

Źródło:

## Policja Podkarpacka

<http://www.podkarpacka.policja.gov.pl/rze/komendy-policji/kppnisko/komunikaty/97757,Bezpieczenstwo-mlodziezy-w-sieci.html>

Artykuł: 29.04.2020



# Bezpieczeństwo młodzieży w sieci

**W czasach masowego korzystania z komputerów, czy urządzeń mobilnych, codziennie stykamy się z siecią internetową. Dostęp do Internetu to już nie tylko gromadzenie i sprawdzanie danych wykorzystywanych do nauki. Internet to kopalnia możliwości i okno na świat, w którym obok wartościowych treści i odpowiedzialnych internautów, spotykamy drastyczne obrazy i agresywnych użytkowników. Na destrukcyjny wpływ internetowych treści szczególnie narażeni są młodzi ludzie. Pierwszym ogniwem, które może zadbać o to, aby do pociech nie trafiały nieadekwatne do ich wieku informacje, są opiekunowie. Dlatego warto wspomnieć o tym, jak robić to bezpiecznie.**

Internet otwiera przed młodym pokoleniem wiele możliwości, ale jednocześnie niesie ze sobą nowe wyzwania. Jego dynamiczny rozwój fascynuje i wciąga, zwłaszcza nastolatków. Dla młodych ludzi sieć nierzadko staje się pozornie prostym narzędziem do kształtowania swojego wizerunku, miejscem złudnie bezpiecznym, gwarantem anonimowości czy panaceum na ich problemy. Internet to kopalnia możliwości i okno na świat, w którym obok wartościowych treści i odpowiedzialnych internautów, spotykamy drastyczne obrazy i agresywnych użytkowników.

Na destrukcyjny wpływ internetowych treści szczególnie narażeni są młodzi ludzie. Młodzi ludzie są również narażeni na utratę kontroli nad korzystaniem z internetu, co może prowadzić do izolacji, a także zaniedbywania nauki, zdrowia czy kontaktów z rówieśnikami.

Lista niebezpieczeństw jest długa i zmienia się wraz z rozwojem nowych technologii. Dorosłym może się wydawać, że nie sposób nadążyć za rozwojem sieci, czy wirtualnymi nawykami i zainteresowaniami ich dzieci. Stąd potrzeba podnoszenia świadomości rodziców na ten temat, mówienia o nowych, niepokojących zjawiskach oraz o tym, jak najskuteczniej postępować w przypadku wirtualnych zagrożeń. Przekaz adresowany do dorosłych powinien być jednak wyważony – samo straszenie to nie metoda. Nie wolno zapominać, że sieć to medium, które

odgrywa ogromną rolę w życiu dzieci i może być przez nie z pożytkiem wykorzystywane. Ważne, żeby rodzice zrozumieli, że nie muszą być ekspertami w dziedzinie nowinek technologicznych i wirtualnych trendów, aby móc rozmawiać z najmłodszymi o ich aktywnościach online. Dorośli powinni towarzyszyć dzieciom w ich pierwszych internetowych krokach i uczyć je, że obecność oraz aktywne uczestnictwo w sieciowym życiu społecznym powinno być oparte na podstawowych, ponadczasowych wartościach, czyli m.in. na szacunku dla drugiego człowieka.

O tym, co powinno obudzić naszą czujność, informujemy opisując metody stosowane w cyberprzestrzeni.

### **Bezpieczeństwo dzieci w sieci**

Dostęp do Internetu to już nie tylko gromadzenie i sprawdzanie danych wykorzystywanych do nauki. Dzieci i młodzież poprzez sieć kontaktują się ze swoimi znajomymi, grają w gry dostępne na platformach, mając w ten sposób dostęp do treści, które nie zawsze skierowane są do nich. Pierwszym ogniwem, które może zadbać o to, aby do pociech nie trafiały nieadekwatne do ich wieku informacje, są opiekunowie. Chroniąc młode pokolenie przed zagrożeniami powinni oni 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

Jeśli jednak jako rodzice nie jesteśmy pewni, jak przestrzec dziecko przed ewentualnymi zagrożeniami, z którymi można się zetknąć w czasie korzystania z Internetu, warto nauczyć młodszych kilku prostych zasad, które mogą zaoszczędzić im nieprzyjemnych sytuacji. Prowadząc takie rozmowy zapewnimy dziecko, że z każdym problemem może zwrócić się do nas – jako opiekunów, ale także do pedagoga czy policjanta, czyli osób, które wiedzą jak postępować, gdy zagrożone jest bezpieczeństwo.

- Osoby poznane w sieci często mogą zmieniać twarze – nieznane w realnym świecie mogą podawać się za kogoś w innym wieku, z innej miejscowości
- Nie spotykajmy się z osobami poznanymi w Internecie
- Informacje, które udostępniamy o sobie na portalach, starajmy się szyfrować – zamiast nazwiska i imienia posługujmy się wymyślonym pseudonimem
- Starajmy się dopytać dziecko o strony z których korzysta - jako coś godnego polecenia
- Interesujmy się tym, co podopieczni robią w czasie wolnym za pomocą komputera, sami wychodźmy z inicjatywą rozmowy o tym, co ciekawi je w sieci, jakie zachowania napotyka, jakie teraz są trendy wśród młodszych użytkowników

### **Phishing**

- Phisher (osoba odpowiedzialna za oszustwo) przeważnie rozpoczyna atak od rozesłania pocztą elektroniczną odpowiednio przygotowanych wiadomości
- Otrzymywane informacje mają formę podobną do tych, które stosują banki, serwisy aukcyjne lub inne instytucje
- Zazwyczaj komunikaty zawierają informację o rzekomym zdezaktywowaniu konta i konieczności jego reaktywowania poprzez odnośnik znajdujący się w mailu
- Celem oszusta najczęściej jest wyłudzenie informacji o danych do logowania, szczególnie kart kredytowych

## **„Robaki” i pharming**

- Przestępcy do poznania poufnych danych wykorzystują złośliwe oprogramowanie, nazywane w zależności od formy: robakiem, koniem trojańskim (trojanem) lub wirusami
- „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
- Najczęściej oszuści stosują w tym celu zainfekowane witryny internetowe, w opisie zawierające chwytliwe hasła, lub fałszywe wiadomości e-mail
- Niebezpieczniejszą dla użytkownika oraz trudniejszą do wykrycia formą phishingu jest tzw. pharming - wpisujących prawidłowe adresy np. swojego banku, przekierowują na fałszywe strony internetowe, gdzie podając ponownie swoje dane, przekazujemy je przestępcy

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.

### **Serfując w sieci pamiętajmy, że:**

- należy regularnie uaktualniać system i oprogramowanie, które jest przez nas używane
- warto zaopatrzyć swój komputer w program antywirusowy, który ostrzeże nas przed niebezpieczeństwem
- nie należy otwierać hiperłączy bezpośrednio z otrzymanego e-maila, szczególnie jeśli nie znamy nadawcy wiadomości
- nie wolno przysyłać mailem żadnych danych osobowych - w żadnym wypadku nie wypełniamy danymi osobistymi formularzy zawartych w wiadomości e-mail
- banki i instytucje finansowe stosują protokół HTTPS tam, gdzie konieczne jest zalogowanie do systemu. adres strony WWW rozpoczyna się wtedy od wyrażenia 'https://', a nie 'http://'. (jeśli strona z logowaniem nie zawiera w adresie nazwy protokołu HTTPS, powinno się zgłosić to osobom z banku i nie podawać na niej żadnych danych)
- każde podejrzenia co do sfingowanych witryn należy jak najszybciej przekazać policjantom lub pracownikom danego banku odpowiedzialnym za jego funkcjonowanie w sieci.

Z uwagi na powszechny dostęp do komputera i urządzeń mobilnych uważajmy na to, komu pozwalamy korzystać z naszych kont i sprzętów. Nigdy nie należy podawać swoich danych do logowania osobom trzecim. Jeśli pozwalamy innym użytkownikom na podłączenie się do naszej sieci, ograniczajmy możliwość podłączania zewnętrznych nośników. Starajmy się regularnie wykonywać kopie bezpieczeństwa, a ważne dla nas pliki zapisywać na zewnętrznych nośnikach, odkładanych w niezagrożone miejsce. Stosując kilka prostych zasad możemy uniknąć stania się ofiarą internetowego przestępcy.

### **Pilnuj swoich haseł.**

- Tworzone przez nas hasło powinno mieć odpowiednią jakość, która coraz częściej jest kontrolowana przez system w którym się logujemy

- Do podstawowych zasad tworzenia hasła należy kombinacja małych i wielkich liter, cyfr i znaków specjalnych, o długości powyżej 8 – 10 znaków
- Używaj potwierdzenia wpisywanego hasła
- Kreowane hasła nie powinny wiązać się z naszymi danymi: imieniem, nazwiskiem, ksywą. Nie powinny też zawierać nazw z bliskiego nam otoczenia, jak miejsce pracy lub imię pupila
- Hasło powinno być unikalne dla każdego odwiedzanego przez na portalu. Dla bezpieczeństwa, co jakiś czas, warto zmienić szyk liter i znaków
- Nie powinniśmy także zapisywać ważnych haseł do kont w plikach dostępnych na komputerze
- Instalując router należy pamiętać o jego odpowiedniej konfiguracji (przy zakupie takiego sprzętu kierujemy się możliwością szyfrowania WPA czy WPA2 – nie ceną)

### **Zakupy w Internecie bez strat**

W okresach świątecznych często jako sposób zakupu prezentu wybieramy drogę internetową. Dostępność e-sklepów i aukcji na popularnych portalach z roku na rok wzrasta. Skracając czas, poświęcany na wędrówkach po galerii w poszukiwaniach potrzebnych nam rzeczy, korzystamy z prostszych metod zakupu. Niestety niejednokrotnie stajemy się wtedy łatwym celem dla cyberprzestępców. Dlatego zamawiając i otrzymując 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 czytamy regulamin sklepu i opis aukcji serwisu z którego korzystamy
- domagajmy się potwierdzenia nadania przesyłki, nie wpłacamy pieniędzy przed potwierdzeniem wygranej licytacji
- nie kasujemy korespondencji ze sprzedającym – w przypadku oszustwa jest ona dowodem potwierdzającym zakup
- sprawdzamy otrzymaną przesyłkę – jeśli towar jest niezgodny z zamówieniem poinformujemy o tym Policję. Zapłacenie za przedmiot i nie otrzymanie go to nic innego jak wyłudzenie czyli oszustwo. Kodeks Karny przewiduje za ten czyn karę nawet do 8 lat pozbawienia wolności

Internet może dać nam wiele dobrego - jeśli umiemy się nim posłużyć. Niezależnie od swojego wieku należy pamiętać, że w sieci nie jesteśmy anonimowi. Wszystko co piszemy i publikujemy zostaje w niej na długi czas. Dlatego umieszczane informacje powinny być przez nas przemyślane. Komentarze, które pozostawiamy na odwiedzanych stronach, powinny dobrze o nas świadczyć. Tak jak w życiu codziennym - odnośmy się do innych z szacunkiem, bez wyzwisk czy zastraszania. Mając świadomość, że to właśnie my tworzymy Internet pamiętajmy, jakim chcielibyśmy go zastać i dbajmy o wspólne bezpieczeństwo w cyberprzestrzeni.