

„Myślące dzieci są bezpieczne w sieci” 2020

Konkurs wiedzy o bezpieczeństwie w Internecie

Materiały do nauki – dla klas 6-8

Konkurs odbędzie się w Twojej szkole
w dniach od **19 maja do 19 czerwca 2020 r.**

Ogłoszenie wyników nastąpi w dniu **22 czerwca 2020 r.**

- Zostaną one przekazane uczniom przez nauczycieli.
- Będą dostępne na profilu Facebook EduNect:

 fb.com/EduNect

Przyjemnej nauki na Konkurs! ;-)



Wstęp

Wciągu ostatnich kilkunastu lat wiele czynności, które odbywały się w realnej rzeczywistości przeszło do świata cyfrowego, do Internetu. Internet stał się nie tylko miejscem rozrywki, ale za jego pośrednictwem: ludzie pracują, uczą się, kupują, nawiązują znajomości, kontaktują się, rozmawiają, bawią się itp.

W Internecie nie jesteśmy anonimowi! Wszędzie zostawiamy ślady. Postępując lekkomyślnie możemy narazić się na duże kłopoty. O niektórych możemy dowiedzieć się po latach!



Prywatność

Jeśli nie dbasz o prywatność na portalach społecznościowych, wystawiasz się na duże ryzyko. Twoje zdjęcia może zobaczyć ktoś, komu nie chcesz ich pokazać. Podobnie jest ze statusami na portalach społecznościowych. Może się nawet zdarzyć tak, że złodziej, widząc gdzie mieszkasz i, że właśnie „meldujesz” się z rodzicami np. w kinie, będzie wiedział, że teraz ma czas, by okraść

Wasze mieszkanie. Podobnie informacja o rodzinnej wycieczce lub wakacjach (gdzie i kiedy) jest „pięknym zaproszeniem” dla złodzieja!

Jeśli nie zmienisz początkowych ustawień prywatności Facebooka, informacje, które tam piszesz, będzie mógł przeczytać każdy! Twoje zdjęcia także nie będą ukryte. Zmień te ustawienia tak, by ważne informacje o Tobie widzieli tylko najbliżsi znajomi. Zaznacz też, by nie można Cię było otagować na zdjęciu albo w poście bez Twojej wiedzy. Nie podawaj swoich danych osobowych, takich jak: imię, nazwisko, numer telefonu czy adres domowy.



Pamiętaj – nie musisz przyjmować wszystkich zaproszeń do znajomych, a na pewno nie od ludzi, których nie znasz. To, ilu masz znajomych na Facebooku, nie świadczy o tym, jak bardzo jesteś fajny/a.

Możesz też paść ofiarą przestępcy „sieciovego”, a nie realnego. W jego ręce może trafić dostęp do Twoich kont mailowych (przede wszystkim, jeśli nie ustawisz trudnego do odgadnięcia hasła) albo kont społecznościowych. Oprócz zablokowania konta może on podszywać się pod Ciebie i wysyłać maile albo publikować statusy. Jeśli zmieni on hasło, nie będziesz w stanie mu przeszkodzić.



Pamiętaj, że zazwyczaj nie ma nic za darmo! Jeśli Ty coś od kogoś dostaniesz, bardzo możliwe, że chętniej mu się czymś zrewanżujesz, np. swoim adresem e-mail, loginem, czy hasłem.

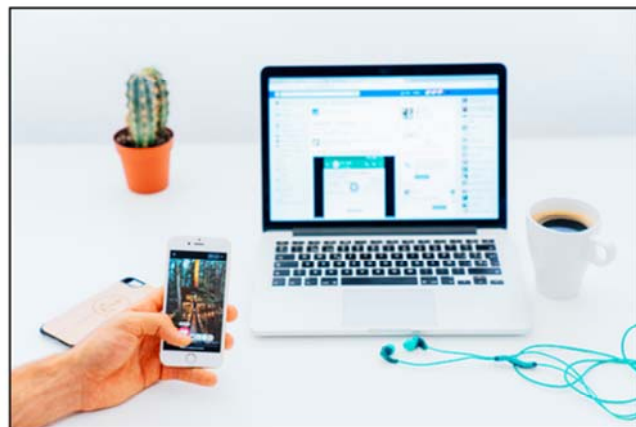
Nie wierz komuś, że jest kimś ważnym i trzeba słuchać jego prośb lub żądań, tylko dlatego, że tak Tobie powiedział przez telefon. To, że w podejrzanym mailu jest nazwa znanej Tobie dużej firmy, nie sprawia, że jest on bardziej wiarygodny. Jeśli masz wątpliwości, pokaż mail dorosłemu albo poproś go do telefonu.

Zanim wyślesz do kogoś (nawet znajomej i zaufanej osobie) informacje o sobie, to zastanów się czy będą one tam bezpieczne. Nie wszyscy dbają o bezpieczeństwo swojego komputera czy smartfonu tak jak Ty!

