CYFROWA WYPRAWKA

Bezpieczeństwo informacji w sieci

Informacje o lekcji

Opracowanie wiedzy w pigułce:	Małgorzata Szumańska
Autorka scenariusza:	Izabela Meyza
Organizacja publikująca:	Fundacja Panoptykon
Źródło:	Lekcja powstała na bazie lekcji „Jak bezpiecznie działać w sieci?" opublikowanej przez Fundację Nowoczesna Polska w ramach projektu „Edukacja medialna" (tekst: Urszula Dobrowolska, scenariusz: Jan Dąbkowski, konsultacja merytoryczna: Michał „rysiek" Woźniak)
Przedmiot:	Informatyka
Sugerowany poziom kształcenia:	Szkoły gimnazjalne
Licencja:	Creative Commons Uznanie autorstwa – Na tych samych warunkach 3.0 Polska

Wiedza w pigułce

Internet jest nie tylko miejscem rozrywki, ale także narzędziem przekazywania różnych informacji. Niestety, często daje złudne poczucie, że łatwo można kontrolować, kto ma dostęp do naszych danych. Nie jest to jednak takie proste. Jeśli nie chcemy, by miały do nich dostęp osoby niepowołane, trzeba się przed takim scenariuszem zabezpieczyć.

W wielu sytuacjach z treścią internetowej komunikacji mogą zapoznać się osoby postronne. Dlatego za jej pomocą nie powinno się przekazywać informacji, które mają poufny charakter – chyba że zdecydujemy się na stosowanie odpowiednich środków zabezpieczających, np. szyfrowania poczty elektronicznej. Służą do tego specjalne narzędzia kryptograficzne (PGP/GPG).

Informacje, które przekazujemy w sieci, mogą trafić w niepowołane ręce różnymi drogami, choćby przy okazji korzystania z niezabezpieczonej sieci Wi-Fi lub przesyłania danych za pomocą protokołu HTTP. Połączenia wymagające logowania powinny być realizowane za pomocą szyfrowanego protokołu HTTPS, a wrażliwe operacje (np. przelewy) wykonywane tylko w zabezpieczonej sieci, do której mamy zaufanie.

Zagrożeniem dla poufności informacji mogą być także wirusy, e-maile i strony wyłudzające dane. Bardzo prozaicznym, ale niestety dość powszechnym problemem jest dostęp osób niepowołanych do niezabezpieczonego sprzętu. Jeśli trafimy na życzliwego „włamywacza", może się skończyć na zabawnym wpisie na portalu społecznościowym, z którego zapomnieliśmy się wylogować. Jednak nie każda niefrasobliwa osoba ma tyle szczęścia.

Wiele osób dba o ochronę swojego komputera, ale zapomina o telefonie. Tymczasem coraz częściej jest on narzędziem korzystania z Internetu oraz usług wymagających udostępniania danych, np. o naszej lokalizacji.

Powinien być odpowiednio zabezpieczony, zwłaszcza że jego mobilny i podręczny charakter sprawia, że jest narażony na zgubienie, kradzież czy wykorzystanie bez naszej wiedzy.

Nie jesteśmy w stanie w 100% zabezpieczyć się przed wszystkimi zagrożeniami. Możemy jednak ograniczyć ryzyka, stosując kilka podstawowych zasad:

1. Jeśli nie musisz podawać swoich danych – nie rób tego. Im mniej informacji o Tobie jest w sieci, tym Twoja aktywność w niej jest bezpieczniejsza i trudniej się pod Ciebie podszyć.
2. Staraj się unikać przekazywania poufnych informacji (np. haseł) pocztą elektroniczną, SMS-ami, czatem (chyba że robisz to za pomocą szyfrowanej poczty lub czatu).
3. Gdy to możliwe, korzystaj z protokołu HTTPS. Przy logowaniu i przesyłaniu danych sprawdź, czy adres w przeglądarce zaczyna się od „https" i widnieje obok niego symbol kłódki. Zainstaluj w swojej przeglądarce wtyczkę HTTPS Everywhere, dzięki której z każdą odwiedzaną stroną, która ma taką opcję, automatycznie będziesz łączyć się przez protokół HTTPS.
4. Unikaj korzystania z niezabezpieczonego Wi-Fi. Jeśli go używasz, unikaj logowania się prawdziwymi danymi i nie wykonuj wrażliwych operacji (np. finansowych).
5. Jeśli korzystasz z komputera dostępnego dla innych osób, używaj w przeglądarkach trybu prywatnego (czasem zwanego „incognito"). Po zakończeniu Twojej sesji przeglądarka automatycznie kasuje całą jej historię oraz ciasteczka.
6. Zabezpieczaj swoje konta w Internecie hasłami, które trudno złamać (co najmniej 8 znaków, małe i wielkie litery, znaki specjalne, bez popularnych słów). Nie powinno to być imię psa ani data urodzin. Używaj różnych haseł do różnych usług i regularnie je zmieniaj. Chroń swoje hasła – nie udostępniaj ich innym, nie zapisuj w widocznym miejscu, nie zapamiętuj w komputerze (ani cudzym, ani własnym).
7. Wyloguj się, kiedy skończysz korzystać z danej usługi.
8. Używaj programu antywirusowego w komputerze i telefonie. Pamiętaj o jego aktualizacji. Aktualizuj również inne programy, z których korzystasz i używaj najnowszych wersji przeglądarek internetowych.
9. Zabezpiecz hasłem (blokadą) dostęp do komputera, telefonu, tabletu.

Pomysł na lekcję

Uczestnicy i uczestniczki będą mieli okazję przyjrzeć się swoim zachowaniom w sieci pod kątem bezpieczeństwa. Następnie, dzięki analizie konkretnych przykładów, zastanowią się, jak można zapobiegać niebezpiecznym sytuacjom.

Cele operacyjne

Uczestnicy i uczestniczki:

- wiedzą, jak dbać o bezpieczeństwo swoich danych w sieci;
- wiedzą, że powinni dbać o bezpieczeństwo połączenia internetowego i sprzętu, przez który łączą się z Internetem (szczególnie gdy przesyłają ważne informacje czy dokonują transakcji finansowych);
- umieją stworzyć bezpieczne hasło internetowe.

Przebieg zajęć

Ćwiczenie 1.

Czas: *5 min*

Metoda: *gra*

Pomoce: *kartki z napisami TAK i NIE, taśma samoprzylepna*

Przed rozpoczęciem zajęć na dwóch przeciwległych ścianach sali przyklej widoczne kartki z napisami TAK i NIE. Poproś uczestników, żeby stanęli na środku sali. Powiedz, że za chwilę będziesz czytać różne stwierdzenia dotyczące działania w Internecie. Jeżeli są to stwierdzenia prawdziwe w przypadku danej osoby, niech przejdzie ona pod kartkę z napisem TAK, jeżeli nie – niech stanie pod napisem NIE.

Następnie przeczytaj zdania, dając uczniom czas na zastanowienie się i zajęcie stanowiska:

- Moje hasło do poczty elektronicznej jest dłuższe niż 7 znaków.
- Używam tego samego hasła do logowania się do poczty i portalu społecznościowego.
- Ostatni raz hasło do poczty zmieniałem/-am dawniej niż pół roku temu.
- Chociaż raz w życiu zdarzyło mi się nie wylogować z serwisu społecznościowego i odejść od komputera.
- Używam programu antywirusowego.
- Na portalu społecznościowym przyjmuję zaproszenie do grona znajomych od wszystkich, którzy mi je wysyłają.
- Chociaż raz w życiu zmieniałem/-am ustawienia prywatności w portalu społecznościowym, z którego korzystam.
- Zawsze czytam regulaminy aplikacji i programów, które ściągam na komputer lub smartfon.

Ćwiczenie 2.

Czas: *10 min*

Metoda: *miniwykład*

Pomoce: *kreda i tablica lub papier dużego formatu i markery*

Po ćwiczeniu zapytaj uczniów o refleksje. Zadaj pytanie:

- Czy coś Was zaskoczyło w Waszych odpowiedziach?

W omówieniu ćwiczenia zwracaj uwagę wychwytywanie przyzwyczajeń czy reguł (np. „Widzę, że nikt z Was nie zmieniał jeszcze ustawień prywatności na portalu społecznościowym. Dlaczego?", „Widzę, że większość z Was zmieniała hasło do poczty w ciągu ostatniego pół roku. Dlaczego uważacie, że trzeba robić to tak często?" lub „Czy ci z Was, którym zdarzyło się odejść od komputera i nie wylogować, mogą powiedzieć, jak się to skończyło? A jak mogło się skończyć?").

Następnie powiedz, że brak dbałości o bezpieczeństwo w sieci możemy obserwować na przykładzie haseł. Przedstaw uczniom wyniki badań dotyczących bezpieczeństwa haseł internetowych:

- Tylko połowa użytkowników sieci używa hasła dłuższego niż 7 znaków.
- 1/3 łączy w haśle litery i cyfry.

- Popularne hasła to 123456, iloveyou, qwerty, abc123.
- W skład hasła wchodzi często drugie imię, imię zwierzęcia czy data urodzenia.
- 1/3 użytkowników sieci zapisuje hasła na kartce lub w notesie.

Następnie zadaj uczniom pytania:

- Czy zaskakują Was te dane?
- Jakie według Was powinno być bezpieczne hasło?
- Czy zamierzacie coś zmienić w Waszych hasłach internetowych?

Zbierz kilka odpowiedzi z grupy. Następnie powiedz, że bezpieczeństwo w Internecie to nie tylko dbałość o hasła i że za chwilę przyjrzymy się sytuacjom, w których szczególnie warto o nie dbać.

Ćwiczenie 3.

Czas: *15 min*

Metoda: *praca w grupach*

Pomoce: *karta pracy „Jak bezpiecznie działać w sieci"*

Podziel uczestników na cztery grupy. Rozdaj grupom karty pracy „Jak bezpiecznie działać w sieci?" i poproś o wykonanie zadań. Daj na to 10 minut. Następnie poproś grupy o przeczytanie odpowiedzi na forum. Jeśli nie padnie to od uczniów, korzystając z „Wiedzy w pigułce", dopowiedz, że istnieje tryb prywatny w przeglądarkach internetowych (przydatny, gdy korzystamy nie ze swojego komputera), oraz wytłumacz, jak sprawdzić, czy na przykład przy zakupach przez Internet połączenie jest szyfrowane za pomocą protokołu HTTPS (więcej informacji w „Wiedzy w pigułce").

Ćwiczenie 4.

Czas: *15 min*

Metoda: *burza mózgów*

Pomoce: *tablica i kreda lub papier i marker*

Nawiązując do poprzedniego ćwiczenia, zaproponuj wspólne stworzenie zasad bezpieczeństwa, których warto przestrzegać w sieci. Na tablicy zapisz: „10 zasad bezpieczeństwa w sieci", a następnie poproś uczestników o podawanie najważniejszych według nich zasad.

Zapisuj ich odpowiedzi. W razie potrzeby nakieruj grupę, korzystając z „Wiedzy w pigułce".

Jeżeli czas pozwoli, po stworzeniu „10 zasad" poproś uczniów, żeby wybrali jedną zasadę, którą uważają za najważniejszą, i opowiedzieli sobie krótko w parach, dlaczego ją wybrali. Jeżeli masz mało czasu, odczytaj na głos zasady wypracowane przez uczniów.

Ewaluacja

Czy po przeprowadzeniu zajęć ich uczestnicy i uczestniczki:

- potrafią stworzyć bezpieczne hasło do poczty elektronicznej lub portalu społecznościowego?
- wiedzą, jak dbać o bezpieczeństwo informacji w sieci?
- wiedzą, jak chronić dane w sytuacjach szczególnej ostrożności (np. zakupy przez Internet)?

Opcje dodatkowe

Jeśli masz więcej czasu, zaproponuj uczestnikom ćwiczenie tworzenia ze zdań tzw. *passphrases*, czyli silnych, ale łatwych do zapamiętania haseł (np. Ala ma 3 duże koty i psa, który jest bury. – Am3dkip,kjb.)

Opcją dodatkową może być zorganizowanie akcji informacyjnej (np. plakatowej) dotyczącej bezpieczeństwa, w której można wykorzystać omówione podczas zajęć zasady.

Materiały

Karta pracy dla grup „Jak bezpiecznie działać w sieci?"

Zadania sprawdzające

Zadanie 1

Prawda czy fałsz?

1. __ Hasło internetowe składające się z ciągu małych liter jest wystarczająco bezpieczne.
2. __ Przed skorzystaniem z Internetu w komputerze kolegi powinienem/powinnam w przeglądarce włączyć tryb prywatny.
3. __ Łącząc się z nieznaną i niezabezpieczoną siecią, mogę bezpiecznie robić zakupy przez Internet. Ważne, że nikomu nie podaję swojego hasła do konta, z którego płacę.
4. __ Nawet jeżeli korzystam z komputera w domu, zawsze powinienem/powinnam wylogować się ze skrzynki pocztowej lub portalu społecznościowego.

Słowniczek

Anonimowość – brak możliwości zidentyfikowania konkretnej osoby.

HTTPS Everywhere – wtyczka do przeglądarek internetowych, która automatycznie włącza protokół HTTPS tam, gdzie istnieje taka możliwość.

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.

Protokół HTTP (ang. *Hypertext Transfer Protocol*) – jeden z podstawowych protokołów (tj. reguł postępowania i kroków podejmowanych przez urządzenie w celu nawiązania łączności i wymiany danych) Internetu, odpowiadający np. za ładowanie stron internetowych.

Protokół HTTPS (ang. *Hypertext Transfer Protocol Secure*) – rozszerzenie protokołu HTTP. Umożliwia przesyłanie w sieci zaszyfrowanych informacji, dzięki czemu dostęp do treści mają jedynie nadawca oraz odbiorca komunikatu.

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).

Rozszerzenie (inaczej: wtyczka) – dodatkowy moduł do programu komputerowego, który rozszerza jego możliwości. Stosowanie wtyczek jest coraz częstszym zabiegiem wśród programistów, a zwłaszcza tych tworzących otwarte oprogramowanie. Zaletą takiego rozwiązania jest to, że użytkownicy mogą wybierać pomiędzy funkcjami, które chcą mieć w programie, a których nie. Poza tym odciąża to autora od pisania całego kodu programu, a zrzuca część tego obowiązku na zewnętrznych programistów. Najpopularniejszymi programami oferującymi wtyczki są przeglądarki internetowe oraz programy pocztowe, np. Mozilla Firefox i Mozilla Thunderbird. W obu przypadkach dzięki wtyczkom można znacząco zwiększyć poziom bezpieczeństwa i prywatności komunikacji.

Czytelnia

1. Małgorzata Szumańska, Anna Obem, *Jak bezpiecznie komunikować się w sieci*, Fundacja Panoptykon [dostęp: 22.12.2014]: http://cyfrowa-wyprawka.org/teksty/jak-bezpiecznie-komunikowac-sie-w-sieci.
2. Anna Obem, Michał „czesiek" Czyżewski, Katarzyna Szymielewicz, *Prywatność – zrób to sam!*, Fundacja Panoptykon [dostęp: 21.07.2014]: http://cyfrowa-wyprawka.org/teksty/prywatnosc-zrob-sam.
3. Kamil Śliwowski, Anna Obem, *Odzyskaj kontrolę w sieci. Odcinek II: wtyczki*, Fundacja Panoptykon [dostęp: 19.10.2015] http://cyfrowa-wyprawka.org/teksty/odzyskaj-kontrole-w-sieci-odcinek-ii-wtyczki.
4. Grzegorz Prujszczyk, Kamil Śliwowski, *Komunikacja* [dostęp: 21.07.2014]: http://www.panoptykon.org/sites/panoptykon.org/files/panoptykon_poradnik_komunikacja.pdf.

Ten materiał jest częścią projektu „Cyfrowa wyprawka" Fundacji Panoptykon.

Projekt współfinansowany ze środków Ministra Kultury i Dziedzictwa Narodowego.