walentynkowym artykule St. Petersburg Times z 1995 r. ostrzegano cyberrandkowiczów „Strzeżcie się, cyberrandkowicze. Może się okazać, że Bambi4You, z którą prowadzisz rozmowę na czacie, tylko udaje, że jest kobietą. Oczywiście, może też być kobietą udającą, że jest mężczyzną, mężczyzną szukającym transwestyty... Możliwości jest wiele”.[1] W tamtych latach nikt nie był w stanie przewidzieć jak popularne staną się oszustwa romantyczne i jaka będzie skala strat finansowych związanych z *romance scams*. Eksperci przewidywali, że do końca 2025 r. branża randek online osiągnie 3,592 miliarda dolarów przychodów.

Takie przychody i zainteresowanie randkami online wykorzystują oszuści internetowi. Dostęp do internetu, aplikacji i mediów społecznościowych sprawił, że obecnie oszuści działają na globalną skalę. Coraz częściej oszustwa związane z randkami i romansami są prowadzone przez grupy przestępcze, korzystające ze sztucznej inteligencji, skryptów i szkoleń, pozwalających na dotarcie do wielu potencjalnych ofiar i maksymalizację zysków.

Aplikacje randkowe i zawieranie znajomości przez internet to przede wszystkim alternatywa dla osób, które mają problem z nawiązywaniem znajomości w realu. Internet daje nam możliwość poznania ludzi z całego świata. Możemy szukać „bratniej duszy” o podobnych poglądach i wyznających te same wartości. Pamiętajmy jednak by zachować czujność, bo w sieci czyha na nas wiele zagrożeń i nie każdy jest tym za kogo się podaje.

Korzystając z portali randkowych i społecznościowych należy pamiętać o uniwersalnych zasadach bezpieczeństwa w sieci. Na co uważać szukając miłości w sieci?

1) J. A. Cutter, Getting it on-line [www.tampabay.com; dostęp: 16.01.2015]
2) 141 Crucial Online Dating Statistics: 2024 Data Analysis & Market Share - Financesonline.com

APLIKACJE I PORTALE RANDKOWE

Masz duży wybór, bo w sieci znajdziesz wiele portali randkowych. Są popularne aplikacje randkowe dostępne na urządzenia mobilne, portale dla różnych grup wiekowych czy skierowane do osób o określonych preferencjach. Internetowe serwisy randkowe wykorzystują złożone algorytmy, aby dopasować miliony użytkowników wśród potencjalnych kandydatów. Technologia stojąca za branżą cały czas się rozwija i generuje rekordowe przychody. Serwisy randkowe to w zasadzie sieci społecznościowe bazujące na zainteresowaniach, upodobaniach i wyglądzie. Znajdziesz aplikacje i serwisy randkowe kierowane do szerokiego grona użytkowników i te wyspecjalizowane, koncentrujące się na konkretnych potrzebach, np. kojarzeniu par wg rasy, religii, wykształcenia, poglądów, czy preferencji seksualnych. Przykładowo:

- Na *Tinderze* poznawanie osoby opiera się o tzw. matching. *Tinder* jest częścią Match Group – firmy technologicznej, która jest właścicielem i operatorem największego globalnego portfolio internetowych serwisów randkowych, w tym platform *OkCupid*, *Hinge*, *Pairs* i *OurTime*, *Meetic*, *Match.com*, *Plenty of Fish*,

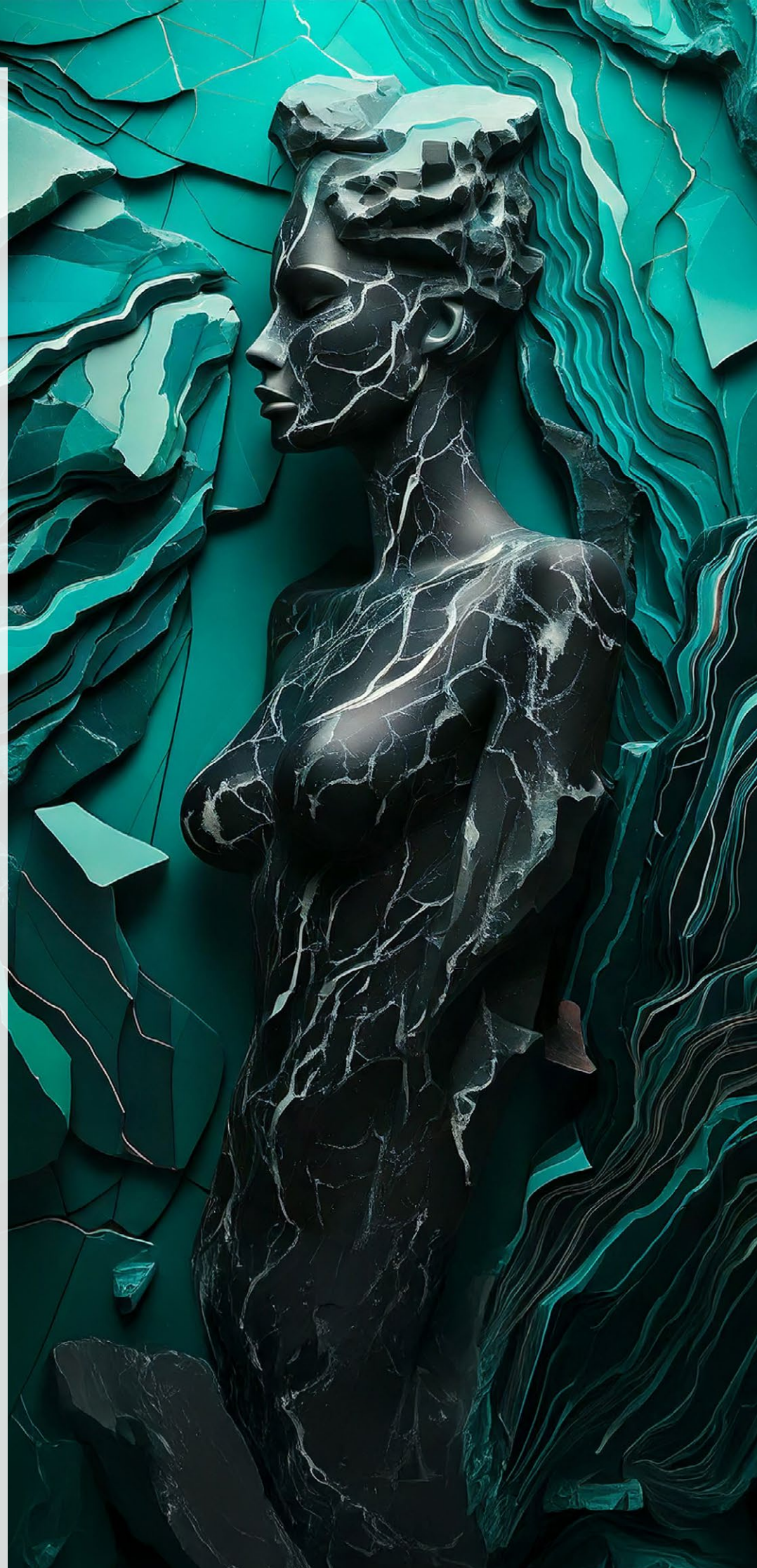
- *Singlowanie.pl* to katolicki portal randkowy, który kojarzy pary preferujące chrześcijańskie wartości.

- *Grindr* i *Romeo* to jedne z najpopularniejszych aplikacji randkowych społeczności LGBTQ, ukierunkowane na mężczyzn homoseksualnych i biseksualnych. *Grindr* był jedną z pierwszych aplikacji, która zawierała dane GPS w swoich wynikach wyszukiwania.

- *Zoe* i *HER* to aplikacje skierowane do społeczności LGBTQ zorientowanej na kobiety, lesbijki, osoby queerowe i osoby niebinarne.

- *Friendsy* to aplikacja dla studentów, w której można np. ustawić filtry w oparciu o kierunek studiów.

Portale i aplikacje oferują podstawowe wersje bezpłatne oraz płatne opcje rozszerzone i pakiety premium. Większość serwisów działa na podobnej zasadzie, a sama rejestracja często jest bezpłatna. Do założenia konta wystarczy wprowadzić podstawowe dane o sobie, ustawić login (nazwę użytkownika, jaką będziemy się posługiwać), adres e-mail oraz hasło. Część aplikacji umożliwia rejestrację i logowanie za pośrednictwem portalu społecznościowego. Wybierając taką opcję zezwalasz na dostęp i wykorzystywanie informacji z twojego konta na danym portalu społecznościowym.



Wybierając aplikację lub portal randkowy:

- Sprawdź czy ma określony regulamin korzystania z usług. Jeśli na stronie portalu nie znajdziesz regulaminu, nie korzystaj z tego portalu. W regulaminie znajdziesz m.in. informacje o warunkach korzystania z portalu/ aplikacji, warunki rozwiązania umowy, szczegóły dot. subskrypcji, informacje o płatnościach i ograniczeniu odpowiedzialności podmiotów.

- Zapoznaj się z polityką prywatności. Polityka prywatności określa jakie dane są zbierane od użytkowników, jak są przetwarzane, jakim podmiotom mogą być udostępniane, które dane są zbierane automatycznie itp. Powinieneś tam również znaleźć informacje w jaki sposób wnieść sprzeciw lub zażądać ograniczenia przetwarzania danych.

- Poznaj opinie innych użytkowników. Jeśli inni użytkownicy wypowiadają się o aplikacji pozytywnie, a liczba pobrań jest wysoka można przejść do jej instalacji. Aplikacje pobieraj wyłącznie z legalnych źródeł. Unikaj portali, gdzie nie ma podanych danych kontaktowych podmiotu prowadzącego serwis randkowy.

Zakładając konto:

- Stwórz silne hasło. Obecnie o sile hasła decyduje głównie jego długość. Używaj też dużych i małych liter, cyfr i znaków specjalnych. Nie podawaj w haśle swojego imienia, czy daty urodzenia. Pamiętaj, że nie powinno ono być takie jak login. Im dłuższe i bardziej skomplikowane hasło, tym trudniej będzie je złamać.

- Ogranicz dane, którymi się dzielisz. Większość podawanych przez Ciebie informacji jest opcjonalna. Aby zachować środki ostrożności, najlepiej podaj tylko te wymagane do założenia konta.

- Wybierz neutralne zdjęcia. Wstawiając zdjęcia na swój profil zwróć uwagę, aby nie pokazywały żadnych identyfikujących szczegółów, np. z nazwą ulicy w tle, czy numerem domu. Nie publikuj intymnych zdjęć i nie przesyłaj takich zdjęć innym użytkownikom serwisów. Nie nękaj też innych użytkowników i użytkowniczek wysyłając nieprzyzwoite zdjęcia.

Cyberflashing **to wysyłanie nieprzyzwoitych zdjęć swojego nagiego ciała, zwłaszcza narządów płciowych, komuś kogo nie znamy, i kto tego nie chce, często za pośrednictwem transferów Bluetooth lub AirDrop.**

W Wielkiej Brytanii, w ustawie o bezpieczeństwie w sieci, wprowadzono przestępstwa, w celu kryminalizacji m.in. cyberflashingu.

Cyberflashowanie w aplikacjach randkowych, AirDrop i innych platformach ma spowodować, że sprawcom grozi do dwóch lat więzienia, jeśli robią to w celu uzyskania satysfakcji seksualnej lub wywołania niepokoju lub upokorzenia. W Polsce nie ma przepisów klasyfikujących wprost *cyberflashing*, jedynie przepisy dot. treści pornograficznych.

Art. 202 § 1 kodeksu karnego: Kto publicznie prezentuje treści pornograficzne w taki sposób, że może to narzucić ich odbiór osobie, która tego sobie nie życzy, podlega karze pozbawienia wolności do lat 3.

Materiały mają charakter pornograficzny w rozumieniu art. 202 kodeksu karnego, gdy treścią prezentacji w tych materiałach jest przedstawienie przejawów płciowości i życia seksualnego człowieka, które koncentruje się wyłącznie na pokazaniu jego techniczno-biologicznych aspektów (z pominięciem jakiejkolwiek warstwy intelektualno-personalistycznej) i zawiera ukazanie narządów płciowych w ich seksualnych funkcjach, jeśli jedyną intencją twórcy tych materiałów było wywołanie podniecenia seksualnego u odbiorcy przekazu[3].

Koszty i rezygnacja z usług:

- Pamiętaj, że część aplikacji oferuje sprzedaż produktów i usług za pośrednictwem Google Play Store, App Store, opłaty naliczanej przez operatora lub innych form płatności.

- Aplikacje oferują konta lub opcje rozszerzone/premium. Pozwalają one korzystać użytkownikom z dodatkowych możliwości, np. niewidoczny profil, który pozwala na sekretne przeglądanie innych profili. Konta premium zazwyczaj są oparte o subskrypcje i mają różne koszty w zależności od wybranego wariantu.

- Sprawdź warunki i koszty subskrypcji. W przypadku wykupienia automatycznie odnawialnej subskrypcji, opłata będzie pobierana za pośrednictwem wybranej metody płatności do momentu jej anulowania. W regulaminie powinieneś znaleźć szczegółowe instrukcje jak zmienić lub zakończyć subskrypcję.

- Odinstalowanie aplikacji nie oznacza usunięcia konta. Przy rejestracji podajemy nasz adres e-mail i możemy się zalogować na konto z innego urządzenia. Dlatego, gdy chcesz zakończyć przygodę z randkowaniem online, przejdź do ustawień danej aplikacji i usuń konto zgodnie z instrukcją. Masz też możliwość

3) Wyrok Sądu Apelacyjnego w Poznaniu - II Wydział Karny z dnia 24 maja 2012 r., II AKa 75/12

skorzystać z prawa o zapomnieniu i zwrócić się do administratora o usunięcie Twoich danych.

Wykorzystanie sztucznej inteligencji

Część firm już korzysta lub testuje funkcje sztucznej inteligencji, np. do selekcji zdjęć lub do wspierania algorytmów wyświetlania poszczególnych profili użytkowników osobom, które mogą być nimi zainteresowane. Ma to poprawić trafność dopasowań w aplikacji. AI jest też używana do tworzenia opisów profili, spersonalizowanych treści, biografii użytkowników itp.

Już teraz użytkownicy mogą ściągnąć „randkowych asystentów", których twórcy reklamują je jako produkty pomagające kobietom i mężczyznom być dowcipniejszymi rozmówcami albo pozwalające pisać za nas wiadomości dopasowane do wybranego stylu konwersacji (przyjacielska rozmowa, flirt itp.). Są też dostępne usługi dające możliwość stworzenia bota, który może rozmawiać z innymi osobami zamiast nas. W tym przypadku użytkownik tworzy cyfrową wersję samego siebie. Bot musi mieć informacje na nasz temat, by mógł generować wiarygodne wiadomości. Zbierane są dane dot. daty urodzenia, adresu, danych rodziny i przyjaciół, wykształcenia, ulubionej muzyki, potraw i wspomnień.

Niektóre aplikacje, jak np. Amori, wykorzystują chatboty AI zwane trenerami randkowymi, które uczą się i dostosowują na podstawie rozmów użytkowników. Te aplikacje gromadzą dane i analizują interakcje użytkowników, preferencje, zachowania. Wykorzystują techniki uczenia maszynowego by odpowiednio dobierać treści i dopasowania dla użytkownika. Popularna w USA aplikacja Rizz wykorzystywana jest do generowania spersonalizowanych odpowiedzi, które schlebiają, angażują i imponują rozmówcy. Użytkownicy mogą przesyłać zrzuty ekranu swoich rozmów z matchami, a nawet bio matchów wraz z ich profilem, aby natychmiastowo zachęcić aplikację do udzielania zabawnych, sprytnych i dowcipnych odpowiedzi do rozmówcy. Aplikacja dostosowuje się do stylu komunikacji użytkownika, analizując jego naturalny styl, ton, humor i słownictwo.

W Polsce wspomaganie randkowania aplikacjami opartymi na AI jeszcze nie jest tak popularne, ale to zapewne kwestia czasu. Aplikacje i portale randkowe to gigantyczne bazy danych określające preferencje użytkowników. W internecie zostawiamy ogromną liczbę śladów cyfrowych,

które są zapisywane przez nasze smartfony, portale społecznościowe, randkowe, Google'a czy karty kredytowe. Na portalach randkowych sami podajemy dane po to by znaleźć partnera według określonych preferencji. Algorytmy aplikacji analizują nasze zachowania, wybory, lokalizację i priorytetyzują wybrane profile. Wg dr Michała Kosińskiego wystarczy ok. 100 do 150 lajków by algorytm mógł opisać naszą osobowość na poziomie najbliższego przyjaciela, a ok 250 lajków by zrobił to dokładniej niż nasz wieloletni partner, mąż, żona[4]. Algorytm wie o nas dużo więcej niż my sami o sobie. Tym samym jesteśmy coraz bardziej podatni na manipulację.

Kopalnie danych

Aplikacje randkowe mogą mieć dostęp do zdjęć, filmów czy bazy kontaktów, które mamy w naszym telefonie, jeśli wyrazimy na to zgodę. Jeśli logujemy się do nich za pośrednictwem konta z innego portalu społecznościowego, czy np. Google, to aplikacja ma dostęp do danych, które udostępniamy „podmiotom trzecim". Dane, które gromadzą aplikacje randkowe są bardzo często sprzedawane innym podmiotom w celu tworzenia spersonalizowanych reklam. Część dostawców aplikacji określa to wprost w regulaminie. W taki sposób dodatkowo zarabiają na użytkownikach. Według analizy 25 aplikacji randkowych przeprowadzonej przez Fundację Mozilla, 22 z nich stanowiła zagrożenie dla prywatności danych[5].

- **Indywidualne konto**
  Nie loguj się do konta w aplikacji randkowej przy użyciu profili założonych np. na Facebooku czy Google. W ustawieniach prywatności zablokuj dostęp do danych ze smartfona wszędzie tam, gdzie jest taka możliwość, np. aparat, książka adresowa, lokalizacja.

- **Zasada ograniczonego zaufania**
  Ogranicz do minimum przekazywanie wrażliwych informacji na swój temat tego typu programom i aplikacjom. Nie dziel się szczegółami życia z botami. Aplikacje służące do ulepszania profili na portalach randkowych, czy generowania „lepszych" wiadomości, to narzędzia często wykorzystywane przez cyberoszustów.

---

4) Michał Kosiński: Wojnę o prywatność już przegraliśmy – Sztuczna Inteligencja

5) Data-Hungry Dating Apps Are Worse Than Ever for Your Privacy

CZY TO TY?
NA CO UWAŻAĆ W SIECI

W sprawach uczuciowych zazwyczaj serce jest o krok przed rozumem, a to nie wszystkim wychodzi na dobre. Szukając swojej drugiej połówki w sieci pamiętaj, że nie każda osoba w internecie jest tą za którą się podaje i nie każda ma dobre intencje. Wiele osób jest podatnych na manipulacje i socjotechnikę, którą wykorzystują m.in. internetowi przestępcy.

Przestępcy wykorzystują iluzję miłości i zaufania, aby manipulować ofiarami, tak by przekazały im pieniądze lub poufne informacje. Ofiary często cierpią nie tylko z powodu strat finansowych, ale także z powodu głębokiej traumy emocjonalnej. Oszuści budują emocjonalne więzi ze swoimi ofiarami poprzez „uwodzenie", stopniowo zdobywając zaufanie i pogłębiając więź emocjonalną. Reakcje chemiczne w mózgu, w tym uwalnianie dopaminy i oksytocyny wpływają na uczucia przywiązania i więzi emocjonalnej, co czyni ofiary bardziej podatnymi na manipulacje oszusta.

Użytkownicy serwisów randkowych jako powszechne zagrożenia wskazują:

- kłamstwa, w celu zwiększenia swojej atrakcyjności,
- zakładanie fałszywych kont, w celu oszukiwania innych,
- otrzymywanie niechcianych zdjęć i wiadomości o charakterze seksualnym,
- naruszenia prywatności, takie jak kradzież tożsamości i danych.

Sextortion

„Sextortion" to forma szantażu. Jest to pochodna „sekstingu", czyli przesyłania wiadomości zawierających treści, zdjęcia, filmy erotyczne i pornograficzne. Powstał on w wyniku połączenia dwóch angielskich słów: sex i extortion (czyli wymuszenie). Polega na grożeniu ofierze opublikowaniem informacji o charakterze intymnym, zdjęć lub filmów. Może wiązać się z wyłudzeniem pieniędzy lub zmuszeniem ofiary do zrobienia czegoś wbrew jej woli. Przestępcy często atakują osoby za pośrednictwem aplikacji randkowych, mediów społecznościowych, kamer internetowych lub stron pornograficznych. Używają fałszywej tożsamości, aby zaprzyjaźnić się z potencjalną ofiarą, zdobyć zaufanie, wyłudzić intymne zdjęcia lub nagrania, a następnie grozić wysłaniem tych materiałów do rodziny i przyjaciół lub publikacją w sieci.

Przestępcy bardzo często pierwsi wysyłają „swoje” nagie zdjęcie lub film, by uśpić czujność ofiary. Zdjęcia mogą być pobrane z sieci lub należeć do innych osób. Potencjalna ofiara czuje się zazwyczaj zobowiązana do odwdzięczenia się swoimi intymnymi materiałami i przekazuje oszustowi materiały, które ten następnie wykorzystuje do szantażu.

Poczucie wstydu i zażenowania sprawia, że ofiary sextortionu często ulegają szantażowi, boją się upokorzenia, płacą okup i nigdy nie mają pewności, czy te materiały kiedyś nie zostaną opublikowane.

Co zrobić?

- Nie panikuj, poszukaj wsparcia;
- Nie płać, nie przesyłaj kolejnych materiałów;
- Zbierz dowody: zrzuty ekranu, wiadomości i obrazy, linki do miejsc, w których informacje są udostępniane online;
- Jeżeli zdjęcia lub filmy zostały udostępnione, skontaktuj się z administratorami stron, na których się znalazły z prośbą o ich usunięcie;
- Zablokuj wszelką komunikację z osobą szantażującą;
- Zgłoś sprawę policji, sextortion to przestępstwo.

Sextortion jest też wykorzystywany do wyłudzenia pieniędzy od osób, które w sieci stawiają na szybkie, niezobowiązujące relacje i rozrywki. Przestępcy wykorzystując wizerunki atrakcyjnych osób nawiązują kontakty z ofiarami. Następnie po nawiązaniu relacji przesyłają linki lub zachęcają do pobrania aplikacji, które prowadzą do pobrania złośliwego oprogramowania. To umożliwia przestępcom dostęp do danych, a także dostęp do obrazu z kamery.

Sextortion scam

To rozsyłanie przez cyberprzestępców wiadomości e-mail z groźbami rozpowszechniania poufnych lub kompromitujących zdjęć, filmów lub informacji o odbiorcy, jeśli nie zapłaci okupu. Przestępcy sugerują, że uzyskali dostęp do zdjęć lub filmów odbiorcy za pośrednictwem kamery internetowej lub włamania do jego urządzeń. Oszuści grożą, że wyślą materiał do kontaktów ofiary lub opublikują go publicznie. Tego typu e-maile, mimo, że mogą zawierać imię i nazwisko odbiorcy, często są wysyłane masowo na tysiące adresów e-mail jednocześnie. Oszuści pozyskują listy e-mailowe różnymi metodami, np. używając baz adresów z wycieków danych.

E-maile mają na celu wywołanie niepokoju i działania pod presją, aby ofiary zapłaciły okup bez sprawdzania roszczeń lub zgłoszenia incydentu. Płatność zazwyczaj odbywa się za pomocą trudnych do wyśledzenia źródeł, za pomocą kryptowalut lub portfeli BitCoin. Przy takich metodach płatności, odzyskanie utraconych środków jest praktycznie niemożliwe.

- Nie klikaj w podejrzane linki, nie ściągaj aplikacji polecanych przez obce osoby;
- Zwracaj uwagę na treść maili, oceń wiadomość, ile danych o Tobie ma oszust, czy są to dane, które mogą pochodzić z sieci, czy też te, które mogą pochodzić z Twojego urządzenia;
- Zmień hasła dostępu i sprawdź swój komputer pod kątem złośliwego oprogramowania lub narzędzi zdalnego dostępu;
- Monitoruj konta bankowe;
- Zabezpiecz dowody i zgłoś przestępstwo na policję.

Catfishing

Catfishing to podszywanie się pod kogoś w sieci, tworzenie fałszywego wizerunku i osobowości. Przetłumaczylibyśmy to dosłownie jako łowienie suma (z ang. _catfish_ to sum). Catfisher to oszust, który wykorzystuje cudze zdjęcia, posługuje się fałszywymi danymi, tworzy fałszywą historię życia, oszukuje potencjalną ofiarę by zrealizować swój cel. Jeśli oszust wykorzystuje zdjęcia i dane innej osoby, możemy już mieć do czynienia z kradzieżą tożsamości. Podszywanie się pod kogoś zazwyczaj ma szkodliwe konsekwencje dla oszukiwanej osoby. Może np. skończyć się wyłudzeniem pieniędzy.

Zjawisko catfishingu opiera się przede wszystkim na socjotechnice, na zdobyciu zaufania ofiary, a w późniejszym etapie zmanipulowania jej do przekazania np. wrażliwych danych, intymnych materiałów lub środków finansowych. Oszuści przygotowują się korzystając z informacji, które mogą znaleźć o nas w internecie, a kontakt może trwać nawet miesiącami by uśpić czujność i wzbudzić zaufanie.

Jak się chronić?

- Zachowaj zdrowy rozsądek i zwracaj uwagę na szczegóły.
- Sprawdź profile w mediach społecznościowych. Powinien Cię zaniepokoić brak znajomych na

portalach społecznościowych lub ich niewielka ilość, brak historii. Oczywiście zdarzają się oszuści z dużą siatką kontaktów, zdjęć i wpisów, które uwiarygodniają profil. Zbyt idealny profil również powinien Cię zaalarmować.

- Do weryfikacji skorzystaj z google grafika. Wrzuć zdjęcie danej osoby i sprawdź czy ta osoba wyświetla się w innych miejscach w sieci i czy przedstawia się tymi samymi danymi.

- Catfishera nie namówisz na rozmowę wideo lub spotkanie. Jeśli ktoś używa fałszywych zdjęć to nie pozwoli się zdemaskować. Nawet jeśli zgodzi się spotkać, to spotkanie odwoła i będzie zwodził ofiarę.

- Nawiązując znajomości online, postaraj się zebrać jak najwięcej informacji na temat swojego rozmówcy. Zwróć uwagę na „luki w historii". Jeśli ktoś tworzy fałszywą tożsamość, prędzej czy później trafisz na nieścisłości. Nie lekceważ sygnałów.

- Nigdy nie przekazuj pieniędzy osobie, której nie znasz. Każda prośba o pożyczkę czy inwestycję sugeruje, że ta osoba ma złe zamiary i chce Cię wykorzystać.

