

Cyberbezpieczeństwo w praktyce



KLASTER
INNOWACJI
SPOŁECZNYCH

Autorzy

Petros Tovmasyan
Paulina Zalewska

Wydawca

Klaster Innowacji Społecznych

Adres redakcji
Ul. O. Jana Siemińskiego 22,
Gliwice

Kontakt

kontakt@klaster.org.pl

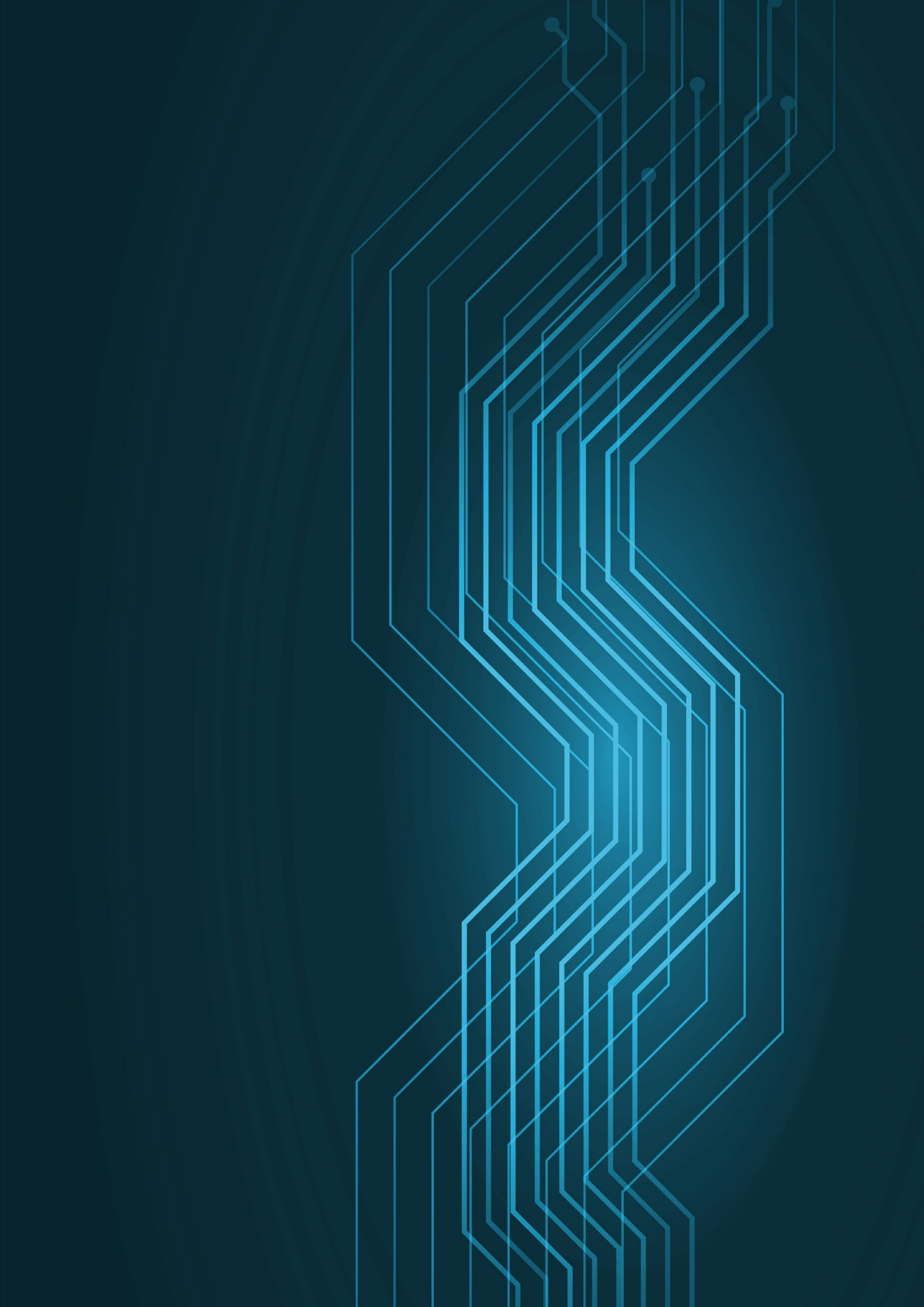
Finansowanie

Zadanie finansowane jest ze środków Ministra Edukacji i Nauki w ramach programu Wsparcia Edukacji.

Publikacja wyraża jedynie poglądy autorów i nie może być utożsamiana z oficjalnym stanowiskiem Ministerstwa Edukacji i Nauki



Ministerstwo
Edukacji i Nauki



Drodzy Czytelnicy,

Żyjemy w erze cyfrowej, gdzie internet stał się nieodłącznym elementem naszego codziennego życia. Niesie on ze sobą nieskończone możliwości do nauki, komunikacji i rozrywki. Jednak, jak każde potężne narzędzie, internet może również być źródłem zagrożeń. Dlatego stworzyliśmy ten podręcznik – „Bezpieczni w Cyfrowym Świecie” – aby wyposażać Was, młodych użytkowników internetu, w wiedzę i narzędzia niezbędne do bezpiecznego poruszania się po cyberprzestrzeni.

Co znajdziesz w tym podręczniku?

Ten podręcznik został zaprojektowany, aby pomóc Ci zrozumieć różne aspekty bezpieczeństwa online. Skupiamy się tutaj na najważniejszych zagrożeniach cyfrowych, takich jak cyberbullying, sexting, phishing, czy zagrożenia związane z prywatnością online. Każdy rozdział oferuje jasne wyjaśnienia, realne przykłady oraz praktyczne porady, jak radzić sobie z potencjalnymi zagrożeniami.

Dlaczego to ważne?

W dobie internetu, umiejętność ochrony siebie i swoich danych online jest równie ważna, co umiejętność czytania i pisanie. Cyberzagrożenia mogą mieć poważne konsekwencje dla Twojego dobrostanu emocjonalnego, reputacji oraz prywatności. Dlatego ważne jest, abyś był świadomy tych ryzyk i wiedział, jak sobie z nimi radzić.

Interaktywne i przystępne

Chcemy, aby ten podręcznik był dla Ciebie interaktywnym przewodnikiem. Znajdziesz tu nie tylko teksty do czytania, ale również ćwiczenia, pytania do samodzielnego rozważenia i miejsca do notowania własnych przemyśleń i doświadczeń. Chcemy, abyś nie tylko przyswajał wiedzę, ale także aktywnie ją przetwarzał i stosował w praktyce.



Twoja podróż do bezpieczeństwa online

Traktuj ten podręcznik jako mapę w podróży po cyberprzestrzeni. Będziemy przewodnikiem, który pomoże Ci nawigować przez różnorodne krajobrazy internetu, unikając pułapek i niebezpieczeństw.

Zachęcamy Cię do aktywnego korzystania z tego podręcznika, zadawania pytań i poszukiwania dalszych informacji. Twoje bezpieczeństwo online zaczyna się tutaj – od świadomości, edukacji i gotowości do działania.

Do dzieła!

Bezpieczeństwo online

Bezpieczeństwo w sieci to zbiór działań, które pomagają Ci unikać niebezpiecznych sytuacji i chronić Twoje osobiste informacje podczas korzystania z internetu. Internet to przestrzeń, w której istnieje wiele potencjalnych zagrożeń, takich jak cyberprzemoc, oszustwa, cyberprzestępczość czy grooming. Młodzi ludzie często nie zdają sobie sprawy z tych zagrożeń ani nie są wystarczająco świadomi, jak się przed nimi chronić. Edukacja na ten temat pozwala im rozpoznawać i unikać niebezpiecznych sytuacji online.

- Ochrona prywatności:
- Krytyczne myślenie
- Przeciwdziałanie cyberprzemocy
- Przygotowanie do pełnego działania w przestrzeni online.
- Wsparcie dla rodziców i opiekunów

Często może wydawać nam się, że jesteśmy zarzucani treściami edukacyjnymi dotyczącymi bezpieczeństwa w sieci. Myślę, że kiedy słyszysz o kolejnych zajęciach mówisz – znowu? Ale zastanówmy się czy tak naprawdę to co słyszymy zawsze powoduje, że zmieniamy swoje zachowanie, zaczynamy postępować inaczej.

Rozmawiasz na temat bezpieczeństwa w Internecie w domu? Mówisz o problemach, wątpliwościach? A czy rozmawiasz o bezpieczeństwie w Internecie w szkole? Jak często ten temat poruszany jest na lekcjach lub przerwach? Czy rozmawiasz ze znajomymi na tematy związane z bezpieczeństwem w Internecie?

Ważne jest, aby rozmawiać o zagrożeniach z rodziną, w szkole i ze znajomymi. Dzięki temu będziemy świadomie korzystać z Internetu. Będziemy w stanie pomóc sobie i innym. Dlaczego treści te są dla nas trudne do poruszania?

Nawet jeśli wiesz, jak uniknąć wszystkich tych rzeczy, są nastolatki, które tego nie robią. Jednym z nich może być twój przyjaciel, rodzeństwo lub kolega z klasy. Dobrzy cyfrowi obywatele chronią siebie i innych w Internecie.

Zadanie “Bezpieczny email”

Istnieją strony internetowe na których istnieje możliwość sprawdzenia czy twój mail jest bezpieczny i nie wyciekł z żadnej bazy danych. Sprawdź czy jesteś bezpieczny.

[Kliknij tutaj](#) by sprawdzić swój email.

Nieodpowiednie treści - czyli jakie?

Pamiętaj o tym, że Twój profil na social mediach to Twoja wizytówka. Sami je tworzymy i budujemy, ale też sami możemy zdecydować do kogo trafiają treści, kto może komentować nasze zdjęcia.

Niektóre interakcje online mogą sprawić, że pocujemy się niekomfortowo lub sprawimy, że inni się tak pocują, np.

- Wysyłanie złośliwych lub niegrzecznych wiadomości – zachowanie może ranić innych i prowadzić do konfliktów. Zawsze warto pamiętać o szacunku w komunikacji online.
- Udostępnianie lub ponowne udostępnianie nieodpowiednich zdjęć – narusza prywatność innych osób i może mieć poważne konsekwencje prawne. Zawsze upewnij się, że masz zgodę na udostępnienie czyjegoś zdjęcia.
- Rozmawianie na tematy wrażliwe – unikaj rozmów na tematy wrażliwe z osobami, których nie znasz osobiście. Przemyśl, czy dana rozmowa jest odpowiednią, zanim ją rozpoczniesz.

Ważne jest, aby nie tylko unikać nieodpowiednich treści online, ale także powstrzymać się od ich publikowania.



Wszyscy mieliśmy interakcje lub sytuacje w aplikacjach lub grach, które sprawiały, że czuliśmy się niekomfortowo. Może miałeś rozmowę, która sprawiła, że poczułeś się niekomfortowo, lub zostałeś oznaczony na zdjęciu, na którym nie podobał ci się twój wygląd, lub komentarz pozostawiony pod twoim postem był niemiły. Może to ty zostawiłeś ten niezbyt miły komentarz lub opublikowałeś zdjęcie bez pytania o zgodę znajomych na zdjęciu.

Prawdopodobnie wiesz już, że w Internecie znajduje się wiele nieodpowiednich, szkodliwych, a nawet niebezpiecznych treści – a niektóre z nich to rzeczy, których nie chciałbyś widzieć. Wiele nastolatków radzi sobie z tymi nieodpowiednimi treściami, unikając ich lub zgłaszając je.

Teraz, gdy jesteś starszy, ważne jest nie tylko unikanie nieodpowiednich treści w Internecie, ale także powstrzymanie się od ich publikowania. Powinieneś być ostrożny w publikowaniu zdjęć i komentarzy, które zawierają nieodpowiednie treści takie jak:

- Picie alkoholu, zażywanie narkotyków i inne działania przestępcze.
- Mowa nienawiści, np. obelgi wobec czyjejś seksualności, rasy lub religii.
- Sprośne lub obraźliwe gesty, wulgaryzmy.
- Odślaniające lub sugestywne obrazy.
- Groźby.





Warto pamiętać, że zachowywanie się odpowiedzialnie i szanowanie innych online to kluczowy element bezpieczeństwa w cyberprzestrzeni. Działa to nie tylko na Twoją korzyść, ale także tworzy pozytywną i bezpieczną atmosferę dla wszystkich użytkowników.

- Publikowanie tych rzeczy w Internecie, niezależnie od tego, czy jest to post prywatny, czy publiczny, może:
- Doprowadzić do tego, że znajomi i rówieśnicy będą plotkować na twój temat lub Cię unikać.
- Wpędzić cię w kłopoty z rodzicami, szkołą lub prawem.
- Ograniczyć obecne lub przyszłe możliwości, takie jak szkolne drużyny sportowe lub kluby.
- Otworzyć drzwi dla innych, którzy mogą cię nękać lub nawet szantażować.
- Wyrządzić ci krzywdę emocjonalną.

Zanim opublikujesz konkretną rzecz - sprawdź czy nie narusza to zasad lub prywatności drugiej osoby.

Publikując treści w Internecie zastanów się czy są one odpowiednie. Określenie, jakie informacje są nieodpowiednie, może być trudne, ale oto dobra zasada. Jeśli coś może wpędzić cię w kłopoty offline, prawdopodobnie wpędzi cię również w kłopoty online.



Aby ograniczyć nieporozumienia, przed opublikowaniem treści w Internecie należy rozważyć następujące kwestie.

- Czy dorośli w moim życiu – rodzice, krewni, nauczyciele, trenerzy i pracodawcy – uznaliby to za stosowne?
- Czy mogę mieć przez to kłopoty w szkole, drużynie sportowej, klubie lub w świetle prawa?
- Kogo mogą zranić lub zawstydzić te treści?
- Czy mój post zawiera informacje o mnie lub innej osobie, które nie powinny być udostępniane?
- Co te treści mówią o tym, jaką osobą jestem? Czy tak chcę być postrzegany?
- Jak może to wpłynąć na moje przyszłe możliwości, takie jak stypendia, przyjęcie na studia i zatrudnienie?
- Jak bym się czuł, gdyby ktoś zrobił to mnie lub komuś, kogo kocham?



TMI – Too much information

Too Much Information oznacza “za dużo informacji”. Używany zazwyczaj gdy rozmówca dzieli się z nami zbyt wieloma prywatnymi informacjami, których nie chcemy wiedzieć lub które powodują, że czujemy się skrępowani. Wyobraź sobie, że piszesz pamiętnik, w którym zapisujesz wszystkie swoje myśli, plany i sekrety, a potem zostawiasz go otwarty w miejscu, gdzie każdy może przeczytać. Udostępnianie w sieci zbyt wielu szczegółów o sobie, takich jak dokładny adres, plany na weekend czy dane rodzinne, może nie tylko zakłócać Twoją prywatność, ale także stwarzać ryzyko dla Twojego bezpieczeństwa.

Czego można dowiedzieć się wchodząc na Twój profil?

Czy udostępniasz informacje o sobie za pośrednictwem portali społecznościowych, takich jak Instagram, i/lub gier online?

Łatwo jest umieścić trochę za dużo informacji o sobie w wielu miejscach online. Możesz nawet nie zdawać sobie sprawy z tego, jak wiele udostępniasz. Starajmy się uważać na to, ile udostępniamy, ponieważ informacje online mogą rozprzestrzeniać się szybko i do wielu osób, dotrzeć do osób, do których nie chcesz, aby dotarła albo zostać przechwycone bez Twojej wiedzy. Nie wiesz, czy ktoś zrobił zrzut ekranu Twoich informacji, zdjęć lub filmów.

Internet nie zachowuje prywatności. Powinieneś nawet uważać na to, co publikujesz, korzystając z aplikacji obiecujących anonimowość, takich jak Discord, Whisper lub Snapchat. Nie można zagwarantować prywatności w Internecie. Nie należy udostępniać informacji o swoim życiu, które powinny być prywatne, ponieważ może to prowadzić do nękania, szantażu i/lub prześladowania.

Dane osobowe

Poświęć chwilę na zastanowienie się nad tym, ile informacji chcesz udostępniać online. Czy jesteś typem osoby, która publikuje aktualizacje statusu 12 razy dziennie czy 12 razy w roku? Bez względu na to, jakim typem udostępniającego jesteś, powinieneś zachować ostrożność przy udostępnianiu danych osobowych, takich jak: hasła, adresy, numery telefonów, plany wakacyjne, informacje o rodzinie.

Nie chodzi o to, że nigdy nie powinieneś udostępniać tych informacji. Istnieje wiele legalnych stron, które tego wymagają. Ale po umieszczeniu informacji w Internecie łatwo jest stracić kontrolę nad tym, kto je widzi i co z nimi robi. Ujawnienie danych osobowych w Internecie może sprawić, że staniesz się celem kradzieży tożsamości, oszustw, włamań komputerowych i innych kłopotów.

Wiem, że wszyscy pewnie o tym wiecie, ale czasami ważne jest sobie o tym przypomnieć. Ważne jest, aby zachować pewne rzeczy w tajemnicy, zarówno online, jak i offline. Nie podzieliłbyś się każdym szczegółem swojego życia ze wszystkimi uczniami w szkole, prawda?



Prywatność w internecie

To koncepcja ochrony Twoich osobistych danych w sieci. To trochę jak budowanie wirtualnego muru wokół Twojego cyfrowego życia. Chodzi o to, aby kontrolować, kto może zobaczyć Twoje zdjęcia, posty i inne informacje, które umieszczasz online. Dbłość o prywatność w internecie oznacza ustawianie prywatnych kont, korzystanie z silnych haseł i bycie ostrożnym w udostępnianiu informacji, które mogą zdradzić Twoje położenie, nawyki lub relacje.

Co zrobić, żeby być bezpiecznym w Internecie? Aby zachować prywatność i bezpieczeństwo, unikaj wykonywania następujących czynności:

- Ustawianie geolokalizacji jako domyślnego ustawienia w aplikacjach lub grach lub pokazywanie jej w postach w mediach społecznościowych.
 - Udostępnianie informacji rodzinnych, takich jak miejsce pracy rodziców.
 - Podawanie innym osobom swoich haseł
 - Ujawnianie szczegółów lub prywatnych informacji o swoim życiu
 - Przenoszenie rozmów na platformę prywatną (na przykład: przeniesienie czatu z gry na Snapchat lub inny prywatny chat)
 - Udostępnianie lub przekazywanie treści o charakterze jednoznacznie seksualnym
- 

Jak się chronić?

Chroń swoje dane osobowe online:

- Twórz silne hasła, takie jak długie frazy, które są łatwe do zapamiętania tylko dla Ciebie (zawierają cyfry i znaki specjalne) i często zmieniaj hasło.
- Korzystaj z ustawień prywatności, aby ograniczyć dostęp do swoich informacji. Może się to często zmieniać, więc nie zapomnij regularnie sprawdzać i upewnić się, że Twoje informacje są nadal ograniczone do osób, które chcesz, aby je widziały.
- Nawet jeśli możesz mieć znaczące relacje online i offline, ważne jest, aby zachować prywatność w Internecie, tak jak w życiu osobistym; nie dziel się wszystkim o swoim życiu z każdym znajomym, którego masz lub z całą szkołą. Ta sama zasada obowiązuje w Internecie.
- Ogranicz dostęp do swojej lokalizacji. Wiele usług i urzędów ma funkcje GPS, które pozwalają udostępniać informacje o tym, gdzie jesteś. Na przykład znaczniki geolokalizacyjne mogą być automatycznie osadzone na zdjęciach wykonywanych za pomocą smartfonów i tabletów. Pamiętaj, aby wyłączyć te funkcje i przekazywać informacje o swoim miejscu pobytu tylko najbliższym przyjaciołom i najbliższej rodzinie.
- Szukaj symbolu kłódki lub „https” w pasku adresu stron internetowych, które proszą o informacje finansowe.
- Nie udostępniaj danych osobowych innych osób – na przykład nigdy nie udostępniaj numeru telefonu komórkowego znajomego online.
- Nie udostępniaj haseł nawet bliskim znajomym, chłopakowi lub dziewczynie, ani członkom rodziny, którzy proszą o nie w Internecie.
- Nie pomagaj znajomym lub rodzinie, którzy kontaktują się z Tobą online za pośrednictwem mediów społecznościowych, poczty e-mail lub SMS-ów, prosząc Cię o informacje, przysługi lub kliknięcie linków. Może to być oszustwo. Zadzwoń i potwierdź, a następnie zapytaj rodziców/opiekunów.
- Zachowaj ostrożność, odpowiadając na wiadomości DM, czaty lub e-maile wysyłane do Ciebie przez osoby, których nie znasz.



