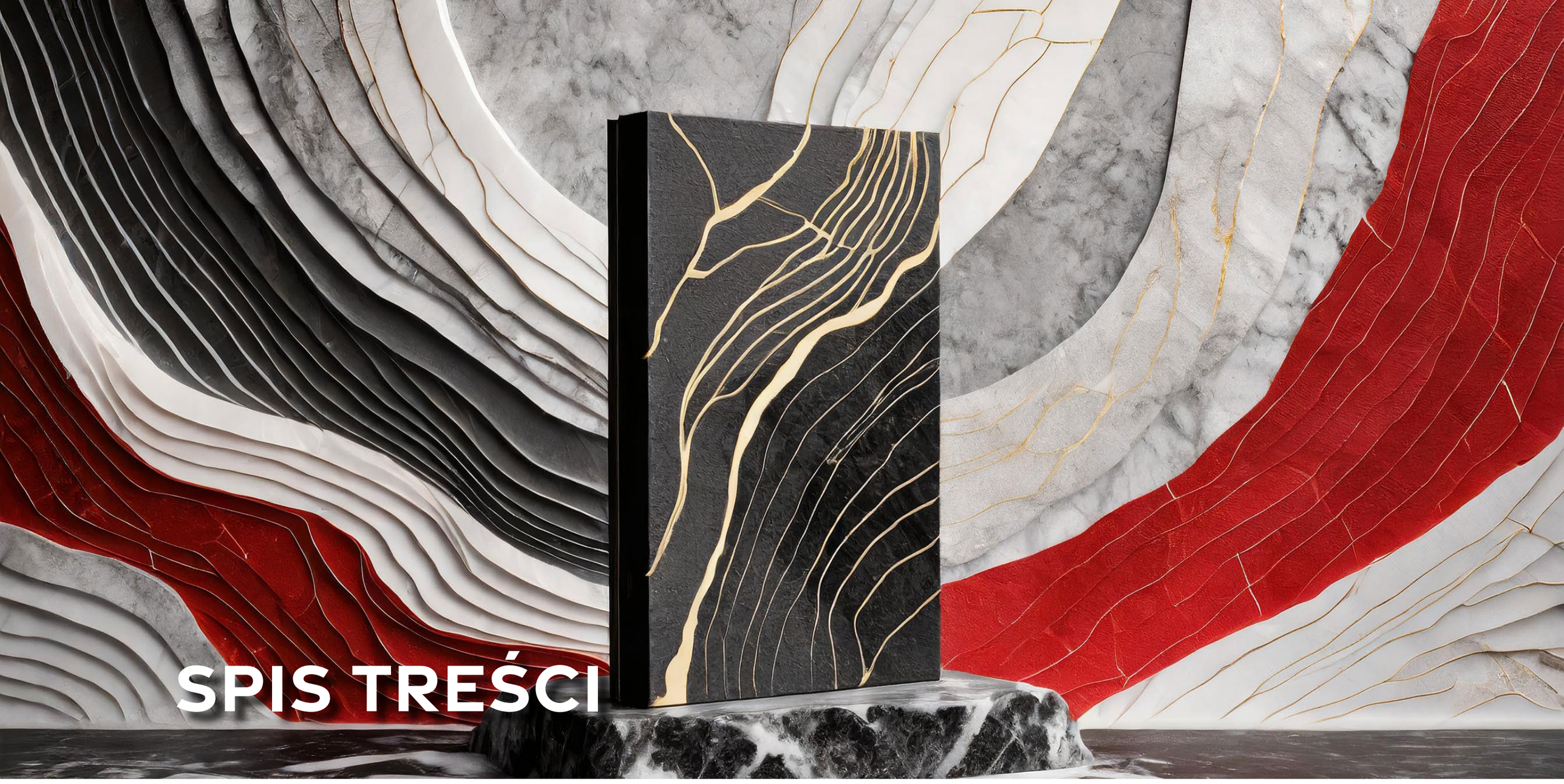
PORADNIK (NIE)ROMANTYCZNY

NA CO UWAŻAĆ W CYBERMIŁOŚCI?

UKE | Urząd Komunikacji Elektronicznej



SPIS TREŚCI

1. **Wstęp**
2. **Aplikacje i portale randkowe**
   - Wybór aplikacji lub portalu randkowego
   - Zakładanie konta
   - Koszty i rezygnacja z usług
   - Wykorzystanie sztucznej inteligencji
3. **Czy to ty? Na co uważać w sieci**
   - Sextortion
   - Sextortion scam
   - Catfishing
   - Deepfake
   - Deepfake porn
4. **A jeśli cię oszukano...**
5. **Poproś o pomoc**
6. **Bibliografia i przypisy**

WSTĘP

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. Na początek branży randek online niektórzy wskazują rok 1959, 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 nowe 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]

Zainteresowanie wirtualnymi randkami wzrosło w trakcie pandemii. Z raportu agencji Spicy Mobile[2] wynika, że wzrosły zasięgi popularnych aplikacji i częstotliwość korzystania z nich.

Na początku 2020 r. branża randek online wygenerowała przychody w wysokości 2,23 miliarda dolarów. Eksperci przewidywali, że do końca 2025 r. branża osiągnie 3,592 miliardy dolarów przychodów. W 2019 r. na całym świecie było około 219,7 milionów internetowych serwisów randkowych lub użytkowników aplikacji[3].

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?

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 iwyglądzie. Znajdziecie 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. Najpopularniejsze portale oferują też dopasowanie do kilku rodzajów orientacji seksualnych.

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.

WYBÓR APLIKACJI LUB PORTALU RANDKOWEGO

- **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.

ZAKŁADANIE KONTA

- **Stwórz silne hasło**

Obecnie o sile hasła decyduje głównie jego długość. Możesz też używać 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 nowe 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 KK, 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[4].

KOSZTY I REZYGNACJA Z USŁUG

- **Zakupy w aplikacji**

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

- **Opcje premium**

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.

- **Usunięcie konta**

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.

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 ma być też używana to tworzenia opisów profili, spersonalizowanych treści, biografii użytkowników itp.

Już teraz użytkownicy mogą ściągnąć „randkowych asystentów", których twórcy reklamują 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.

- **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.

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.

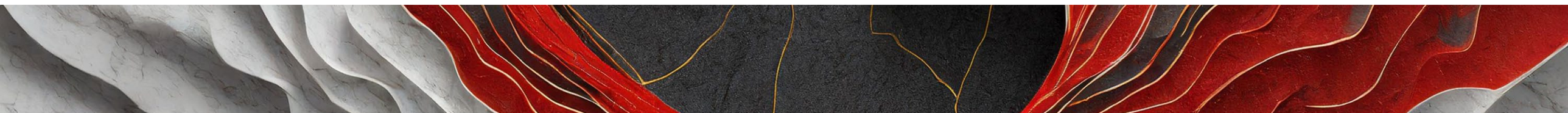
Użytkownicy serwisów randkowych jako powszechne zagrożenia wskazują:

- 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. Termin pojawił się już w latach 50-tych w USA. 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.

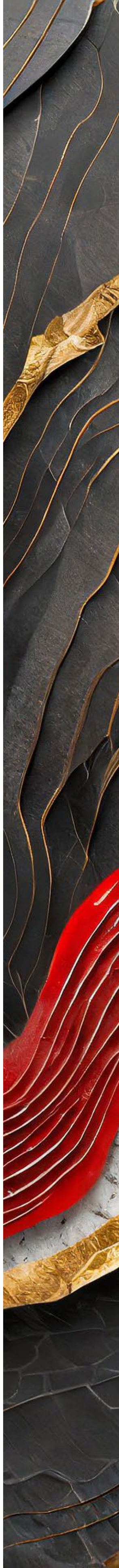
CATFISHING

„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. Przestępcą 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[5]". 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.

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.

DEEPFAKE PORN

Deepfake są często wykorzystywane przy produkcji materiałów pornograficznych. Według badania z 2019 r. The State of Deepfakes, przeprowadzonego przez firmę Deeptrace[6], 96 % treści video typu deepfake dotyczyło pornografii. 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 setki 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.[7] 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.

A JEŚLI CIĘ OSZUKANO...

- **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.

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

Bibliografia/przypisy:

1 J. A. Cutter, Getting it on-line [www.tampabay.com; dostęp: 16.01.2015]
2 Polacy w trakcie pandemii chętniej korzystają z aplikacji randkowych | SpicyMobile
3 141 Crucial Online Dating Statistics: 2024 Data Analysis & Market Share - Financesonline.com
4 Wyrok Sądu Apelacyjnego w Poznaniu - II Wydział Karny z dnia 24 maja 2012 r., II AKa 75/12
5 Romance scammers favorite lies exposed (ftc.gov)
6 Deepfake_report.pdf (regmedia.co.uk)
7 Deepfake porn is out of control (wired.com)

TEKST: MILENA GÓRECKA
NACZELNIK WYDZIAŁU KAMPANII EDUKACYJNO- INFORMACYJNYCH
DEPARTAMENT POLITYKI KONSUMENCKIEJ UKE

PROJEKT I OPRACOWANIE GRAFICZNE: WOJCIECH GUNIA
WYDZIAŁ KOMUNIKACJI UKE

UKE | Urząd Komunikacji Elektronicznej