- Pamiętaj, że gdy prześlesz komuś swoje zdjęcia, filmy lub inne pliki, tracisz nad nimi kontrolę. Intymne materiały mogą być wykorzystane np. do szantażu.

Catfisherzy szukają swoich ofiar w sieciach społecznościowych, internetowych serwisach randkowych, aplikacjach do czatowania itp. Przestępcami mogą być osoby działające indywidualnie lub należące do organizacji przestępczej. Przykładowo w 2020 r. zidentyfikowano aplikacje randkowe, których celem było nagrywanie nagich mężczyzn by następnie ich szantażować. Ofiary natrafiały na aplikacje głównie poprzez reklamy na stronach z pornografią lub otrzymywały link poprzez popularne komunikatory. Amerykańska Federalna Komisja Handlu (FTC) opublikowała raport o statusie „oszustw romantycznych[6]". W samych Stanach Zjednoczonych zgłoszone straty ofiar w 2022 r. wyniosły 1,3 mld USD. Oszustem może też okazać się osoba, która Cię zna, chce Cię upokorzyć lub sprawić Ci przykrość. Według większości statystyk znacznie częściej ofiarami catfishingu padają mężczyźni.

Mimo, że finansowe wymuszenia seksualne są popełniane wirtualnie, mają poważne skutki offline. Po groźbach i agresji ofiary czują się samotne, zawstydzone i przestraszone. Wielu pokrzywdzonych nie potrafi poprosić o pomoc i wsparcie.

---

6) Romance scammers favorite lies exposed (ftc.gov)

Nigeryjski książę, amerykański żołnierz, aktor...

Oszustwa romantyczne są popełniane przez przestępców z różnych części świata, z których każdy wnosi do przestępstwa swoje unikalne metody i taktyki kulturowe. Regiony zaangażowane w oszustwa romantyczne na masową skalę to między innymi Afryka Zachodnia, Azja Południowo-Wschodnia i część Ameryki Łacińskiej. Przestępcy ci wykorzystują anonimowość internetu do budowania fałszywych tożsamości i manipulowania swoimi ofiarami emocjonalnie i finansowo.

Na stronie Departamentu Sprawiedliwości USA tylko z końca 2024 r. znajdziecie komunikaty związane z aresztowaniami obywateli Nigerii, którzy byli powiązani z oszustwami romantycznymi:

- Czterech obywateli Nigerii skazanych w związku z międzynarodowymi oszustwami romantycznymi[7].
- Nigeryjczyk skazany na więzienie federalne za oszukiwanie seniorów przez manipulację[8].
- Obywatel Nigerii aresztowany pod zarzutem wielomilionowego oszustwa romantycznego[9].

Oszuści z Afryki Zachodniej, szczególnie z Nigerii zasłynęli na tyle, że rodzaj oszustw romantycznych został powiązany z krajem. Przestępcy ci zazwyczaj podszywają się pod bogatych obcokrajowców, pracowników platform wiertniczych, byłych gwiazd porno, personelu wojskowego lub biznesmenów mieszkających za granicą. Sieci oszustw w Afryce Zachodniej są dobrze zorganizowane i często obejmują wiele osób współpracujących ze sobą.

Przestępcy z Azji Południowo-Wschodniej, najczęściej wykorzystują oszustwa romantyczne w powiązaniu z innymi formami oszustw internetowych, takimi jak oszustwa inwestycyjne lub kryptowalutowe. Przestępcy wybierają ofiary za pomocą aplikacji randkowych i nakłaniają je do inwestowania w fałszywe fundusze inwestycyjne.

---

7) Western District of Tennessee | Four Nigerian Citizens Sentenced in Connection with International Romance Scams | United States Department of Justice
8) Southern District of Illinois | Nigerian National Sentenced to Federal Prison for Defrauding Seniors through Manipulation, Romance Scams | United States Department of Justice
9) Western District of Washington | Nigerian national arrested on arrival in U.S. on indictment for multi-million-dollar romance fraud | United States Department of Justice

Polska nie zostaje w tyle. Oszustwa i *romance scam* dotykają coraz więcej osób. Nie mamy wiarygodnych statystyk pokazujących skalę tego procederu, bo wiele osób nie zgłasza się do organów ścigania. Kilka przykładów z naszego podwórka:

Na amerykańskiego żołnierza/żołnierkę

Oszuści wyszukują w sieci, m.in. na portalach randkowych samotne osoby i nawiązują z nimi kontakt. Posługując się zdjęciami z sieci, przedstawiają się jako amerykański żołnierz lub weteran, który aktualnie jest poza granicami swojego kraju. Oszust poprzez regularny kontakt i przedstawienie fałszywych historii z życia zdobywa zaufanie ofiary. Buduje wizerunek bohatera, osoby wyjątkowej, człowieka czynu, pełnego troski o los innych. Wmawia potencjalnej ofierze, że przez swoje poświęcenie dla kraju i ludzi, swojej misji, jest osobą samotną i szuka bratniej duszy. Budowanie więzi może trwać kilka tygodni a nawet miesięcy. Oszust w tym czasie sprawdza podatność ofiary i jej sytuację finansową. Po zdobyciu zaufania prosi o pomoc finansową na zakup biletu lotniczego do Polski lub bardzo drogie leczenie. Gdy ofiara oszustwa prześle pieniądze na konto przestępcy, kontakt się urywa.

Mieszkaniec Nysy poznał „żołnierkę", która chciała na stałe osiąść w Polsce i zainwestować tu 1,5 mln dolarów. „Pani kapitan" poprosiła mężczyznę o założenie konta na popularnym komunikatorze, żeby mogli sobie pisać wiadomości i zapoznać się. Amerykańska żołnierka pisała o swoim życiu, doświadczeniach i nakłaniała go do pogłębiania znajomości. Zaproponowała, że wyśle kurierem paczkę ze wszystkimi swoimi pieniędzmi. 1,5 miliona dolarów w gotówce będzie w skrzynce, którą przywiezie do Nysy kurier i którą mężczyzna ma złożyć do depozytu w jednym z banków. W końcu dobrze się już poznali i żołnierka mu ufa. Mężczyzna faktycznie dostał potwierdzenie nadania paczki kurierem, a po kilku dniach informację, że kuriera zatrzymała policja, urząd celny i paczka została zatrzymana do czasu opłacenia przesyłki przez kuriera. Mężczyzna przelał pieniądze na konto wskazane przez oszustkę i zrobił jeszcze kilka innych wpłat, mamiony obietnicą, że odzyska swoje pieniądze z procentem zaraz po tym jak przysyłka dotrze. W efekcie oszustwa mężczyzna stracił 200 tys. zł.

Na amerykańskiego aktora

Oszust podaje się za amerykańskiego aktora, który szuka prawdziwej miłości, z daleka od złudnego blichtru Hollywood. Szuka stabilizacji i obiecuje wspólną przyszłość.

