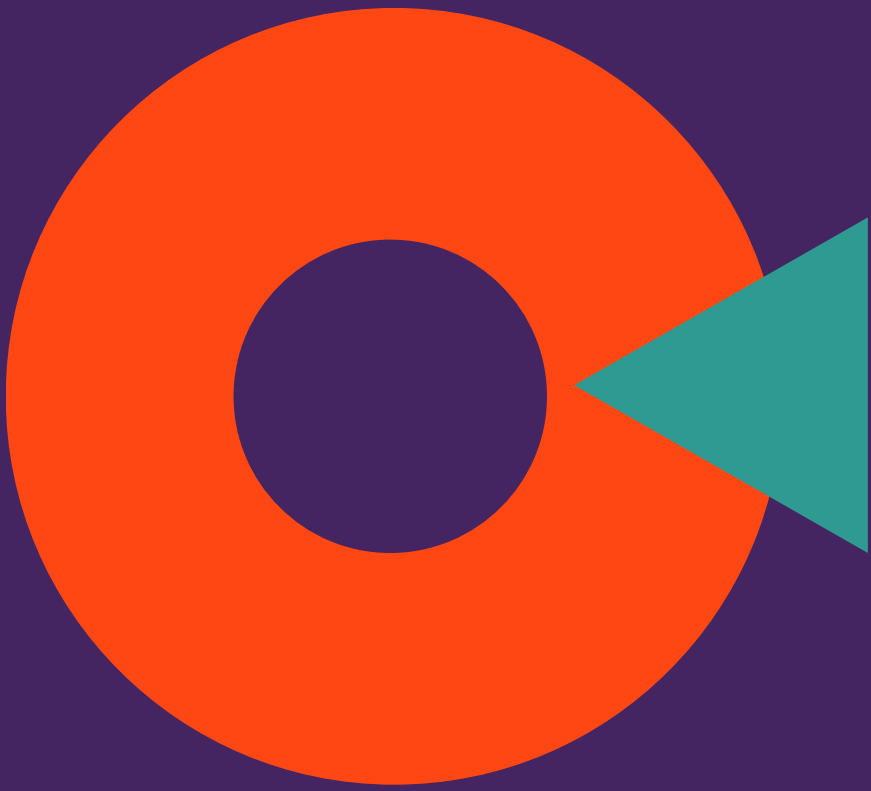
FUNDACJA CZAS KOBIET

CYBERPRZEMOC W ZWIĄZKACH

PORADNIK



DLA KOGO i PO CO POWSTAŁ TEN PORADNIK?

Publikacja opisuje formy cyberprzemocy występującej w bliskich związkach – to temat wciąż mało poruszany, mimo że Fundacja regularnie spotyka się z nim w swojej działalności.

Poradnik przedstawia różne oblicza zjawiska cyberprzemocy oraz zawiera konkretne wskazówki, jak jej skutecznie przeciwdziałać - od strony technicznej i prawnej.

Istnieje ogromna dysproporcja w dostępie do informacji między osobami stosującymi przemoc, a osobami jej doświadczającymi. Celem tej publikacji jest przechylenie szali na korzyść osób dotkniętych cyberprzemocą oraz tych, którzy chcą zdobyć wiedzę, jak pomóc innym.

Liczymy, że sprawcy cyberprzemocy uświadomią sobie, że ich działania są przestępstwem – anonimowość w sieci jest złudna, a za swoje czyny poniosą konsekwencje.

CZYM JEST CYBERPRZEMOC W ZWIĄZKACH?

Cyberprzemoc to forma przemocy, która do zastraszania, poniżania lub kontrolowania drugiej osoby wykorzystuje dostępną technologię. Może przyjmować różne formy, takie jak nękanie online, publikowanie obraźliwych treści, groźby, stalking cyfrowy, a nawet śledzenie i monitorowanie korespondencji partnera. Często dochodzi też do impersonacji, czyli podszywania się pod inną osobę.

Jednym z najbardziej niepokojących aspektów cyberprzemocy w związkach jest to, że sprawca może działać anonimowo i na odległość. Często stanowi to utrudnienie w identyfikacji, a tym samym pociągnięcie do odpowiedzialności. W efekcie osoby dotknięte cyberprzemocą czują się bezsilne. Wiele z nich nie zdaje sobie sprawy, że doświadcza takiej przemocy, ponieważ bywa ona maskowana jako „troska" lub „zazdrość".

