edukacja medialna

Twoje bezpieczeństwo w internecie

WIEDZA W PIGUŁCE

Internet nie jest tylko miejscem rozrywki. Za jego pośrednictwem załatwiamy różne ważne sprawy. Dbajmy wówczas, aby niepowołane osoby nie miały dostępu do istotnych informacji. To niełatwe, ponieważ w takcie podróży po sieci mimowolnie pozostawiamy po sobie ślady.

Informacje o nas mogą zostać przechwycone lub pozyskane przez internetowych przestępców. Częściej jednak sami dajemy innym dostęp do nich. Sieć nie mogłaby przecież istnieć bez nadzorujących ją osób. Dostawcy usług internetowych, administratorzy serwisów i programiści umożliwiają nam korzystanie z internetu. Aby efektywniej wykonywać swoją pracę, gromadzą o nas pewne dane. Np. Google wykorzystuje zbierane informacje, aby dostosowywać wyniki wyszukiwania do użytkownika. Czyni to, m.in. skanując treść e-maili czy zapisując wyszukiwane przez Ciebie frazy.

Używając darmowych narzędzi internetowych często nieświadomie godzimy się na wykorzystywanie naszych danych w różnych celach. Ich krążenie po internecie umożliwia np. rozsyłanie reklamowego spamu. Dlatego też nieraz informacje o nas stają się towarem — są sprzedawane reklamodawcom.

Aby bezpieczniej korzystać z internetu, wykorzystuj nastepujące metody:

1. **Bądź anonimowy.** Jeśli nie musisz podawać swoich danych prywatnych — nie rób tego. Im mniej informacji o tobie jest w sieci, tym jesteś bezpieczniejszy.

2. **Ustaw „silne" hasła.** Ważne, aby twoje hasła były jak najdłuższe. Miej wiele haseł i czasem je zmieniaj.

3. **Sprawdzaj, czy łączysz się bezpiecznie (przez połączenie https://).** Bezpieczne połączenia oznacza się za pomocą zielonego zaznaczenia lub kłódeczki koło paska adresu. Czasem występuje problem z bezpieczeństwem połączenia i 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. **Zainstaluj program: Adblock, NoScript, Flashblock, Cookie Monster**. Te programy blokują niepożądane elementy stron. Np. Adblock nie tylko usunie reklamy, lecz także ograniczy przepływ informacji o historii przeglądania.

5. **Stosuj tryb prywatny w przeglądarkach.** Jest przydatny, jeśli korzystasz z komputera dostępnego dla innych osób. Po zakończeniu sesji kasowana jest cała jej historia oraz ciasteczka.

6. **Wyloguj się po pracy.** Nie można o tym zapomnieć!

POMYSŁ NA LEKCJĘ

Osoby uczestniczące w zajęciach poznają zasady bezpiecznego korzystania z internetu, a także usystematyzują i utrwalą sobie wiedzę na temat rodzajów zagrożeń i zabezpieczeń. Poznają także korzyści i zagrożenia płynące z anonimowości w internecie.

Cele operacyjne

Uczestnicy i uczestniczki:

- wiedzą, że muszą dbać o bezpieczeństwo swoich danych, haseł, sprzętu, przez który łączą się z internetem, połączenia internetowego (szczególnie, gdy przesyłają ważne informacje czy robią transakcje finansowe);
- wiedzą o istnieniu i działaniu programów antywirusowych, a także antyreklamowych i antyskryptowych rozszerzeń do przeglądarek;
- umieją zachowywać się bezpiecznie w sieci i mogą doradzać innym, jak to robić;
- nie otwierają linków i plików, a także nie klikają w bannery reklamowe przed upewnieniem się, że są bezpieczne;
- odpowiedzialnie publikują materiały i informacje dotyczące ich samych lub innych osób (za ich zgodą), przewidując konsekwencje, jakie może to spowodować;
- wiedzą, że anonimowość w internecie może mieć dobre i złe strony;
- wiedzą, że anonimowość w sieci może być pozorna i że możliwe jest ustalenie autora danej informacji, nawet jeżeli nie podał swoich danych;
- wiedzą, że wiarygodność w internecie może zależeć nie od podania swoich danych, ale od przedstawianych argumentów i dowodów dotyczących postawionych przez siebie tez;
- umieją odróżnić działanie obywatelskie od szkodliwego przeszkadzania i obrażania w internecie.

Przebieg zajęć

1.

Czas: 20 min
Forma: praca indywidualna, praca wgrupach
Pomoce: papier dużego formatu, markery, ksero/drukarka do wydruku kart pracy **„Test bezpieczeństwa internetowego”** i **„Legalna Spółdzielnia”**

Podziel grupę na 2 podgrupy. Pierwsza będzie zajmowała się bezpieczeństwem, a druga anonimowością w internecie. W czasie wykonywania prac w podgrupach, sprawdzaj, czy uczestnicy nie potrzebują pomocy czy interpretacji instrukcji.

Bezpieczeństwo

Rozdaj podgrupie **karty pracy „Test bezpieczeństwa internetowego”**. W karcie są polecenia dotyczące pracy podgrupy.

Anonimowość

Rozdaj podgrupie **karty pracy „Legalna Spółdzielnia”**. W karcie są polecenia dotyczące pracy podgrupy.

2.

Czas: 25 min
Forma: prezentacja, dyskusja

Podgrupy prezentują efekty swojej pracy. Słuchająca podgrupa na koniec każdej prezentacji może dodawać swoje przykłady. W zależności od wiedzy grupy, na koniec skomentuj i podsumowuj prezentacje podgrup na forum. W razie pasywności poproś o uzupełnienie osoby z drugiej podgrupy, naprowadzaj na problematyczne czy dyskusyjne sytuacje i ich rozwiązania.

Na koniec poproś grupę o wymienienie sytuacji z życia:

- w których najmniej dba się o bezpieczeństwo korzystania z internetu,
- w których należy pozostać anonimowym albo ujawnić swoją tożsamość.

Poproś o uzasadnienie dlaczego.

Ewaluacja

Czy po przeprowadzeniu zajęć ich uczestniczki i uczestnicy:

- są przekonane/przekonani, że warto dbać o bezpieczeństwo swoich danych, haseł, sprzętu, przez który łączą się z internetem, połączenia internetowego (szczególnie, gdy przesyłają ważne informacje czy robią transakcje finansowe)?
- mają świadomość ewentualnych skutków i odpowiedzialności, jaka ciąży na nich w momencie publikowania informacji i materiałów dotyczących ich samych lub innych osób?
- wiedzą, kiedy lepiej działać w internecie pod nazwiskiem, a kiedy zachować anonimowość?
- są świadome/świadomi, że anonimowość w sieci może być pozorna, jeśli się o nią odpowiednio nie zadba?

Opcje dodatkowe

Elementem utrwalającym wiedzę i pokazującym szerzej efekty zajęć może być mini-kampania czy mini-akcja uświadamiająca skierowana do znajomych i najbliższych: np. stworzenie plakatów i umieszczenie ich w miejscach publicznych i internecie.

MATERIAŁY

Karta pracy „Test bezpieczeństwa internetowego"
Karta pracy „Legalna Spółdzielnia"

ZADANIA SPRAWDZAJĄCE

Zadanie 1.

Ustal hierarchię bezpieczeństwa w internecie:

Kategorie:

- a — bardzo bezpieczne
- b — średnio bezpieczne
- c — najmniej bezpieczne

Hasło:
Elementy do przyporządkowania:

- .....czarny [rozwiązanie: 3]
- .....czarnyKotBialyKoT [rozwiązanie: 1]
- .....czarny01 [rozwiązanie: 2]

Podawanie prawdziwych danych w internecie:
Elementy do przyporządkowania:

- .....podczas zakupów on-line na zaufanej stronie [rozwiązanie: 1]
- .....na stronie, gdzie można się dowiedzieć, ile się będzie miało dzieci w przyszłości [rozwiązanie: 3]
- .....żeby móc podyskutować na forum [rozwiązanie: 2]

Aktualizacja programów zabezpieczających system (np. antywirus):
Elementy do przyporządkowania:

- .....jak sobie przypomnę [rozwiązanie: 2]
- .....nigdy o tym nie pamiętam [rozwiązanie: 3]
- .....aktualizują się automatycznie [rozwiązanie: 1]

SŁOWNICZEK

- **AdBlock**: jedno z najpopularniejszych rozszerzeń do przeglądarek internetowych, automatycznie blokuje i usuwa reklamy ze stron internetowych. Zwiększa wygodę i bezpieczeństwo korzystania z sieci. Ogranicza przepływ informacji o historii przeglądania.
- **NoScript**: rozszerzenie do przeglądarek internetowych, automatycznie blokuje skrypty uruchamiane przez strony internetowe w przeglądarce.
- **CookieMonster**: rozszerzenie do przeglądarek internetowych, pozwala bardzo dokładnie kontrolować ciasteczka i to, jakie strony (i na jak długo) mogą je ustawiać.
- **FlashBlock**: rozszerzenie do przeglądarek internetowych domyślnie blokujące wszystkie filmiki typu flash na stronach internetowych, pozwalające je uruchomić jednym kliknięciem myszki.
- **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.
- **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).
- **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.

- **anonimowość**: brak możliwości zidentyfikowania osoby.
- **rozszerzenie**: (inaczej: wtyczka), dodatkowy moduł do programu komputerowego, który rozszerza jego możliwości. Stosowanie wtyczek jest coraz częstszym zabiegiem wśród twórców programów, 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.
- **skrypt**: prosty program uruchamiany przez stronę internetową. Skrypty są zwykle używane do tworzenia animowanych menu i innych udogodnień, ale bywają też wykorzystywane do śledzenia internautów. Zdarza się, że zawierają złośliwy kod, który wykorzystuje luki w programie przeglądarki do infekowania komputerów użytkowników.

CZYTELNIA

- Prujszczyk Grzegorz, Śliwowski Kamil, **Browsing, wirtualne zagrożenia** [PDF], [dostęp: 22.11.2012] , Dostępny w Internecie http://www.ceo.org.pl/sites/default/files/library-files/browsing.pdf, licencja: CC-BY-NC-SA.
- Prujszczyk Grzegorz, Śliwowski Kamil, **Bezpieczeństwo informacyjne w serwisach Web 2.0** [PDF], [dostęp: 22.11.2012], Dostępny w Internecie: http://www.ceo.org.pl/sites/default/files/library-files/web20.pdf, licencja: CC-BY-NC-SA.
- **Aplikacje mobilne — szare komórki Twojej komórki** [PDF], tłum. Fundacja Dzieci Niczyje, [data dostępu: 14.01.2013], Dostepny w Internecie: http://fdn.pl/sites/default/files/FDN_aplikacje-mobilne.pdf.
- Dziennik Gazeta Prawna, **Debata DGP: Anonimowość w Internecie** [online], [dostęp: 14.02.2013], Dostępny w Internecie: http://www.gazetaprawna.pl/anonimowosc-w-internecie.

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/twoje-bezpieczenstwo-w-internecie/.

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.
V. Ocena zagrożeń i ograniczeń, docenianie społecznych aspektów rozwoju i zastosowań informatyki.

Etyka, III poziom edukacyjny
Cele kształcenia
I. Kształtowanie refleksyjnej postawy wobec człowieka, jego natury, powinności moralnych oraz wobec różnych sytuacji życiowych.
IV. Podjęcie odpowiedzialności za siebie i innych oraz za dokonywane wybory moralne; rozstrzyganie wątpliwości i problemów moralnych zgodnie z przyjętą hierarchią wartości i dobrem wspólnym.