W przypadku z Białegostoku, oszust zdobył zaufanie kobiety do tego stopnia, że uwierzyła w plany zamieszkania razem w Polsce. Mężczyzna twierdził, że wysłał jej pół miliona złotych na zakup wspólnego domu, jednak przesyłka utknęła u kuriera, który zażądał 9 tys. zł podatku od darowizny. Kobieta przelała kwotę na podane konto, ale nie otrzymała paczki z 500 tys. zł. „Kurier" twierdził, że pieniądze nie dotarły i konieczne jest jego powtórzenie. Dopiero po weryfikacji transakcji w banku, zdała sobie sprawę, że padła ofiarą oszustwa i zgłosiła sprawę policji.

Mieszkanka Piaseczna na portalu społecznościowym poznała mężczyznę, który podawał się za syna amerykańskiego aktora Clinta Estwooda, który z powodu zerwania kontraktu reklamowego znalazł się w trudnej sytuacji prawnej. Miesiącami korespondowali ze sobą. Oszust twierdził, że chce odwiedzić Polskę, rozważał kupno ziemi i nieruchomości w naszym kraju. Przeszkodą były jedynie jego zablokowane konta bankowe w USA oraz jak przekonywał, choroba ojca i utrata płynności finansowej. Uwiarygodnieniu służyły przekazywane przez niego „rodzinne historie", czy kopie paszportu. Namówił kobietę do licznych poleceń transakcji finansowych na podawane jej za pośrednictwem linków konta. Wpłaty, które robiła w dolarach amerykańskich oraz kryptowalucie w przyszłości, jak przekonywał, miały jej zagwarantować znaczne zyski, a obecnie miały pomóc w leczeniu ojca. W całym procesie pojawiały się jeszcze liczne informacje z rzekomych „banków" o konieczności dodatkowych przelewów, podania danych osobowych, numerów kart płatniczych itp. Łącznie na różnego rodzaju transakcje, także te w kryptowalucie, kobieta przelała ponad 600 tys. złotych. Gdy kobieta poprosiła „syna amerykańskiego aktora" o obiecaną umowę na prowadzone przez nich działania finansowe, kontakt się urwał.

Sugar daddy

Sugar dating to zjawisko jakim określa się relację opartą o korzyści finansowe osób z różnych klas społeczno-ekonomicznych, z różnymi oczekiwaniami co do zakresu relacji. Sugar daddys to zazwyczaj zamożni mężczyźni w średnim wieku, nierzadko mający rodziny/będący w stałym związku. Sugar babes to najczęściej studentki, które układy z dobrze sytuowanymi mężczyznami traktują jako szansę na podniesienie statusu i zasmakowanie życia „w luksusie". Warto zaznaczyć, że coraz popularniejsze są również „sugar mommies", czyli niezależne, dobrze sytuowane kobiety, które na tej samej zasadzie nawiązują relację z młodymi, atrakcyjnymi mężczyznami.

W sieci są portale wyspecjalizowane w sponsoringu, a nawet takie, które są ukierunkowane, np. na randki na poszczególne nisze czy na związki pozamałżeńskie. Osoby zainteresowane tym rodzajem znajomości korzystają też z ogłoszeń i mediów społecznościowych. Tego typu źródła nie należą do bezpiecznych. To tam jest najwięcej fałszywych profili i oszustów wykorzystujących to zjawisko.

Salt daddy i *salt mammy* – to oszuści, którzy podszywają się pod zamożne osoby i jedynie budują fałszywy wizerunek potencjalnego sponsora. W rzeczywistości, zamiast oferować wsparcie finansowe, sami liczą na zysk. Nie szukają też relacji, a jedynie wykorzystują swoje ofiary.

Oszuści *salt daddy* obiecują wsparcie finansowe, podarunki, sponsorowanie wydatków, a w rzeczywistości sami zbierają informację o swoich ofiarach, szczególnie na temat ich sytuacji finansowej. Po zmanipulowaniu i zdobyciu zaufania oszuści mogą np. symulować chwilowe kłopoty finansowe i prosić o pieniądze na pokrycie rzekomych nagłych wypadków, takich jak rachunki medyczne lub inwestycje biznesowe. Niektórzy oszuści wykorzystują relacje oparte o sponsoring do zdobycia intymnych zdjęć. Gdy oszust uzyska dostęp do intymnych treści, może szantażować swoją ofiarę żądając dodatkowych intymnych treści lub pieniędzy.

Jeśli świadomie decydujesz się na sugar dating, a relacja z sugar daddy wiąże się ze wsparciem finansowym, pamiętaj o bezpieczeństwie transakcji płatniczych.

- Korzystaj wyłącznie ze sprawdzonych platform płatniczych;
- Uważaj na wszelkie prośby o wysłanie pieniędzy lub podanie informacji o koncie bankowym;
- Wybieraj osoby, które mają weryfikowalną tożsamość i jasno określają intencje i charakter znajomości;
- Nie spiesz się i zachowaj rozsądek na każdym etapie relacji.

Fałszywe strony dla fetyszystów

Oszuści wykorzystują szczególne upodobania i tworzą fałszywe strony internetowe zaspokajające określone fetysze. Proszą o płatność z góry lub dane osobowe, obiecując dostęp do ekskluzywnych treści lub usług.

Oszuści często wyszukują osoby na platformach społecznościowych lub stronach internetowych poświęconych konkretnym fetyszom. Szukają odpowiednich hashtagów lub forów, na których gromadzą się entuzjaści danego fetyszu. Identyfikują potencjalne ofiary, inicjują rozmowy i stopniowo budują zaufanie, by następnie wyłudzić pieniądze za obietnicę specjalnych treści.

Oszuści tworzą też fałszywe profile internetowe na różnych platformach, podszywając się pod sprzedawców treści, np. dla fetyszystów stóp. Używają atrakcyjnych zdjęć lub skradzionych obrazów, aby zwiększyć swoją wiarygodność. Po nawiązaniu kontaktu z potencjalnymi nabywcami kuszą ich ofertami, takimi jak obniżone ceny na ekskluzywne treści. Ofiary są często proszone o płatności z góry za pośrednictwem przelewów bezpośrednich lub zakupu kart podarunkowych.

W oszustwach związanych z fetyszami oszuści wykorzystują specyficzne potrzeby konsumenta i sprzedają podróbki lub produkty niskiej jakości po zawyżonych cenach. Mogą tworzyć sklepy internetowe lub oferty, twierdząc, że oferują autentyczne lub wysokiej jakości przedmioty fetyszowe, takie jak ubrania, akcesoria lub zabawki. Jednak po dokonaniu płatności oszukani klienci otrzymują podróbki lub towary niespełniające norm.

Czytając o treściach dla fetyszystów, część z nas pomyśli „mnie to nie dotyczy”. Nie do końca, bo jedną z bardzo popularnych platform sprzedażowych, gdzie możemy trafić na fetyszystów jest np. Vinted czy OLX.

Klienci sklepów i platform dla fetyszystów powinni pamiętać o standardowych zasadach bezpieczeństwa dotyczących każdej transakcji internetowej.

- **Sprawdź sprzedawcę lub usługę**
  Sprawdź dane kontaktowe, regulamin sklepu, metody płatności. Poszukaj opinii klientów, referencji lub rekomendacji z zaufanych źródeł. Legalne platformy często mają mechanizmy weryfikacji wiarygodności sprzedawców i ochrony kupujących przed oszustwami.

- **Korzystaj z bezpiecznych metod płatności**
  Wybieraj bezpieczne metody płatności, unikaj przelewów bezpośrednich lub korzystania z metod płatności, które nie zapewniają żadnego odwołania w przypadku nieuczciwych działań.

- **Nie działaj pod presją i nie łap się na zaniżoną cenę**
  Uważaj na sprzedawców lub osoby, które naciskają na natychmiastową płatność. Nie

korzystaj z ofert, które wydają się zbyt piękne, aby mogły być prawdziwe, lub gdy sprzedawca prosi o dane osobowe niezwiązane z transakcją.

- **Przeczytaj to, co drobnym drukiem**
  Zanim pomyślisz o subskrypcji jakichkolwiek usług lub zawarciu umów, przeczytaj regulamin. Szukaj ukrytych klauzul, zasad automatycznego odnawiania lub jakichkolwiek informacji wskazujących na potencjalną nieuczciwą działalność.

Deepfake

Deepfake **to treści wizualne i dźwiękowe, które zostały zmanipulowane przy użyciu zaawansowanego oprogramowania w celu zmiany wyglądu osoby, przedmiotu lub środowiska.**

Do obróbki obrazu wykorzystywane są rozwiązania sztucznej inteligencji. Deepfake najczęściej polega na „wymianie twarzy", w której czyjaś twarz jest cyfrowo mapowana na twarz innej osoby.

Deepfake są tworzone przez algorytmy na podstawie prawdziwych zdjęć, filmów, czy próbek głosu. Mogą mieć formę:

- rekonstrukcji twarzy - oprogramowanie jest używane do zmian rysów czyjejś twarzy, bez zamiany twarzy na twarz innej osoby,

- generowanie twarzy - oprogramowanie pozwala na stworzenie nowej twarzy, która nie jest twarzą prawdziwej osoby,

- syntezy mowy - oprogramowanie służy do tworzenia modelu czyjegoś głosu.

Jednym z najgłośniejszych przykładów wykorzystania deepfaków była historia 53-letniej Francuzki, która w programie telewizyjnym opowiedziała jak padła ofiarą oszustwa z wykorzystaniem wizerunku popularnego aktora Brada Pitta. Przez ponad półtora roku była manipulowana przez oszustów, którym przekazała łączną kwotą 830 000 euro, będąc przekonaną, że pomogła panu Pittowi w jego rzekomym leczeniu raka nerki.

Deepfake porn

Deepfake są często wykorzystywane przy produkcji materiałów pornograficznych. Według badania z 2019 r. The State of Deepfakes, przeprowadzonego przez firmę Deeptrace[10] 96 % treści video typu deepfake dotyczyło pornografii.

---

10) Deepfake_report.pdf (regmedia.co.uk)
11) Deepfake porn is out of control (wired.com)

Często ofiarami deepfake porn padają znane osoby, aktorzy, muzycy, celebryci.

Przykładem deepfake porn jest wykorzystanie zdjęć Taylor Swift w styczniu 2024 r. Pornograficzny deepfake na bazie wizerunku celebrytki był rozpowszechniany na platformie X, a następnie udostępniony przez inne portale społecznościowe. Zanim platforma zareagowała i ostatecznie usunęła zdjęcia, to zebrały one 47 milionów wyświetleń. Wyraźne zdjęcia przedstawiały piosenkarkę w serii kompromitujących, brutalnych materiałów wykorzystanych bez jej wiedzy i zgody, docierając do masowej publiczności, która według szacunków liczyła setki milionów użytkowników.

Większość treści typu deepfake porn wykorzystuje wizerunki kobiet i służy do ich nękania. W ciągu pierwszych dziewięciu miesięcy 2023 r. obecność pornografii deepfake w internecie wzrosła o 54 % w porównaniu z 2022 r.[II] Tworzenie tego typu treści jest coraz łatwiejsze dzięki rozwojowi sztucznej inteligencji.

Ofiarą deepfake porn mogą być nie tylko „znane twarze", ale każdy użytkownik sieci. Celem fałszywych materiałów pornograficznych jest wyrządzenie krzywdy drugiej osobie, ośmieszenie, upokorzenie, a także szantaż. Do stworzenia takiego materiału wystarczą zdjęcia udostępnione przez potencjalną ofiarę w mediach społecznościowych i podłożenie ich do filmu czy zdjęcia o charakterze pornograficznym.

Co zrobić?

- Pamiętaj o ustawieniach prywatności na profilach społecznościowych,

- Unikaj korzystania z aplikacji, które przetwarzają zdjęcia lub filmy oraz rejestrują głos. Przykładem są aplikacje, które pokazują Twój wygląd za kilkadziesiąt lat, jako gwiazdy filmowej, lalki, postaci z książki itp.

Jeśli kiedykolwiek zdjęcie lub film z Twoim udziałem trafił do sieci, to musisz liczyć się z tym, że mogą kiedyś zostać wykorzystane.

JAK OSZUŚCI WYBIERAJĄ OFIARY?

Oszuści „romantyczni” i inni cyberprzestępcy wybierają osoby w sieci na podstawie podatności na ataki, dostępności celu, podatności na manipulację i potencjalne korzyści finansowe.

Aktywność w mediach społecznościowych, portalach randkowych i towarzyskich

Oszuści szukają osób wrażliwych emocjonalnie wśród użytkowników mediów społecznościowych, takich jak Facebook, Instagram lub serwisów randkowych. Celem często są osoby, które rozstały się z partnerem, straciły bliską osobę lub są po trudnych przejściach. Oszuści wybierają np. osoby publikujące posty o niedawnych rozwodach, problemach finansowych lub samotności. Takie, które szukają bliskości, zrozumienia i nie radzą sobie z samotnością. W złym stanie emocjonalnym są bardziej podatne na manipulację.

Kategorie wiekowe

Przestępcy kierują swoje działania na określone grupy demograficzne. Przykładowo osoby starsze są uważane za bardziej ufne, mniej zorientowane w tematyce zagrożeń internetowych, a jednocześnie zazwyczaj mają większe oszczędności. Częściej to osoby starsze są ofiarami „internetowych tulipanów”. Za to młodsze osoby częściej są ofiarami sextortionu i ataków ukierunkowanych na pewne grupy, np. korzystające z określonej aplikacji, platformy do gier czy portalu randkowego.

Publiczne bazy i wycieki danych

Organizacje przestępcze i oszuści działający na większą skalę wykorzystują wycieki danych lub kupują bazy zawierające dane osobowe, takie jak adresy e-mail, historia finansowa lub status związku, które następnie mogą wykorzystać do spersonalizowanych ataków.

Ślepy los

Romance scammers wysyłają masowe e-maile lub wiadomości z mediów społecznościowych do przypadkowych osób, mając nadzieję na reakcję i odpowiedź. W takim przypadku mamy do czynienia z masowym phishingiem.

Społeczności

Oszuści infiltrują grupy o określonych preferencjach seksualnych, wspólnych upodobaniach i zainteresowaniach, takie jak

fora internetowe czy nawet grupy wsparcia. Dołączając do tych grup, obserwują i wybierają potencjalne cele, z którymi wchodzą w interakcje.

To są tylko przykłady, które powtarzają się najczęściej. W oszustwach romantycznych istotne jest wybranie celu, który będzie podatny na zastosowane techniki socjotechniczne.

Jak oszuści uwodzą?

Cyberprzestępcy stali się mistrzami w uwodzeniu ludzi online, wykorzystując ludzkie uczucia i emocje. Nawiązują emocjonalną więź z ofiarą, a następnie manipulują nią w celu wyłudzenia pieniędzy lub wykorzystują w inny wyrafinowany sposób. Zaczyna się zazwyczaj od niewinnej wiadomości, interakcji w mediach społecznościowych czy pozornie niewinnego flirtu. Proces oszustwa romantycznego można podzielić na kilka głównych etapów.

- **Pierwszy kontakt:** Oszustwo zwykle zaczyna się od fałszywego atrakcyjnego profilu w serwisie randkowym lub w mediach społecznościowych. Oszust starannie buduje fikcyjny wizerunek osoby stabilnej finansowo, godnej zaufania, autorytetu, np. lekarz/lekarka, żołnierz, aktorka, obcokrajowiec itp. Rodzaj zawodu lub fikcyjny kraj pochodzenia są wymówką do usprawiedliwienia braku osobistego spotkania. Oszust jest przyjazny, wysyła pochlebne wiadomości i zaczepia potencjalną ofiarę w celu przyciągnięcia jej uwagi.

- **Budowanie zaufania:** Po nawiązaniu kontaktu oszust rozpoczyna proces uwodzenia. Poświęca dużo czasu na kontakt z ofiarą, pisze, wysyła wiadomości. Oszuści matrymonialni opowiadają romantyczne historie, dzielą się troskami, fałszywymi szczegółami z życia. Udają cierpliwych, pełnych ciepła i troski, darzą ofiary atencją i bardzo szybko deklarują miłość i oddanie. Celem jest stworzenie więzi emocjonalnej wystarczająco silnej, aby uśpić czujność ofiary.

- **Izolacja:** W kolejnych etapach oszuści izolują swoje ofiary od innych osób, przyjaciół czy rodziny. Zniechęcają je do mówienia innym o relacji, która ich łączy. W ten sposób wzmacniają kontrolę i obniżają ryzyko, że ktoś zwróci uwagę, że osoba może być ofiarą manipulacji.

- **Wsparcie finansowe i inwestycje na wspólne życie:** Po zbudowaniu zaufania i wystarczającej więzi oraz uzależnieniu

od siebie ofiary, oszuści wprowadzają wątek kłopotów finansowych, nagłego wypadku, problemów zdrowotnych itp. To wszystko wymaga nieprzewidzianych nakładów finansowych. Ofiara jest namawiana do przelewów bankowych a czasem tak zmanipulowana, że sama proponuje pokrycie ewentualnych kosztów. W końcu chodzi o wsparcie „bliskiej osoby", z którą planuje wspólną przyszłość. Inny rodzaj wyłudzenia wiąże się z nakłonieniem ofiary do określonych inwestycji, np. w kryptowaluty. Oszust zapewnia o dużych zyskach z inwestycji, które pomogą w rozpoczęciu wspólnego życia. Gdy ofiara wyśle pieniądze, oszustwo często się nie kończy. Oszuści często proszą o więcej i utrzymują zaangażowanie ofiary. Mogą wymyślać kolejne sytuacje awaryjne i obiecywać spotkanie i szybki zwrot środków z odsetkami.

- **Zniknięcie:** Gdy oszust wyciągnie z ofiary wszystkie oszczędności lub zorientuje się, że ofiara zaczyna coś podejrzewać i przestaje być uległa, po prostu znika. Kontakt się urywa, oszust przestaje odpowiadać na wiadomości, może skasować fałszywe profile, a ofiara zostaje oszukana, zrujnowana finansowo i emocjonalnie.

CO JEŻELI ZOSTANIEMY OSZUKANI?

- Poszukaj pomocy!
- Jeśli doszło do kradzieży danych, wyłudzenia bądź szantażu powiadom policję.

Kodeks karny określa przestępstwa przeciwko wolności oraz oszustwo i oszustwo komputerowe:

Art. 190 § 1 kodeksu karnego: Kto grozi innej osobie popełnieniem przestępstwa na jej szkodę lub na szkodę osoby dla niej najbliższej, jeżeli groźba wzbudza w osobie, do której została skierowana lub której dotyczy, uzasadnioną obawę, że będzie spełniona, podlega karze pozbawienia wolności do lat 3.

Art. 190a § 2 kodeksu karnego: Kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej, podlega karze pozbawienia wolności od 6 miesięcy do 8 lat.

Art. 191a § 1 kodeksu karnego: 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.

Art. 286 § 1 kodeksu karnego: 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.

Art. 287 § 1 kodeksu karnego: 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.

Pamiętaj! Ściganie tych przestępstw odbywa się na wniosek pokrzywdzonego.

Podszywanie się pod kogoś w sieci może zostać uznane za przestępstwo, ale nie zawsze uda się dotrzeć do sprawcy. Mimo, że „serce nie sługa”, zachowajmy rozsądek.

POPROŚ O POMOC!

116sos.pl – wsparcie dla osób w kryzysie emocjonalnym
Zadzwoń: 116123
Napisz: Formularz kontaktowy 116sos.pl

Centrum Wsparcia dla Osób Dorosłych w Kryzysie Psychicznym
Zadzwoń: 800 70 22 22
Napisz do specjalisty: Kontakt - Centrum Wsparcia

Fundacja Feminoteka – wsparcie dla kobiet doświadczających przemocy
Zadzwoń: 888 88 33 88

Instytut Przeciwdziałania Wykluczeniom – Telefon Zaufania dla Mężczyzn
Zadzwoń: 608 271 402
Napisz: pomoc@pomesku.org

UKE | Urząd Komunikacji Elektronicznej

Autorka:
MILENA GÓRECKA
Naczelnik Wydziału Kampanii Edukacyjno-Informacyjnych
Departament Polityki Konsumenckiej UKE

Opracowanie graficzne:
WOJCIECH GUNIA
Wydział Komunikacji
Biuro Prezesa UKE

2025