DZIEŃ BEZPIECZNEGO INTERNETU 2021

Data publikacji 09.02.2021

Dzisiaj obchodzimy Dzień Bezpiecznego Internetu. Podobnie jak w zeszłym roku, hasłem przewodnim Dnia Bezpiecznego Internetu (DBI) jest #DziałamyRazem. Z inicjatywy Komisji Europejskiej obchody DBI początkowo odbywały się jedynie w Europie, jednak od kilku lat swoim zasięgiem docierają do państw z całego świata. Głównym zadaniem organizowania takiego dnia było i jest propagowanie działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych, zaznajomienie rodziców, nauczycieli i wychowawców z problematyką bezpieczeństwa online oraz promocją pozytywnego wykorzystywania Internetu.

Organizacją tego wydarzenia w Polsce zajmuje się Polskie Centrum Programu Safer Internet, w skład którego wchodzą Państwowy Instytut Badawczy NASK oraz Fundacja Dajemy Dzieciom Siłę. Organizatorzy poprzez to wydarzenie zachęcają szkoły, biblioteki, organizacje pozarządowe, firmy i inne instytucje do realizowania lokalnych inicjatyw na rzecz młodych internautów.

Internetem czy też siecią nazywamy ogólnoświatowy system połączeń między komputerami. Jego początki sięgają końca lat 60. XX wieku, natomiast w Polsce zagościł dopiero w latach 90. Jest to sukces rozwoju technologicznego cywilizacji, a także odpowiedz na potrzeby współczesnego człowieka[1]. W obecnych czasach większość ludzi nie wyobraża sobie życia bez korzystania z Internetu, służy on nie tylko do pracy, nauki czy zabawy, ale również do zdalnego wykonywania codziennych domowych czynności. Niestety równie często wykorzystywany jest przez przestępców do dokonywania kradzieży czy oszustw. Dlatego warto zastosować się do kilku poniższych wskazówek i rad.

♦ **Co zrobić, aby dostęp do Internetu był bezpieczny:**

- aktualizuj oprogramowanie systemowe (Windows, Linuks, iOS),
- stosuj silne hasła dostępu do systemu oraz sieci domowych. Do podstawowych zasad tworzenia hasła użyj kombinacji dużych i małych liter, cyfr i znaków specjalnych, o długości powyżej 8-10 znaków. Ponadto, hasło nie powinno wiązać się z naszymi danymi: imieniem, nazwiskiem, pseudonimem (ksywą), datą urodzenia. Nie powinno też zawierać nazw z bliższego otoczenia, takich jak: miejsce pracy, imię pupila, danych dzieci/męża. Używaj potwierdzenia wpisanego hasła,
- nie udostępniaj „sąsiadom" swojej sieci Internet (Wi-Fi), zabezpiecz ją silnym hasłem, a jeżeli pozwalamy innym użytkownikom na podłączenie się do naszej sieci, ograniczmy możliwość podłączania zewnętrznych nośników.

♦ **Co zrobić, aby korzystanie z Internetu było bezpieczne:**

- aktualizuj oprogramowanie antywirusowe kupione wyłącznie z legalnego źródła,
- pamiętaj, że treści zamieszczone w sieci (zdjęcia, posty, komentarze) nigdy nie zostaną usunięte,
- nie otwieraj załączników w nieznanych lub budzących wątpliwość co do nadawcy wiadomościach e-mail,
- nie przesyłaj mailem danych osobistych. W żadnym wypadku nie wypełniaj danymi osobistymi formularzy zawartych w wiadomości e-mailowej,
- nie należy otwierać hiperłącza bezpośrednio otrzymanego mailem, szczególnie jeżeli nie znamy nadawcy wiadomości,
- pamiętaj, że banki i instytucje finansowe stosują protokół HTTPS tam, gdzie konieczne jest zalogowanie się do systemu. Dlatego, zwracaj uwagę na adres strony www, która rozpoczyna się od wyrażenia „https://", a nie „http://". Jeżeli strona logowania nie zawiera w adresie nazwy protokołu HTTPS, zgłoś to do banku, a przede wszystkim nie podawaj żadnych danych,
- nie podawaj swoich danych do logowania osobom trzecim.

♦ **Jak robić bezpieczne zakupy w sieci:**

- nie udostępniaj numerów PIN oraz haseł do bankowości elektronicznej,
- robiąc zakupy w sieci uważaj na wyjątkowe okazje i promocje,
- zawsze sprawdzaj wiarygodność sprzedawcy i opinie na jego temat,
- korzystaj z komputera lub urządzenia mobilne wyposażonego w oprogramowanie antywirusowe,
- sprawdzaj miesięczne wyciągi swoich płatności z karty, BLIK. W przypadku podejrzanych transakcji skontaktuj się ze swoim bankiem i zablokuj kartę,
- zawsze sprawdzaj, czy adres strony banku posiada tzw. kłódeczkę (protokół HTTPS),
- unikaj publicznych sieci Wi-Fi.

