edukacja medialna

Kto nas śledzi w sieci?

WIEDZA W PIGUŁCE

Przekonanie o anonimowości w Internecie jest złudne. Każdy z nas pozostawia w sieci informacje na swój temat. Czasem udostępniamy je świadomie, a czasem — mimowolnie, nie zdając sobie z tego sprawy. Gdy wchodzisz na jakąś stronę, automatycznie zostają jej przesłane: Twój adres IP oraz informacje o przeglądarce (m. in. wersja przeglądarki, system operacyjny, język i czcionki). Są to dane, dzięki którym można Cię zidentyfikować. Aby sprawdzić, jak niewiele osób ma podobne ustawienia, możesz skorzystać z Panopticlick.eff.org. Im nasze ustawienia są bardziej nietypowe, tym łatwiej nas zidentyfikować i śledzić w sieci.

Różne podmioty (szczególnie komercyjne) są zainteresowane tymi danymi. Starają się zebrać ich jak najwięcej i w tym celu śledzą naszą aktywność w sieci. Wykorzystywane są do tego różne narzędzia; najpopularniejsze to ciasteczka (ang. **cookies**; służą one również do innych celów, np. poprawnego wyświetlania strony czy logowania). Na Twoim komputerze są zapisywane nie tylko ciasteczka strony WWW, z której korzystasz, ale również ciasteczka pochodzące od firm zewnętrznych (ang. **third part cookies**), do których stron odwołuje się strona, którą odwiedzasz. Za pomocą wtyczki Collusion możesz zobaczyć, kto na poszczególnych stronach próbuje Cię w ten sposób śledzić.

Jeśli na stronie, z której aktualnie korzystasz, znajdują się wtyczki Facebooka, Google+ czy innych serwisów społecznościowych (np. przycisk „Lubię to"), informacje na Twój temat wędrują również tam. Co więcej: jeżeli jesteś zalogowana/-y na te konta (choćby w tej chwili strony tych serwisów w Twojej przeglądarce były zamknięte) — zostaniesz zidentyfikowana/-y jako konkretna osoba. Jak widzisz, administratorzy serwisów społecznościowych, z których korzystasz, mogą bez większej trudności śledzić Twoją aktywność w sieci. Warto o tym pamiętać i wylogować się stamtąd podczas surfowania po Internecie. Jednak nawet jeśli nie jesteś zalogowana/-y — Facebook, Google lub inny serwis ustawią odpowiednie ciasteczko. Nie będzie ono przywiązane do Twojego profilu, ale po zalogowaniu — o ile nie usuniesz go wcześniej — określone informacje zostaną ze sobą połączone.

Tak jak trzeba myć ręce przed jedzeniem i zęby po posiłku, tak też należy zadbać o higienę podczas korzystania z Internetu. Nigdy nie zabezpieczymy się w stu procentach przed zagrożeniami związanymi z korzystaniem z Internetu, ale dzięki określonym zachowaniom możemy wyraźnie ograniczyć poziom śledzenia.

W tym celu warto zainstalować kilka przydatnych wtyczek do przeglądarek internetowych, jak np. Adblock (blokuje reklamy), Ghostery (blokuje wybrane skrypty śledzące), HTTPS Everywhere (automatycznie włącza bezpieczny protokół HTTPS tam, gdzie to możliwe) oraz Better Privacy (zarządza **flash cookies**, umożliwia ich skuteczne usuwanie przy zamykaniu przeglądarki). Warto też pamiętać o odpowiednich ustawieniach obsługi ciasteczek w swojej przeglądarce — np. o wyłączeniu obsługi ciasteczek umieszczanych przez witryny inne niż odwiedzana strona (alternatywnie można korzystać z odpowiednich wtyczek, np. Cookie Monster).

POMYSŁ NA LEKCJĘ

Zajęcia mają charakter praktyczny. Uczestnicy zapoznają się z wtyczką do przeglądarek, która pozwala monitorować, kto nas śledzi w Internecie. Poznają działanie narzędzi ograniczających śledzenie i nauczą się, jak z nich korzystać.

Cele operacyjne

Uczestnicy i uczestniczki:

- wiedzą, że ich aktywność w sieci jest śledzona przez różne podmioty;
- potrafią sprawdzić za pomocą wtyczki do przeglądarki Collusion, kto zbiera na ich temat informacje, gdy odwiedzają strony internetowe;
- potrafią wymienić wtyczki do przeglądarek internetowych zwiększające prywatność w sieci i opisać ich działanie.

Przebieg zajęć

1.

Czas: 5 min
Forma: wprowadzenie
Pomoce: **karta pracy dla grup „Świadomie w sieci"**

Powiedz, że na dzisiejszych zajęciach uczestnicy i uczestniczki będą pracować w 2-osobowych zespołach przy komputerach. Do wykonania będą mieli kilka zadań. Podziel uczestniczki i uczestników na zespoły. Każdemu zespołowi rozdaj **kartę pracy dla grup „Świadomie w sieci"**. Zwróć uwagę na:

- sprawne wykonywanie zadań (nietracenie czasu na inne czynności),
- zadawanie pytań w razie wątpliwości czy trudności.

2.

Czas: 10 min
Forma: praca wgrupach
Pomoce: pracownia komputerowa (jeden komputer na 2 osoby), **karta pracy dla grup „Świadomie w sieci"**

Poproś grupy o zapoznanie się z instrukcją do zadania 1 i o jego wykonanie. Po kilku minutach zapytaj grupy, jakich udzieliły odpowiedzi. Podsumuj, zwracając uwagę, że rozszerzenie Collusion daje nam wiedzę, kto jest zainteresowany informacjami o nas w sieci.

3.

Czas: 15 min
Forma: praca wgrupach
Pomoce: pracownia komputerowa (jeden komputer na 2 osoby), **karta pracy dla grup „Świadomie w sieci"**

Poproś grupy o zapoznanie się z instrukcją do zadania 2 i jego wykonanie. Po 10 minutach poproś grupy o podanie nazw podmiotów, które pojawiły się w ich grafie Collusion. Podsumowując, zwróć uwagę, że Collusion pokazuje nam, iż informacje o nas gromadzą

nie tylko strony internetowe, które odwiedzamy, ale również podmioty powiązane z nimi. Zachęć uczestników i uczestnicy do zainstalowania rozszerzenia w domu.

4.

Czas: 15 min
Forma: praca wgrupach
Pomoce: pracownia komputerowa (jeden komputer na 2 osoby), **karta pracy dla grup „Świadomie w sieci"**

Poproś grupy o zapoznanie się z instrukcją do zadania 3. Po 10 minutach chętne zespoły poproś o prezentację w 3–4 zdaniach wybranej wtyczki. Możesz również opowiedzieć o wtyczkach, korzystając z definicji, które znajdziesz w Słowniczku.

Ewaluacja

Czy uczestniczki i uczestnicy po przeprowadzonych zajęciach:

- wiedzą, że ich aktywność w sieci jest śledzona przez różne podmioty?
- potrafią zainstalować w przeglądarce wtyczkę Collusion i sprawdzić jej działanie?
- potrafią wymienić, jakie wtyczki do przeglądarek internetowych zwiększają prywatność w sieci; potrafią opisać ich działanie?

Opcje dodatkowe

Jeśli masz dostęp do rzutnika, filmik z ćwiczenia 2 warto obejrzeć wspólnie.

Jeśli masz więcej czasu i dostęp do rzutnika, otwórz stronę `https://panopticlick.eff.org` i kliknij przycisk „Test me". Tabela, która się wyświetla, pokazuje, jakie informacje są dostępne w trakcie korzystania z przeglądarki internetowej. Pogrubiona liczba na górze wskazuje, jak unikatowa — wśród innych testowanych — jest informacja wysyłana z Twojej przeglądarki. Zwróć uwagę, jak duża liczba informacji jest udostępniana przy samym wejściu do sieci. Zachęć uczniów do powtórzenia ćwiczenia na własnych komputerach w domu.

MATERIAŁY

Karta pracy dla grup „Świadomie w sieci"

ZADANIA SPRAWDZAJĄCE

Zadanie 1.

Przyporządkuj wtyczki do ich opisu.

Wtyczki:
Kategorie:

- Better Privacy
- Adblock
- HTTPS Everywhere
- Ghostery

Opisy:
Elementy do przyporządkowania:

- Wtyczka do przeglądarek internetowych blokująca wybrane skrypty śledzące. [rozwiązanie: 4]
- Wtyczka do przeglądarek internetowych, która zarządza flash cookies, a po zakończonej sesji usuwa je z dysku. [rozwiązanie: 1]
- 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; zmniejsza możliwość śledzenia użytkowników poprzez zapobieganie pobierania informacji z domen reklamodawców. [rozwiązanie: 2]
- Zwiększa bezpieczeństwo komunikacji w Internecie, wymuszając komunikację za pośrednictwem szyfrowanego protokołu HTTPS tam, gdzie jest to możliwe. [rozwiązanie: 3]

SŁOWNICZEK

- **Ghostery**: wtyczka do przeglądarek internetowych, która blokuje wybrane skrypty śledzące.
- **HTTPS Everywhere**: wtyczka do przeglądarek internetowych, która automatycznie włącza protokół HTTPS tam, gdzie istnieje taka możliwość.
- **Better Privacy**: wtyczka do przeglądarek internetowych, która zarządza flash cookies i umożliwia ich skuteczne usuwanie np. przy zamykaniu przeglądarki.
- **Protokół HTTPS**:
- **Flash cookies**: informacje przechowywane na komputerze przez wtyczkę Flash do przeglądarki. Zwykle wykorzystywane są podobnie jak standardowe ciasteczka, ale stanowią znacznie poważniejsze zagrożenie dla prywatności. Flash cookies pozwalają na zbieranie bardziej szczegółowych danych i znacznie większej ich liczby niż inne rodzaje ciasteczek. Mogą przesyłać informacje do zdalnego serwera bez wiedzy użytkowniczki czy użytkownika i nigdy nie wygasają.
- **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.
- **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.
- **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.

- **adres IP**: IP to protokół komunikacyjny używany powszechnie w Internecie i sieciach lokalnych. Adres IP to liczba, która jest nadawana każdemu urządzeniu lub grupie urządzeń połączonych w sieci. Służy on ich identyfikacji. Jeden adres publiczny może być współdzielony przez wiele komputerów połączonych w podsieć. W takiej sytuacji każdy komputer w podsieci ma adres z puli adresów prywatnych. Większość komputerów korzysta z adresów IP przydzielanych dynamicznie, tylko w czasie podłączenia komputera do sieci. Po jego wyłączeniu dany adres IP może zostać przypisany innemu urządzeniu.
- **anonimowość**: brak możliwości zidentyfikowania osoby.
- **cyfrowy ślad**: informacje na temat aktywności konkretnych osób w sieci, magazynowane na serwerach dostawców internetu i właścicieli stron. Tworzą go m.in. zdjęcia, informacje o kupionych produktach, nicki, wpisy na blogach, ale również dane, które zostawiamy w sieci mimowolnie, np. adres IP czy informacja o systemie operacyjnym, z którego korzystamy.
- **profilowanie**: oparty na określonych algorytmach mechanizm, który służy kategoryzowaniu ludzi według ich cech, zachowań, preferencji. Jest stosowany m.in. w marketingu internetowym w celu prezentowania reklam dopasowanych jak najściślej do potrzeb określonych użytkowniczek i użytkowników sieci, w branży bankowej i ubezpieczeniowej w celu oceny klienta, a także przez państwo w celu zwiększenia bezpieczeństwa (np. No Fly List w USA).

CZYTELNIA

- Gary Kovacs, „**Śledzenie śledzących**", TED [dostęp: 9.06.2013]: `http://www.ted.com/talks/gary_kovacs_tracking_the_trackers.html`.
- Grzegorz Prujszczyk, Kamil Śliwowski, „**Browsing wirtualne zagrożenia**" [dostęp: 13.06.2013]: `http://www.panoptykon.org/sites/panoptykon.org/files/panoptykon_poradnik_browsing.pdf`.
- Grzegorz Prujszczyk, Kamil Śliwowski, „**Bezpieczeństwo informacyjne w serwisach web 2.0**" [dostęp: 13.06.2013]: http://www.panoptykon.org/biblioteka/bezpieczenstwo-informacyjne-w-serwisach-web-20.
- **TOR and HTTPS**, EFF [dostęp: 13.06.2013]: https://www.eff.org/pages/tor-and-https.

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

Źródło: http://edukacjamedialna.edu.pl/lekcje/kto-nas-sledzi-w-sieci/.

Publikacja zrealizowana w ramach projektu „Świadomie i bezpiecznie w świecie mediów i informacji".

Podstawa programowa:

Informatyka, IV 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.
Treści nauczania
Bezpieczne posługiwanie się komputerem, jego oprogramowaniem i korzystanie z sieci komputerowej.
Wykorzystywanie komputera i technologii informacyjno-komunikacyjnych do rozwijania zainteresowań, opisywanie zastosowań informatyki, ocena zagrożeń i ograniczeń, aspekty społeczne rozwoju i zastosowań informatyki.

Nowa podstawa programowa:

Informatyka, liceum i technikum
Treści nauczania
zapoznaje się z możliwościami nowych urządzeń cyfrowych i towarzyszącego im oprogramowania.
objaśnia funkcje innych niż komputer urządzeń cyfrowych i korzysta z ich możliwości.
rozwiązuje problemy korzystając z różnych systemów operacyjnych.
charakteryzuje sieć internet, jej ogólną budowę i usługi, opisuje podstawowe topologie sieci komputerowej, przedstawia i porównuje zasady działania i funkcjonowania sieci komputerowej typu klient-serwer, peer-to-peer, opisuje sposoby identyfikowania komputerów w sieci.
stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji.