edukacja medialna

Twój cyfrowy ślad

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. Zastanów się, czy 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?".

Miej świadomość, że w Internecie udostępniamy informacje na swój temat nie tylko samodzielnie, tj. w sposób świadomy (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). Twoje e-maile odebrane przez usługę Gmail są skanowane i na podstawie najczęściej występujących słów zostają dobrane reklamy. Niektóre aplikacje w smartfonie żądają m. in. dostępu do Twojej listy kontaktów czy zawartości kalendarza. Wyszukiwarka Google zapamiętuje historię zapytań — a w oparciu o treści, które tam pozostawiasz, można Cię zidentyfikować (przydatne: Tosdr.org).

Udostępnianie danych na swój temat ma swoje konsekwencje krótko — i długoterminowe. Zamieszczenie filmu z imprezy na YouTube dziś może Ci się wydawać świetnym pomysłem, ale czy chcesz, by mógł zobaczyć go Twój potencjalny pracodawca? Internet to globalna tablica ogłoszeń: każdy może się zapoznać z zamieszczonymi tam materiałami i wyciągnąć z nich wnioski — niekoniecznie po Twojej 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. 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 dla uczestników i uczestniczek:

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

1.

Czas: 15 min
Forma: 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:

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

3. W razie potrzeby uzupełnij wypowiedzi uczestników, korzystając z **materiału pomocniczego „Informacje o nas w sieci — odpowiedzi"**.

2.

Czas: 5 min
Forma: 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.

3.

Czas: 25 min
Forma: praca wgrupach, prezentacja
Pomoce: **karta pracy „Ograniczanie informacji"**, **materiał pomocniczy dla prowadzących „Informacje o nas w sieci — odpowiedzi"**, długopisy

Podziel uczestniczki i uczestników na grupy 4-osobowe. 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 po przeprowadzeniu zajęć ich uczestnicy i uczestniczki:

- 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. [rozwiązanie: prawda] [Prawda/Fałsz]
2. Odpowiednie ustawienia prywatności na portalu społecznościowym ograniczają liczbę dostępnych o nas informacji. [rozwiązanie: prawda] [Prawda/Fałsz]
3. Większość informacji da się skutecznie usunąć z sieci. [rozwiązanie: falsz] [Prawda/Fałsz]
4. Zamieszczanie informacji o sobie w sieci może mieć trudne do przewidzenia konsekwencje w przyszłości. [rozwiązanie: prawda] [Prawda/Fałsz]
5. Dostawca Internetu nie gromadzi żadnych informacji o użytkownikach sieci. [rozwiązanie: falsz] [Prawda/Fałsz]

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

- **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.
- **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.
- **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).
- **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

- Barbara Gubernat, „**Internet wie, co robisz**", Fundacja Panoptykon [dostęp: 23.06.2013]: http://www.panoptykon.org/wiadomosc/internet-wie-co-robisz.
- 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.

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/twoj-cyfrowy-slad/.

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.
aktywnie uczestniczy w realizacji projektów informatycznych rozwiązujących problemy z różnych dziedzin, przyjmuje przy tym różne role w zespole realizującym projekt i prezentuje efekty wspólnej pracy.
postępuje zgodnie z zasadami netykiety oraz regulacjami prawnymi dotyczącymi: ochrony danych osobowych, ochrony informacji oraz prawa autorskiego i ochrony własności intelektualnej w dostępie do informacji; jest świadomy konsekwencji łamania tych zasad.
stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji.