9 LUTY 2021 r.

DZIEŃ BEZPIECZNEGO INTERNETU

DZIAŁAJMY RAZEM!

DBI.PL

Dzień Bezpiecznego Internetu 2021 obchodzić będziemy 9 lutego

Od 2004 roku w 45 krajach na świecie, w tym również w Polsce, Dzień Bezpiecznego Internetu był dotychczas (luty 2021) obchodzony piętnastokrotnie. Został ustanowiony z inicjatywy Komisji Europejskiej w ramach programu "Safer Internet".

Chodzi głównie o to, by dzieci i młodzież nie były narażone na niebezpieczeństwa w trakcie korzystania z zasobów internetowych.

POZNAJ ZASADY BEZPIECZNEGO INTERNETU!

Co zrobić aby dostęp do internetu był bezpieczny:

- Aktualizuj oprogramowanie systemowe (Windows, Linuks, iOS),
- Stosuj silne hasła dostępu do systemu oraz sieci domowych,
- Nie udostępniaj „sąsiadom” swojej sieci Internet (WiFi).

Co zrobić aby korzystanie z internetu było bezpieczne:

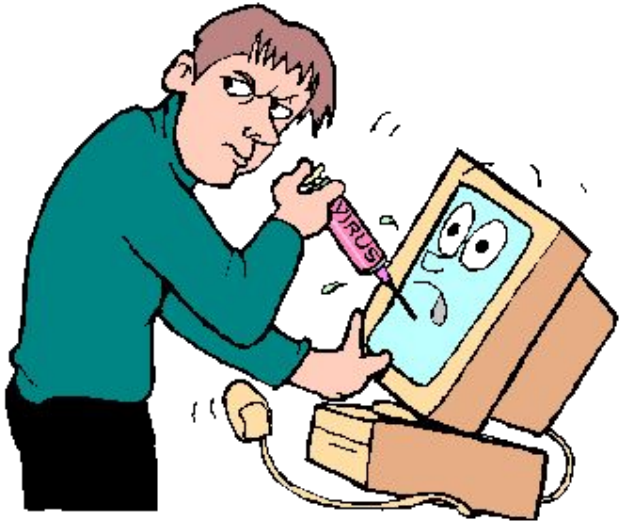
- Aktualizuj oprogramowanie antywirusowe,
- Pamiętaj treści zamieszczone w sieci (zdjęcia, posty, komentarze) nigdy nie zostaną usunięte,
- Nie otwieraj nieznanych załączników w wiadomościach e-mail,
- Nie udostępniaj swoich danych w Internecie.

Co zrobić aby Twoje dziecko było bezpieczne w sieci:

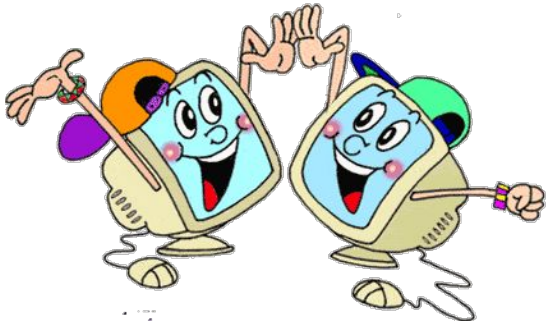
- Rozważ zainstalowanie oprogramowania do kontroli rodzicielskiej,
- Nie pozostawiaj dziecka samego w sieci – pokaż mu dobre strony Internetu, pokaż jak może rozwijać swoje pasje, ostrzeż o zagrożeniach które mogą z niego płynąć,
- Jeśli masz wątpliwości możesz zgłosić je wyspecjalizowanym komórkom do Walki z Cyberprzestępczością znajdującym się w Komendach Wojewódzkich Policji (Komendzie Stołecznej Policji).

Najczęstsze zagrożenia:

- **Złośliwe oprogramowanie,**
  Instalacja złośliwego oprogramowania może doprowadzić do przejęcia Twojego komputera przez Cyberprzestępców, a w efekcie może być narzędziem do popełniania przestępstw internetowych.
- **Hejt,**
  Często wystawianie złych wręcz kompromitujących komentarzy to rozrywka dla młodego internauty. Niestety Hejt w sieci może być przyczyną samobójstwa.