**Prywatność w Internecie
nie istnieje!**

Zdjęcia w sieci

Zdjęcia to piękne pamiątki z naszego życia. Ale Internet to narzędzie, które z pięknych chwil może zrobić koszmar. Po wrzuceniu zdjęcia np. na Facebooka praktycznie **tracimy nad nim kontrolę**. Powielane, kopiowane i udostępniane może znaleźć się na tysiącach serwerów - nie ma mowy o trwałym i skutecznym usunięciu. Warto pamiętać o tym, że wybierając zdjęcia do



publikacji nie powinniśmy zamieszczać zdjęć, które przedstawiają sytuacje z wczesnego etapu naszego życia. Po wielu latach zapomnimy o nich lecz mogą wrócić, gdy ktoś będzie chciał Ciebie skompromitować lub zrobić krzywdę. Nasz rówieśnik może takie zdjęcie odnaleźć i wykorzystać przeciwko nam. Mogą powstać przeróbki, czy memy i takie zdjęcie po latach, np. w nowej szkole, może przysporzyć nam wielu przykrości.

Nasze zdjęcia mogą stać się przedmiotem fascynacji osób o skłonnościach pedofilskich. Pod żadnym pozorem nie należy umieszczać w sieci fotografii naszego nagiego ciała, a także zdjęć, na których widnieją obiekty pozwalające rozpoznać miejsce, w którym mieszkamy.

Znajomość w sieci

W Internecie, tak jak w życiu, spotykamy zarówno dobrych jak i złych ludzi. Poznając osobę w sieci (w Internecie) zazwyczaj nie posiadamy wielu informacji na jej temat. Zdarza się, że nie jest tym, za kogo się podaje i

próbuję wydobyć od Ciebie poufne informacje, intymne zdjęcia lub przekonać Cię do zrobienia czegoś, co będzie niezgodne z prawem lub niebezpieczne dla twojego zdrowia i życia. Może również dążyć do tego, aby wyłudzić od



Ciebie pieniądze lub cenne rzeczy. W przypadku znajomości z sieci warto zachować szczególną ostrożność, ponieważ **nigdy nie wiadomo, kto jest po drugiej stronie**.

Jeśli podejrzewasz, że osoba, z którą nawiązałeś kontakt w Sieci ma wobec Ciebie złe zamiary postaraj się zachować korespondencję z tą osobą w historii komunikatora, e-mailach, SMS-ach itp. Spróbuj przypomnieć sobie wszystkie informacje, które posiadasz na temat tej osoby. Porozmawiaj o tym z rodzicami czy inną zaufaną osobą dorosłą. Rodzice lub prawni opiekunowie mogą podjąć działania, które zapewnią Ci bezpieczeństwo. Jeśli czujesz, że trudno Ci będzie przeprowadzić taką rozmowę skorzystaj z telefonu zaufania dla dzieci i młodzieży pod numerem 116 111.

Pamiętaj, że masz prawo odmówić rozmów na tematy intymne i każdy powinien to uszanować.

Masz prawo przerwać każdy kontakt, który Cię niepokoi i powinieneś powiedzieć o wszystkim rodzicom lub opiekunom prawnym. Masz również prawo zgłosić administratorowi portalu każdą sytuację, która nie jest zgodna z jego regulaminem.

Uważaj!
Nigdy nie wiesz na pewno
kto jest po drugiej stronie sieci!

Oto kilka wskazówek jak bezpiecznie kontaktować się z innymi:

- Staraj się spotykać przede wszystkim z osobami, które poznałeś w świecie realnym.
- Nie podawaj nieznajomym swoich danych osobowych, takich jak numer telefonu i adres, numer komunikatora, e-mail.
- Posługuj się nickiem (przezwyisko, pseudonim). Nie podawaj prawdziwego imienia i nazwiska.
- Nie rozmawiaj z osobami poznanymi w Sieci na tematy związane ze sferą seksualną człowieka.
- Nie opowiadaj nieznajomym o Twoich prywatnych sprawach ani o Twojej rodzinie.
- Bądź ostrożny z wysyłaniem zdjęć, nigdy nie wiesz gdzie mogą później trafić.

Cyberprzemoc

Cyberprzemoc to takie zachowanie, które krzywdzi emocjonalnie drugiego człowieka. Osoby, które stosują cyberprzemoc używają do tego celu Internetu albo telefonów komórkowych. W przeciwieństwie do przemocy fizycznej, cyberprzemoc nie zostawia śladów na ciele i nie widać jej gołym okiem. Osoby, które doświadczyły cyberprzemocy czują się zranione i bardzo przeżywają to, co je spotkało. Pojawiają się u nich nieprzyjemne myśli i uczucia takie jak bezradność, wstyd, upokorzenie, strach a czasem



również złość. Osoba, której przytrafiła się taka sytuacja często ma wrażenie, że wszyscy widzieli lub mogą zobaczyć te nieprzyjemne materiały. Obawia się, że jej znajomi odwrócą się od niej i nie będzie mogła liczyć na ich wsparcie. To powoduje, że czuje się bardzo samotna w tym, co ją spotkało.

Cyberprzemoc to takie zachowania jak:

- ośmieszanie, obrażanie, straszenie, nękanie czy też poniżanie kogoś za pomocą Internetu, albo telefonu komórkowego,
- podszywanie się pod kogoś w portalach społecznościowych, na blogach, wiadomościach e-mail lub komunikatorach,
- włamanie się na czyjeś konto (np. pocztowe, w portalu społecznościowym, konto komunikatora),
- publikowanie oraz rozsyłanie filmów, zdjęć, albo informacji, które kogoś ośmieszają,
- tworzenie obrażających kogoś stron internetowych lub blogów,
- pisanie obraźliwych komentarzy na forach, blogach, portalach społecznościowych.



Jeśli doświadczasz cyberprzemocy:

- Pamiętaj, że nie jesteś sam. Powiedz o tym zaufanej osobie dorosłej - z jej pomocą będzie Ci łatwiej poradzić sobie z tą sytuacją.
- Postaraj się nie kontaktować ze sprawcą cyberprzemocy i nie odpowiadać na jego zaczepki. Dzięki temu unikniesz prowokowania go do dalszych działań.
- Zachowaj wszystkie dowody cyberprzemocy - nie kasuj sms - ów, e-maili, rozmów na czatach lub komunikatorach.
- Jeśli ktoś dokucza Ci na jakiejś stronie WWW, zrób **zrzut ekranu** - aby zachować to, co widzisz na ekranie wciśnij klawisz "Print Screen" (Prt Sc), a następnie otwórz program tekstowy (np. Word) lub graficzny (np. Paint) i wklej tam screen naciskając jednocześnie klawisze "Ctrl" i "V". **Pamiętaj, aby zapisać plik.**
- Skorzystaj z telefonu zaufania dla dzieci i młodzieży pod numerem 116 111 lub wyślij wiadomość przez stronę **www.116111.pl**.

Jeśli jesteś świadkiem cyberprzemocy:

- nie przesyłaj dalej ośmieszających wiadomości.
- pomóż pokrzywdzonej osobie poprzez poinformowanie kogoś dorosłego o jej sytuacji.
- powiedz pokrzywdzonej osobie o telefonie zaufania lub sam/a zadzwoń pod numer 116 111, aby dowiedzieć się, co można zrobić w tej sytuacji.

**Przez Internet
też można krzywdzić!
Nie rób tego!**

Hejt

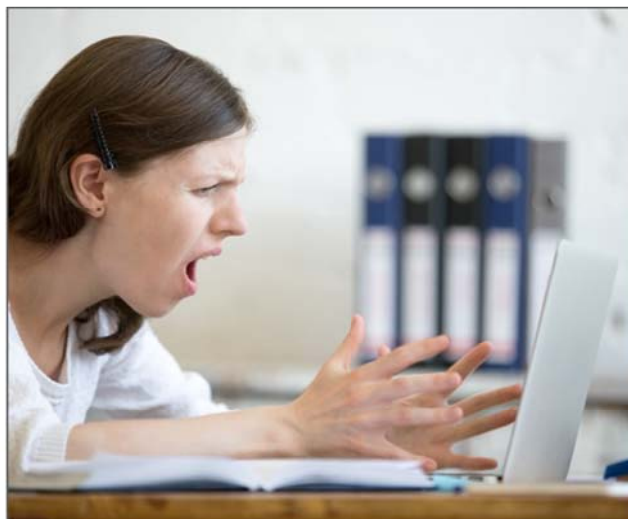
Czym jest hejt?

Tłumacząc z języka angielskiego to nienawiść („*hate*”) Najprościej mówiąc, jest to obraza i ośmieszenie drugiej osoby w Internecie.

Świadomość tego, że w Internecie możemy być anonimowi wzmacnia w nas tego typu zachowanie.

Bardzo często bywa tak, że osoby nieśmiałe i ciche w życiu prywatnym, w cyberprzestrzeni stają się po prostu złośliwe. Hejter nie widzi reakcji osoby, którą poniża i ośmiesza, przez co nie zdaje sobie sprawy z ogromu krzywdy jaką jej wyrządza.

Emocje, które kierują hejterami opierają się na pogardzie dla drugiej osoby, przez co traktują ich jak przedmioty. Tak wynika z jednego z raportów „Mowa nienawiści, mowa pogardy”.



Dlaczego hejtujemy?

Hejt bywa odpowiedzią na nudę. Jest metodą na udowodnienie znajomym swojej siły czy też przejawem zazdrości. Możliwość hejtowania czasem też przynosi ulgę.

Jakie mogą być konsekwencje hejtu?

Jeśli zachowasz się jak hejter to pamiętaj, że treści, które trafiły do Internetu już w nim zostaną.

Wyobraź sobie że masz 25 lat, kończysz studia i chcesz rozpocząć pracę. W trakcie procesu rekrutacyjnego potencjalny pracodawca z ciekawości wpisuje Twoje dane do Internetu i co znajduje? Niemile i obraźliwe wpisy na temat innych osób. Czy wzbudzi to jego zaufanie?

Z kolei osoby hejtowane czują się poniżane, otoczenie postrzega je jako osoby do wyśmiewania. Ich kondycja psychiczna spada, boją się zderzenia z rzeczywistością.



Co można shejtować?