Sprawdź czy wiesz?

Pytanie: Co powinieneś zrobić, gdy aplikacja prosi Cię o dostęp do Twojej lokalizacji?

Odpowiedzi:

- A) Zawsze zgadzać się.
- B) Odmówić dostępu.
- C) Zgadzać się tylko, jeśli jest to niezbędne dla funkcjonowania aplikacji.

Poprawna odpowiedź:

C) Zgadzać się tylko, jeśli jest to niezbędne dla funkcjonowania aplikacji.

Zadanie “Stwórz swoje silne hasło!”

Wymyśl silne hasło i sprawdź czy jest bezpieczne na tej [stronie](#)



Manipulacje w sieci

To działania, które mają na celu wpływanie na Twoje opinie, decyzje lub zachowania poprzez fałszywe informacje, oszustwa lub naciski w internecie. To jak ktoś próbuje przekonać Cię do zrobienia czegoś, co normalnie byś nie zrobił, używając nieuczciwych trików lub wprowadzając Cię w błąd.

Manipulacje emocjonalne w sieci polegają na tym, że osoba komunikuje się z osobą uważaną za dziecko za pośrednictwem Internetu z zamiarem popełnienia przestępstwa seksualnego lub uprowadzenia.

Jest to szeroka kategoria wykorzystywania online i obejmuje sextortion, w której dziecko jest przygotowywane do robienia zdjęć o charakterze jednoznacznie seksualnym i/lub ostatecznie spotyka się z kimś twarzą w twarz w celach seksualnych lub angażuje się w rozmowę seksualną online, lub, w niektórych przypadkach, sprzedaje i/lub handluje zdjęciami seksualnymi dziecka.

Ten rodzaj wykorzystywania ma miejsce na wszystkich platformach.

Sprawdź czy wiesz?

Pytanie: Jak możesz rozpoznać fałszywe wiadomości (fake news)?

Odpowiedzi:

- A) Sprawdzając informacje w wiarygodnych źródłach.
- B) Wierząc we wszystko, co przeczytasz.
- C) Pytając przyjaciół, co oni myślą.

Poprawna odpowiedź: A) Sprawdzając informacje w wiarygodnych źródłach.



Grooming

Grooming to manipulacja, która odnosi się do zachowań, w których osoba dorosła używa internetu, aby nawiązać relację z młodą osobą i zyskać jej zaufanie w celu wykorzystania seksualnego lub innej formy nadużycia. Grooming obejmuje serię działań mających na celu zyskanie zaufania ofiary oraz zmanipulowanie jej emocjonalnie i psychicznie, by osiągnąć kontrolę nad nią. Dorosły stopniowo buduje relację, by później skłonić młodą osobę do zrobienia czegoś, czego normalnie by nie zrobiła.

Typowy proces groomingu może obejmować:

- Budowanie zaufania: Osoba dorosła może zaczynać od nawiązania przyjaznych relacji z dzieckiem lub młodzieżą, często udając się za mentora lub przyjaciela.
- Tworzenie zależności emocjonalnych: Groomer może wykorzystywać psychologiczne techniki, takie jak komplementy, pocieszanie i wspólne doświadczenia, by zyskać zaufanie ofiary i ugruntować związek emocjonalny.
- Stopniowe wprowadzanie treści seksualnych: Groomer stopniowo wprowadza treści seksualne do rozmów lub działań, zaczynając od niewinnego flirtu lub rozmowy na ten temat.
- Manipulacja i kontrola: Groomer może wykorzystywać dowody lub informacje zdobyte podczas procesu groomingu do wywierania presji na ofiarę i manipulowania nią, by wykonywała żądane czynności seksualne lub poddawała się wykorzystaniu.
- Zagrożenia i szantaż: W miarę jak grooming postępuje, groomer może grozić lub szantażować ofiarę, by utrzymać ją w kontroli i zapobiec ujawnieniu działań.

Jedną z taktyk stosowanych w uwodzeniu jest izolowanie i uniemożliwienie zabrania głosu przez osobę uwodzoną.

Ktoś, kto próbuje cię uwodzić, może...

- schlebiać,
- rozmawiać na tematy dla dorosłych,
- wysyłać prezenty,
- prosić o zachowanie rozmowy w tajemnicy,
- nastawiać Cię przeciwko rodzinie,
- udostępniać lub prosić o zdjęcia,
- szantażować.

Odrzucanie propozycji

Czasami możesz czuć presję, aby spełnić prośbę. Czasami sprawy dzieją się po prostu zbyt szybko i podejmujesz pochopne decyzje. Czasami nie czujemy się komfortowo, mówiąc „nie” lub nie wiemy, jak odpowiedzieć. Nieczęsto zdarza się, że nastolatki wysyłają obnażające zdjęcia lub filmy. Zanim podejmiesz decyzję, cofnij się, poświęć trochę czasu na przemyślenie tej decyzji i porozmawiaj z przyjacielem lub zaufaną osobą dorosłą. Nagabywanie o charakterze seksualnym to każda niechciana prośba lub prośba złożona przez osobę dorosłą (podaj kilka przykładów/zobacz uwagi prowadzącego). Masz prawo powiedzieć NIE. Przećwicz sposoby odrzucania niechcianych próśb.

Co zrobić, jeśli otrzymasz niechciane próśby o charakterze seksualnym?

- Nie angażuj się dalej w rozmowę.
- Zablokuj rozmówcę.
- Nie umawiaj się offline.
- Powiedz o tym zaufanej osobie dorosłej.
- Zgłoś się to do administratora strony, zgłoś to na stronie dyzurnet.pl oraz incydent.cert.pl
- Nie usuwaj swojego konta.

Ważne jest, aby powiedzieć dorosłej osobie, której ufasz, nawet jeśli poradziłeś sobie już z tą sytuacją. Niektórzy nastolatki nie chcą rozmawiać z dorosłymi, ponieważ:

- martwią się, że dorosły zareaguje przesadnie,
- boją się, że zostaną obwinieni,
- sądzą, że dorosły nie może im pomóc,
- są zawstydzeni,
- będą mieli kłopoty,
- nie czują się bezpiecznie dzieląc się tymi informacjami z dorosłymi w ich życiu,
- czują wstyd, zakłopotanie i poczucie winy,
- myślą, że sami poradzą sobie z tą sytuacją.

Jednak powiedzenie o tym komuś, na przykład nauczycielowi, pedagogowi szkolnemu, rodzicowi lub innemu krewnemu, może być dobrym posunięciem. Pomogą Ci w podjęciu kolejnych kroków, np. w podjęciu decyzji, jakie dowody zachować. Mogą również pomóc Ci uzyskać pewien punkt widzenia na sytuację. Nikt nie powinien sprawiać, że czujesz się niekomfortowo w Internecie, zwłaszcza dorośli. Poproś osobę dorosłą, z którą czujesz się komfortowo, aby Ci pomogła Ci i zgłosiła ją w odpowiednie miejsce.

Zgłoś naruszenie

Możesz zgłosić każdego kto:

- wysyła Ci zdjęcia dla dorosłych,
- prosi Cię o przestanie swoich zdjęć,
- rozmawia z Tobą na tematy wrażliwe/intymne,
- chce się z Tobą spotkać offline,
- szantażuje Cię, abyś wysłał pieniądze lub więcej treści,
- udostępnia Twoje zdjęcia.

Może wydawać się, że łatwiej jest po prostu ignorować tego typu prośby, zamiast je zgłaszać, ale zgłaszając je, pomagasz uczynić Internet znacznie bezpieczniejszym dla swoich przyjaciół, rodzeństwa i rówieśników. Osoba kontaktująca się z Tobą może kontaktować się z dziećmi młodszymi lub bardziej bezbronnymi od Ciebie i robić to samo.

Nie usuwaj swojego konta. Robiąc to, usuwasz dowody, które mogą pomóc w schwytaniu i powstrzymaniu tego drapieżnika.

Sprawdź czy wiesz?

Pytanie: Co robić, gdy dorosły, którego poznałeś online, prosi Cię o spotkanie w realnym świecie?

Odpowiedzi:

- A) Umówić się bez mówienia nikomu.
- B) Odmówić i powiadomić dorosłego.
- C) Poprosić o więcej zdjęć tej osoby.

Poprawna odpowiedź:

- B) Odmówić i powiadomić dorosłego.





Sexting

Sexting to wysyłanie, otrzymywanie lub udostępnianie wiadomości, zdjęć lub filmów o charakterze seksualnym, zwłaszcza przez telefon komórkowy. Choć może wydawać się to prywatną czynnością między osobami, które sobie ufają, istnieje ryzyko, że takie materiały mogą zostać udostępnione innym osobom bez Twojej zgody.

Dlaczego nastolatkwie się na to decydują?

- Schlebia im to – seksting oznacza, że ktoś uważa, że jesteś atrakcyjny.
- Czują presję, szczególnie jeśli pochodzi od osoby w której są zauroczeni.
- Chcą być zabawni.

Ilu nastolatków uprawia seksting?

- 19,3% wysłało wiadomość tego typu,
- 14,5% przekazało dalej,
- 34,8% otrzymało taką wiadomość.

Dane pochodzą z [badania](#) przeprowadzonego przez firmę Thorn.

14,5 procent nastolatków, którzy rozsyłają nagie treści postępuje niewłaściwie. Przyczyniają się do znęcania i dręczenia ofiar sekstingu.

Dane pochodzą z badania metaanalizy.

Jakie są konsekwencje udostępnienia zdjęcia?

- Może się zgubić lub znaleźć w niewłaściwym miejscu.
- Można go udostępniać bez pozwolenia.
- Może stać się źródłem zawstydzenia, wstydu i/lub poczucia winy.
- Może to skutkować plotkami, plotkami i/lub cyberprzemocą.
- Może to skutkować konsekwencjami prawnymi.
- Może to skutkować szantażem w celu uzyskania większej ilości treści bądź uzyskania pieniędzy. Jest to przestępstwo i nazywa się to sekstorcją.

Sprawdź czy wiesz?

Pytanie: Czy wysyłanie intymnych zdjęć komuś, kogo dobrze znasz, jest bezpieczne?

Odpowiedzi:

- A) Tak, jeśli tej osobie ufasz.
- B) Nie, ponieważ raz wysłane, zdjęcia mogą być łatwo udostępnione innym.
- C) Tylko, jeśli osoba ma powyżej 18 lat.

Poprawna odpowiedź: B) Nie, ponieważ raz wysłane, zdjęcia mogą być łatwo udostępnione innym.



Zobacz film i zastanów się kto dokonał pierwszego wyboru w filmie? Większość osób uważa, że to dziewczyna zdecydowała o wysłaniu lub niewysłaniu zdjęcia, ale to prośba chłopca o zdjęcie była świadomą decyzją. Niezależnie od tego czy zdawał sobie sprawę z konsekwencji swojej prośby. Jakie inne decyzje zostały podjęte w filmie?

Inni postanowili podzielić się zdjęciem, podsycając plotki; niektórzy uczniowie zdecydowali się nie udostępniać.

W 2021 roku 20% nastolatków stwierdziło, że widziało nagie zdjęcie lub film innej osoby bez jej wiedzy.

Jak pomóc ofierze sextingu?

Jeśli to Ty chcesz poprosić o zdjęcie, pamiętaj, że podejmujesz decyzję, która może przerodzić się w ryzykowną sytuację. Zadaj sobie pytania, które pomogą ocenić, czy warto ryzykować:

- Jak może to wpłynąć na Ciebie i Twojego partnera, jeśli zdjęcie wycieknie?
- Dlaczego chcesz mieć to zdjęcie?
- W jaki inny bezpieczny i zdrowy sposób możesz wyrazić to, że zależy Ci na tej osobie i że ją lubisz?
- Jeśli ktoś poprosi Cię o udostępnienie zdjęcia, powinniście wspólnie przeprowadzić otwartą i szczerą rozmowę.
- Gdy nagie zdjęcie lub film wymknie się spod Twojej kontroli, nie masz na to wpływu.



Gdzie zgłosić naruszenia prywatności?

Obraźliwe komentarze czy wulgaryzmy powinniśmy zgłaszać do administratorów stron lub moderatorów forów dyskusyjnych. Najczęściej służą do tego specjalne przyciski lub formularze powiadomień. Jeśli ich nie ma, wykorzystujemy dane zamieszczone w zakładce „Kontakt” danej witryny.

Poważne przypadki cyberprzemocy, będące naruszeniem prawa (np. groźby karalne, propozycje seksualne, publikowanie nielegalnych treści itp.), powinny zostać zgłoszone na policję lub do prokuratury. W imieniu osoby niepełnoletniej zgłoszenia dokonują rodzice lub opiekunowie prawni.

Do Twojej dyspozycji jest też działający 24 godziny na dobę zespół Dyżurnet.pl. Jego misją jest podejmowanie działań na rzecz tworzenia bezpiecznego Internetu. Dyżurnet.pl to zespół ekspertów NASK, działający jako punkt kontaktowy do zgłaszania nielegalnych treści w Internecie.

Wysyłając zgłoszenie do Dyżurnet.pl należy przede wszystkim podać adres strony, na której znajdują się potencjalnie nielegalne treści. Korzystając z formularza trzeba zaznaczyć, czego sprawa dotyczy. Zgłoszenia są anonimowe. Podawanie adresu e-mail, czy innych danych jest nieobowiązkowe. Jeśli użytkownik poda adres e-mail, po wysłaniu zgłoszenia, otrzyma informację o podjętych krokach lub prośbę o podanie dokładniejszych informacji. Przesyłając zgłoszenie warto napisać wszystkie informacje, które mogą być nam pomocne.

Jeżeli widzisz w sieci, coś co Cię niepokoi – nie wahaj się. Reaguj, zgłaszaj! Gdzie?

Incydenty naruszające bezpieczeństwo w sieci: incydent.cert.pl

Nielegalne treści w Internecie: <https://dyzurnet.pl>

Zanim prześlesz dalej - pomyśl

Jedno na pięć dzieci twierdzi, że widziało udostępniane nagie zdjęcia bez zgody tej osoby, a wśród dzieci w wieku od 13 lat liczba ta rośnie do prawie jednego na cztery. (*badania Thorn)

Zanim udostępnisz dalej:

- Pomyśl, jak czułbyś się, gdyby to było zdjęcie Twojego rodzeństwa lub przyjaciela.
- Pomyśl o szkodach, jakie możesz wyrządzić udostępniając dalej, bo jeśli to udostępnisz, inni też to udostępnią.
- Pomyśl o odpowiedzialności, którą ponosisz, możesz powstrzymać znęcanie się nad osobą ze zdjęcia.
- Porozmawiaj ze znajomymi o tym, aby nie udostępniać dalej i okazać wsparcie. Daj znać, jeśli inni udostępniają takie zdjęcia lub uprawiają seksting.

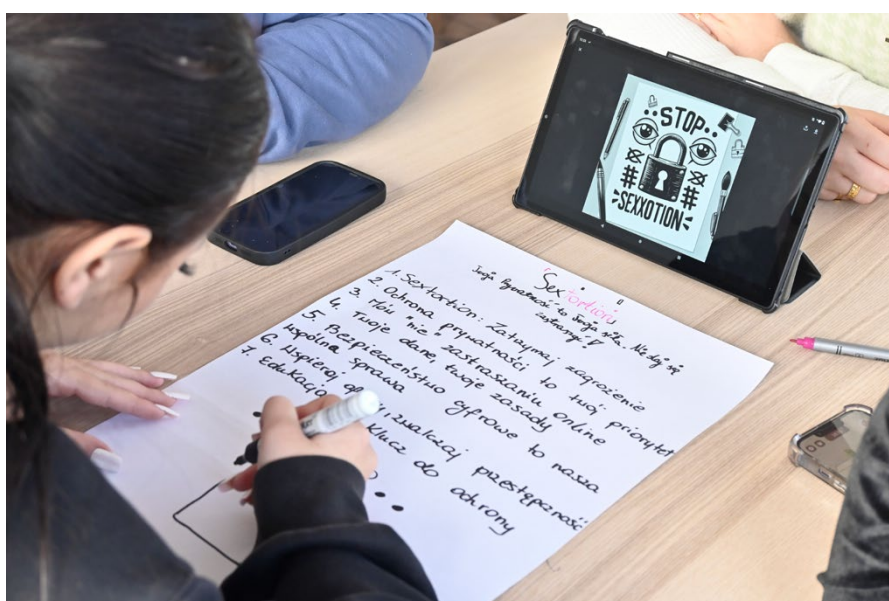
Sextortion

Sextortion to forma wykorzystywania seksualnego dzieci i młodzieży, polegająca na groźbach lub szantażowaniu, najczęściej z możliwością udostępnienia ich nagiego lub seksualnego wizerunku, przez osobę żądającą od dziecka dodatkowych treści seksualnych, aktywności seksualnej lub pieniędzy.

Odnotowano dramatyczny wzrost liczby przypadków molestowania seksualnego, zwłaszcza przypadków wyłudzeń finansowych, w przypadku których sprawca żąda od dziecka pieniędzy. W ostatnich przypadkach najczęstszym celem ataków byli nastoletni chłopcy.

Sekstorcja może przybierać różne formy. Zwykle sprawca kontaktuje się z dzieckiem i nawiązuje z nim relację, a następnie prosi o nagie zdjęcia lub filmy. Potem zaczyna się sekstorcja. Proces uwodzenia zmienia się w czasie; czasami zajmuje to dużo czasu, a w niektórych przypadkach może trwać nawet kilka minut lub godzin.

Przestępstwo to może mieć miejsce, gdy dziecko udostępniło zdjęcie osobie, którą wydawało się, że zna lub której ufa, ale w wielu przypadkach jest osoba poznana w Internecie, która uzyskała od dziecka zdjęcia o charakterze seksualnym w wyniku podstępu, przymusu lub w inny sposób. W wielu przypadkach szantażyści mogli ukraść lub zrobić zdjęcia innej osoby i komunikują się za pośrednictwem fałszywego konta. Szantażujący mógł również wysłać zdjęcia.



Taktyki sextortion

Istnieją pewne taktyki stosowane przez przestępców, aby wywierać presję na dzieciach i nastolatkach.

Czy wiesz jakie taktyki sextortion mogą być stosowane przez przestępców?

- Wzajemność („Pokażę ci, jeśli ty pokażesz mi pierwszy”).
- Udawanie, że pracuje się dla agencji modelek, w celu uzyskania zdjęć seksualnych nieletnich.
- Rozwijanie więzi z nieletnim poprzez nawiązanie przyjaźni lub związku romantycznego.
- Używanie wielu fałszywych tożsamości online w celu skontaktowania się z osobą nieletnią.
- Udawanie młodszego i/lub osoby płci przeciwnej.
- Uzyskanie dostępu do konta internetowego osoby nieletniej bez zezwolenia i kradzież jej zdjęć lub filmów o charakterze seksualnym.
- Groźenie utworzeniem zdjęć lub filmów o charakterze seksualnym nieletnich przy użyciu narzędzi do edycji cyfrowej.