- **Niebezpieczne gry,**
  Bardzo często Internet dla dziecka to „wypełniacz” czasu, w którym znajdzie wiele wyzwań/zadań. Niektóre z nich, mogą doprowadzić do samookaleczenia lub śmierci.
- **Kontakt dziecka z treściami pornograficznymi** (kontakt z pedofilami), uwodzenie w Internecie (child grooming).
  Działania podejmowane przez osoby w sieci w celu zaprzyjaźnienia się i nawiązania więzi emocjonalnej z dzieckiem, tak aby w późniejszym czasie zmniejszyć jego opory przed kontaktem w świecie rzeczywistym, który w efekcie może doprowadzić do seksualnego wykorzystania.



- **Materiały epatujące p**
  W Internecie można znaleźć filmy/zdjęcia za przemoc lub nawołujące do nienawiści. Młodzi mogą brać zły przykład z takich informacji i je do świata realnego.
- **Uzależnienie od**
  Gdy dziecko zbyt długo korzysta z Internetu, a pozbaw dostępu do sieci powoduje złość i rozdrażnienie mo to pierwsza oznaka uzależnienia. Warto wówczas nawiązać kontakt ze specjalistą zanim stracisz kontakt z dzieckiem.
- **Kontakt z internetowymi oszustami**
  W sieci Internet pojawiają się różnego rodzaju ogłoszenia część z nich to po prostu próba oszustwa. Pamiętaj, aby przed zakupem w sieci dokładnie zweryfikować sprzedawcę, można np. poczytać opinie o sklepie. Przy zakupie droższych rzeczy warto dołożyć parę złotych i dokonać zakupu za pobraniem. Wówczas przy odbiorze towaru, jeszcze przy dostawcy możesz otworzyć paczkę i sprawdzić czy towar jest zgodny z zamówieniem. Jeżeli nie masz prawo odmówić jego przyjęcia.

DZIEŃ BEZPIECZNEGO INTERNETU

KORZYSTAJ Z OPROGRAMOWANIA ANTYWIRUSOWEGO

PAMIĘTAJ, ŻE OSOBA PO DRUGIEJ STRONIE NIE ZAWSZE JEST TYM, ZA KOGO SIĘ PODAJE

NIE PODAWAJ W SIECI DANYCH OSOBOWYCH I HASEŁ

NIE WYSYŁAJ ZDJĘĆ NIEZNAJOMYM

GDY COŚ CIĘ NIEPOKOI, SKONSULTUJ TO Z RODZICAMI

USUWAJ PODEJRZANE WIADOMOŚCI E-MAIL

OSTROŻNIE POBIERAJ PLIKI

Wirusy komputerowe jak im zapobiegać

8 rad ekspertów – ochrona komputera przed wirusami

✅ **Chroń wszystkie swoje urządzenia i usługi**

Urządzenia, z których korzystasz do pracy z danymi firmowymi, muszą być koniecznie chronione dobrym rozwiązaniem antywirusowym. Nieuwaga przy wymianie danych z innym użytkownikiem może skutkować dostaniem się danych w niepowołane ręce – aby tego uniknąć, koniecznie zadbaj o bezpieczny sposób ich przekazywania. Zadbaj o solidne, unikatowe hasła do sprzętów i programów, z których korzystasz.

✅ **Aktualizuj oprogramowanie!**

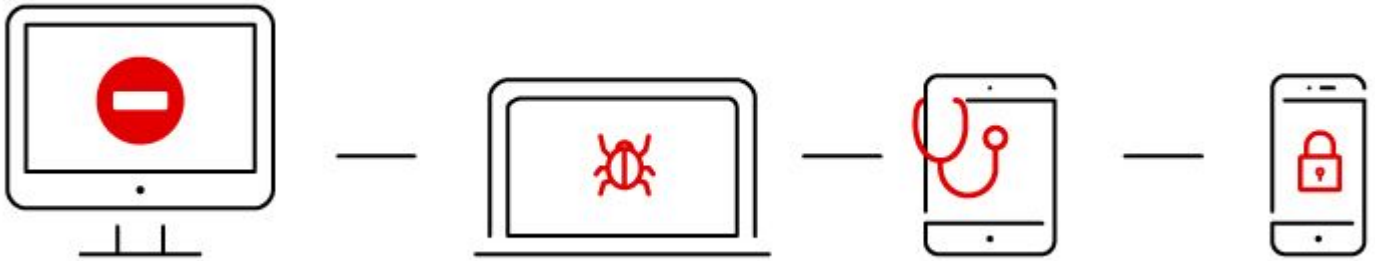
Nowe luki w zabezpieczeniach systemów i aplikacji pojawiają się bardzo często. Wykorzystują je przestępcy, którzy zdają sobie sprawę z beztroski użytkowników.

✔ Zadbaj o konfigurację sieci Wi-Fi

Ochrona urządzeń nic nie da, jeśli atakujący dostanie się do domowej sieci Wi-Fi. Ustaw silne hasło i wybierz szyfrowanie WPA2.

✔ Zadbaj o konfigurację domowego routera

Zmień domyślne hasło do zarządzania routerem. Zadbaj także o jego cykliczną aktualizację.



✔ Korzystaj z połączenia VPN w obcych sieciach

Połączenie VPN jest świetnym rozwiązaniem gdy musisz pracować w sieciach, nad którymi nie masz kontroli. Atakujący często tworzą własne sieci Wi-Fi, które podszywają się pod inne sieci (np. kawiarni, w której właśnie przebywasz).

✔ Blokuj urządzenie pod koniec pracy

Nie daj komuś szansy na podejrzenie zawartości ekranu swojego firmowego komputera. Pamiętaj, aby blokować swój sprzęt za każdym razem, kiedy się od niego oddalasz.

✔ Korzystaj ze sprzętu firmowego tylko do pracy

Aktywność prywatna powinna odbywać się z użyciem urządzeń prywatnych. Nie korzystaj z urządzeń i usług niezaaprobowany dział IT Twojej firmy.

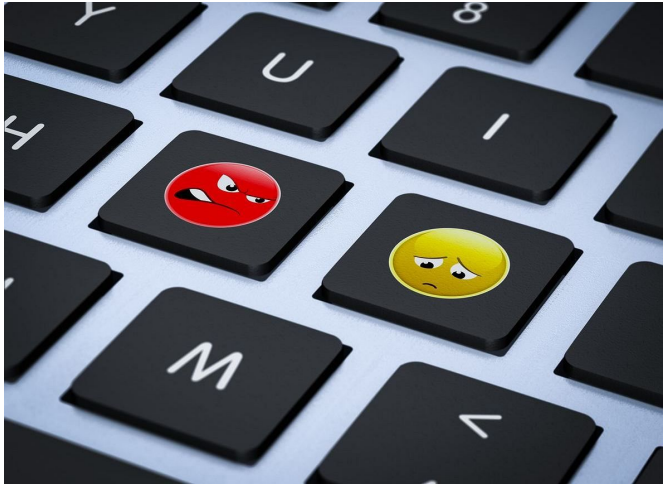
✔ Bądź czujny podczas home office

Na poczcie firmowej i stronach także mogą się pojawiać cyberzagrożenia. Podczas pracy w systemie home office zwracaj szczególną uwagę na e-maile z linkami i załącznikami.

Cyberprzemoc

Cyberprzemoc to seria agresywnych zachowań, celowo i regularnie skierowanych przeciwko bezbronnej osobie. Cyberprzemoc określana jest jako współczesny rodzaj przemocy rówieśniczej. Najczęściej kojarzona jest z agresją słowną, ale może przyjmować także bardziej nieoczywiste formy

Cyberprzemoc ma najczęściej formę słowną – pojawia się np. w komentarzach, na memach czy nagraniach wideo. Może też być bardziej zawoalowana: polegać na wykluczeniu z grupy, manipulowaniu czy nienawiązywaniu relacji.



Jakie są formy cyberprzemocy?

Najczęstsze z nich to:

- publikowanie poniżających filmów lub zdjęć;
- publikowanie ośmieszających, wulgarnych, komentarzy i postów;
- włamania na konta serwisów społecznościowych;
- flood, czyli wiadomościami w komunikatorze, telefonami, SMSami
- podszywanie się pod inne osoby;
- wykluczanie z ineternetowych społeczności

O czym warto pamiętać?

1. Nawet pozornie niewinny żart może być rodzajem cyberprzemocy. Uważajmy na to, co piszemy.
2. Na niektóre formy cyberprzemocy grozi odpowiedzialność karna.
3. Na przemoc nie wolno odpowiadać tym samym.
   Jeśli czujesz, że sprawa Cię przerasta, skontaktuj się ze specjalistami lub odpowiednimi służbami.
4. Pamiętaj, że w serwisach społecznościowych wszelkie przejawy cyberprzemocy można zgłosić do administratorów (zgłoś nadużycie).
5. Gdy padasz ofiarą cyberprzemocy, zachowaj dowód: zrób zrzut ekranu, zachowaj SMSy lub wiadomości.
6. Jako świadek cyberprzemocy – reaguj i sprzeciwiaj się.

Odpowiedzialność karna za hejt

Choć żaden z przepisów nie mówi konkretnie o hejcie, za zachowania, które mieszczą się w jego definicji, grożą konsekwencje prawne. Za zniesławienie i zniewagę w internecie można otrzymać karę grzywny lub usłyszeć wyrok ograniczenia lub pozbawienia wolności do roku. Za nawoływanie do nienawiści i dyskryminacji również grozi kara grzywny, ograniczenia wolności lub jej pozbawienia, ale do lat 2. Ofiara hejtu może również z własnej inicjatywy wnieść pozew o naruszenie jej dóbr osobistych przez hejtera.

Czym jest hejt i jak rozpoznać jego ofiary:

Hejt ("hate") z języka angielskiego oznacza "nienawiść", a słowem tym określamy jej szerzenie w internecie. Hejt może się przejawiać nie tylko za pomocą słów, ale i grafik (memów, gifów) czy filmów - w tych dwóch ostatnich przypadkach niestety łatwiej zapada w pamięć.

Hejt to pełne nienawiści działania, które przede wszystkim odnoszą się do Internetu. Hejt może być skierowany ku jednej osobie, przedstawicielom konkretnego narodu czy osobom
o innym światopoglądzie niż hejter.
Dosłownie każdy może stać się obiektem hejtu.

Przyczyny hejtu:

- chęć obrażenia innych,
- przekonanie o byciu osobą anonimową,
- zazdrość (na przykład w stosunku do osób, które osiągają sukcesy),
- zły nastrój, negatywne emocje, kumulację złego samopoczucia,
- istnienie stereotypów oraz uprzedzeń w stosunku do określonych grup społecznych,
- silne poglądy polityczne,
- niezadowolenie ze swojej sytuacji życiowej.

Konsekwencje hejtu

Choć samo dodanie pełnego nienawiści posta na Facebooku czy forum internetowym bądź udostępnienie takiej samemu sprawcy może wydawać się niegroźne, niesie za sobą ogromne konsekwencje w przypadku ofiar hejtu.
Obniża się jej poczucie własnej wartości, staje się mniej odporna na czytane w internecie treści i zaczyna wierzyć, że stawianie oporu nie ma sensu.

Poddawana hejtowi osoba często cierpi na bezsenność, żyje w ciągłym stresie, zaczyna bać się wyrażać własne zdanie w internecie. Może nawet dojść do izolowania się osobie poddanej internetowej agresji od reszty społeczeństwa, wystąpienia u niej nerwicy, depresji, a nawet prób samobójczych.

Jak bronić się przed hejtem?

Najprostszą i zarazem najtrudniejszą odpowiedzią jest: unikać czytania negatywnych opinii, a zwłaszcza odpowiadania na nie. Nie bez powodu karierę robi hasło: "nie karmić trolla" - odpowiedź na agresję jeszcze bardziej agresora podburza. To jednak dla hejtowanej i żyjącej w ciągłym napięciu osoby trudne zadanie - nie jest łatwo zignorować negatywne komentarze na swój temat.

Kolejnym wyjściem jest zgłoszenie pełnego hejtu wpisu administratorowi danej strony, który nie tylko może usunąć konkretny komentarz, ale zablokować konto danej osoby. Możliwość zgłaszania hejtu mają też często postronni użytkownicy.

Ważna jest również profilaktyka - prowadzonych jest wiele akcji społecznych, warsztatów z zakresu przemocy w internecie, skierowanych przede wszystkim do młodzieży. Jednym z takich projektów są Cybernauci, realizowani przez Fundację Nowoczesna Polska.


STOP
HATE