Hejt dotyczy nie tylko konkretnej osoby. Może być skierowany także do danego narodu, płci, wyznawców religii, a nawet do jakiejś sytuacji czy wydarzenia. Wykorzystuje nie tylko słowo pisane, ale także grafikę czy filmy. Hejty pojawiają się głównie na dużych, publicznych forach o tematyce politycznej czy poruszającej kwestie światopoglądowe.

Pamiętaj, że wyrażając swoje zdanie w Internecie mające charakter namawiania do nienawiści czy dyskryminacji podlegasz karze grzywny, ograniczenia lub pozbawienia wolności do lat 2.

Zasady antyhejtowe:

- Przemyśl, zanim odpowiesz na komentarz hejterski.
- Jeżeli jesteś na kogoś zły – napisz na kartce to, co chcesz wyrazić i wyrzucić ją.
- Jeśli coś Ci się nie podoba – wyraż swoje zdanie kulturalnie. W końcu masz do tego prawo.
- Nie reaguj agresją na agresję – hejter odbierze to, jako prowokację.
- Nie udostępniaj i nie lajkuj hejtów.
- Odróżniaj hejt od subiektywnej krytyki.
- Jeśli to, co robisz lub mówisz jest hejtowane, nie rezygnuj z tego przez hejterów.

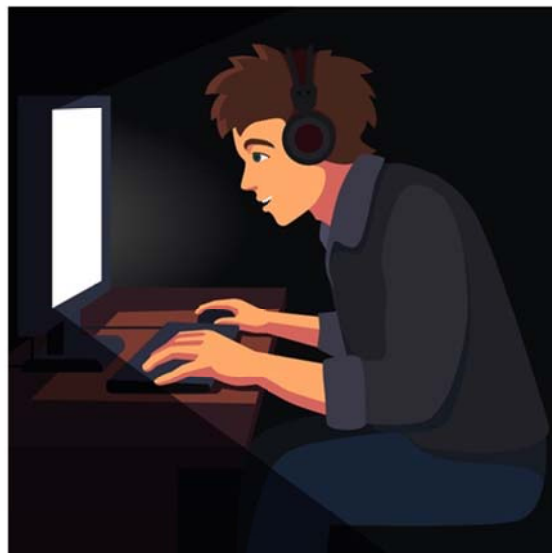
**Hejt to mowa nienawiści
w Internecie.**

Przemyśl, zanim odpowiesz!

Nadmierne korzystanie

Należy zachować zdrowy rozsądek korzystając z sieci! Nadmierne korzystanie z Internetu źle wpływa na Twój organizm. Może to się objawiać częstymi bólami głowy, pogorszeniem wzroku, a nawet problemami z zasypianiem. Osoby takie stają się agresywne, czują niepokój, mają trudności z koncentracją. A do tego dochodzi brak ruchu, nieregularna dieta i nierzadko brak higieny osobistej.

Oprócz problemów zdrowotnych mogą pojawić się problemy o podłożu socjalnym – pojawiają się problemy w relacji z rodziną i rówieśnikami. Bardzo często osoby, które spędzają dużo czasu w Internecie nie interesują się życiem realnym – zaniedbują domowe obowiązki, unikają spotkań koleżeńskich. Wystarcza im po prostu to, co jest w sieci.



Nie spędzaj każdej wolnej chwili przy komputerze czy telefonie! Spora część użytkowników przebywa online za długo i nie jest w stanie tego kontrolować. Warto samemu ustalić sobie pewien limit czasu i starać się go nie przekraczać. A przede wszystkim pielęgnuj swoje kontakty ze znajomymi i rodziną, bo tego nie zastąpi żadna strona internetowa!

Jakie są pierwsze objawy nadmiernego korzystania z sieci?

- silna potrzeba korzystania z Internetu,
- brak kontroli czasu spędzanego w sieci,
- problem z powstrzymaniem się od korzystania z komputera,
- niepokój i rozdrażnienie przy próbie przerwania korzystania z sieci,
- zaniedbanie relacji z bliskimi,
- spędzanie coraz większej ilości czasu przy komputerze.



**Korzystanie z Internetu:
rozsądnie i z głową!**

Gdy rozpoznajesz u siebie te objawy – porozmawiaj z rodzicami lub zadzwoń pod numer **116 111**.

Zakupy

Raport „E-commerce w Polsce 2017. Gemius dla e-Commerce Polska” przeprowadzony w 2017 r. mówi, że 54 % internautów robi zakupy w sieci. 82 % ankietowanych uważa za przewagę nad sklepami stacjonarnymi fakt, że możliwość zakupów dostępna jest przez całą dobę. Najczęściej kupowane są: sprzęt elektroniczny, kosmetyki oraz książki.

Według twórców raportu, w porównaniu do poprzedniego roku, znacznie wzrosła liczba osób uznających zakupy przez Internet, jako łatwe. Również wzrost pojawił się w słupku dotyczącym większej różnorodności produktów w Internecie.



Czy zakupy przez Internet są bezpieczne?

Zdania na pewno są podzielone. Jedni uważają, że jest to szybki i wygodny sposób zakupów bez wychodzenia z domu. Z drugiej natomiast strony oszustw internetowych jest coraz więcej – opłacone produkty nie docierają do kupców lub też różnią się od opisu w sieci, wykradzione zostają poufne dane osobowe, numery kart kredytowych.

