CYFROWA WYPRAWKA

# Informacja – cena internetowych usług

## Informacje o lekcji

| | |
|---|---|
| Opracowanie wiedzy w pigułce: | Małgorzata Szumańska |
| Autorka scenariusza: | Izabela Meyza |
| Organizacja publikująca: | Fundacja Panoptykon |
| Źródło: | Lekcja powstała na bazie lekcji „Informacje o nas w sieci" opublikowanej przez Fundację Nowoczesna Polska w ramach projektu „Edukacja medialna" (tekst: Joanna Ruta Baranowska, scenariusz: Weronika Paszewska, konsultacja merytoryczna: Piotr Waglowski, Dorota Głowacka) |
| Przedmiot: | Informatyka |
| Sugerowany poziom kształcenia: | Szkoły gimnazjalne |
| Licencja: | Creative Commons Uznanie autorstwa – Na tych samych warunkach 3.0 Polska |

## Wiedza w pigułce

Korzystanie z Internetu nieuchronnie wiąże się z udostępnianiem informacji o sobie. Niektóre z nich ujawniamy świadomie (np. opisywanie swoich zainteresowań na portalach społecznościowych). Wiele usług zachęca do podawania różnych danych (np. przy zawieraniu umowy, przez podsuwanie ankiet), jednak sporo cyfrowych śladów zostawiamy po sobie mimowolnie, czasem nawet nie zdając sobie z tego sprawy.

Już samo wejście na dowolną stronę internetową uruchamia przepływ danych. Administrator strony automatycznie uzyskuje: nasz adres IP oraz informacje o przeglądarce, z której korzystamy (m.in. wersja, system operacyjny, język i czcionki). Strony, które odwiedzamy, wykorzystują różne mechanizmy służące pozyskaniu informacji. Najpopularniejsze są ciasteczka (ang. *cookies*), czyli specjalne pliki zapisywane na komputerze użytkownika. Ciasteczka mogą służyć różnym celom – część z nich jest niezbędna do prawidłowego wyświetlania strony bądź logowania. Zadaniem pozostałych jest zdobycie cennych informacji.

Warto wiedzieć, że w Internecie jesteśmy śledzeni nie tylko przez strony, na które akurat wchodzimy. Na komputerach mogą być zapisywane również ciasteczka innych stron (ang. *third party cookies*). Informacje o nas mogą trafiać do baz danych firm udostępniających systemy do prowadzenia statystyk (np. Google Analytics) lub serwisów społecznościowych (np. Facebook, Google+).

Zbierane w sieci dane są tak szczegółowe, że pozwalają na śledzenie konkretnych użytkowników. Nawet jeśli nie podamy swojego imienia i nazwiska albo nasze dane zostaną zanonimizowane (czyli oderwane od personaliów), nasza identyfikacja jest możliwa. Badania naukowców z Massachusetts Institute of Technology

pokazują, jak niewiele potrzeba, by konkretną osobę odróżnić od innych: wystarczy znać cztery lokalizacje, w których bywa.

Tylko pozornie korzystanie z internetowych usług (np. z wyszukiwarek, portali społecznościowych, gier) jest darmowe. Ceną jest udostępnianie informacji o sobie. Na podstawie informacji o cechach i zachowaniach (np. płci, wieku czy historii wyszukiwań) poszczególni ludzie są dzieleni na kategorie (wkładani do różnych szufladek). W ten sposób internetowe firmy starają się określić, jakie produkty najlepiej pasują do użytkownika oraz jakie reklamy i kiedy do niego skierować.

Ten mechanizm nazywany jest profilowaniem. Wykorzystywany jest nie tylko przez branżę reklamową, ale i przez najpopularniejsze wyszukiwarki (np. Google, Bing). Bazując na historii zapytań, dopasowują one wyniki do użytkowników. Dzięki temu na przykład pasjonat gier online będzie otrzymywał od wyszukiwarki odpowiedzi dopasowane (statystycznie) do swoich zainteresowań. Tak właśnie działa efekt bańki filtrującej (ang. *filter bubble*). Na krótką metę może ułatwiać życie, podsuwając najbardziej oczywiste rozwiązania, na dłuższą – ograniczać dostęp do różnych informacji.

Jeśli chcesz chronić informacje o sobie i mieć kontrolę nad tym, w jaki sposób są one wykorzystywane przez internetowe firmy, przejstrzegaj następujących zasad:

1. Korzystaj z nicków, a nie imienia i nazwiska. Udostępniaj jak najmniej danych na swój temat.
2. Zastanów się, z jakich usług w sieci chcesz korzystać (np. portali społecznościowych).
3. Jeśli możesz coś nabyć w kiosku obok domu, nie kupuj tego przez Internet.
4. Zwróć uwagę na regulamin usług, z których korzystasz (np. na to, do jakich danych ma dostęp aplikacja instalowana na komórce). Nie korzystaj z usług, które pobierają wiele danych w niejasnym celu.
5. Świadomie konfiguruj ustawienia prywatności serwisów, z których korzystasz. Staraj się ograniczać ilość informacji, które mogą trafić do innych osób.
6. Nie korzystaj z programów, które zbierają i udostępniają Twoją lokalizację, np. dodając ją do Twojego wpisu.
7. Wyloguj się za każdym razem, gdy skończysz korzystać z jakiejś usługi (z poczty, serwisów społecznościowych itp.).
8. Zadbaj o czyszczenie ciasteczek. Wykorzystaj ustawienia przeglądarki lub odpowiednich wtyczek (np. CookieMonster). Korzystaj z innych narzędzi pomagających chronić prywatność (Disconect, Better Privacy).
9. Korzystaj z wyszukiwarek internetowych, które nie wykorzystują profilowania, np. z Duckduckgo.com, Ixquick.com.

## Pomysł na lekcję

Uczestnicy i uczestniczki dowiedzą się, jakie informacje o ich aktywności w sieci są zbierane i zastanowią się nad tym, jakie to może mieć skutki. Dowiedzą się także, w jaki sposób ich dane mogą być przetwarzane i wykorzystywane w celach marketingowych.

## Cele operacyjne

Uczestnicy i uczestniczki:

- wiedzą, że poruszając się po sieci, przekazują różnym podmiotom informacje o sobie (świadomie bądź nieświadomie);
- wiedzą, że ich dane mogą być gromadzone w celach marketingowych;
- są bardziej świadomi swoich działań związanych z prywatnością w sieci.

## Przebieg zajęć

### Ćwiczenie 1.

***Czas:*** *10 min*

***Metoda:*** *burza mózgów*

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

Zadaj uczniom pytanie:

- Z jakich stron w Internecie najczęściej korzystacie?

Mogą to być konkretne strony lub sposoby korzystania z Internetu (np. granie w gry, przeglądanie gazet internetowych, serwisy newsowe, portale społecznościowe). Zapisuj informacje uzyskane od grupy w formie mapy myśli.

Następnie podsumuj wypowiedzi uczniów (np. „Widzę, że często korzystacie z portali społecznościowych" czy „Część z Was korzysta z serwisów newsowych").

Zadaj kolejne pytanie:

- Czy za wejście na którąś z tych stron trzeba płacić?

Zwróć uwagę na to, że najczęściej w Internecie nie płacimy za treści, z których korzystamy (np. za artykuły, gry, czytanie blogów). Możemy na przykład czytać artykuły na portalu informacyjnym, za co zazwyczaj nie płacimy (a za gazetę z kiosku – tak). Zadaj kolejne pytanie: „Jak myślicie, dlaczego to jest możliwe?". Zwróć uwagę, że za tymi treściami stoją konkretni ludzie, którzy je opracowali (np. dziennikarz, który pisze artykuł do gazety, zwykle musi wykonać tyle samo pracy co dziennikarz, który publikuje na portalu internetowym, a czytanie tego ostatniego jest bezpłatne).

Powiedz, że większość treści w Internecie tylko pozornie jest darmowa. Bardzo wiele stron żyje z reklam, sięga po nasze dane i sprzedaje je firmom, które analizują nasze zachowania w sieci. Zaznacz, że na dzisiejszych zajęciach bliżej przyjrzymy się temu problemowi.

### Ćwiczenie 2.

***Czas:*** *20 min*

***Metoda:*** *praca w grupach*

***Pomoce:*** *karta pracy nr 1 i nr 2 „Informacje o nas w sieci"*

Podziel uczniów na 4- lub 5-osobowe grupy. Każdej grupie daj wydrukowaną instrukcję nr 1 i poproś o wykonanie zadania. Kiedy wszystkie grupy skończą, poleć, żeby przekazały kartkę z odpowiedziami grupie siedzącej obok (np. zgodnie z ruchem wskazówek zegara). Wszystkim grupom rozdaj kartki z instrukcją nr 2. Kiedy grupy skończą, poproś o przeczytanie wyników pracy na forum. Następnie poproś, by osoby, których dotyczą opisy, ujawniły się i powiedziały, ile z tego opisu się zgadza. Zauważ, że gdyby grupy miały dostęp tylko do jednej informacji o osobie, trudniej byłoby coś o niej powiedzieć, natomiast kilka danych daje znacznie więcej. Zwróć też uwagę na to, jak na podstawie kilku pozornie niezwiązanych ze sobą informacji można stworzyć obraz danej osoby, a także na to, że nie zawsze jest on prawdziwy.

Powiedz, że nawet jeśli podajemy w Internecie informacje, które wydają się nieważne, ktoś może te informacje wyłapywać i na ich podstawie tworzyć nasz obraz. Na podstawie „Wiedzy w pigułce" opowiedz uczestnikom, jak działa profilowanie w sieci (możesz zapytać, czy zdarzyło im się wpisywać w wyszukiwarkę tę samą frazę na dwóch różnych komputerach; zauważ, że wyniki są inne, ponieważ są sprofilowane pod konkretnych użytkowników komputerów).

Zapytaj, nawiązując do poprzedniego ćwiczenia:

- Jak myślicie, czy łatwo jest kogoś zidentyfikować na podstawie informacji, które o sobie zamieszcza?

Zwróć uwagę, że nawet jeżeli nie podamy swojego imienia i nazwiska, a podamy dużo z pozoru nieistotnych danych na swój temat (np. osoba z III klasy waszego gimnazjum, która jest dziewczynką, ma psa, granatowy plecak i słucha muzyki rockowej – staraj się podać przykład adekwatny do klasy), to będzie nas można łatwo zidentyfikować. Powiedz, że jeszcze łatwiej nas zidentyfikować, kiedy korzystamy z Internetu w komórce (podaj przykład badań robionych przez naukowców z Massachusetts Institute of Technology z „Wiedzy w pigułce").

## Ćwiczenie 3.

***Czas:*** *10 min*

***Metoda:*** *burza mózgów*

***Pomoce:*** *brak*

Zapytaj uczniów:

- Po co ktoś chciałby pozyskiwać Wasze dane?

Korzystając z „Wiedzy w pigułce", powiedz, że informacje, które zamieszczamy na swój temat w Internecie, są zbierane głównie w celach marketingowych.

Zwróć uwagę, że tylko pozornie wyszukiwarki (np. Google) czy portale społecznościowe (np. Facebook) są bezpłatne. W rzeczywistości, korzystając z nich, udostępniamy swoje dane, które mogą być poddane analizie, dzięki czemu wiadomo, jakimi reklamami możemy być zainteresowani.

Zaznacz, że taka sytuacja może się pozornie wydawać atrakcyjna, bo zazwyczaj trafiają do nas produkty, które chcemy dostać.

Zapytaj:

- Czy widzicie jakieś minusy zamieszczania swoich danych w sieci?

Zbierz wypowiedzi grupy. Nawiązując do poprzedniego ćwiczenia, podkreśl, że obraz tworzony na podstawie naszych danych wcale nie musi być prawdziwy, lecz stereotypowy (zauważ, że kiedy ktoś proponuje nam

produkty na podstawie stereotypu dotyczącego np. płci, wieku czy miejsca zamieszkania, możemy czuć się niekomfortowo). Przypomnij też, że kiedy zamieszczamy informacje na swój temat w sieci, musimy mieć świadomość, że one nie znikają po zakończeniu naszej pracy. Mogą zostać tam na zawsze.

### Ćwiczenie 4.

***Czas:*** *5 min*

***Metoda:*** *praca w parach*

***Pomoce:*** *brak*

Na koniec poproś, żeby uczestnicy w parach odpowiedzieli sobie na pytanie:

- Jakich informacji o sobie na pewno nie warto publikować w sieci?

## Ewaluacja

Czy po przeprowadzeniu zajęć ich uczestnicy i uczestniczki:

- mają świadomość, że duża część treści dostępnych Internecie jest tylko pozornie darmowa?
- wiedzą, że poruszając się po sieci, zostawiają w niej wiele śladów?
- wiedzą, że informacje publikowane i zbierane przy okazji korzystania z sieci mogą być wykorzystywane w celach marketingowych?

## Opcje dodatkowe

Opcją dodatkową może być wspólne obejrzenie wystąpienia Gary'ego Kovacsa „Śledzenie śledzących" (http://www.ted.com/talks/gary_kovacs_tracking_the_trackers.html?quote=1583 dostępny z polskimi napisami). Po wystąpieniu porozmawiajcie o tym, kto śledzi w Internecie użytkowników. Pytania pomocnicze:

- Co pokazywał program zaprezentowany przez Gary'ego?
- Jak Gary i jego córka spędzali czas w sieci?
- W jakich celach ktoś może zbierać o nas informacje?

## Materiały

Karta pracy nr 1 i nr 2 „Informacje o nas w sieci"

## Zadania sprawdzające

Zadanie 1

Prawda czy fałsz?

1. __ W Internecie możliwe jest zidentyfikowanie kogoś, kto nie podał swojego imienia i nazwiska. Wystarczy zebrać odpowiednią ilość informacji o nim.
2. __ Informacje zbierane w sieci wykorzystywane są głównie przez administratorów portali po to, żeby mnie chronić przed internetowymi przestępcami.

3. __ Niektóre gazety internetowe są darmowe, bo ich redakcje nie muszą płacić za druk.

## Słowniczek

**Adres IP** – IP to protokół komunikacyjny używany powszechnie w Internecie i sieciach lokalnych. Adres IP to liczba, która jest nadawana każdemu urządzeniu lub każdej grupie urządzeń połączonych w sieć. 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.

**Bańka filtrująca** (ang. *filter bubble*) – sytuacja, w której na skutek działania określonego algorytmu osoba korzystająca z sieci otrzymuje wyselekcjonowane informacje, dobrane na podstawie informacji dostępnych na jej temat, takich jak lokalizacja czy historia wyszukiwania.

**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 są w stanie 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.

**Geolokalizacja** – określenie fizycznego położenia geograficznego osoby i urządzenia telekomunikacyjnego za pomocą systemu GPS lub adresu IP.

**Media społecznościowe** – różnorodne narzędzia umożliwiające użytkownikom Internetu rozbudowaną interakcję. W zależności od charakteru tej interakcji wyróżniamy wśród nich fora, czaty, blogi, portale społecznościowe, społeczności gier sieciowych, serwisy crowdfundingowe i wiele innych.

**Nick** (ang. *nickname* – przezwisko, pseudonim) – podpis (niebędący imieniem i nazwiskiem) wykorzystywany przez użytkowników sieci.

**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).

**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, *Co warto wiedzieć o śledzeniu i profilowaniu w sieci?*, Fundacja Panoptykon [dostęp: 21.07.2014]: http://cyfrowa-wyprawka.org/teksty/co-warto-wiedziec-o-sledzeniu-profilowaniu-w-sieci.
2. 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.
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. 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.
5. Kamil Śliwowski, Anna Obem, *Odzyskaj kontrolę w sieci. Odcinek V: alternatywne wyszukiwarki*, Fundacja Panoptykon [dostęp: 19.10.2015]: http://cyfrowa-wyprawka.org/teksty/odzyskaj-kontrole-w-sieci-odcinek-v-alternatywne-wyszukiwarki.
6. Eli Pariser, *Uważaj na internetowe »bańki z filtrami«*, TED [dostęp: 21.07.2014]: http://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles.html.



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

*Projekt współfinansowany ze środków Ministra Kultury i Dziedzictwa Narodowego.*