Twój cyfrowy ślad

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

Z Internetu korzystamy w wielu codziennych sytuacjach, zarówno w celach prywatnych, jak i oficjalnych. Zwykle nie zastanawiamy się nad tym, że posługując się urządzeniem podłączonym do sieci, pozostawiamy po sobie mnóstwo cyfrowych śladów – nie tylko w wyniku celowego zamieszczania informacji w postaci tekstu, zdjęć czy wideo, ale także (często nieświadomie) na skutek korzystania z aplikacji w smartfonie czy przeglądarki internetowej.

W Internecie każdy z nas kształtuje swój wizerunek: udzielając się na forach dyskusyjnych, komentując artykuły, korzystając z portali społecznościowych (Facebook, Flickr, Filmweb), prowadząc blogi. Czy zawsze warto te aktywności podejmować pod własnym nazwiskiem? Materiałów raz zamieszczonych w sieci nie da się tak po prostu usunąć. Dobrze czasem zapytać: „Jeśli ktoś znałby mnie tylko z sieci, to co mógłby o mnie powiedzieć? " i… „Czy na pewno by mi się to podobało?".

Trzeba mieć świadomość, że w Internecie udostępniamy informacje na swój temat nie tylko samodzielnie, tj. w sposób intencjonalny (statusy, komentarze), ale także w sposób automatyczny (zestaw informacji podawanych przez przeglądarkę, w tym adres IP, język, system operacyjny, czcionki) oraz półautomatyczny (geolokalizacja – np. przez Endomondo, popularną aplikację na smartfona). E-maile odebrane przez usługę Gmail są skanowane i na podstawie najczęściej występujących słów są użytkownikom dobierane reklamy. Niektóre aplikacje w smartfonie żądają m.in. dostępu do listy kontaktów czy zawartości kalendarza. Wyszukiwarka Google zapamiętuje historię zapytań – a w oparciu o treści, które tam pozostawiasz, można Cię zidentyfikować (przydatne: Tosdr.org). Smartfon, nawet przy wyłączonej funkcji GPS, zapamiętuje lokalizacje na podstawie sieci Wi-Fi, które „spotyka" w różnych miejscach.

Udostępnianie danych na swój temat ma swoje konsekwencje krótko- i długoterminowe. Zamieszczenie filmu z imprezy na YouTube dziś może się wydawać świetnym pomysłem licealiście, ale za kilka miesięcy lub lat to nagranie może obejrzeć potencjalny pracodawca. Internet to globalna tablica ogłoszeń: każdy może się zapoznać z zamieszczonymi tam materiałami i wyciągnąć z nich wnioski – niekoniecznie po naszej myśli. Gdy

opublikujemy coś w sieci, tracimy kontrolę nad informacją. Może ona zostać wykorzystana przez kogoś na naszą niekorzyść. Niestety, nie zawsze jesteśmy w stanie to przewidzieć.

Twoje dane gromadzą różne podmioty, m.in. operatorzy sieci komórkowych, producenci telefonów i oprogramowania, dostawcy usług internetowych, agencje reklamowe. Dla wielu stanowią łakomy kąsek: część firm dzięki reklamom zarabia na nich już teraz, ubezpieczyciel lub bank może zrobić z nich użytek w przyszłości, a do wszystkiego – w razie potrzeby – otrzyma dostęp państwo.

Wskazówki, które warto przekazać uczestnikom i uczestniczkom zajęć:

1. Pamiętaj, by podawać tylko dane niezbędne do skorzystania z określonej usługi.
2. Unikaj posługiwania się prawdziwym nazwiskiem. Nigdy nie publikuj w sieci intymnych informacji; unikaj publikowania prywatnych danych.
3. Jeśli korzystasz z serwisów społecznościowych, zadbaj o odpowiednie ustawienia prywatności. Im mniej informacji udostępniasz osobom postronnym, tym lepiej. Zważ jednak, że dostęp do tego, co zamieszczasz, zawsze ma usługodawca, który może się tym podzielić z innymi podmiotami – a na to nie masz już wpływu. Zastanów się, czy na pewno warto z tych serwisów korzystać.
4. Zastanów się, czy korzystać z usług sklepów internetowych. Może lepiej zrobić zakupy poza siecią i – zamiast mnożyć swoją kartą płatniczą elektroniczne ślady – zapłacić gotówką?
5. Staraj się nie udostępniać informacji o sobie w sposób półautomatyczny. Na przykład nie korzystaj z możliwości „oznaczanie się" w miejscu pobytu.

Pomysł na lekcję

W trakcie zajęć przybliżony zostanie temat udostępniania w sieci informacji o sobie. Uczestnicy i uczestniczki zapoznają się z różnymi sposobami udostępniania informacji: automatycznym, półautomatycznym i samodzielnym. Przedstawione zostaną przykładowe sposoby służące ograniczeniu liczby udostępnianych informacji i ułatwieniu dbania o prywatność w sieci. Uczestnicy i uczestniczki będą mieli okazję zastanowić się, które z nich są skłonni wykorzystać.

Cele operacyjne

Uczestnicy i uczestniczki:

- rozumieją, że informacje mogą być udostępniane w sieci nie tylko samodzielnie przez użytkowników;
- wiedzą, jakie informacje udostępniają o sobie, używając przeglądarki internetowej, smartfonów i aplikacji;
- wiedzą, że ujawnianie informacji o sobie w sieci może mieć różne trudne do przewidzenia konsekwencje;
- wiedzą, że informacji z sieci nie da się usunąć;
- umieją ograniczać liczbę informacji udostępnianych o sobie w sieci;
- wiedzą, jakie zachowania pomagają chronić prywatność.

Przebieg zajęć

Ćwiczenie 1.

Czas: *15 min*

Metoda: *praca indywidualna, rozmowa*

Pomoce: *wydrukowany i pocięty materiał pomocniczy dla grup „Informacje o nas w sieci", materiał pomocniczy dla prowadzących „Informacje o nas w sieci – odpowiedzi"*

Podziel uczestników i uczestniczki na pary. Każdej parze rozdaj jedną historię z wydrukowanego i pociętego materiału pomocniczego dla grup „Informacje o nas w sieci". Poproś o zapoznanie się z historiami. Następnie rozpocznij rozmowę, zadając pytanie: „Jakie informacje o sobie udostępniali w sieci Justyna i Hubert?". Podziel tablicę na 2 części: Justyna i Hubert. Zapisuj na tablicy przykłady podawane przez grupy.

Pytania pomocnicze, które możesz zadać:

- Jakich konsekwencji może doświadczyć Justyna, jeśli informacja, o której godzinie biega, wpadnie w niepowołane ręce?
- Kto może być zainteresowany informacjami o hobby Huberta?

W razie potrzeby uzupełnij wypowiedzi uczestników, korzystając z materiału pomocniczego dla prowadzących „Informacje o nas w sieci – odpowiedzi".

Ćwiczenie 2.

Czas: *5 min*

Metoda: *miniwykład osoby prowadzącej*

Pomoce: *Wiedza w pigułce*

Korzystając z Wiedzy w pigułce, opowiedz, jakie informacje udostępniamy o sobie w sieci:

- informacje zamieszczane automatycznie (informacje o systemie operacyjnym, przeglądarce internetowej, zestawie zainstalowanych czcionek, numerze IP);
- informacje zamieszczane półautomatycznie (geolokalizacja, informacje w plikach zdjęciowych o godzinie wykonania zdjęcia i modelu aparatu fotograficznego, statusy na portalach społecznościowych – np. dotyczące geolokalizacji);
- informacje zamieszczane samodzielnie (statusy na portalach społecznościowych, wpisy na forach, e-maile).

Zwróć uwagę, że informacje o nas gromadzą różne podmioty: operatorzy sieci komórkowych, producenci telefonów i oprogramowania, usługodawcy internetowi. Informacje, które raz znajdą się w sieci, pozostają w niej na zawsze – sieć nie zapomina.

Ćwiczenie 3.

Czas: *25 min*

Metoda: *praca w grupach, prezentacja*

Pomoce: *karta pracy „Ograniczanie informacji", materiał pomocniczy dla prowadzących „Ograniczanie informacji – odpowiedzi", długopisy*

Podziel uczestniczki i uczestników na 4-osobowe grupy. Każdej grupie rozdaj jedną historię z karty pracy „Ograniczanie informacji". Poproś grupy o zastanowienie się nad odpowiedziami na pytania i wymienienie zachowań, które ograniczyłyby liczbę ujawnianych o sobie informacji w sieci. W razie potrzeby wprowadź uczestników do ćwiczenia, podając przykład sytuacji, w której odpowiedzialne zachowanie uchroniłoby osobę przed negatywnymi konsekwencjami (np. nieumieszczenie zdjęć z imprezy w sieci, na które trafił potencjalny pracodawca i zrezygnował z zatrudnienia). Po 10 minutach poproś grupy o prezentację swoich rozwiązań.

Podsumowując, zwróć uwagę na to, że:

- każda nasza aktywność w sieci zostawia po sobie ślad;
- nie powinniśmy podawać swojego imienia, nazwiska, adresu zamieszkania w sieci tak, żeby inni mieli do nich łatwy dostęp;
- trzeba zwracać uwagę, jakie informacje o sobie ujawniamy i udostępniać tylko te, które są niezbędne;
- sieć nie zapomina, raz zamieszczone informacje bardzo trudno z niej usunąć;
- nie wszystkie konsekwencje zamieszczonych o nas informacji da się przewidzieć;
- niezależnie od ustawień prywatności informacje, które nie są widoczne dla innych użytkowników, są znane usługodawcy.

Ewaluacja

Czy uczestnicy i uczestniczki po przeprowadzonych zajęciach:

- rozumieją, że informacje mogą być udostępniane w sieci nie tylko samodzielnie przez użytkowników?
- wiedzą, jakie informacje udostępniają o sobie, korzystając z przeglądarki internetowej, smartfonów i aplikacji?
- wiedzą, że ujawnianie informacji o sobie w sieci może mieć różne, trudne do przewidzenia konsekwencje?
- wiedzą, że informacji z sieci nie da się usunąć?
- umieją ograniczać liczbę informacji udostępnianych o sobie w sieci?
- wiedzą, że są zachowania, które pomagają chronić ich prywatność?

Opcje dodatkowe

Ćwiczenie 3 można rozwinąć lub zmodyfikować o podawanie przez uczestników i uczestniczki przykładów sytuacji, w których ktoś nie zadbał o swoją prywatność. Mogą to być zachowania w sieci, w których szczególnie warto ograniczyć liczbę ujawnianych informacji i zadbać o swoją prywatność.

Materiały

- Materiał pomocniczy dla grup „Informacje o nas w sieci"
- Karta pracy „Ograniczanie informacji"
- Materiał pomocniczy dla prowadzących „Informacje o nas w sieci – odpowiedzi"

- Materiał pomocniczy dla prowadzących „Ograniczanie informacji – odpowiedzi”

Zadania sprawdzające

Zadanie 1

Zaznacz zdania prawdziwe i fałszywe:

1. __ Informacja o naszym położeniu dodawana do nowego statusu na portalu społecznościowym to przykład informacji zamieszczonej półautomatycznie.
2. __ Odpowiednie ustawienia prywatności na portalu społecznościowym ograniczają liczbę dostępnych o nas informacji.
3. __ Większość informacji da się skutecznie usunąć z sieci.
4. __ Zamieszczanie informacji o sobie w sieci może mieć trudne do przewidzenia konsekwencje w przyszłości.
5. __ Dostawca Internetu nie gromadzi żadnych informacji o użytkownikach sieci.

Zadanie 2

Zaznacz prawidłowe odpowiedzi (więcej niż jedna). Informacje o nas zamieszczane w sieci automatycznie to:

- ☐ numer IP
- ☐ informacja o systemie operacyjnym
- ☐ zawartość dysku twardego
- ☐ informacja o używanej przeglądarce internetowej
- ☐ informacja o modelu komputera
- ☐ informacja o stanie baterii komputera
- ☐ zestaw czcionek zainstalowanych w systemie

Słowniczek

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.

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.

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.

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).

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).

Czytelnia

1. Barbara Gubernat, *Internet wie, co robisz*, Fundacja Panoptykon [dostęp: 23.06.2013]: http://www.panoptykon.org/wiadomosc/internet-wie-co-robisz.
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 III: ustawienia prywatności na Facebooku*, Fundacja Panoptykon [dostęp: 19.10.2015] http://cyfrowa-wyprawka.org/teksty/odzyskaj-kontrole-w-sieci-odcinek-iii-ustawienia-prywatnosci-na-facebooku.
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.

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

Projekt współfinansowany ze środków Ministra Kultury i Dziedzictwa Narodowego.