Dlatego, jeżeli chcesz coś kupić w sieci, najlepiej poproś o pomoc rodziców. Nie wolno podawać numeru karty kredytowej ani wypełniać ankiet czy formularzy internetowych, gdzie wpisujesz swoje dane osobowe i adresowe.

**Dużo, tanio... a może kiepsko?
Pomyśl zanim kupisz online!**

Prawo autorskie



Prawo autorskie jest jedną z dyscyplin prawa cywilnego, w którego skład wchodzi prawa własności intelektualnej i prawa przysługujące autorowi danego utworu.

Przedmiotem ochrony są utwory, do których zaliczyć można:

- utwory pisane słowem (np. książka), symbolem matematycznym (np. wzór naukowy) czy znakiem graficznym (np. logo firmy)
- utwory plastyczne (np. obraz), fotograficzne (np. zdjęcie), architektoniczne (np. projekt), muzyczne (np. melodia), sceniczne (np. sztuka w teatrze), choreograficzne (np. układ taneczny).



Dlatego pamiętaj, że korzystając ze źródeł w Internecie zawsze podawaj ich **źródła**, a przede wszystkim sprawdzaj ich wiarygodność. Odrabiając lekcje pamiętaj, że **nie wszystkie treści zamieszczone w sieci są prawdziwe!**

**Nie przywłaszczaj sobie treści z Internetu.
To jest czyjaś praca!**

Netykieta

Netykieta to ogół zasad obowiązujący wszystkich internautów. Dużo osób nie słyszało o takim pojęciu, ale jest ono niezwykle ważne w wirtualnym świecie. Nie są to sztywne nakazy i zakazy, a raczej uświadamianie i pouczanie.

Trzy główne zasady netykiety to:

1. MYŚL
2. NIE DZIAŁAJ NA CZYJĄŚ SZKODĘ
3. NIE NADUŻYWAJ

Przykładami netykiety jest:

- zakaz spamowania / wysyłania „łańcuszków szczęścia”,
- pisownia zgodnie z polskimi zasadami,
- zakaz pisanie nie na temat / po kilka razy to samo,
- nie obrażaj innych i nie prowokuj kłótni,
- zakaz pisanie wielkimi literami,
- używanie emotikon z umiarem,
- zwracanie się po nicku lub imieniu (nigdy po nazwisku),
- zakaz uporczywego kontaktowania z osobami, które sobie tego nie życzą.

**Jeśli chcesz być dobrze
traktowany w Internecie
to traktuj innych dobrze!**

Zabezpiecz swoje urządzenie

Jak powszechnie wiadomo w Internecie krąży mnóstwo wirusów, które mogą uszkodzić telefon, tablet czy komputer. Najważniejsze jest to, aby mieć zainstalowany program antywirusowy!

Oto najważniejsze zasady, jak mieć bezpieczny sprzęt:

1. Wprowadź **hasło dostępu** do telefonu, aby nikt nie mógł go użyć.
2. Nie korzystaj z **nieznanych połączeń WiFi** (zwłaszcza darmowych). Jeżeli nie trzeba wpisywać hasła, może to być niebezpieczna sieć.
3. Jeżeli zgubisz telefon, pamiętaj, że zawsze możesz nim **zarządzać**. Wystarczy włączyć funkcję zdalnego zarządzania i wykonywania kopii zapasowych (przykładowo w ustawieniach telefonu funkcja „Znajdź telefon”).
4. Staraj się **nie pobierać nieznanych aplikacji** - Twój telefon jest również narażony na wirusy. Sprawdzaj, jakich uprawnień wymaga aplikacja. Często zdarza się, że jest to dostęp do zdjęć lub kontaktów.
5. Istnieją tzw. **trojany**, które przypominają gry ściągane na urządzenia przenośne. Po ich instalacji pieniądze znikają z konta - wykonywane są odpłatne telefony i SMS-y typu premium.



6. **Sprawdzaj maile** – zdarza się, że przychodzą od nieznanych osób załączniki, które wprowadzają wirus na Twoje urządzenie. **Nie otwieraj załączników** z nieznanych źródeł!

**Zapobieganie
cyberprzestępstwom: unikalne
hasła i czujność w sieci.**

Gdy dzieje się coś złego

Gdy czujesz, że dzieje się coś złego - bez zastanowienia porozmawiaj o tym z rodzicami lub inną bliską Ci osobą. Pokaż im stronę, która wywołuje u Ciebie niepokój lub fragment czatu z obcą osobą.

Jeżeli ktoś ktokolwiek:

- przestraszył Cię,
- groził Ci,
- zamieścił Twoje zdjęcie bez zgody,
- pisał krępujące treści,
- włamał się na Twoje konto,
- pisał wulgarnym językiem w sieci lub prywatne wiadomości do Ciebie,
- nawiązał z Tobą kontakt i prosi o poufne dane takie jak: imię, nazwisko czy adres,
- nieznajomy nalega na spotkanie, wysyła niemoralne zdjęcia lub prosi o to Ciebie -

zgłoś to osobie dorosłej.

Podobnie, jeżeli stracisz kontrolę nad czasem, który spędzasz w Internecie poproś o pomoc. Możesz zadzwonić do konsultantów Telefonu Zaufania dla Dzieci i Młodzieży **pod bezpłatny numer 116 111**.

**Objawy
cyberprzemocy?
Nie wstydź się!
Poproś o pomoc!**



Nieuprawniony dostęp

Kradzież danych polega na uzyskaniu informacji, np. danych osobowych, od konkretnej osoby, przez osoby, które nie mają na to pozwolenia.

Pamiętaj, że każdy z nas ma prawo do ochrony danych osobowych zgodnie z Ustawą o Ochronie danych osobowych z dnia 29 sierpnia 1997 roku.



Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Jest to zatem każda informacja, dzięki której możliwe jest ustalenie tożsamości.

Przykładem danej osobowej jest więc:

- imię i nazwisko,
- adres IP komputera,
- zdjęcie,
- adres e-mail,

a przy ich pomocy można ustalić kim jest dana osoba.



Kiedy najbardziej narażeni jesteśmy na nieuprawniony dostęp?

- Kiedy korzystamy z programów niewiadomego pochodzenia - mogą zawierać wirusy uszkadzające nasz dysk w komputerze lub przekazujące informacje o tym, co robimy na swoim urządzeniu.
- Gdy otwieramy okienko w Windows, korzystamy z linków i aplikacji z nieznanych źródeł.
- Kiedy korzystamy z serwisów, portali bez zabezpieczeń (np. bez regulaminu czy kontaktu z administratorem).
- Gdy podajemy hasło dostępu do naszych kont i profili innym osobom.
- Kiedy dane o sobie przekazujemy innym, a nie jest to wymagane (np. na serwisach, portalach czy z innymi użytkownikami sieci).

BĄDŹ CZUJNY!

**Niezależnie od użytego
zabezpieczenia nie masz
pewności czy będzie ono
wystarczające!**

Seksting

Seksting polega na wysyłaniu innym osobom za pośrednictwem Internetu lub telefonu komórkowego swoich intymnych zdjęć lub filmów. Jest to niebezpieczne zjawisko, ponieważ w części przypadków takie zdjęcia i filmy są niezgodne z prawem. Poza tym raz wysłane intymne materiały mogą pozostać w posiadaniu osoby, która je otrzymała i zostać użyte przez nią w dowolny sposób. Często zdarza się, że trafiają w ręce niepowołanych osób i stają się **narzędziem cyberprzemocy**: szantażu czy zastraszania osoby, która się na nich znajduje. Mogą również zostać opublikowane w widoku publicznym bez zgody osoby, która na nich jest. Uważaj na aplikację Snapchat - została ona wymyślona przede wszystkim z myślą o rozsyłaniu zdjęć intymnych.

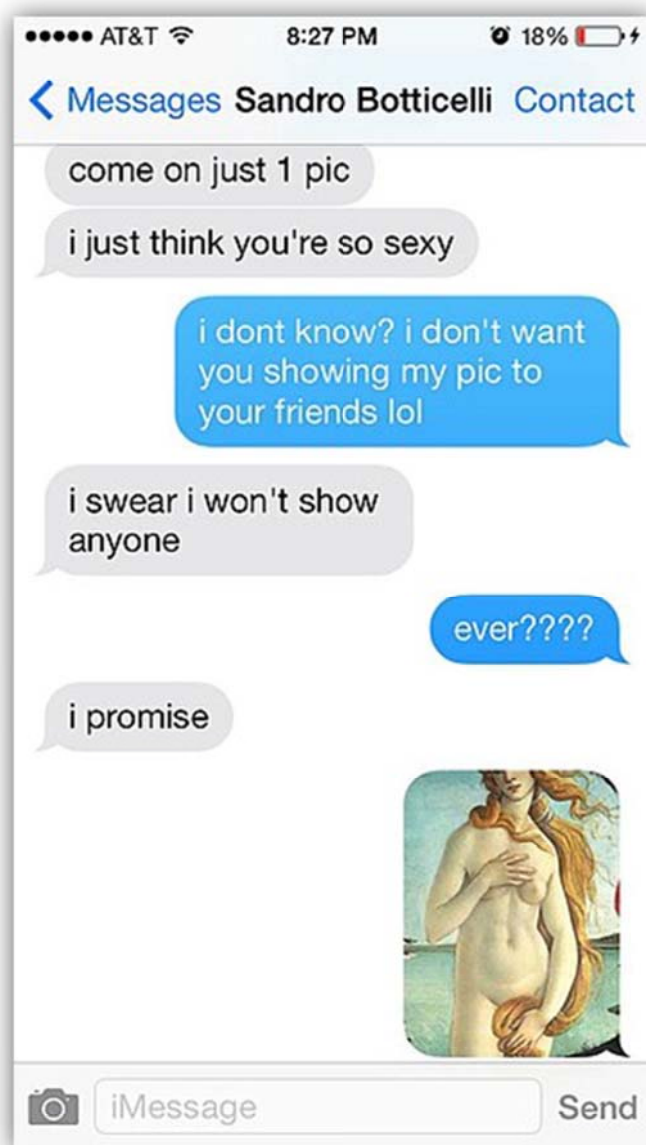
W wieku dojrzewania to naturalne, że czasem zastanawiasz się i chcesz sprawdzić, co na Twój temat myślą inni ludzie. Masz prawo do tego, aby się wyróżnić i zaimponować swoim rówieśnikom. Możesz też być ciekawy zachowań, których jeszcze nie próbowałeś. Zdarza się, że inna osoba może Cię zachęcać do wysłania takich zdjęć na dowód uczuć, które odczuwasz wobec niej. W takich sytuacjach wysłanie innym osobom lub opublikowanie roznegliżowanej fotki może się okazać bardzo złym pomysłem, który spowoduje niebezpieczne i przykre konsekwencje.