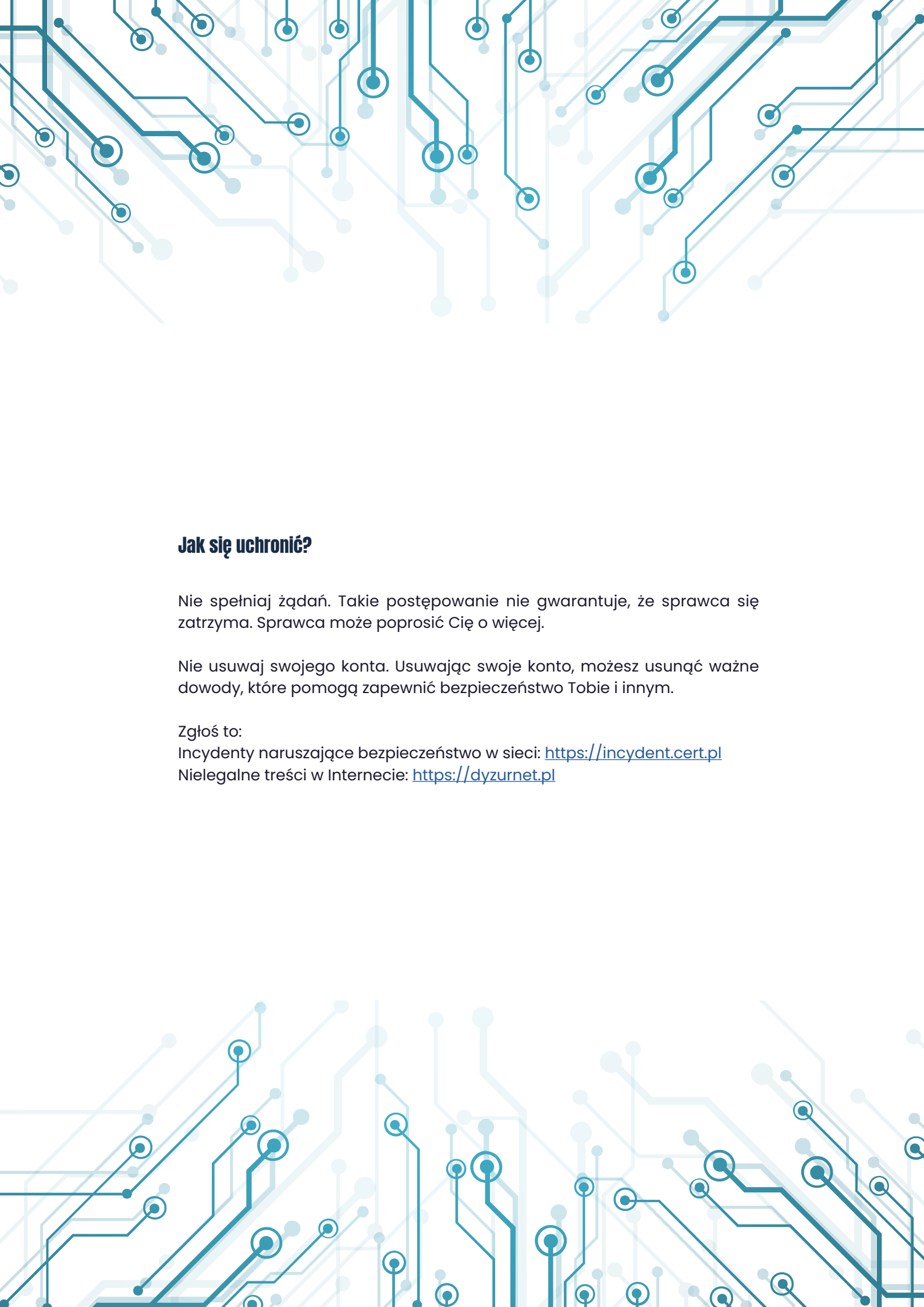
Sprawdź czy wiesz?

Pytanie: Co robić, gdy ktoś grozi, że opublikuje Twoje prywatne zdjęcia, jeśli nie spełnisz jego żądań?

Odpowiedzi:

- A) Spełnić żądania.
- B) Zignorować tę osobę.
- C) Powiadomić dorosłego lub odpowiednie służby.

Poprawna odpowiedź: C) Powiadomić dorosłego lub odpowiednie służby.



Jak się uchronić?

Nie spełniaj żądań. Takie postępowanie nie gwarantuje, że sprawca się zatrzyma. Sprawca może poprosić Cię o więcej.

Nie usuwaj swojego konta. Usuwając swoje konto, możesz usunąć ważne dowody, które pomogą zapewnić bezpieczeństwo Tobie i innym.

Zgłoś to:

Incydenty naruszające bezpieczeństwo w sieci: <https://incydent.cert.pl>

Nielegalne treści w Internecie: <https://dyzurnet.pl>

Cyberprzemoc

Cyberprzemoc to wszelkie agresywne zachowania w internecie, takie jak nękanie, poniżanie, grożenie lub rozpowszechnianie fałszywych informacji o kimś innym. To jak bycie prześladowanym w szkole, ale dzieje się to w świecie cyfrowym, gdzie sprawca może pozostać anonimowy.

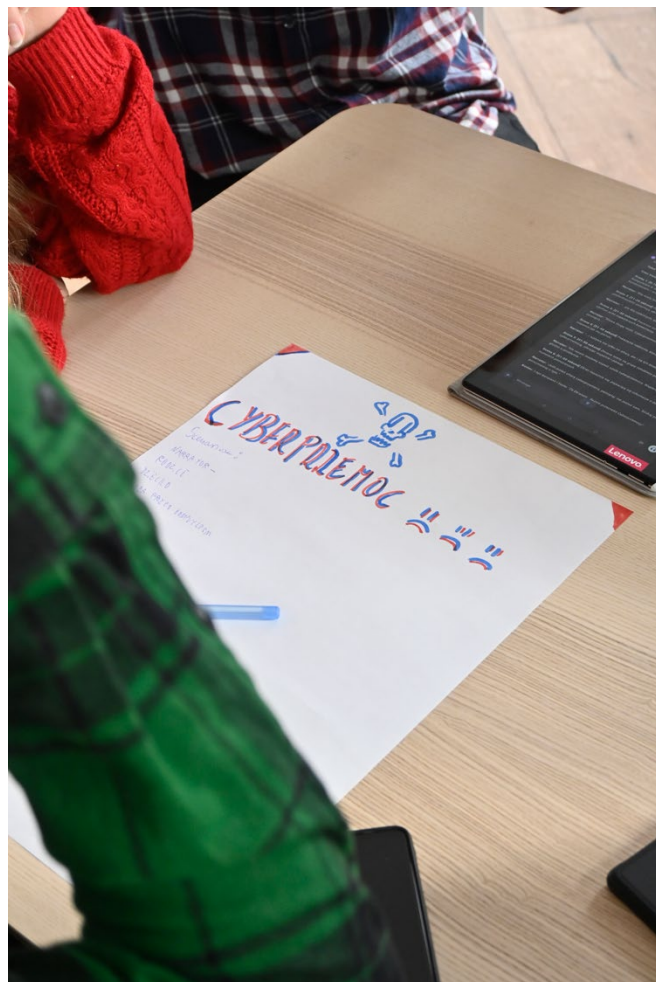
Oto kilka przykładów:

- Kradzież czyjejś tożsamości w celu utworzenia fałszywego profilu
- Udostępnianie nagich i/lub kompromitujących zdjęć innej osoby
- Nagrywanie i publikowanie filmów z walk

Przykłady cyberprzemocy:

- Rozpowszechnianie plotek za pośrednictwem wiadomości tekstowych, czatów grupowych lub w inny sposób.
- Tworzenie grupy nienawiści na jakiś temat.
- Publikowanie złośliwych komentarzy w Internecie.
- Photoshopowanie czyjegoś zdjęcia, aby go zawstydzić.

Niektóre z tych rzeczy mogą wydawać Ci się bardziej żartami niż znęcaniem się, ale nawet jeśli nie miałeś zamiaru zranić czyichś uczuć, nadal może to być cyberprzemoc.



Ofiary cyberprzemocy

Jak byś się czuł będąc ofiarą cyberprzemocy?

Być może:

- Doświadczysz niskiej samooceny
- Poczujesz się samotny i odizolowany od przyjaciół i rodziny
- Stresujesz się chodzeniem do Internetu lub do szkoły
- Czujesz się nękany przez rówieśników
- Czujesz się przygnębiony lub towarzyszy Ci niepokój
- Poczujesz się samotny lub odizolowany
- Poczujesz się beznadziejnie
- Doświadcz poważnego cierpienia psychicznego

Jak przeciwstawić się przemocy?

- Nie zachęcaj do znęcania się. Np nie klikaj reakcji „Lubię to!” pod złośliwymi postami, komentarzami. Nie udostępniaj złośliwych postów bądź komentarzy.
- Nie bierz udziału w nękaniu tylko po to, żeby się dopasować.
- Stań w obronie ofiary.
- Porozmawiaj ze swoimi przyjaciółmi o tym, jak nie dawać przyzwolenia na nękanie.

Bądź upstanderem!

Upstander to osoba postronna, która dostrzega czyny lub wypowiedzi niesprawiedliwe i zajmuje stanowisko, przerywając i rzucając wyzwanie sytuacjom, które normalizują dyskryminację i potencjalną przemoc.

Czasami ludzie czują, że mają prawo do tego aby dokuczać komuś w Internecie (na przykład, jeśli ta osoba też ich dręczyła). Jednak sytuacja związana z cyberprzemocą może łatwo wymknąć się spod kontroli i nie wiadomo, co może się wydarzyć. Pamiętaj, że nawet jeśli jesteś za ekranem, rozmawiasz z prawdziwymi ludźmi. To, że nie widzisz ich reakcji, nie oznacza, że nie czują się zranieni. Wyobraź sobie, jakie uczucia wywołałyby te komentarze.

Bądź upstanderem:

- Gdy tylko będzie to bezpieczne, powiedz sprawcy, żeby przestał.
- Dotrzyj do osoby, która jest ofiarą przemocy i okaż swoje wsparcie.
- Zgłoś prześladowcę.
- Porozmawiaj ze znajomymi o byciu upstanderem.

Sprawdź czy wiesz?

Pytanie: Co robić, jeśli jesteś świadkiem cyberprzemocy?

Odpowiedzi:

- A) Dołączyć i pomóc prześladowcy.
- B) Zignorować sytuację.
- C) Powiadomić dorosłego lub odpowiednią instytucję.

Poprawna odpowiedź: C) Powiadomić dorosłego lub odpowiednią instytucję.

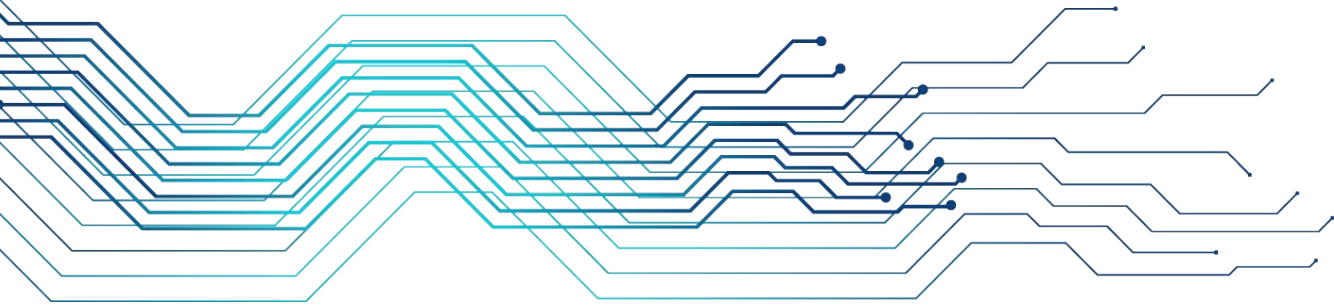


Aplikacja Szkolna Akademia Cyberbezpieczeństwa

Opracowaliśmy autorską aplikację, dzięki której lepiej poznasz cyberzagrożenia, z którymi możesz spotkać się w Internecie. Wejdź na stronę <https://cyberbezpieczni.glide.page/> i opracuj wszystkie lekcje. Dzięki lekcjom dowiesz się jak rozpoznać zagrożenia oraz jak sobie z nimi radzić. Na koniec opracujesz autorską kampanię profilaktyczną, aby przestrzec swoich rówieśników i pomóc im w walce.



Aplikacja



Klaster Innowacji Społecznych



Jesteśmy organizacją skupioną na przyszłości edukacji, gdzie wykorzystuje się innowacyjne technologie. Nasza wizja to szkoły, w których nowoczesne narzędzia i metody nauczania idą w parze z potrzebami uczniów XXI wieku. Dążymy do stworzenia bezpiecznego środowiska, w którym technologia staje się mostem łączącym wiedzę z codziennym życiem młodzieży. Poprzez innowacje i współpracę, kształtujemy przyszłość edukacji na Śląsku.

Strona www

