

ABC bezpieczeństwa w sieci

WIEDZA W PIGUŁCE

Każdego dnia porozumiewamy się z ludźmi. Kiedy robisz zakupy, nie przeszkadza Ci, że ktoś jest świadkiem wymiany zdań ze sprzedawcą. Nie chcesz jednak, aby Twoją poufną rozmowę z przyjaciółką słyszała osoba postronna.

Komunikacja publiczna i komunikacja prywatna znacznie się od siebie różnią. W komunikacji publicznej uczestniczy duża liczba osób, w komunikacji prywatnej — niewielka i ściśle określona grupa. Komunikujemy się publicznie, kiedy bierzemy udział w dyskusji podczas wieczoru autorskiego czy spotkania z politykiem, gdy zamieszczamy posty na forum internetowym, publikujemy artykuł w gazecie, udostępniamy filmy lub zdjęcia na blogu. W przypadku wymiany listów i e-maili, rozmowy z rodziną i przyjaciółmi (np. na przyjęciu urodzinowym), SMS-owania bądź porozumiewania się przez komunikator internetowy lub telefon możemy natomiast mówić o komunikacji prywatnej.

Poza nadawcą i odbiorcą do wiadomości prywatnej w serwisie społecznościowym oraz na forum ma wgląd administrator. Korzystanie z tej formy komunikacji przypomina zatem podawanie przez koleżankę z ławki liściku — niezłożonego i bez koperty — do kolegi siedzącego pod oknem. Koleżanka, jeśli zechce, jest w stanie zapoznać się z treścią. W przypadku szkolnego forum wiadomość prywatną może przeczytać nauczyciel.

Jeśli zamieścisz jakieś dane (zdjęcia, pliki tekstowe) na dysku swojego komputera, to dostęp do nich będą miały właściwie tylko osoby korzystające z tego sprzętu. Jeśli udostępniasz określoną informację w Internecie — tracisz nad nią kontrolę. Sieć nie zapomina, zamieszczone materiały pozostają tam na zawsze. Dotyczy to nie tylko serwisów społecznościowych, ale praktycznie każdej aktywności w Internecie.

W sieci — podobnie jak w rzeczywistości poza nią — należy przestrzegać zasad bezpieczeństwa. Oto 8 wskazówek, które uczestnicy i uczestniczki powinni poznać:

1. Jeśli nie masz pewności, z kim rozmawiasz, nie podawaj żadnych informacji na swój temat.
2. Nie zdradzaj innym swoich haseł. Układaj takie, które będą trudne do odgadnięcia (to nie może być Twoja data urodzenia ani imię!). Zamiast liter możesz wykorzystać cyfry, które są do nich podobne (l = 1, 0 = 0, A = 4 itp.). Hasło powinno zawierać nie mniej niż 8 znaków, w tym cyfry oraz wielkie litery. W różnych serwisach posługuj się różnymi hasłami.
3. Nie pozwalaj na zapamiętywanie przez przeglądarkę haseł do poczty elektronicznej i serwisów, z których korzystasz — w przeciwnym razie każda osoba pracująca na tym komputerze będzie mogła załogować się na Twoje konto. Po skończonej pracy wyloguj się — inaczej ktoś może się pod Ciebie podszyc.
4. Jeśli korzystasz z serwisów społecznościowych, zadбай o odpowiednie ustawienia prywatności. Im mniej informacji udostępniasz osobom postronnym, tym lepiej. Zastanów się, czy na pewno warto z tych serwisów korzystać. Pamiętaj, że zgodnie z regulaminem Facebooka możesz założyć tam konto dopiero po ukończeniu 13. roku życia.
5. Na forach dyskusyjnych czy blogach posługuj się nickiem (pseudonimem), a nie swoim imieniem i nazwiskiem. Unikaj publikowania informacji o sobie w sieci.

6. Nie korzystaj z możliwości automatycznego „oznaczania się” w miejscu pobytu. Geolokalizacja ma swoje zalety (np. można pochwalić się zwiedzaniem ciekawego miasta), ale i wady — jeżeli ktoś planuje spotkanie bliskiej osobie niezapowiedzianej wizyty, przez przypadek może zepsuć efekt niespodzianki. Ponadto ujawnianie swojego miejsca pobytu umożliwia śledzenie, a niekiedy może być nawet niebezpieczne.
7. Zwracaj uwagę na komunikaty pojawiające się w trakcie ściągania gier i aplikacji na telefony komórkowe i smartfony. Możesz się z nich dowiedzieć, do jakich Twoich danych żąda dostępu pobierana usługa. Uważaj, na co wyrażasz zgodę.
8. W razie wątpliwości odnośnie do tego, jak w danej sytuacji postąpić, poproś o radę swoich rodziców lub innych dorosłych, którym ufasz.

ZADANIA SPRAWDZAJĄCE

Zadanie 1.

Prawda czy fałsz?

1. Na forum internetowym powinienem/powinnam logować się swoim imieniem i nazwiskiem. [Prawda/Fałsz]
2. Nieważne, skąd ściagam gry internetowe na telefon. Ważne tylko, co ściagam. [Prawda/Fałsz]
3. Jeżeli zamieszcze zdjęcie w Internecie, a potem je usunę, to ono zniknie i już nikt nigdy go nie zobaczy. [Prawda/Fałsz]
4. Nawet jeżeli korzystam z komputera w domu, zawsze muszę się wylogować ze skrzynki pocztowej lub portalu społecznościowego. [Prawda/Fałsz]

SŁOWNICZEK

- **anonimowość**: brak możliwości rozpoznania osoby.
- **media społecznościowe**: różnorodne narzędzia umożliwiające użytkownikom internetu kontaktowanie się ze sobą, np. fora, czaty, blogi, portale społecznościowe, społeczności gier sieciowych i wiele innych.
- **nick**: nazwa użytkownika, pseudonim zastępujący prawdziwe imię i nazwisko
- **prywatność**: możliwość utrzymania informacji i danych o sobie w tajemnicy
- **geolokalizacja**: określenie fizycznego położenia geograficznego osoby i urządzenia telekomunikacyjnego za pomocą systemu GPS lub adresu IP.

Tekst: Urszula Dobrzańska, scenariusz: Izabela Meyza, konsultacja merytoryczna: Wojciech Budzisz, Michał "rysiek" Woźniak. Materiał pochodzi z serwisu edukacjamedialna.edu.pl prowadzonego przez Fundację Nowoczesna Polska.

Udostępniono na licencji [Creative Commons Uznanie autorstwa - Na tych samych warunkach 3.0](https://creativecommons.org/licenses/by/3.0/).

Źródło: <http://edukacjamedialna.edu.pl/lekcje/abc-bezpieczenstwa-w-sieci/>.

Publikacja zrealizowana w ramach projektu „Świadomie i bezpiecznie w świecie mediów i informacji” dofinansowanego ze środków MKiDN.

Podstawa programowa:

Zajęcia komputerowe, II poziom edukacyjny

Cele kształcenia

I. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem; świadomość zagrożeń i ograniczeń związanych z korzystaniem z komputera i Internetu.

II. Komunikowanie się za pomocą komputera i technologii informacyjno-komunikacyjnych.

III. Wyszukiwanie i wykorzystywanie informacji z różnych źródeł; opracowywanie za pomocą komputera rysunków, motywów, tekstów, animacji, prezentacji multimedialnych i danych liczbowych.

V. Wykorzystywanie komputera do poszerzania wiedzy i umiejętności z różnych dziedzin, a także do rozwijania zainteresowań.

Podstawa programowa 2017:

Informatyka, IV-VI klasa

Treści nauczania

Uczeń posługuje się technologią zgodnie z przyjętymi zasadami i prawem; przestrzega zasad bezpieczeństwa i higieny pracy.

Uczeń uznaje i respektuje prawo do prywatności danych i informacji oraz prawo do własności intelektualnej.

Uczeń wymienia zagrożenia związane z powszechnym dostępem do technologii oraz do informacji i opisuje metody wystrzegania się ich.

Edukacja dla bezpieczeństwa, IV-VIII klasa

Treści nauczania

Uczeń dobiera i demonstruje umiejętności komunikacji interpersonalnej istotne dla zdrowia i bezpieczeństwa (odmowa, zachowania asertywne, negocjowanie).