Pamiętaj, że nikt nie ma prawa zmuszać Cię do wysłania takich zdjęć i narzucać Ci oglądania intymnych zdjęć innej osoby. Dlatego warto kilka razy się zastanowić, zanim zdecydujesz się podzielić z kimś takimi zdjęciami. Pamiętaj, że relacje z ludźmi czasem się zmieniają. Osoba, która jest Ci bliska dziś - za kilka miesięcy lub lat może mieć do Ciebie inne nastawienie. Zdarza się, że do urządzenia takiego jak telefon/tablet dostęp uzyskują niepowołane osoby, które również mogą wejść w posiadanie Twoich zdjęć.

Jest jeszcze jedna rzecz, na którą warto zwrócić uwagę. Świadomość tego, że praktycznie każdy użytkownik może nagrać to, co widzi na ekranie może pomóc Ci pozostać bardziej ostrożną/ostrożnym podczas korzystania z serwisów oferujących videoczaty. Zdarza się, że spotkania online są nagrywane i stają się materiałami używanymi do szantażu osoby, która się na nich znajduje.

Jeśli zdarzyło się, że ktoś namawia Cię na wysłanie intymnych zdjęć lub filmów, albo już takie materiały są w posiadaniu innych osób i obawiasz się o to, co będzie dalej – porozmawiaj o tym z rodzicami/prawnymi opiekunami lub skorzystaj z telefonu zaufania dla dzieci i młodzieży.

Pamiętaj, że wysyłając swoje intymne zdjęcie lub film, tracisz kontrolę nad tym, co się z nimi dalej stanie.



**Twoja prywatność
powinna być dla Ciebie
największym skarbem!**

Hakerzy i włamania

Pojęcia „haker” i „włamanie” są w dzisiejszych czasach powszechnie znane. **Haker to inaczej włamywacz internetowy.**

Czy każdy z nas zdaje sobie sprawę jak blisko czyha niebezpieczeństwo? Czy nie istnieje ryzyko, że ktoś włamie nam się na konto (np. mailowe lub facebookowe) i pobierze dane, które mogą nam zaszkodzić? Wystarczy, że haker zainstaluje na Twoim urządzeniu specjalny program, tzw. **malware** lub sam zrobisz to nieświadomie.

Otwierając link w podejrzanym mailu (nawet od znajomej osoby), wchodząc w stronę, którą polubił znajomy na Facebooku, dajesz hakerowi możliwość włamania. Dobrym nawykiem jest najechanie kursorem na przesłany link, bez klikania w niego. Jeżeli adres, który pojawi się na dole przeglądarki, jest inny od tego w treści strony, ktoś zwyczajnie usiłuje Cię oszukać. To, że wiadomości pochodzą od znanych Ci osób nie oznacza, że one musiały Ci je wysłać. Być może do włamania doszło także na ich urządzeniu!

Złośliwe oprogramowanie może być ukryte w plikach jpg np. ze zdjęciami lub filmami, doc (zwykły tekst w Wordzie), pdf czy arkuszach Excel. Wykorzystują one luki w zabezpieczeniach i instalują automatycznie malware na urządzeniu. Unikaj stron z pirackimi grami lub filmami, nie otwieraj podejrzanym linków – one również wykorzystują luki w przeglądarkach internetowych.

Po czym poznasz, że Twoje urządzenie może być zainfekowane? Oto kilka przykładów:

- Komputer długo się nie wyłącza.
- Na portalach społecznościowych pojawiają się niby Twoje komentarze, których nie jesteś twórcą.
- System Windows (lub inny) nie chce się zaktualizować.
- Program antywirusowy nie chce się zaktualizować.
- Internet działa dużo wolniej.
- Znajomi dostają maila z Twojego konta, ale nie ty go pisałeś.



- Na ekranie wyświetlają się dziwne komunikaty lub otwierają się okienka.

Pamiętaj, że te oznaki nie zawsze sugerują, że stało się coś złego! Warto jednak sprawdzić komputer jakimś programem antywirusowym. W razie problemów, program antywirusowy możesz zgrać na pendrive na innym urządzeniu i wtedy zainstalować na swoim. Jeśli natomiast problem jest z kontem facebookowym, pocztowym czy bankowym – natychmiast należy zmienić hasło.

Nie tylko haker może włamać się na Twoje konto. Może to być również Twój znajomy, czy ktoś kto dobrze Cię zna. Dlatego **należy unikać prostych haseł** typu moja data urodzenia, ksywa, imię zwierzaka czy miejscowość w której mieszkasz. Bardzo dobrym sposobem jest użycie w hasle różnych kombinacji – małych i dużych liter, cyfr i znaków specjalnych.

HAKERZY
Internetowi włamywacze,
a może ktoś znajomy?

Trudność haseł:

hasło 6-znakowe	liczba kombinacji	czas złamania
same cyfry	1000000	9,7 sekundy
małe litery	308915776	50 minut
duże i małe litery	19770609664	53 godziny
wszystkie znaki ASCII	6053450000000	2 lata

hasło 7-znakowe	liczba kombinacji	czas złamania
same cyfry	10000000	97 sekund
małe litery	8031810176	22 godziny
duże i małe litery	1028070000000	116 dni
wszystkie znaki ASCII	817215000000000	252 lata

Słownik pojęć

Cyberprzemoc - stosowanie przemocy poprzez: prześladowanie, zastraszanie, nękanie, wyśmiewanie innych osób z wykorzystaniem Internetu i narzędzi typu elektronicznego takich jak: SMS, e-mail, witryny internetowe, fora dyskusyjne w Internecie, portale społecznościowe i inne. Osobę dopuszczającą się takich czynów określa się stalkerem.

Hejter - określenie osoby, która wyraża kłótniwe i agresywne komentarze w Internecie. Wrogie komentarze mogą być postrzegane jako akt cyberprzemocy i nękania psychicznego. W sposób napastliwy i używając tzw. mowy nienawiści (nazwa pochodzi od spolszczenia angielskiego słowa hate) krytykuje daną rzecz lub osobę (najczęściej publiczną).

Internet - ogólnoświatowy system połączeń między komputerami, określany również jako sieć sieci.

Konto użytkownika - zbiór zasobów i uprawnień w ramach danego systemu przypisanych konkretnemu użytkownikowi systemu komputerowego. Konto posiada unikalną nazwę (login) i hasło.

Netykieta - zbiór zasad przyzwoitego zachowania w Internecie, swoista etykieta obowiązująca w sieci.

Nick - przezwisko, pseudonim. Czasem używany jest w polskich programach do określenia loginu lub identyfikatora.

Otagowanie – metoda oznaczania i umieszczania odnośników do grup danych. Pozwala to na odwoływanie się do nich według pewnej cechy.

Post (inf.) – komentarz, głos w dyskusji, informacja wysłana na grupę lub forum dyskusyjne, napisana w określonym temacie wypowiedź.

Profil - część serwisu społecznościowego zawierająca informacje o użytkowniku.

Serwis społecznościowy - serwis internetowy, który służy do budowania sieci społecznych oraz stosunkach społecznych, które opierają się na podobnych zainteresowaniach, wspólnym życiu zawodowym lub prywatnym, itp. Umożliwia kontakt ze znajomymi oraz dzielenie się informacjami, zainteresowaniami, itp.

Wirus komputerowy - program komputerowy posiadający zdolność powielania się, tak jak prawdziwy wirus, stąd jego nazwa. Wirus do swojego działania potrzebuje i wykorzystuje system operacyjny, aplikacje oraz tożsamość użytkownika komputera.



Spis treści

Wstęp	1
Prywatność.....	1
Zdjęcia w sieci	3
Znajomość w sieci	3
Cyberprzemoc.....	4
Hejt	6
Nadmierne korzystanie	7
Zakupy	8
Prawo autorskie	9
Netykieta.....	9
Zabezpiecz swoje urządzenie	10
Gdy dzieje się coś złego	11
Nieuprawniony dostęp.....	11
Seksting.....	12
Hakerzy i włamania	14
Słownik pojęć	15



Źródła

<https://sieciaki.pl/warto-wiedziec/porady> (dostęp: maj 2020)

<https://sieciaki.pl/warto-wiedziec/zagrozenia> (dostęp: maj 2020)

<http://websecurity.pl/jak-zachowac-bezpieczenstwo-w-sieci/> (dostęp: maj 2020)

<https://116111.pl/problemy/internet,cid,31> (dostęp: maj 2020)

<https://116111.pl/problemy/nie-hejtuj-zyskaj-przyjaciela,aid,159> (dostęp: maj 2020)

https://pl.wikipedia.org/wiki/Prawo_autorskie (dostęp: maj 2020)

<https://pl.wikipedia.org/wiki/Sexting> (dostęp: maj 2020)

<https://plblog.kaspersky.com/czas-zabezpieczyc-swoje-urzadzenia-mobilne/3374/> (dostęp: maj 2020)

Autorzy materiałów



EduNect

EduNect Sp. z o.o.

ul. Grabiszyńska 214/7

53-235 Wrocław

email: lekcje@edunect.pl

www: www.edunect.pl

FB: www.facebook.com/EduNect

Sonia Parusel i Przemysław Malinka

Zespół Szkolno-Przedszkolny w Ostrożnicy

ul. Kościelna 42, 47-280 Ostrożnica

email: zsp@zspostroznica.pl

www: www.zspostroznica.pl

Utworzono: Wrocław i Ostrożnica, maj 2020 r.