KOMENDA POWIATOWA POLICJI W RADOMSKU

http://radomsko.policja.gov.pl/era/informacje/57096,DZIEN-BEZPIECZNEGO-INTERNETU.html
2023-06-06, 11:51

DZIEŃ BEZPIECZNEGO INTERNETU

9 lutego 2021 roku obchodzimy Dzień Bezpiecznego Internetu. Głównym celem DBI jest inicjowanie i propagowanie działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych, zaznajomienie rodziców, nauczycieli i opiekunów z problematyką bezpieczeństwa online oraz promocja pozytywnego wykorzystywania Internetu. Ideą DBI jest podkreślanie siły współdziałania w dbaniu o cyfrowe bezpieczeństwo, zarówno na poziomie międzynarodowym, jak również lokalnym.

Policyjny profilaktyk społeczny - mł. asp. Agnieszka Kropisz przygotowała pezentację multimedialną "Uzależnienie od Internetu", którą przekazała nauczycielom z Zespołu Szkół Drzewnych i Ochrony Środowiska w Radomsku. W prezentacji tej znajdziejmy podstawowe zagadnienia dotyczące zagrożeń płynących z niewłaściwego korzystania z Internetu, wskazówki - jak nie stać się ofiarą przemocy w sieci oraz jak korzystać z Internetu aby nie krzywdzić innych. Pedagodzy korzystają z prezentacji podczas zajęć on-line.

Jedną z aktywności, która od początku wymaga mądrego przewodnictwa, jest kontakt młodych ludzi z Internetem. Kiedyś – nowe zjawisko, dziś – codzienność, niezmiennie jednak wyzwanie dla rodziców i nauczycieli. Pomimo że odpowiednio dobrane treści internetowe mogą mieć pozytywny wpływ na rozwój dzieci, to zbyt wczesne i intensywne korzystanie z urządzeń elektronicznych może być dla nich szkodliwe.

Każdy użytkownik Internetu, przed rozpoczęciem korzystania z jego pozytywnych możliwości, powinien zapoznać się z zasadami bezpieczeństwa w sieci. W trosce o swoje dane należy pamiętać o istniejących zagrożeniach, które często wiążą się z pobieraniem oprogramowania z niepewnych serwerów czy odpowiadaniem na podejrzaną pocztę elektroniczną. Coraz częściej ofiarami internetowych przestępców możemy stać się na portalach społecznościowych, otwierając wiadomości od nieznanych użytkowników.

Chroniąc młode pokolenie przed zagrożeniami opiekunowie powinni pamiętać o:

- informowaniu dziecka o bezpiecznych i szkodliwych konsekwencjach używania Internetu
- kontrolowaniu stron, jakie przeglądają podopieczni
- możliwości zablokowania niewłaściwych zdaniem rodzica stron
- zgłoszeniu każdej niepokojącej treści do której mogą mieć dostęp dzieci

CYBERPRZEMOC I INNE FORMY AGRESJI W SIECI

Cyberprzemoc i agresja elektroniczna w Internecie to zjawiska – pośrednio lub bezpośrednio – dotyczące większości polskiej młodzieży.

Do podstawowych form cyberprzemocy zalicza się: wyzywanie, nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie w Internecie kompromitujących informacji, zdjęć, filmów, podszywanie się w

cyberprzestrzeni pod kogoś wbrew jego woli, a także wykluczanie z grupy rówieśniczej online (np. poprzez usunięcie kogoś z grona znajomych na portalu społecznościowym). Rozwój internetu oraz nieograniczona inwencja młodych ludzi powodują, że trudno wskazać wszystkie formy składające się na cyberprzemoc.

Ważną rolę w zwalczaniu agresji w cyberprzestrzeni pełnią rówieśnicy ofiar przestępstwa (tzw. świadkowie). Osoby te obserwują w Internecie wiele niepokojących sytuacji, np. obraźliwe i krzywdzące wpisy, publikacje lub komentarze. Trzeba też pamiętać o tym, że świadkowie agresji w sieci niekiedy – w efekcie celowego lub nierozważnego działania, a czasami w poczuciu strachu przed odrzuceniem przez grupę rówieśniczą – sami krzywdzą ofiarę. Dzieje się tak dlatego, że osoby te w wielu przypadkach bardzo naturalnie przechodzą z roli świadka w rolę agresora, komentując w określony sposób kompromitujące materiały, udostępniając je lub w jakiś inny sposób wyrażając aprobatę dla negatywnych treści (np. lajkują w serwisie Facebook).

Rodzicu pamiętaj!

- Rozmawiaj z dzieckiem na temat przemocy w sieci, hejtu i mowy nienawiści. Ustalcie wspólnie, w jaki sposób można reagować na te zjawiska.
- Rozmawiaj z dzieckiem o tym, co może być uznane za mowę nienawiści i dlaczego jest ona szkodliwa.
- Rozmawiaj z dzieckiem o tym, jak może reagować jako świadek cyberprzemocy. Poinformuj dziecko, w jaki sposób może pomóc ofierze agresji w sieci, jednocześnie nie narażając się samemu na przemoc.
- Dowiedz się, czy w szkole/placówce edukacyjnej, do której uczęszcza twoje dziecko, istnieją spisane procedury działania w przypadku wykrycia cyberprzemocy, a także czy są realizowane zajęcia profilaktyczne na ten temat.

FOMO – co to takiego?

FOMO (skrót od angielskiego wyrażenia fear of missing out) to uczucie lęku lub niepokoju przed wykluczeniem z jakiejś społeczności lub pominięciem. **FOMO** jest kolejnym zagrożeniem wynikającym z uzależnienia się od Internetu, portali społecznościowych, znajomości zainicjowanych w sieci. Wpływa również negatywnie na ogólną kondycję psychofizyczną i funkcjonowanie zarówno dorosłych, młodzieży, jak i dzieci w świecie.

Rodzicu pamiętaj!

- Obserwuj dziecko i zwróć szczególną uwagę na niepokojące zachowania (np. nadmierną agresję, odizolowanie, nadwrażliwość, utratę zainteresowania innymi aktywnościami).
- Staraj się dopytać dziecko o strony z których korzysta - jako coś godnego polecenia.
- Interesuj się tym, co podopieczni robią w czasie wolnym za pomocą komputera, sam wyjdź z inicjatywą rozmowy o tym, co ciekawi je w sieci, jakie zachowania napotyka, jakie teraz są trendy wśród młodszych użytkowników.
- Pamiętaj, że filtr kontroli rodzicielskiej pomaga ograniczyć kontakt dziecka z potencjalnie niebezpiecznymi dla niego stronami internetowymi, zawierającymi szkodliwe treści. Zwróć uwagę na to, że dzieci i młodzież rzadziej łączą się z internetem, korzystając z komputera stacjonarnego, a coraz częściej wykorzystują do tego celu urządzenia mobilne (np. smartfon, tablet, konsolę do gry).

Uświadamiaj dziecko

- Osoby poznane w sieci często mogą zmieniać twarze – nieznane w realnym świecie mogą podawać się za kogoś w innym wieku, z innej miejscowości
- Informacje, które udostępniamy o sobie na portalach, starajmy się szyfrować – zamiast nazwiska i imienia posługujmy się wymyślonym pseudonimem
- Wspieraj dzieci, pomagając im uodpornić się na obraz świata rozpowszechniany w Internecie, a w szczególności w mediach społecznościowych. Wyjaśnij, że bardzo często promuje się wyidealizowany świat i nierealne do osiągnięcia kanony piękna. Pomóż dzieciom i młodzieży stworzyć ich pozytywny wizerunek online. Nie zaniedbuj rozmów o tym, co warto, a czego nie warto ujawniać w sieci.
- Uczul dziecko na zagrożenia związane z korzystaniem z publicznych/ otwartych sieci Wi-Fi (hotspotów). Mogą one w nieograniczony sposób umożliwiać dostęp do szkodliwych treści i narażać najmłodszych użytkowników

sieci na wiele zagrożeń (np. na utratę danych i/lub nawiązanie niebezpiecznych kontaktów).

NIE KAŻDA WIADOMOŚĆ PRZECZYTANA W SIECI JEST PRAWDZIWA. INTERNET JEST KOPALNIĄ WIEDZY, A NIESTETY CZĘSTO TEŻ PRZESTRZENIĄ NIESPRAWDZONYCH I POTENCJALNIE SZKODLIWYCH DONIESIEŃ I PORAD, W KTÓREJ KAŻDY MOŻE PRZEDSTAWIĆ SIĘ JAKO EKSPERT OFERUJĄCY NAJLEPSZE ROZWIĄZANIE PROBLEMU.

PHISHING

Phisher (osoba odpowiedzialna za oszustwo) przeważnie rozpoczyna atak od rozesłania pocztą elektroniczną odpowiednio przygotowanych wiadomości.

W celu sprawdzenia wiarygodności linku można kliknąć prawym klawiszem myszy na frazę lub obrazek zawierające aktywny link i użyć funkcji kopiowania (w zależności od przeglądarki funkcja ta może brzmieć: „Kopiuj adres odnośnika", „Kopiuj łącze" lub „Kopiuj skrót"). Następnie można wkleić skopiowany link w bezpiecznym miejscu (np. programie Notatnik) i sprawdzić, jaką witrynę ten link otworzy. Niekiedy oszuści tworzą kopię strony, sprawiając, że wygląda ona identycznie jak oryginalna. Różnice mogą dotyczyć np. użycia innej litery w adresie www.

Bywa jednak i tak, że prawdziwa domena zostaje zamaskowana i użytkownicy widzą pozornie prawidłowy adres strony. Jeśli kliknie się w link, należy powstrzymać się przed podawaniem jakichkolwiek danych na stronie, zanim nie zweryfikuje się autentyczności witryny. Każda strona, która umożliwia logowanie, powinna posiadać adres zaczynający się od liter https. Na lewo od tego adresu przeglądarka wyświetla ikonę. Jeśli widać zamkniętą kłódkę (zielonego koloru), oznacza to, że strona posiada aktualny, szyfrowany certyfikat, potwierdzający jej autentyczność – innymi słowy, godny zaufania wystawca certyfikatu potwierdza, że dana strona jest tą, za którą się podaje.

ZAKUPY W INTERNECIE BEZ STRAT

Zamawiając i odbierając wybrany przedmiot zwróćmy uwagę na:

- podaną cenę produktu – gdy jest zbyt niska może to sugerować towar podrobiony
- przed zakupem zorientujmy się kim jest osoba sprzedająca - mając pozytywne opinie możemy być pewniejsi zakupu
- sprawdzajmy od kiedy konto sprzedawcy widnieje w serwisie i ilu użytkowników korzystało z jego usług
- za każdym razem czytajmy regulamin sklepu i opis aukcji serwisu z którego korzystamy
- domagajmy się potwierdzenia nadania przesyłki, nie wpłacajmy pieniędzy przed potwierdzeniem wygranej licytacji
- nie kasujmy korespondencji ze sprzedającym – w przypadku oszustwa jest ona dowodem potwierdzającym zakup
- sprawdzajmy otrzymają przesyłkę – jeśli towar jest niezgodny z zamówieniem poinformujmy o tym Policję.

"ROBAKI" I PHARMING

Sisi – Pogromczyni nudy! – odc. 7 – „Och, te wirusy… komputerowe" https://youtu.be/ljSlcM80j-c