edukacja medialna

Jak bezpiecznie działać w sieci?

WIEDZA W PIGUŁCE

Internet nie jest tylko miejscem rozrywki. Za jego pośrednictwem robimy przelewy bankowe czy organizujemy akcje społeczne. Gdy załatwiamy coś ważnego, zwykle zależy nam na tym, aby niepowołane osoby nie miały dostępu do pewnych informacji.

Ochrona prywatności w internecie nie jest łatwa. Wielu jej użytkowników ma korzyści z posiadania twoich danych osobowych — wśród nich są m.in. reklamodawcy. Dlatego też, niestety, często twoje dane są sprzedawane w celach marketingowych.

Odpowiedzialne, bezpieczne korzystanie z sieci pomaga w chronieniu twojej prywatności. Nie musisz godzić się na każde ciasteczko, które pomaga w śledzeniu twoich internetowych działań. Możesz się chronić przed internetowymi szpiegami na wiele różnych sposobów:

1. **Tryb prywatny („incognito") w przeglądarkach.** Jest przydatny, jeśli korzystasz z komputera dostępnego dla innych osób. Po zakończeniu twojej sesji przeglądarka automatycznie kasuje całą jej historię oraz ciasteczka.

2. **Ustawienie „silnego" hasła.** Zabezpieczaj swoje konta w internecie hasłami, które bardzo trudno złamać. Ważne jest to, aby były jak najdłuższe, a mimo to łatwe do zapamiętania. Nie ustawiaj wszędzie takiego samego hasła.

3. **Bezpieczne połączenie https://** W niektórych sytuacjach jest niezbędne, np. w kontaktach z bankowością internetową. Oznacza się je za pomocą zielonego elementu na pasku adresu (np. kłódeczki). Komunikaty przesyłane między użytkownikiem a daną stroną są wówczas dodatkowo szyfrowane. Dzięki temu dane nie mogą być przechwytywane i zmieniane przez niepowołane osoby. Czasem zdarza się, że pojawiają się ostrzeżenia o błędach certyfikatu. Nie ignoruj ich, zwłaszcza jeśli witryna nie jest godna zaufania lub wcześniej nie pojawiał się na niej błąd.

4. **Wylogowanie się po skończonej pracy.** Oczywiste, a jednak — można o nim zapomnieć!

5. **Stosowanie pseudonimów.** Jeśli nie musisz podawać swoich danych prywatnych — nie rób tego. Im mniej informacji o tobie jest w sieci, tym twoja aktywność w niej jest bezpieczniejsza.

Sposoby na ograniczenie dostępu do danych stosuj rozważnie. Z narzędzi do ukrywania tożsamości nie będziesz miał pożytku, jeśli np. zalogujesz się na Facebooka. Nie pomoże też bardzo długie hasło, którego nie zapamiętasz. Jeśli zapiszesz je na kartce — możesz ją zgubić. Działaj z głową!

ZADANIA SPRAWDZAJĄCE

Zadanie 1.

Oznacz zdania jako prawdziwe lub fałszywe:

- Wystarczy mieć jedno dobre hasło do wszystkich kont internetowych. [Prawda/Fałsz]
- Aby zakupy online były bezpieczne, wystarczy bezpieczne połączenie (https://). [Prawda/Fałsz]

- Telefon komórkowy jest narażony w internecie na wirusy i wyłudzanie danych. [Prawda/Fałsz]
- Treść, która raz została umieszczona w internecie, nie da się z niego usunąć. [Prawda/Fałsz]

SŁOWNICZEK

- **ciasteczka**: (ang. cookie), małe pliki tekstowe zapisywane na dysku użytkownika podczas korzystania ze stron WWW, które zapamiętują określone informacje o ustawieniach przeglądarki (np. wybrany język strony WWW, dane logowania) lub przesyłają pewne informacje z powrotem na serwery danej strony (np. ustawienia zabezpieczeń lub produkty w koszyku w sklepie internetowym). Ciasteczka mogą narażać użytkownika na wiele zagrożeń, gdyż działają w sposób niewidoczny i mogą zapamiętywać wiele wrażliwych informacji. Nowelizacja prawa telekomunikacyjnego nałożyła na właścicieli stron WWW obowiązek zamieszczenia w widocznym miejscu informacji o tym, że witryna korzysta z ciasteczek, oraz wskazówek na temat tego, jak można wyłączyć ich obsługę.
- **połączenie https://**: połączenie przeglądarki ze stroną internetową zapewniające szyfrowanie komunikacji, a tym samym znacznie utrudniające dostęp do treści osobom innym niż nadawca i odbiorca. Szyfrowanie niezbędne jest w bankowości elektronicznej i w innych sytuacjach, w których podajesz swoje prawdziwe dane. Korzystanie z połączenia https:// zaleca się każdorazowo przy logowaniu.
- **certyfikat strony**: elektroniczny podpis strony internetowej, niezbędny do nawiązania połączenia https://.
- **anonimowość**: brak możliwości zidentyfikowania osoby.
- **prywatność**: sfera życia człowieka, w którą nie należy wkraczać bez pozwolenia. Ma ona swój aspekt cielesny, terytorialny, informacyjny i komunikacyjny. Prywatność jest chroniona przez prawo (m.in. przez Konstytucję RP i akty prawa międzynarodowego). Ograniczenie prawa do prywatności możliwe jest tylko w określonych sytuacjach (na przykład ze względu na bezpieczeństwo publiczne czy ochronę zdrowia).
- **tryb prywatny**: (inaczej: incognito) sposób działania przeglądarki internetowej, który zapewnia wykasowanie wszystkich danych zapisanych podczas przeglądania (historia, ciasteczka) po zamknięciu przeglądarki (lub po wyłączeniu trybu prywatnego).

Tekst: Urszula Dobrowolska, scenariusz: Jan Dąbkowski, konsultacja merytoryczna: Michał "rysiek" Woźniak. Materiał pochodzi z serwisu edukacjamedialna.edu.pl prowadzonego przez Fundację Nowoczesna Polska.

Źródło: http://edukacjamedialna.edu.pl/lekcje/jak-bezpiecznie-dzialac-w-sieci/.

Publikacja zrealizowana w ramach projektu Cyfrowa Przyszłość, dofinansowanego ze środków Ministerstwa Kultury i Dziedzictwa Narodowego.

Podstawa programowa:

Informatyka, III poziom edukacyjny
Cele kształcenia
I. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem, wykorzystanie sieci komputerowej; komunikowanie się za pomocą komputera i technologii informacyjno-komunikacyjnych.

Nowa podstawa programowa:

Informatyka, VII-VIII klasa
Treści nauczania
Uczeń ocenia krytycznie informacje i ich źródła, w szczególności w sieci, pod względem rzetelności i wiarygodności w odniesieniu do rzeczywistych sytuacji, docenia znaczenie otwartych zasobów w sieci i korzysta z nich.
Uczeń opisuje kwestie etyczne związane z wykorzystaniem komputerów i sieci komputerowych, takie jak: bezpieczeństwo, cyfrowa tożsamość, prywatność, własność intelektualna, równy dostęp do informacji i dzielenie się informacją.

Wiedza o społeczeństwie, IV-VIII klasa
Treści nauczania
Uczeń przedstawia korzyści i zagrożenia wynikające z korzystania z zasobów internetu; rozpoznaje przemoc w cyberprzestrzeni i wyjaśnia, jak należy na nią reagować.

Informatyka, liceum i technikum
Treści nauczania
postępuje zgodnie z zasadami netykiety oraz regulacjami prawnymi dotyczącymi: ochrony danych osobowych, ochrony informacji oraz prawa autorskiego i ochrony własności intelektualnej w dostępie do informacji; jest świadomy konsekwencji łamania tych zasad.
respektuje obowiązujące prawo i normy etyczne dotyczące korzystania i rozpowszechniania oprogramowania komputerowego, aplikacji cudzych i własnych oraz dokumentów elektronicznych.
stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji.
opisuje szkody, jakie mogą spowodować działania pirackie w sieci, w odniesieniu do indywidualnych osób, wybranych instytucji i całego społeczeństwa.