To pokazuje**, jak ważna jest edukacja w temacie cyberprzemocy w bliskich związkach. Chcemy, aby osoby nią dotknięte nie bały się prosić o pomoc.**

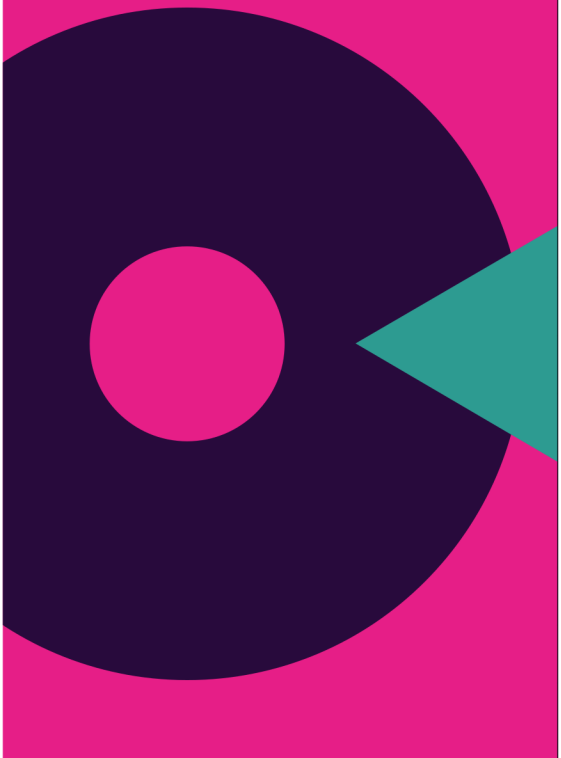
CYBERPRZEMOCOMETR

Aby lepiej zobrazować problem cyberprzemocy, stworzyliśmy autorski „cyberprzemocometr" – narzędzie prezentujące konkretne zachowania, oznaczone kolorami wraz z ich interpretacją.

Wyjaśnia on, które z nich są bezpieczne, a które powinny wzbudzić czujność.

FUNDACJA CZAS KOBIET

→ CYBERPRZEMOCOMETR



Moja relacja jest zdrowa, jeśli osoba z którą jestem:	Pomaga mi w konfiguracji urządzeń i kont
	Jesteśmy połączeni w mediach społecznościowych
	Bardziej się pasjonuje elektroniką, więc konfiguruje urządzenia dla nas obojga
Tylko jeśli wyrażam na to zgodę, to osoba z którą jestem,	Zna moje hasła i kody dostępu do urządzeń
	Mamy wspólne pliki w chmurze, np. zdjęcia
	Udostępniamy sobie lokalizację
	Mamy wspólną subskrypcję, wspólny dostęp do billingów
Mówię STOP, w moim związku jest przemoc, jeśli osoba, z którą jestem:	Nie mam dostępu / hasła do domowego wifi i innych wspólnych urządzeń, np. „smart home”
	Nakłania mnie do robienia i wysyłania intymnych zdjęć / odmawia ich usunięcia
	Ogranicza mnie w korzystaniu z urządzeń i dostępie do rzeczy, które chcę robić online
	Kontroluje mnie z kim i jak często się kontaktuję
	Otrzymuję niechciane wiadomości po rozstaniu
	Nakłania mnie do instalowania aplikacji i programów, bez wyjaśnienia po co i do czego służą
Chronię się, proszę o pomoc, jestem w poważnym niebezpieczeństwie, jeśli osoba z którą jestem:	Bez mojej wiedzy i zgody przegląda moje wiadomości i zdjęcia
	Loguje się do moich kont pocztowych
	Zabrania mi ustawienia własnego hasła lub blokady ekranu w telefonie
	Zmusza mnie do instalacji kontroli rodzicielskiej
	Znajduję ukryte przekierowania poczty
	Znajduję oprogramowanie szpiegujące na telefonie lub komputerze
	Znajduję podsłuchy i kamery w domu
	Mam trackery w ubraniach, torebce, plecaku
	Mam tracker w samochodzie
	Zmusza mnie do robienia i wysyłania intymnych zdjęć i nagrań.
	Szantażuje mnie lub publikuje intymne materiały („revenge porn”)
	Zna treść moich rozmów i korespondencji, mimo że nie jest świadkiem i nie ma do nich dostępu
	Wie, gdzie jestem, mimo że nie może zdobyć tej wiedzy w żaden racjonalny sposób
	Otrzymuję w dużej ilości niechciane wiadomości i telefony, również z groźbami

SAMOPOMOC i PREWENCJA

Cyberprzemoc jest realnym zagrożeniem, przed którym można i warto się chronić. Świadomość własnych praw, znajomość technik ochrony danych oraz narzędzi bezpieczeństwa w sieci to kluczowe kroki, które mogą pomóc zabezpieczyć się przed szkodliwymi działaniami w przestrzeni cyfrowej.

Wzmacnianie kompetencji cyfrowych oraz edukacja w zakresie cyberprzemocy pozwala nie tylko zwiększyć czujność, ale także reagować w sposób skuteczny i świadomy.

Poniżej przedstawiamy przykłady działań, które mogą zwiększyć Twoje bezpieczeństwo:

1. Jeśli możesz, wymień urządzenia na fabrycznie nowe. Jeżeli nie masz takiej możliwości, przywróć swój aparat do ustawień fabrycznych – spowoduje to usunięcie wszystkich danych, dlatego decydując się na ten krok nie zapomnij o zapisaniu wszystkich istotnych loginów i haseł.

UWAGA: Jeśli masz wspólny billing ze sprawcą przemocy, pamiętaj, że będzie miał on dostęp do listy Twoich połączeń, jednak nie do ich treści.

2. Zapewnij fizyczne bezpieczeństwo sobie i sprzętowi.

SAMOPOMOC i PREWENCJA

3. Ustaw skomplikowane hasło do komputera i telefonu.

UWAGA: Jeśli mieszkasz ze sprawcą przemocy unikaj biometrii (odcisku palca) - zbyt łatwo można wykorzystać moment snu lub celowo odurzyć osobę, żeby odblokować telefon.

4.Włącz dwuskładnikowe uwierzytelnianie wszędzie, gdzie jest to możliwe.

UWAGA: Oprócz hasła wymagane jest dodatkowe potwierdzenie, aby uzyskać dostęp do konta – na przykład aplikacja uwierzytelniająca lub kod SMS. Dzięki włączeniu wieloetapowego uwierzytelniania nikt nie dostanie się do Twoich danych, nawet jeśli pozna hasło. Przykładowe usługi, których to dotyczy: Google, Facebook, Apple, Onet, WP.

5. Sprawdź w ustawieniach swojej poczty czy nie masz włączonych przekierowań.

UWAGA: Przekierowanie poczty to operacja polegająca na automatycznym przekierowaniu przychodzących maili na inny adres skrzynki e-mail. W ten sposób sprawca, bez konieczności każdorazowego logowania się na Twoje konto mailowe, może otrzymywać Twoje wiadomości. Przykładowe usługi, których to dotyczy: Gmail, Onet, WP.

6.Wyłącz w ustawieniach poczty obsługę protokołów SMTP, POP3 oraz IMAP (o ile ich nie potrzebujesz). **Przykładowe usługi, których to dotyczy: Gmail, Onet, WP, Outlook.**

UWAGA: Protokoły te nie wspierają dwuskładnikowego uwierzytelniania przy logowaniu.

SAMOPOMOC i PREWENCJA

7.Sprawdź listę urządzeń zalogowanych na Twoim koncie i usuń (wyloguj) te nieznane.

8. Odinstaluj programy zdalnego dostępu (jeśli takie są zainstalowane na Twoim komputerze), np. TeamViewer, OpenVPN, AnyDesk.

9. Zmień hasło do sieci wifi i do routera oraz sprawdź czy nie są ustawione na nim przekierowania portów.

10. Odinstaluj z telefonu wszystkie aplikacje, których nie rozpoznajesz i nie używasz.

11. Regularnie aktualizuj oprogramowanie komputera (zwłaszcza przeglądarki internetowej) i urządzeń przenośnych.

UWAGA: Oprogramowanie szpiegujące często wykorzystuje luki w zabezpieczeniach oprogramowania komputera - aktualizacje pozwalają się przed tym uchronić.

12. Sprawdź w komunikatorach (np. WhatsApp, Signal, Viber) czy nie ma tam podłączonych nieznanych urządzeń.

UWAGA: Zazwyczaj możesz to zrobić w menu aplikacji pod opcją “powiązane urządzenia” lub podobną.

WARTO PAMIĘTAĆ!

- Nie usuwaj wiadomości, które są grożące lub obraźliwe - to może być dowód.
- Nie przesyłaj nikomu nagich zdjęć. Jeśli jednak zdarzyło się to wcześniej, pisemnie zażądaj ich usunięcia od osoby, która je posiada. Koniecznie zachowaj pismo lub zrób zrzut ekranu wiadomości.

PRZEPISY PRAWA, NA KTÓRE MOŻNA SIĘ POWOŁAĆ

Rozpowszechnianie intymnych zdjęć bez zgody:

Art. 191a kodeksu karnego

§ 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.

PRZEPISY PRAWA, NA KTÓRE MOŻNA SIĘ POWOŁAĆ

Nieuprawniony dostęp do danych:

Art. 267 kodeksu karnego

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1-4 na-stępuje na wniosek pokrzywdzonego.

PRZEPISY PRAWA, NA KTÓRE MOŻNA SIĘ POWOŁAĆ

Nieuprawniony dostęp do danych:

Art. 268 kodeksu karnego

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

PRZEPISY PRAWA, NA KTÓRE MOŻNA SIĘ POWOŁAĆ

Stalking:

Art. 190a kodeksu karnego

§ 1. Kto przez uporczywe nękanie innej osoby lub osoby dla niej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, przez co wyrządza jej szkodę majątkową lub osobistą.

§ 3. Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od lat 2 do 15.

§ 4. Ściganie przestępstwa określonego w §1 lub 2 następuje na wniosek pokrzywdzonego.

PRZEPISY PRAWA, NA KTÓRE MOŻNA SIĘ POWOŁAĆ

Pomawianie w internecie:

Art. 212 kodeksu karnego

§ 1. Kto pomawia inną osobę, grupę osób, instytucję, osobę prawną lub jednostkę organizacyjną niemającą osobowości prawnej o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności, podlega grzywnie albo karze ograniczenia wolności.

§ 2. Jeżeli sprawca dopuszcza się czynu określonego w §1 za pomocą środków masowego komunikowania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ 3. W razie skazania za przestępstwo określone w §1 lub 2 sąd może orzec nawiązkę na rzecz pokrzywdzonego, Polskiego Czerwonego Krzyża albo na inny cel społeczny wskazany przez pokrzywdzonego.

§ 4. Ściganie przestępstwa określonego w §1 lub 2 odbywa się z oskarżenia prywatnego.

GDZIE SZUKAĆ POMOCY?

POLICJA

Jeśli grozi Ci niebezpieczeństwo, otrzymujesz groźby lub kiedy ktoś łamie prawo możesz złożyć zawiadomienie o przestępstwie w najbliższym komisariacie policji oraz żądać ścigania i ukarania sprawcy. Służby mają obowiązek przyjąć od ciebie zawiadomienie. Przygotuj się do przesłuchania - możesz opisać wszystkie sytuacje na kartce, aby niczego nie pominąć.

Zabierz ze sobą wszystkie dowody – wydruki, telefon, laptop. Wcześniej wykonaj kopię danych potwierdzających działanie sprawcy i umieść ją w bezpiecznym miejscu, np. w chmurze na dysku, do którego hasło znasz tylko Ty lub przekaż zaufanej osobie na nośniku danych.

WAŻNE: Rozmawiaj z zaufanymi ludźmi – rodziną, znajomymi, osobami z pracy - o tym, co Cię spotyka i jak jesteś traktowana. Osoby będą mogły w późniejszym postępowaniu potwierdzić te informacje.

UWAGA: Jeżeli zdecydujesz się na nagranie przemocowych sytuacji musisz pamiętać, że filmy te mogą zostać uznane za niewiarygodne. Dzieje się tak, ponieważ wskazują jedynie wybrany fragment sytuacji, a nie całe zajście.

GDZIE SZUKAĆ POMOCY?

CO ROBIĆ, GDY POLICJA ODMAWIA PRZYJĘCIA ZGŁOSZENIA?

- Jasno poinformuj funkcjonariusza, że znasz swoje prawa i że ma obowiązek przyjęcia od Ciebie zgłoszenia.
- Zażądaj podania imienia, nazwiska, stopnia służbowego funkcjonariusza, a także nazwiska osoby przełożonej.
- Jeśli powyższe działania nie doprowadzą do zmiany podejścia i funkcjonariusz nadal będzie odmawiał przyjęcia zawiadomienia, przygotuj je na piśmie i wyślij do prokuratury listem poleconym lub złóż osobiście w biurze podawczym Prokuratury lub Sądu.
- Pamiętaj o podaniu konkretnej daty, kiedy udałaś się na komisariat policji oraz że odmówiono przyjęcia od Ciebie zawiadomienia

GDZIE SZUKAĆ POMOCY?

OPERATOR SERWISU

Operator serwisów (np. Google) ma zazwyczaj dwie podstawy działania, na które możesz się powołać: łamanie prawa i łamanie własnego regulaminu.

Zgłaszaj wszelkie akty przemocy - podszywanie się, wysyłanie niechcianych wiadomości, publiczne szkalowanie.

PAMIĘTAJ: Na mocy RODO/GDPR masz prawo do:

· uzyskania kopii wszystkich swoich danych (włącznie z danymi logowania na Twoje konto, które mogą być przydatne w ściganiu przemocy),

· “bycia zapomnianym” - na Twoje żądanie, operator ma obowiązek bezpowrotnie usunąć wszystkie dane związane z Twoim kontem (ważne, aby wcześniej zabezpieczyć dowody, jeśli sytuacja tego wymaga).

GDZIE SZUKAĆ POMOCY?

OPERATOR TELEFONii i iNTERNETU

Operator ma obowiązek udostępnić Tobie historię połączeń (billingi). Jeśli podejrzewasz, że Twoja karta SIM została sklonowana, możesz wystąpić o jej wymianę. Masz również prawo do złożenia wniosku o zmianę numeru telefonu.

UWAGA: Informacje pozwalające na identyfikację przypadków cyberprzemocy operator może udostępnić wyłącznie na żądanie organów ścigania, a nie osoby prywatnej.

GDZIE SZUKAĆ POMOCY?

FUNDACJA CZAS KOBIET

W Fundacji Czas Kobiet wspieramy kobiety, których prawa są łamane, które doświadczają różnych form przemocy, w tym cyberprzemocy. Udzielamy bezpłatnej i specjalistycznej pomocy m.in. interwencyjnej, psychologicznej, prawnej oraz technicznej.

W ramach konsultacji z zakresu cyberberbezpieczeństwa nasi specjaliści wytłumaczą, w jaki sposób może dochodzić do naruszania prywatności czy nękania, przejrzą konfigurację sprzętu i kont online, zabezpieczając dowody i słabe punkty oraz odcinając sprawcę. Działania te uniemożliwią kolejne naruszenia prywatności.

CO ROBIĆ W SYTUACJI, GDY...

... jesteś w przemocowym związku

Jeśli jesteś w przemocowym związku lub podejrzewasz, że ktoś Cię szpieguje, warto podjąć kroki, aby chronić swoją prywatność i zabezpieczyć swoje dane. Zacznij cyfrowo odcinać się od sprawcy, aby zminimalizować ryzyko inwigilacji.

Co robić?

Zadbaj o swoje bezpieczeństwo i zdrowie - cyfrowe odcięcie się może być zauważone przez agresora i spowodować nasilenie zachowań przemocowych. Zastosuj kroki z sekcji “samopomoc” tego poradnika.

Jeśli mieszkasz z osobą, której nie ufasz, unikaj biometrii do odblokowywania urządzeń (np. odcisk palca).

Zapisuj wszelkie przypuszczenia, podejrzane sytuacje i zbieraj dowody, np. zrzuty ekranu.

Skorzystaj z konsultacji technicznej w Fundacji Czas Kobiet.

CO ROBIĆ W SYTUACJI, GDY...

...otrzymujesz niechciane wiadomości i telefony

Jeśli ktoś uporczywie wysyła Tobie niechciane wiadomości lub dzwoni, nawet jeśli treści są neutralne, a tym bardziej gdy pojawiają się groźby, jest to działanie niezgodne z prawem. Takie nękanie stanowi przestępstwo stalkingu, a w przypadku gróźb – dodatkowe naruszenie prawa.

Co robić?

Nie usuwaj wiadomości ani nie czyść rejestru połączeń. Rób zdjęcia, zrzuty ekranu. Stwórz oś czasu wydarzeń. Jawnie przeciwstawiaj się danej osobie. Próbuj komunikować, że nie życzysz sobie utrzymywania kontaktu – organy ścigania mogą oczekiwać od ciebie „aktywnego przeciwstawiania się".

Zgłoś ten fakt na Policję - im więcej dowodów w postaci wiadomości z dokładnymi stemplami czasowymi posiadasz, tym większa szansa, że organy ścigania, we współpracy z operatorami, będą mogły ustalić nadawcę. Stalkerzy często zmieniają numery telefonów, używają anonimizerów i zakładają liczne konta, by utrudnić ich identyfikację, dlatego dokumentowanie każdego kontaktu jest kluczowe.

CO ROBIĆ W SYTUACJI, GDY...

...ktoś się pod Ciebie podszywa i publikuje treści w Twoim imieniu

Jeśli ktoś zakłada fałszywe profile w mediach społecznościowych, na portalach randkowych, komunikatorach i podszywa się pod Ciebie, publikując treści oraz wysyłając wiadomości w Twoim imieniu:

Co robić?

Zgłoś ten fakt operatorowi serwisu i zażądaj potwierdzenia zgłoszenia (nr incydentu / nr zgłoszenia).

Podczas zgłoszenia zaznacz, że oczekujesz od nich zabezpieczenia dowodów na potrzeby ewentualnego postępowania.

Zawiadom Policję.

Zabezpiecz dowody, wiadomości, zrzuty ekranu, adresy www (URL).

Notuj co i kiedy się wydarzyło (oś czasu) - jest to pomocne przy ewentualnym postępowaniu karnym.

CO ROBIĆ W SYTUACJI, GDY...

...ktoś szantażuje Cię publikacją intymnych materiałów

Jeśli ktoś szantażuje Cię publikacją intymnych materiałów pozyskanych od ciebie, nagranych bez twojej wiedzy lub jeśli publikuje je bez twojej zgody - dotyczy to także materiałów wygenerowanych cyfrowo (deepfake, deepporn):

Co robić?

Zabezpiecz dowody, wiadomości, zrzuty ekranu, adresy www (URL).

Notuj co i kiedy się wydarzyło (oś czasu) - jest to pomocne przy ewentualnym postępowaniu karnym.

Zawiadom Policję.

CO ROBIĆ W SYTUACJI, GDY...

...ktoś publicznie hejtuje Cię w internecie

Kiedy spotyka Cię duża ilość agresywnych wiadomości w mediach społecznościowych ze strony grupy osób (klasy, lokalnej społeczności):

Co robić?

Zgłoś ten fakt operatorowi serwisu i zażądaj potwierdzenia zgłoszenia (nr incydentu / nr zgłoszenia).

Podczas zgłoszenia zaznacz, że oczekujesz zabezpieczenia dowodów na potrzeby ewentualnego postępowania.

Zawiadom Policję.

Zabezpiecz dowody, wiadomości, zrzuty ekranu, adresy www (URL).

Notuj co i kiedy się wydarzyło (oś czasu) - jest to pomocne przy ewentualnym postępowaniu karnym.

FUNDACJA CZAS KOBIET

Każdy ma PRAWO do bezpiecznego korzystania z technologii – zarówno w życiu prywatnym, jak i zawodowym.

SKONTAKTUJ SiĘ Z NAMi!

Fundacja Czas Kobiet
Al. Marcinkowskiego 24
61-745 Poznań

www.facebook.com/FundacjaCzasKobiet
fundacja_czas_kobiet
biuro@czaskobiet.pl
czaskobiet.org
577 998 112

nr konta: 90 1020 4027 0000 1402 1851 3392

nr IBAN:

PL90102040270000140218513392

KRS 0001037553 / REGON 525374530 / NIP 7792555064