

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 złożenie 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 ściągnięcia 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.

POMYSŁ NA LEKCJĘ

Uczestnicy i uczestniczki dowiedzą się, co dzieje się z informacjami, które zamieszczają w Internecie. Następnie poznają podstawowe zasady bezpieczeństwa w sieci i zastanowią się, jak można się chronić przed zagrożeniami, które niesie użytkowanie Internetu.

Cele operacyjne

Uczestnicy i uczestniczki:

- znają różnicę między komunikacją prywatną i publiczną w sieci i poza nią;
- potrafią wskazać zagrożenia związane z korzystaniem z Internetu w telefonach komórkowych i innych urządzeniach;
- wiedzą, jakich zasad należy przestrzegać, żeby się przed tymi zagrożeniami chronić.

Przebieg zajęć

1.

Czas: 10 min

Forma: praca indywidualna

Pomoce: małe karteczki, długopisy

Rozdaj uczestnikom i uczestniczkom małe karteczki. Poproś, żeby przypomnieli sobie jakąś informację DOTYCZĄCĄ KAŻDEGO Z NICH, którą ostatnio zamieścili w Internecie, i zapisali ją na karteczce. Mogą pomyśleć też o swoim zdjęciu, które zamieścili i krótko napisać, co przedstawia. Kiedy skończą, poproś, żeby wyobrazili sobie, że tę kartkę przyczepiają na szkolnej tablicy z ogłoszeniami bądź na tablicy na głównym placu w mieście (dopasuj do kontekstu Waszej miejscowości). Staraj się zbudować sugestywny obraz sytuacji, daj uczestnikom czas na jej wyobrażenie. Po chwili dodaj modyfikację: poproś, żeby uczestnicy wyobrazili sobie, że kartki zostają na tablicy ogłoszeń na zawsze, że ktoś będzie mógł je przeczytać nawet za pół wieku, np. ich dzieci, wnuki. Znów daj chwilę na wyobrażenie sytuacji.

Po zakończeniu doświadczenia poproś, żeby schowali kartki do kieszeni lub odłożyli na bok. Zapytaj:

1. Co czuliście, wyobrażając sobie, że karteczka z informacją o was wisi na szkolnej tablicy?
2. Kto mógłby ją przeczytać? (Nakieruj na to, że oprócz uczniów, nauczycieli i rodziców do szkoły mógłby wejść każdy i mieć dostęp do ich prywatnych informacji: refleksji, wiedzy o tym, co myślą i co akurat robią).

3. Co mógłbyś z tą wiedzą o was zrobić?
4. Co czuliście, wiedząc, że kartka zostanie na tablicy na zawsze?

Następnie powiedz, że właśnie tak działają portale społecznościowe. To, co zamieszczamy na swoich profilach, może być widoczne dla innych: naszych znajomych i nieznajomych. Dodatkowo: to, co zamieszczamy w Internecie, może zostać tam na zawsze. Nigdy nie wiemy, kto i jak może to wykorzystać.

Na koniec ćwiczenia poproś uczestników i uczestniczki o ponowne wyciągnięcie kartek. Zadaj pytanie:

1. Spójrzcie na te kartki raz jeszcze. Czy po tym ćwiczeniu zamieścilibyście takie zdjęcie lub taką informację o sobie?

2.

Czas: 10 min
Forma: burza mózgów
Pomoce: tablica i kreda lub marker

Napisz na tablicy dwa hasła KOMUNIKACJA PRYWATNA i KOMUNIKACJA PUBLICZNA. Powiedz, że to, co piszemy na naszym profilu na portalu społecznościowym lub zamieszczamy na tablicy szkolnej, można zaliczyć do komunikacji publicznej. Powiedz, że oprócz komunikacji publicznej istnieje też komunikacja prywatna. Poproś uczestników i uczestniczki o podawanie przykładów obu rodzajów komunikacji i zapisuj je na tablicy pod hasłami. Podkreśl, że mogą podawać przykłady nie tylko z Internetu.

Jeżeli nie padnie od uczestników, konieczne dopowiedz lub ich nakieruj na to, że z komunikacją prywatną mamy do czynienia w przypadku korzystania z:

- listu,
- e-maila,
- prywatnych wiadomości na portalach społecznościowych,
- czatu i komunikatorów internetowych,
- telefonu (rozmowa, SMS).

Komunikacja publiczna obejmuje:

- korzystanie z forów internetowych,
- zamieszczanie informacji na blogach i portalach społecznościowych,
- dyskusję na forum klasy.

Podkreśl, że w sieci i poza nią obowiązują podobne zasady, lecz istnieją też pewne różnice: w Internecie nigdy nie wiemy, z kim rozmawiamy i kto czyta informacje o nas, bo zawsze ktoś się może podawać za kogoś innego. Poza tym informacje przekazywane w Internecie są zapośredniczone (czyta je też administrator).

Zadaj pytanie:

- z których sposobów komunikacji korzystacie najczęściej?

Zbierz kilka odpowiedzi z grupy. Powiedz, że za chwilę przyjrzymy się, jak dbać o bezpieczeństwo, komunikując się przez Internet.

3.

Czas: 15 min
Forma: praca w grupach
Pomoce: karta pracy „Bezpieczeństwo w sieci”

Podziel uczestników na cztery grupy i rozdaj **karty pracy „Bezpieczeństwo w sieci”**. Następnie poproś uczestników o przeczytanie odpowiedzi na forum.

4.

Czas: 10 min
Forma: burza mózgów
Pomoce: tablica i kreda lub marker

Nawiązując do poprzedniego ćwiczenia, zaproponuj wspólne stworzenie zasad bezpieczeństwa, których warto przestrzegać w sieci. Na tablicy zapisz: „Kodeks bezpieczeństwa w sieci” i zadaj uczestnikom pytanie:

- Co możemy robić, żeby dbać o nasze bezpieczeństwo w sieci?

Zapisuj odpowiedzi uczestników. Jeśli będzie taka potrzeba, wykorzystaj wskazówki z „Wiedzy w pigułce” do uzupełnienia ich wypowiedzi.

Po stworzeniu „Kodeksu” poproś uczestników i uczestniczki, żeby wybrali zasadę, która wydaje im się najważniejsza, i opowiedzieli sobie krótko w parach, dlaczego akurat ją wybrali.

Ewaluacja

Czy po przeprowadzeniu zajęć ich uczestnicy i uczestniczki:

- rozumieją, że zamieszczanie niektórych informacji o sobie w sieci może stanowić problem?
- potrafią podać przykłady komunikacji prywatnej i publicznej w sieci?
- znają sposoby dbania o bezpieczeństwo w sieci?
- wiedzą, że w sieci trzeba przestrzegać podobnych zasad bezpieczeństwa jak poza nią?

Opcje dodatkowe

Opcją dodatkową może być stworzenie ulotek i plakatów na temat bezpieczeństwa w sieci, które posłużą do zrobienia w szkole akcji społecznej dotyczącej tego tematu. Inną propozycją jest zrobienie ogólnoszkolnego konkursu na plakat związany z bezpieczeństwem w sieci.

MATERIAŁY

Karta pracy „Bezpieczeństwo w sieci”

ZADANIA SPRAWDZAJĄCE

Zadanie 1.

Prawda czy fałsz?

1. Na forum internetowym powinienem/powinnam logować się swoim imieniem i nazwiskiem. [rozwiązanie: fałsz] [Prawda/Fałsz]
2. Nieważne, skąd ściągam gry internetowe na telefon. Ważne tylko, co ściągam. [rozwiązanie: fałsz] [Prawda/Fałsz]

3. Jeżeli zamieszczę zdjęcie w Internecie, a potem je usunę, to ono zniknie i już nikt nigdy go nie zobaczy. [rozwiązanie: fałsz] [Prawda/Fałsz]
4. Nawet jeżeli korzystam z komputera w domu, zawsze muszę się wylogować ze skrzynki pocztowej lub portalu społecznościowego. [rozwiązanie: prawda] [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.

CZYTELNIA

- **Jak dzieci i młodzież chronią swoją prywatność?**, GIODO [dostęp: 23.06.2013]: http://www.giodo.gov.pl/560/id_art/4699/j/pl/
- **Postrzeganie zagadnień związanych z ochroną danych i prywatnością przez dzieci i młodzież — raport z badań**, GIODO [dostęp: 19.09.2013]: <http://panoptykon.org/sites/panoptykon.org/files/raport-koncowy-z-badan.pdf>.

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