CYBERPRZEMOC, CYBERBEZPIECZEŃSTWO,SEXTING

Drodzy Uczniowie

Na naszych oczach rzeczywistość, w której żyjemy, staje się hybrydowa. Realne miesza się często z wirtualnym, a to, co do tej pory odbywało się tradycyjnie – przeniosło się do internetu. Internet i sieć komórkowa w Waszym środowisku stały się jednym z najpopularniejszych mediów. Są przez Was postrzegane jako ulubiona – a w ostatnim czasie podstawowa – forma spędzania wolnego czasu, nauki, komunikowania się oraz poszukiwania informacji. Ostatnio coraz częściej Internet staje się istotnym środowiskiem, w którym zaspakajacie swoje potrzeby społeczne związane z przynależnością do grupy rówieśniczej. Niestety technologie informacyjne i komunikacyjne wykorzystywane są również jako narzędzia agresji i przemocy.

Poniżej przekazujemy w pigułce ważne informacje, abyście byli bezpieczni w sieci.

1.Porozmawiaj z bliską osobą-poszukaj wsparcia i pomocy. Rozmowa z przyjacielem, osobą dorosłą pomoże Ci zapanować nad emocjami i poczuć się lepiej.

2. Zachowaj dowody. Zanim podejmiesz próby uśnięcia obraźliwych wiadomości- pamiętaj, że są ważnym dowodem nękania. Zrób zrzut ekranu.

3. Zgłoś incydent. Skorzystaj z telefonu zaufania 116 111.

4. Prowadź rozmowę na swoich zasadach- nie daj się wciągnąć w spirale agresji.

5. Odetnij się od agresora. Możesz zablokować osobę , która Cię atakuje.

Jeśli byłeś lub będziesz świadkiem cyberprzemocy w szkole, nie pozostawaj obojętny. Pamiętaj, Ty też możesz pomóc.

Co możesz zrobić, gdy jesteś świadkiem cyberprzemocy wobec kolegi lub koleżanki?

1. Wyraź sprzeciw.
2. Zgłoś cyberprzemoc.
3. Nie udostępniaj.
4. Zaangażuj innych.
5. Poinformuj dorosłego.
6. Podpowiedz koledze lub koleżance gdzie może szukać pomocy.
7. Okaż wsparcie nękanej osobie.

PRZYDATNE STRONY

Jeśli chcesz się dowiedzieć więcej na temat bezpieczeństwa w sieci, jak nie stać się ofiarą cyberprzemocy, jak bezpiecznie korzystać z internetu, zachęcamy Cię do odwiedzenia stron internetowych instytucji działających na

rzecz bezpieczeństwa najmłodszych użytkowników internetu. Znajdziesz tam ciekawe informacje, materiały i porady – nie tylko dotyczące cyberprzemocy.

OSE IT Szkoła https://it-szkola.edu.pl/

Akademia NASK https://akademia.nask.pl

Program Safer Internet www.saferinternet.pl

Dyżurnet.pl www.dyzurnet.pl

Cybernauci www.cybernauci.edu.pl

Cyfrowobezbezpieczni www.cyfrowobezpieczni.pl

Fundacja Dbam o Mój Zasięg https://dbamomojzasieg.pl/

GDZIE SZUKAĆ POMOCY?

Istnieją różne zespoły i linie pomocowe zajmujące się sprawami dotyczącymi bezpieczeństwa dzieci, także w internecie. Na stronach internetowych tych instytucji znajdziesz informacje i wskazówki, które podpowiedzą Ci, jak rozwiązać problem cyberprzemocy. Możesz również skorzystać ze wsparcia i porad pracujących tam specjalistów, dzwoniąc na infolinię, korzystając z czatu lub wysyłając e-mail. Nie wahaj się skorzystać z pomocy.

TELEFON ZAUFANIA DLA DZIECI I MŁODZIEŻY

116 111

DZIECIĘCY TELEFON ZAUFANIA RZECZNIKA PRAW DZIECKA

800 12 12 12

DYŻURNET.PL

801 615 005

Informacje dla MŁODZIEŻY pozwalające zrozumieć zagrożenia występujące w cyberprzestrzeni oraz porady jak skuteczne stosować sposoby zabezpieczenia się przed tymi zagrożeniami:

Do najpopularniejszych zagrożeń w cyberprzestrzeni, z którymi może spotkać się każdy człowiek należą**:**

- ataki z użyciem szkodliwego oprogramowania (*malware*, wirusy, robaki, itp.),
- kradzieże tożsamości,
- kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych,
- blokowanie dostępu do usług,
- spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- ataki socjotechniczne (np. *phishing*, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję),
- Zagrożenia seksualne(cyberseks,sexting).

Sposoby zabezpieczenia się przed zagrożeniami:

- Zainstaluj i używaj oprogramowania przeciw wirusom i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym.
- Aktualizuj oprogramowanie oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie).
- Nie otwieraj plików nieznanego pochodzenia.
- Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
- Nie używaj niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony).
- Co jakiś czas skanuj komputer i sprawdzaj procesy sieciowe – jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłające twoje hasła i inne prywatne dane do sieci może się zainstalować na komputerze mimo dobrej ochrony – należy je wykryć i zlikwidować.
- Sprawdzaj pliki pobrane z Internetu za pomocą skanera.
- Staraj się nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
- Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich.
- Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu.
- Aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki.
- Pamiętaj o uruchomieniu firewalla.
- Wykonuj kopie zapasowe ważnych danych.
- Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.
- Nie przesyłaj za pomocą sieci komórkowej bądź internetu tekstów, zdjęć czy filmów nacechowanych seksualnie.

- Pamiętaj, że **sexsting** jest zjawiskiem niebezpiecznym. Dostęp do internetu i telefonów komórkowych, połączony z brakiem świadomości zagrożenia płynącego z pozornie nieszkodliwych działań, może prowadzić do kłopotów i nieszczęść.
  Młodzi ludzie bez oporów dzielą się bardzo intymnymi zdjęciami z innymi osobami. Nawet jeśli wydaje im się, że adresat jest osobą bliską oraz godną zaufania, materiały z łatwością mogą trafić w niepowołane ręce bądź zostać upublicznione. To wiąże się ze stresem, upokorzeniem, wstydem, nieprzyjemnościami, wyśmiewaniem i odrzuceniem przez rówieśników, co w skrajnych przypadkach kończy się depresją bądź próbami samobójczymi. Zdjęcia czy intymne filmiki są wykorzystywane do zemsty czy szantażu.

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych.