SZKOLNA ENCYKLOPEDIA WIEDZY

BEZPIECZEŃSTWO W SIECI

Wstęp

Internet to medium, którego dynamiczny rozwój i potencjał potrafią wykorzystać przede wszystkim młodzi ludzie. Jest nieodłącznym elementem ich życia społecznego, codziennej aktywności i rozrywki. Dziś trudno wyobrazić sobie nastolatka, który potrafiłby obejść się bez nowych technologii. Do bezpiecznego korzystania z sieci trzeba się jednak odpowiednio wcześnie przygotować…

Przygodę z urządzeniami, które umożliwiają dostęp do sieci Internet rozpoczynają coraz młodsze dzieci. Już w pierwszej klasie szkoły podstawowej sporo uczniów ma za sobą wiele godzin spędzonych z komputerami, tabletami, telefonami komórkowymi, smartfonami i innymi urządzeniami rejestrującymi dźwięk bądź obraz. W czasach, w których dostęp do sieci jest powszechny, a przesyłanie danych łatwe i możliwe na wiele sposobów należy być świadomym skutków nieroztropnych działań.

Niniejsze opracowanie nie jest typową encyklopedią. Oprócz wyjaśnień haseł związanych z bezpieczeństwem w sieci znajdują się tutaj wskazówki i porady, których stosowanie pozwala minimalizować różnorodne zagrożenia internetowe. Na te zagrożenia narażeni są przede wszystkim użytkownicy Internetu, ale również sprzęt umożliwiający komunikację sieciową. Poznając coraz bardziej świat Internetu powinno się równocześnie uczyć zasad kultury w nim wymaganych. Kultura powinna być na pierwszym miejscu.

Netykieta - zbiór zasad dobrego wychowania obowiązującego w Internecie. Jest to elektroniczny savoir vivre, sieciowa etykieta. Za nieprzestrzeganie jej możemy np. otrzymać „bana” (zablokowanie dostępu) na liście dyskusyjnej bądź forum.

Oto podstawowe uogólnione zasady netykiety, o których należy pamiętać, korzystając z komputera i innych urządzeń przystosowanych do komunikacji sieciowej:

- Nie używaj komputera/urządzeń, aby szkodzić innym
- Nie zakłócaj pracy na komputerach/urządzeniach innych
- Nie zaglądaj bez pozwolenia do cudzych plików
- Nie używaj komputera/urządzeń do kradzieży
- Nie używaj komputera/urządzeń do podawania fałszywych informacji
- Nie używaj programów, za które nie zapłaciłeś
- Nie używaj zasobów cudzych komputerów/urządzeń bez autoryzacji
- Nie przywłaszczaj sobie efektów pracy intelektualnej innych
- Myśl o społecznych konsekwencjach programów, które piszesz
- Używaj komputera/urządzeń ostrożnie i z rozwagą

Oprócz zasad netykiety ważne, by mieć na uwadze poniższe punkty, gdy czatujesz, używasz komunikatora internetowego, czy też udzielasz się na forach dyskusyjnych:

1. Bądź dyskretny.

   Informacje, które publikujesz, stają się publiczne i widoczne dla wszystkich. Nie wstawiaj informacji lub obrazków, których nie chcesz udostępniać całemu światu. Uważaj – mogą zostać przekazane dalej!

2. Bądź anonimowy.

   Nie dziel się prywatnymi lub bardzo osobistymi informacjami. Nigdy nie zamieszczaj lub wysyłaj czegokolwiek, co może posłużyć do zlokalizowania Ciebie lub innej osoby (na przykład imienia i nazwiska, adresu e-mail, czy też adresu domowego lub numeru telefonu).

3. Zachowaj dystans.

   Nie organizuj spotkań z przypadkowymi osobami poznanymi w sieci. Jeśli już musisz, spotykaj się wyłącznie w bezpiecznych i publicznych miejscach, powiadom kogoś o swoich planach i przyprowadź ze sobą znajomego. Jeśli nie jesteś pełnoletni, poproś rodziców lub opiekunów o pozwolenie i weź ich ze sobą.

4. Bądź szczery.

   Możliwe, że kusi Cię udawanie kogoś, kim nie jesteś. Pamiętaj, że inni ludzie również mogą myśleć w ten sam sposób. Potrafią podawać się za kogoś, kim w rzeczywistości nie są.

5. Bądź uprzejmy.

   Nie wdawaj się w zbędne dyskusje z natrętnymi osobami. Jeśli ktoś Cię obraża, po prostu odejdź od komputera. Powiadom dorosłego lub administratora o danej osobie i jej zachowaniu. To ma być przede wszystkim zabawa, czyż nie?

6. Uważajcie na wirusy

   Nie otwieraj, nie odpowiadaj i nie przesyłaj dalej e-maili, czy też wiadomości z komunikatora, jeśli nie znasz osoby wysyłającej i nie sprawdziłeś zawartości programem antywirusowym. Może ona zawierać niebezpieczne oprogramowanie (takie jak spyware, czy wirusy), lub być obraźliwa.

7. Zachowaj bezpieczeństwo.

Używaj oprogramowania zabezpieczającego (np. skanerów antywirusowych). Upewnij się, że system operacyjny jest zaktualizowany i zabezpieczony na wypadek, gdyby e-mail nieumyślnie zainfekował komputer.

8. Zachowaj prywatność.

Nigdy nie udostępniaj haseł lub podpowiedzi do nich.

9. Bądź kreatywny.

Upewnij się, że Twoja tożsamość internetowa nie ujawnia żadnych osobistych informacji. Bądź kreatywny i wyjątkowy!

10. Uważaj.

Jeśli coś brzmi zbyt dobrze, żeby było prawdą, prawdopodobnie nią nie jest! Sprawdzaj fakty, jeśli czegoś nie jesteś pewny.

Definicje i opisy wybranych pojęć najczęściej stosowanych przez osoby aktywne internetowo. Wśród nich znajdują się przede wszystkim te, które są szczególnie ważne dla zrozumienia bezpieczeństwa w sieci i zjawiska cyberprzemocy.

Aplikacje mobilne – programy instalowane na urządzeniach przenośnych np. notebookach, tabletach, telefonach komórkowych, smartfonach. Aplikacje mobilne są szczególnie lubiane przez dzieci i młodzież, gdyż dają dostęp do gier, portali społecznościowych i muzyki. Bezpieczne korzystanie z tych programów wymaga dobrego rozeznania w tej kwestii, ze względu na to, iż łatwo naruszyć prywatność użytkownika (zbierane są dane osobowe, geolokalizacyjne) lub narazić go na niespodziewane wydatki.

Szczególnymi pułapkami są wyskakujące okienka lub linki do ofert z zakamuflowanymi opłatami. Ich kliknięcie może prowadzić do nieświadomego złożenia zamówienia i zgody na pobranie opłaty, o której użytkownik dowiaduje się dopiero po otrzymaniu rachunku.

Innymi przykrymi niespodziankami mogą być zakupy wewnątrz aplikacji, tzw. mikro płatności. Wiele programów reklamowanych jako bezpłatne, w szczególności gry, otwarcie kusi najmłodszych wirtualnymi zakupami. Często podczas korzystania z aplikacji, aby przejść do następnego poziomu lub korzystać z bardziej zaawansowanych funkcji gry wymagany jest zakup wirtualnych walut, żetonów czy punktów. Takie zakupy często nie wymagają przejścia przez standardowy proces zamawiania produktu i ostatecznie zabawa gratisową aplikacją może drogo kosztować,

szczególnie jeśli dane karty kredytowej rodzica lub opiekuna są połączone z kontem w sklepie, z którego korzysta dziecko. Koszty mogą być również dodawane do miesięcznego rachunku telefonicznego.

Blog - inaczej pamiętnik sieciowy. Rodzaj strony internetowej z chronologicznie uporządkowanymi (zazwyczaj osobistymi) wiadomościami napisanymi przez blogera (autora bloga). W większości przypadków możliwe jest dodawanie komentarzy do wpisów pojawiających się na danym blogu przez jego czytelników. Tradycyjne blogi składają się z treści pisanych, istnieją jednak również **fotoblogi** (blogi składające się głównie ze zdjęć), wideoblogi (stworzone z plików filmowych), **moblogi** (z treścią przesyłaną za pomocą urządzeń mobilnych) czy mikroblogi (składające się z krótkich treści do 160 znaków).
Blogosfera - określenie wszystkich blogów znajdujących się w sieci.

CAPTCHA *(Completely Automated Public Turing test to tell Computers and Humans Apart)* - technika zabezpieczająca strony internetowe (portale społecznościowe, fora dyskusyjne, blogi, itp.) przed przedostawaniem się do nich danych nie pochodzących od człowieka, lecz tworzonych automatycznie przez roboty internetowe.

Child grooming - działania podejmowane w celu zaprzyjaźnienia się i nawiązania więzi emocjonalnej z dzieckiem (małoletni poniżej lat 15). Potocznie poprzez *child grooming* rozumie się uwodzenie dzieci przez Internet.

Cookie (ciasteczko) - plik, w którym zapisane są preferencje użytkownika danej strony internetowej. Przy kolejnych wizytach strona otwierana jest zgodnie z danymi zawartmi w ciasteczku.

Cracker (z ang., dosłownie *łamacz*) – osoba zajmująca się łamaniem zabezpieczeń komputerowych (crackingiem).

Cyberprzemoc - przemoc z użyciem technologii informacyjnych i komunikacyjnych (głównie Internet oraz telefony komórkowe).

Cyberstalking - odmiana stalkingu, w której sprawca prześladuje swoją ofiarę przy użyciu komputera lub poprzez sieć komputerową i wewnątrz niej. Tego rodzaju prześladowanie może przybierać następujące formy:

- **prześladowanie przy użyciu poczty elektronicznej:** przesyłanie e-maili na konto pocztowe ofiary wbrew jej woli (tzw. spam), uniemożliwianie ofierze

korzystania ze skrzynki e-mailowej, rozsyłanie elektronicznych listów bez wiedzy ofiary za pośrednictwem jej konta e-mail,

- **prześladowanie w Internecie:** rozpowszechnianie w Internecie informacji, w tym także nieprawdziwych o ofierze i zdjęć ofiary wbrew jej woli, podszywanie się pod ofiarę na czatach, listach dyskusyjnych, przesyłanie wiadomości, komunikowanie się z ofiarą poprzez komunikatory,
- **atakowanie komputera ofiary:** włamywanie się do komputera ofiary, umyślne i podstępne zawirusowywanie komputera ofiary, instalowanie w komputerze ofiary programów szpiegujących i koni trojańskich, niszczenie danych zapisanych na twardych dyskach komputera ofiary.

Czat (chat) - usługa internetowa umożliwiająca komunikację wielu osób korzystających z czata w tzw. pokojach. Czatownicy (użytkownicy czatu) mogą prowadzić rozmowę prywatną z jedną osobą lub rozmowę publiczną, widoczną dla wszystkich osób, które czatują (korzystają z czatu) w danym momencie.

Emotikona (uśmieszek, smiley, buźka) - symboliczny wyraz nastroju przedstawiony w postaci ciągu znaków, przypominających ludzką twarz obróconą o 90° w kierunku przeciwnym do wskazówek zegara, używany przez internautów.

Flame - obelga przysyłana przez uczestników kłótni internetowej.

Flamer - osoba biorąca udział w kłótni internetowej.

Flog - fałszywy blog, stworzony przez ludzi opłacanych przez firmy, chcące wypromować swoje produkty czy usługi.

Forum dyskusyjne - forma grupy dyskusyjnej w postaci strony internetowej, na której użytkownicy forum mogą wymieniać się spostrzeżeniami i informacjami na dany temat.

Grupa dyskusyjna - forma rozmowy odbywająca się w internecie, nie odbywająca się w czasie rzeczywistym.

Haker (ang. *hacker*) – osoba włamująca się do sieci i systemów komputerowych, posiadająca bardzo duże, praktyczne umiejętności informatyczne (lub elektroniczne).

Kłótnia internetowa (flame war, flaming) - inaczej nazywana wojną na obelgi. Kłótnia w środowisku internetowym (najczęściej w grupach, listach lub forach dyskusyjnych), do której dochodzi zazwyczaj przy różnicy zdań dwu lub więcej internautów. Nie liczą się w niej argumenty ani zasady netykiety, jej celem jest jedynie wzajemne znieważanie się osób biorących w niej udział. Czasami mianem kłótni internetowej określa się również długie dyskusje internautów o przeciwnych poglądach, w których nie pojawiają sie obelgi, a konkretna argumentacja.

Komunikator internetowy - program internetowy umożliwiający przesyłanie komunikatów w czasie rzeczywistym pomiędzy dwoma (lub więcej) komputerami/urządzeniami poprzez sieć komputerową.

K**ontrola rodzicielska –** program służący do blokowania dostępu do części witryn (pornograficznych, propagujących przemoc, narkotyki, zawierających wulgaryzmy) lub niektórych usług, takich jak komunikatory, programy p2p. Nowsze systemy operacyjne komputerów, tabletów, smartfonów zawierają już kontrolę rodzicielską, bądź bardzo łatwo można ją doinstalować.

Lista dyskusyjna - forma grupy dyskusyjnej, w której osoby zapisane do listy otrzymują automatycznie rozsyłane e-maile dotyczące wybranej tematyki.

Łańcuszki internetowe - forma spamu, w którym zawarte jest polecenie lub prośba o przesłanie wiadomości do jak największej liczby internautów. Przybierają różną formę, od prośby o pomoc i łańcuszków szczęścia po ostrzeżenia o wirusach komputerowych czy szantaż.

Poczta elektroniczna (e-mail) - usługa internetowa, służąca do przesyłania wiadomości tekstowych (e-maili, listów elektronicznych).

Portal internetowy - internetowy serwis składający się z tematycznie różnorodnych informacji, skierowany do szerokiego grona odbiorców; często wzbogacony wyszukiwarką internetową, czatem, pocztą elektroniczną czy działem aktualnych wiadomości, itp.

Portal społecznościowy - interaktywna witryna internetowa, współtworzona przez użytkowników portalu. Służy głównie do komunikacji poprzez czaty, komunikatory, blogi czy fora.

Wśród portali możemy wyróżnić tematyczne lub skierowane do konkretnej grupy społecznej, portale ogólne, towarzyskie czy randkowe, mogą być przeznaczone do publikowania zdjęć lub plików wideo internautów, umożliwiać komentowanie i wyrażanie opinii na dany temat, itp. Konta na portalach społecznościowych mogą samodzielnie zakładać osoby, które ukończyły 13 lat, w przeciwnym razie powinny mieć zgodę rodziców lub prawnych opiekunów.

Sexting - wysyłanie wiadomości o zabarwieniu seksualnym przy pomocy telefonu komórkowego do innych użytkowników telefonów komórkowych bądź umieszczanie ich na stronach internetowych lub portalach społecznościowych.

Spam - wiadomości elektroniczne, zazwyczaj będące reklamą lub niepotrzebnymi treściami przesyłanymi przez prywatnego użytkownika do wielu internautów, najczęściej niechciane przez odbiorców.

Spim - spam rozsyłany za pośrednictwem komunikatorów internetowych.

Splog (spam blog) - blog stworzony przez robota internetowego zawierający przypadkowe, niezwiązane ze sobą treści. Służy do fałszywego pozycjonowania stron.

Trollowanie (trolling) - obrażanie i ośmieszanie pewnej grupy ludzi bądź innego użytkownika w środowisku internetowym (zazwyczaj w miejscach, gdzie prowadzone są dyskusje - fora dyskusyjne czy czaty) lub celowe poruszanie kontrowersyjnych tematów, w celu sprowokowania kłótni internetowej.

Trollowanie pochodzi od zwrotu Trolling for fish, który oznacza łowienie ryb na haczyk; wypowiedzi internetowego trolla (osoby trollującej) mają na celu wciągnąć innych w bezsensowną dysusję. Internauci często używają wyrażenia "nie karmić trolla", by reszta użytkowników nie odpowiadała na tego typu zachowanie.

Transfer danych – jedna z podstawowych możliwości komputerów i telefonów komórkowych. Niewyłącznie transferu danych w telefonie komórkowym w niektórych sytuacjach (przebywanie za granicą lub w jej pobliżu) najczęściej prowadzi do gigantycznych opłat związanych z roamingiem.

Wortal - portal internetowy, który publikuje informacje z jednej dziedziny lub z dziedzin tematycznie pokrewnych.

XXX - określenie strony internetowej zawierającej treści pornograficzne.

Zapora sieciowa (firewall) - forma zabezpieczenia sieci i systemów przed niepowołanym dostępem do komputera lub przed napływem niechcianych danych.

Złośliwe oprogramowanie (**malware**) - różne aplikacje i skrypty, które mają szkodliwe i przestępcze bądź złośliwe działanie w stosunku do użytkowników komputerów. Warto podkreślić tutaj, że jest to głównie problem dotykający tych wszystkich komputerów/urządzeń, które pracują w środowisku Microsoft Windows. Przykłady złośliwego oprogramowania:

- wirusy - programy, czy też fragmenty wrogiego wykonalnego kodu, który się sam dołącza, bądź zamienia na inny program w celu reprodukcji. Robi to bez zgody użytkownika,

- robaki - podobne do wirusów, rozmnażają się jedynie za pośrednictwem sieci. Od wirusów różnią się tym, że nie potrzebują programu do żywienia. Najczęściej powielają się one przez pocztę elektroniczną,

- wabbity - programy rezydentne, który nie powielają się przez sieć. Wynik działania takich programów to jedna operacja. Przykładem może być powielenie tego samego pliku aż do wyczerpania zasobów pamięci komputera,

- trojany – programy, które nie rozmnażają się tak jak wirusy, ale ich działanie jest równie szkodliwe dla użytkownika. Trojan potrafi ukryć się pod nazwą lub częścią pliku pomocnego dla użytkownika. Potrafi on wykonać takie operacje tle, które są szkodliwe dla użytkownika. Z pomocą trojana otwiera się port w komputerze, przez który haker może dokonać włamania,

- backdoor – program, który przejmuje kontrolę nad zainfekowanym komputerem i w ten sposób umożliwia wykonanie na nim różnych czynności administracyjnych, takich jak usuwanie i zapis danych. Backdoor podszywa się pod pliki i programy, które są najczęściej używane. Haker ma możliwość administrowania systemem przez Internet i dzieje się to wbrew woli i wiedzy użytkownika,

- programy szpiegujące (spyware) - zbierają informacje o osobie fizycznej bądź prawnej bez jej wiedzy. Szczególnie interesują się informacjami o odwiedzanych witrynach, hasłach dostępowych, numerach kart płatniczych, adresach e-mail. Często występują one jako dodatkowe i ukryte komponenty większego programu. Są oporne na usuwanie i jakąkolwiek ingerencję ze strony użytkownika. „Szpiedzy" mogą sami i bez wiedzy użytkownika pobierać i uruchamiać pliki z sieci. Wśród programów szpiegujących liczną grupę stanowią dodatki do przeglądarek, wykonujące operacje bez wiedzy użytkownika (tzw. Hijacker Browser Helper Object),

- exploit - jest kodem, który umożliwia zdalne przejęcie kontroli nad komputerem poprzez sieć i wykorzystuje w tym celu dziury w programach i systemach operacyjnych,

- rootkit - jest jednym z najbardziej niebezpiecznych narzędzi używanych przez hakerów. Wykorzystywany on jest do przejęcia całkowitej kontroli nad komputerem użytkownika. Jest on bardzo trudny do usunięcia, nawet nie wystarczy w tym celu całkowite formatowanie dysku twardego. Często zagnieżdża się w pamięci flash BIOS - u płyty głównej

- keylogger - występuje w dwóch postaciach: programowej i sprzętowej. Z jego pomocą odczytywane i zapisywane są wszystkie naciśnięcia klawiszy użytkownika, co wiąże się z przechwyceniem adresów, kodów, czy innych cennych informacji w niepowołane ręce.

W tym miejscu warto wspomnieć o fałszywym oprogramowaniu ochronnym. Hakerzy wykorzystują naiwność internautów i często proponują fałszywe oprogramowanie ochronne, które tak naprawdę okazuje się szkodliwe dla komputera. Aby uniknąć takich wpadek warto jest w celu pobrania takiego oprogramowania korzystać z zaufanych stron. Szczególną uwagę należy zwrócić na darmowe antywirusy. Bądźmy więc w tej kwestii bardzo ostrożni i korzystajmy tylko ze sprawdzonych i znanych programów.

Czasem można doświadczyć fałszywego alarmy lub żartu. Zaliczamy do nich rzekomo nowe i groźne wirusy, jak również rzekome wykrycie zainfekowanych plików, które są wywołane przez programy antywirusowe posiadające najwyższy poziom analizy heurystycznej. Żarty komputerowe najczęściej robione są początkującym użytkownikom komputerów.

Na koniec jeszcze kilka ważnych wskazówek dla użytkowników sieci:

- Pamiętaj o uruchomieniu firewalla. Najlepiej na poziomie średniej ochrony z możliwością ustalania reguł. Jeżeli nie jesteś pewien czy sobie poradzisz z ręczną obsługą reguł, możesz ustawić średni lub nawet wysoki poziom ochrony.
- 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, często nie mają jej programy darmowe).
- 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, nawet jeśli wydają się niezarażone (ostrożności nigdy za wiele).
- Staraj się nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje (pieniądze, darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) - często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
- Ważna zasada dotycząca bezpieczeństwa osobistego: 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.
- Pamiętaj, że żaden bank nie wysyła e-maili do swoich klientów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.

Do tych zasad można jeszcze dodać jedną, niekoniecznie związaną bezpośrednio z Internetem. Jeżeli chcesz być pewien bezpieczeństwa swojego komputera nie podłączaj do niego dysków przenośnych ani kart pamięci nieznanego pochodzenia, nie podłączaj też swojego dysku do nieznanego komputera.

Źródła opracowania:

Wikipedia

www.bezpiecznypc.pl/zapobieganie.php

www.bezpiecznypc.pl/artykuly.php

www.ea.com/pl/1/bezpieczenstwo-w-sieci

www.dziecisawazne.pl/dziecko-bezpieczne-w-sieci/

www.bezpieczneinterneciaki.pl/bezpieczenstwo-dzieci-w-internecie

Bezpieczeństwo dzieci online Kompendium dla rodziców i profesjonalistów PCPSI Warszawa 2014

Grażyna Koba *Informatyka dla klas IV – VI szkoły podstawowej*