CYFROWA WYPRAWKA

Kto nas śledzi w sieci?

Informacje o lekcji

Eksperci:	Wojciech Budzisz, Kamil Śliwowski, Michał „rysiek" Woźniak
Autorka wiedzy w pigułce:	Urszula Dobrzańska
Autorka scenariusza:	Weronika Paszewska
Organizacja publikująca:	Fundacja Panoptykon
Przedmiot:	Informatyka
Sugerowany poziom kształcenia:	Szkoły ponadgimnazjalne
Licencja:	Creative Commons Uznanie autorstwa – Na tych samych warunkach 3.0 Polska

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 Lightbeam (która zastąpiła starszą wtyczkę 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 widać, administratorzy serwisów społecznościowych, z których korzystamy, mogą bez większej trudności śledzić naszą 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), Disconnect (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 Lightbeam, 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

Ćwiczenie 1.

Czas: *5 min*

Metoda: *wprowadzenie osoby prowadzącej*

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.

Ćwiczenie 2.

Czas: *10 min*

Metoda: *praca w grupach*

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 Lightbeam daje nam wiedzę, kto jest zainteresowany informacjami o nas w sieci.

Ćwiczenie 3.

Czas: *15 min*

Metoda: *praca w grupie*

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 Lightbeam. Podsumowując, zwróć uwagę, że Lightbeam pokazuje nam, iż informacje o nas gromadzą nie tylko strony internetowe, które odwiedzamy, ale również podmioty powiązane z nimi. Zachęć uczestników i uczestniczki do zainstalowania rozszerzenia w domu.

Ćwiczenie 4.

Czas: *15 min*

Metoda: *praca w grupie*

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 uczestnicy i uczestniczki po przeprowadzonych zajęciach:

- wiedzą, że ich aktywność w sieci jest śledzona przez różne podmioty?
- potrafią zainstalować w przeglądarce wtyczkę Lightbeam 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.

Better Privacy	Wtyczka do przeglądarek internetowych blokująca wybrane skrypty śledzące.
Adblock	Wtyczka do przeglądarek internetowych, która zarządza *flash cookies*, a po zakończonej sesji usuwa je z dysku.
HTTPS Everywhere	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.
Disconnect	Zwiększa bezpieczeństwo komunikacji w Internecie, wymuszając komunikację za pośrednictwem szyfrowanego protokołu HTTPS tam, gdzie jest to możliwe.

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.

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 konkretnej osoby.

Better Privacy – wtyczka do przeglądarek internetowych, która zarządza *flash cookies* i umożliwia ich skuteczne usuwanie np. przy zamykaniu przeglądarki.

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.

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.

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.

Disconnect – 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.

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).

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.

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. Gary Kovacs, *Śledzenie śledzących*, TED [dostęp: 9.06.2013]: http://www.ted.com/talks/gary_kovacs_tracking_the_trackers.html.
2. Małgorzata Szumańska, *Co warto wiedzieć o śledzeniu i profilowaniu w sieci*, Fundacja Panoptykon [dostęp: 23.12.2014]: http://cyfrowa-wyprawka.org/teksty/co-warto-wiedziec-o-sledzeniu-profilowaniu-w-sieci.
3. Anna Obem, Michał „czesiek" Czyżewski, Katarzyna Szymielewicz, *Prywatność – zrób to sam!*, Fundacja Panoptykon [dostęp: 23.12.2014]: http://cyfrowa-wyprawka.org/teksty/prywatnosc-zrob-sam.
4. Kamil Śliwowski, Anna Obem, *Odzyskaj kontrolę w sieci. Odcinek I: przeglądarka*, Fundacja Panoptykon [dostęp: 19.10.2015] http://cyfrowa-wyprawka.org/teksty/odzyskaj-kontrole-w-sieci-odcinek-przegladarka.
5. 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.
6. Kamil Śliwowski, Anna Obem, *Odzyskaj kontrolę w sieci. Odcinek IV: Google*, Fundacja Panoptykon [dostęp: 19.10.2015] http://cyfrowa-wyprawka.org/teksty/odzyskaj-kontrole-w-sieci-odcinek-iv-google.
7. *TOR and HTTPS*, EFF [dostęp: 13.06.2013]: https://www.eff.org/pages/tor-and-https.

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

Projekt współfinansowany ze środków Ministra Kultury i Dziedzictwa Narodowego.