♦ **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, ale ostrzeż je także o zagrożeniach, które mogą z niego płynąć,
- rozmawiaj z dzieckiem na temat:
  - zasad poruszania się w Internecie,
  - zachowania się w różnych sytuacjach,
  - zapewnij, że z każdym problemem może zwrócić się do rodziców, pedagoga w szkole czy policjanta – osób, które wiedzą jak postąpić, gdy zagrożone jest bezpieczeństwo,
- jeśli masz wątpliwości dotyczące treści w sieci, możesz je zgłosić wyspecjalizowanym komórkom *do walki z cyberprzestępczością*, znajdującym się w komendach wojewódzkich/Komendzie Stołecznej Policji,
- blokuj niewłaściwe twoim zdaniem strony,
- osoby poznane w sieci mogą podawać się za kogoś innego (częsta zmiana twarzy, wieku i miejscowości),
- nie należy się spotykaj z osobami poznanymi w Internecie.

♦ **Najczęstsze zagrożenia czyhające na twoje dziecko w sieci:**

- **trolling**

  Celowe zaognianie wymiany zdań między użytkownikami serwisu internetowego (dyskusyjnego, społecznościowego). W efekcie dochodzi do odejścia od pierwotnego tematu rozmowy w kierunku obelg, gróźb, następuje eskalacja agresji,

- **flaming**

Celowe zaognianie wymiany zdań między użytkownikami serwisu internetowego (dyskusyjnego, społecznościowego). Taką dyskusję należy niezwłocznie zgłosić moderatorom w celu zablokowania, usunięcia. W przypadku wyczerpania znamion czynu zabronionego należy zabezpieczyć treść dyskusji oraz powiadomić organy ścigany,

- **hejt**

  Hejt – oznacza nienawiść, czyli zjawisko społeczne o charakterze poniżającym obserwowane w środowisku Internetu[2]. Często wystawianie złych, wręcz kompromitujących komentarzy to rozrywka dla młodego internauty. Niestety, hejt w sieci w skrajnych przypadkach może doprowadzić młodego człowieka do zaniżonej oceny, depresji, a nawet samobójstwa,

- **treści pro-ana**

  Pro-ana to termin odnoszący się do promowania anoreksji jako świadomego wyboru i pożądanego stylu życia. Ruch pro-ana jest bardzo aktywny w Internecie i szczególnie popularny wśród dziewcząt. Uczestników tego ruchu nazywa się porcelanowymi motylami.

  Przejawem działań ruchu pro-ana są bardzo często blogi dziewcząt, które opisują swoją obsesyjną walkę o nienaganną figurę. Hasło przewodnie brzmi "Jeśli nie jesteś szczupła, to znaczy, że nie jesteś atrakcyjna".

  Uczestnicy tego ruchu komunikują się między sobą, tworzą grupy zamknięte i fora, na których wymieniają się doświadczeniami. Doradzają sobie jak ukrywać przed rodzicami fakt niejedzenia, wymieniają dietami 500 kalorii bądź maskowania spadku wagi.

  Ana pochodzi od słowa anoreksja, czyli patologicznego zaburzenia polegającego na obsesyjnym głodzeniu się. Celem takiego działania jest chorobliwie wychudzona sylwetka. Wiąże się to z bardzo wieloma problemami związanymi z niedożywieniem. W skrajnych przypadkach może prowadzić do śmierci[3],

- **child grooming**

  Działania podejmowane w celu zaprzyjaźnienia się i nawiązania więzi emocjonalnej z dzieckiem, aby zmniejszyć jego opory i później wykorzystać seksualnie. Jest to również mechanizm używany w celu nakłonienia dziecka do prostytucji czy udziału w pornografii dziecięcej,

- **cyberprostytucja**

  Nazywana jest również wirtualną prostytucją i ma na celu uzyskanie korzyści materialnych za udostępnianie i przekazywanie materiałów (zdjęć bądź nagrań pornograficznych) o charakterze erotycznym lub pornograficznym z własnym udziałem,

- **sextorion**

  Szantaż internetowy opierający się na groźbie ujawnienia nagich, kompromitujących zdjęć. Sprawca żąda od swojej ofiary kolejnych fotografii, pieniędzy lub chce ją wykorzystać,

- **patostreamy**

  Transmisja na żywo, prowadzona w serwisach internetowych (np. YouTube), w trakcie której prezentowane są liczne zachowania powszechnie uznawane za będące dewiacjami społecznymi, zwłaszcza takie jak: libacje alkoholowe, wulgaryzmy, przemoc domowa. Wobec autorów patostreamów, w których aktywności dostrzeżono czyny zabronione, podejmowane są działania zmierzające do pociągania ich do odpowiedzialności prawnej,

- **ksenofobia**

  Może dotyczyć negatywnych zachowań wobec obcokrajowców, osób z innego kręgu kulturowego, innego wyznania, rasy, orientacji seksualnej,

- **kradzież tożsamości**

  Wykorzystywanie identyfikujących danych personalnych, np. numeru karty kredytowej, jako narzędzia do popełnienia innych przestępstw.

- **uzależnienie od Internetu**

Gdy dziecko zbyt długo korzysta z Internetu, a pozbawienie go dostępu do sieci powoduje złość i rozdrażnienie, może być to pierwsza oznaka uzależnienia. Warto wówczas nawiązać kontakt ze specjalistą, zanim straci się kontakt z dzieckiem,

♦ **Najczęstsze zagrożenia czyhające na wszystkich użytkowników sieci:**

- **phishing**

  Podszywanie się m.in. pod inna osobę, firmy kurierskie, urzędy administracji, operatorów telekomunikacyjnych, czy nawet naszych znajomych w celu wyłudzenia poufnych informacji, takich jak nasze dane do logowania np. do kont bankowych lub używanych przez nas kont społecznościowych, czy systemów biznesowych. Dzieje się tak poprzez wysyłanie fałszywych e-maili lub przekierowywanie na fałszywe strony internetowe, gdyż są one łudząco podobne do prawdziwych stron banków, serwisów aukcyjnych, legalnych organizacji czy agencji rządowych. Zazwyczaj komunikaty zawierają informację o rzekomym zdezaktywowaniu konta i konieczności jego reaktywowania przez odnośnik znajdujący się w e-mailu. Celem oszusta najczęściej jest wyłudzenie informacji o danych do logowania, szczegółów kart kredytowych,

- **Malware, „robaki" i pharming**

  Szkodliwy typ oprogramowania, który ma na celu potajemnie uzyskać dostęp do urządzenia bez wiedzy użytkownika. Do takiego szkodliwego oprogramowania zalicza się oczywiście tzw. wirusy, robaki, konie trojańskie, oprogramowanie szpiegujące czy rejestratory klawiszy. „Robaki" przedostają się do naszego komputera jako samodzielne nośniki i w ramach wszystkich dostępnych nam sieci replikują się. Dodatkowo mogą samodzielnie niszczyć pliki czy wysyłać pocztę spam. Oszuści najczęściej stosują w tym celu zainfekowane witryny internetowe, w opisie zawierające chwytliwe hasła lub fałszywe wiadomości e-mail. Trudniejszą do wykrycia i niebezpieczniejszą dla użytkownika formą phishingu jest tzw. pharming. W tym przypadku odwiedzający prawdziwą stronę np. swojego banku, są przekierowywani na podszywające się pod nią strony internetowe, które instalują na ich urządzeniach złośliwe oprogramowanie lub zabierają dane osobowe, hasła, dane do kont bankowych, które otrzymują przestępcy.

Pamiętaj, że:

- Internet może dać wiele dobrego, pod warunkiem, że potrafimy z niego właściwie korzystać,
- w sieci nie jesteśmy anonimowi (niezależnie od wieku),
- wszystko co piszemy, publikujemy w sieci, pozostaje na długi czas – dlatego, informacje, które umieszczamy powinny być przemyślane,
- komentarze, które umieszczamy na danych stronach, świadczą o nas. Dlatego, tak jak w życiu codziennym odnośmy się do innych z szacunkiem, bez wyzwisk czy zastraszania.

Internet tworzą ludzie, w tym my. Dlatego pamiętajmy, jakim chcielibyśmy go zastać i dbajmy o wspólne bezpieczeństwo w cyberprzestrzeni.

Przydatne linki:

Dzień Bezpiecznego Internetu ►

https://dyzurnet.pl/ - Dyżur.net

https://dyzurnet.pl/formularz/?pl - zgłaszanie nielegalnych treści,

http://www.saferinternet.pl/ - bezpieczeństwo dzieci online,

800 100 100 - telefon dla nauczycieli i rodziców.

---

[1]Źródło: www.wikipedia.org.pl

[2] Źródło: www.wikipedia.org

[3] https://www.sferis.pl/blog/zagrozenia-internetowe/

(Biuro Prewencji KGP)