Co wie o Tobie Twój telefon?

Informacje o lekcji

Ekspert:	Kamil Śliwowski
Autorka wiedzy w pigułce:	Anna Obem
Autorka scenariusza:	Izabela Meyza
Organizacja publikująca:	Fundacja Panoptykon
Przedmiot:	Informatyka
Sugerowany poziom kształcenia:	Gimnazjum
Licencja:	Creative Commons Uznanie autorstwa – Na tych samych warunkach 3.0 Polska

Wiedza w pigułce

Z chwilą pojawienia się na rynku smartfonów zmienił się sposób, w jaki korzystamy z Internetu i komunikujemy się ze światem. Urządzenia, które łączą w sobie funkcje telefonu, komputera osobistego, aparatu i kamery, albumu ze zdjęciami, komunikatora internetowego, latarki i wielu innych, noszą w kieszeniach coraz młodsi użytkownicy. Wykorzystują je do łączenia się z Internetem, robienia zdjęć, nagrywania filmów, dzielenia się nimi z innymi, informowania o tym, gdzie właśnie przebywają, a także do wielu innych celów, które niewiele mają wspólnego z pierwotną funkcją telefonu komórkowego – dzwonieniem i wysyłaniem krótkich wiadomości tekstowych.

Dla młodych telefon staje się narzędziem odzyskania ograniczonej w innych sferach wolności – daje możliwość wyrażenia siebie, kontaktu ze światem. Jednak jest też druga strona medalu, związana z gromadzeniem wielu osobistych informacji. W ten sposób narzędzie, które daje nam wolność i swobodę działania, może nas też ograniczać i kontrolować.

Trudno znaleźć inne tak popularne urządzenie, które zbiera tyle informacji o użytkowniku, co smartfon. Dane trafiają do telefonu (i w kolejne ręce) na różne sposoby. Część z nich wprowadzamy świadomie, np. zapisując kontakty, robiąc zdjęcia czy nagrywając filmy. Więcej udostępniamy mimochodem, np. słuchając muzyki, „lajkując" materiały w sieci czy korzystając z wielu nie zawsze potrzebnych aplikacji, informujemy producentów oprogramowania i dostawców usług internetowych o swoich upodobaniach, nastroju w danej chwili i miejscu, w którym przebywamy, o tym, czego nie wiemy i czego się boimy.

Samo podłączenie telefonu do sieci komórkowej, umożliwiające wykonywanie połączeń i wysyłanie wiadomości, pozwala operatorowi sieci uzyskać wiele informacji: np. znana jest mu nasza przybliżona lokalizacja, wie, z kim, kiedy i jak długo rozmawiamy. Korzystanie z komunikatorów, takich jak Whatsapp czy Facebook Messenger, oznacza, że przesyłane przez nas informacje przechodzą nie tylko przez ręce operatora, ale również producentów aplikacji. Funkcja GPS pozwala jeszcze dokładniej nas zlokalizować. Jeśli łączymy się z Internetem przez sieć komórkową, operator dodatkowo uzyskuje informacje o naszej aktywności w sieci. Jeśli zaś przez sieć Wi-Fi – dane z telefonu mogą zostać przechwycone przez osobę

administrującą tą siecią, a w przypadku niezabezpieczonych sieci – przez wszystkich znajdujących się w jej zasięgu.

Nowe modele telefonów wyposażane są w kolejne czujniki i funkcje. Na przykład żyroskopy, które pojawiały się już w starszych modelach telefonów, obecnie służą do analizy aktywności użytkownika – dostarczają producentowi informacji, kiedy ten biega, jeździ na rowerze czy siedzi. Telefony wyposażane są też w czytniki odcisków palców, skanery tęczówki oka i aplikacje analizujące fazy snu.

Nowoczesny telefon to komputer z pamięcią, w której zapisywane są wszystkie operacje i dane. Ich trwałe usunięcie nie jest – podobnie jak w przypadku zwykłego komputera – proste. Ponadto kopie danych mogą trafiać na serwery producentów oprogramowania (w zależności od tego, jaki system operacyjny jest zainstalowany w smartfonie: Google – dla Androida, Apple – dla iPhone'a, Microsoft – dla Windows Phone'a), a część danych na serwery dostawców aplikacji. Wyrażamy na to zgodę przy instalacji aplikacji. Niektórzy producenci oprogramowania uzyskują dzięki temu dostęp do danych, z których spora grupa nie jest niezbędna do prawidłowego działania programu. Na przykład popularna latarka (aplikacja Tiny Flashlight na Androida) ma dostęp nie tylko do aparatu, ale też do mikrofonu; ma do niego dostęp również aplikacja Facebooka.

Informacje o właścicielu telefonu i jego aktywności trafiają w różne miejsca, a dostęp do nich może uzyskać wiele różnych podmiotów, zarówno instytucje publiczne, jak i firmy. Policja wykorzystuje dane telekomunikacyjne (np. dane abonentów i billingi, które uzyskuje od operatorów) do ścigania przestępstw i w celach prewencyjnych. Dane użytkownika są też powszechnie, podobnie jak w przypadku innych urządzeń podłączonych do Internetu, wykorzystywane do celów komercyjnych. To, co „wie" o nas telefon, pozwala stworzyć dokładny profil konsumencki, szczególnie cenny dla reklamodawców i dostawców usług internetowych. Jednocześnie smartfona łatwiej niż inne urządzenia (mniej przenośne i częściej zostawiane w domu) można stracić – a wraz z nim wszystkie zapisane w nim informacje, które mogą w ten sposób trafić w niepowołane ręce.

Konsekwencje wykorzystywania danych przez różne podmioty są zróżnicowane. Profilowanie treści przekazu pod kątem indywidualnych cech użytkownika może skutkować mniej lub bardziej skutecznym manipulowaniem nim poprzez reklamy. Ostatnio dużą popularność w sieciach handlowych zyskuje technologia *beacon*: są to specjalne czujniki, które, w połączeniu z odpowiednią aplikacją, pozwalają na analizowanie zachowań klientów, np. jak często robią zakupy, w jakich sklepach, przy jakich produktach spędzają najwięcej czasu, a następnie – wysyłanie im spersonalizowanych ofert. Takie technologie mają na celu przede wszystkim zwiększenie sprzedaży. Wraz z ich upowszechnianiem się można zapomnieć o anonimowych – i przemyślanych – zakupach.

Innego rodzaju przykre konsekwencje mogą nas spotkać, jeśli nagrania czy zdjęcia z telefonów – zwłaszcza sytuacji intymnych – trafią w niepowołane ręce albo skradziony smartfon zostanie wykorzystany, żeby kogoś oszukać. Informacje zapisane w formie cyfrowej można bardzo łatwo powielać i upubliczniać. Mogą trafić do sieci, gdy je świadomie opublikujemy, ale też przypadkowo, jeśli naciśniemy nie ten klawisz, co trzeba. Ktoś, komu kiedyś przesłaliśmy zdjęcie czy nagranie, może je – wbrew naszej woli – upublicznić, np. żeby nas ośmieszyć czy się odegrać.

Wielu przykrych sytuacji można uniknąć, stosując się do kilku zasad, które powinni poznać uczestnicy zajęć:

1. Nie dokumentuj telefonem ryzykownych ani wstydliwych zachowań.

2. Nie rób sobie ani innym zdjęć, których nie chciałbyś(-abyś) zobaczyć w Internecie bądź które mogą zaszkodzić Tobie lub innym.
3. Instaluj tylko te aplikacje, z których chcesz rzeczywiście korzystać. Zawsze czytaj informację, która wyświetla się, gdy chcesz zainstalować nowy program w telefonie – jeśli masz wątpliwości, czy chcesz udostępniać dany zasób informacji, zrezygnuj z instalacji. Świadomie zarządzaj aplikacjami na swoim telefonie: dowiedz się, jak działają, przeczytaj opinie innych użytkowników.
4. Zwracaj uwagę, do jakich informacji aplikacje chcą uzyskać dostęp i czy jest to niezbędne do prawidłowego działania aplikacji. Jeśli umożliwia to Twój system operacyjny, weryfikuj, ile danych aplikacja pobrała lub wysłała podczas pracy w tle.
5. Zastanów się, czy na pewno chcesz dać się skusić na „niesamowitą promocję dostępną tylko teraz i tylko tutaj", o której informację dostałeś(-aś) na swojego smartfona.
6. Blokuj telefon hasłem.
7. Zainstaluj program antywirusowy – pomoże Ci on uniknąć instalacji złośliwych aplikacji (*malware*), które udają pożyteczne oprogramowanie; można trafić na nie również w oficjalnych sklepach z aplikacjami (np. Google Play).
8. Jeśli zdarzy Ci się za pomocą smarftona zarejestrować zdarzenie, podczas którego ktoś inny łamie prawo, powiedz o tym osobie dorosłej, do której masz zaufanie.

Pomysł na lekcję

W czasie zajęć uczestnicy i uczestniczki zastanowią się, jakie informacje o nich posiada ich smartfon i komu może je udostępnić. Wypracują też zasady, które pomogą im podejmować świadome decyzje i dbać o prywatność przy korzystaniu ze smartfonów.

Cele operacyjne

Uczestnicy i uczestniczki:

- wiedzą, jakie informacje o nich zbiera ich smartfon i komu może je udostępnić;
- rozumieją, w jaki sposób używanie tego urządzenia może wpływać na ograniczenie ich prywatności;
- potrafią chronić swoją prywatność, korzystając ze smartfona.

Przebieg zajęć

Ćwiczenie 1.

Czas: *5 min*

Metoda: *miniwykład*

Pomoce: *karta pracy nr 1 „Wyobraź sobie kogoś, kto…"*

Przed zajęciami na tablicy lub dużej kartce papieru narysuj kontury człowieka. Powieś je w miejscu widocznym dla uczestników. Zajęcia zacznij tajemniczo od zdania: „Wyobraźcie sobie kogoś, kto…". Następnie czytaj po kolei różne zakończenia zdania z Karty pracy nr 1, przyklejając je wewnątrz postaci.

Kiedy przeczytasz wszystkie, zapytaj uczestników, czy znają kogoś takiego. Podpowiedz, że to wszystko wie o nich ich smartfon.

Powiedz, że w dalszej części zajęć uczestnicy dowiedzą się, komu smartfon może te informacje przekazywać i jak mogą dbać o prywatność, nie rezygnując z jego używania.

Uwaga! Sylwetka człowieka będzie potrzebna w ćwiczeniu 4. Zachowaj ją!

Ćwiczenie 2.

Czas: *10 min*

Metoda: *dyskusja*

Pomoce: *tablica i kreda lub papier i marker*

Powiedz, że żeby poznać odpowiedź na pytanie, dlaczego smartfon wie o nas to, czego być może nie wiedzą nawet rodzice i przyjaciele, zastanowimy się najpierw nad tym, do czego go używamy. Zadaj pytanie: „Do czego można używać smartfona?". Odpowiedzi możesz zapisywać na tablicy. W razie potrzeby naprowadź młodzież na funkcje:

- rozmowy telefoniczne;
- SMS-y;
- e-maile;
- wyszukiwanie informacji w Internecie;
- korzystanie z portali społecznościowych;
- kamera (robienie zdjęć i filmów);
- dyktafon (nagrywanie rozmów, lekcji, wykładów);
- lokalizacja (np. prowadzenie samochodu lub statusy na Facebooku);
- notatnik;
- kalendarz;
- książka telefoniczna (gromadzenie numerów telefonów znajomych);
- zegarek i budzik;
- przechowywanie dokumentów, plików, zdjęć itp. na twardym dysku.

Podsumuj: nowoczesny telefon to urządzenie wielofunkcyjne – aparat, telefon, kalendarz i komputer w jednym. Smartfon posiada wiele różnych funkcji, które wiążą się z gromadzeniem i przekazywaniem informacji o nas. Dodatkowo, nosimy go prawie zawsze przy sobie – wiele osób spędza z nim więcej czasu niż z rodziną i przyjaciółmi, a nocą kładzie go przy łóżku. Zadaj pytanie:

- Co mogłoby się stać, gdyby te informacje trafiły w niepowołane ręce?

Ćwiczenie 3.

Czas: *15 min*

Metoda: *praca w parach*

Pomoce: *karta pracy nr 2 „Smartfon, czyli kto?" wydrukowana dla każdej pary*

Powiedz, że wiele z informacji, którymi „dzielimy się" z telefonem, nie tylko jest w nim przechowywanych, ale też przekazywanych dalej. Powiedz: „Do tej pory używaliśmy stwierdzenia, że smartfon «coś o nas wie».

Teraz spróbujemy odpowiedzieć na pytanie: «Smartfon, czyli kto?», czyli zastanowimy się, kto może mieć dostęp do informacji z naszego telefonu". Podziel uczestników na pary, rozdaj każdej z nich kartę pracy nr 2 „Smartfon, czyli kto?" i poproś o wykonanie zadania.

Po uzupełnieniu kart zapytaj:

- Czy coś Was zaskoczyło w tym ćwiczeniu?
- Do kogo najczęściej wędrują informacje o Was?
- Które z tych informacji udostępniamy świadomie, a które telefon udostępnia sam?

Zbierz kilka odpowiedzi z grupy. Następnie na podstawie „Wiedzy w pigułce" opowiedz o tym, w jaki sposób za pomocą smartfona udostępniamy informacje o nas. Zauważ, że wiele z tych informacji wędruje do kilku podmiotów (np. wiedzę o lokalizacji ma operator sieci komórkowej, producent aplikacji wykorzystywanej przez biegaczy czy nawigacja samochodowa) i że często ich kopia jest przechowywana na smartfonie (printscreen, SMS-y, historia połączeń itp.). Dodatkowo niektórzy producenci oprogramowania do smartfonów (np. Google produkujący system Android czy Apple – producent iOS) przechowują kopię naszego twardego dysku na swoich serwerach.

Zauważ, że gdyby zrobić zestawienie wszystkich informacji o nas, które przechowujemy w telefonie i przez niego przekazujemy, w wielu przypadkach można by zrekonstruować całe nasze życie.

Ćwiczenie 4.

Czas: *15 min*

Metoda: *dyskusja*

Pomoce: *tablica i kreda lub papier i marker*

Powróć do namalowanego na tablicy człowieka-smartfona i zadaj pytanie:

- Jakie konsekwencje może mieć to, że ktoś (lub coś) posiada tyle informacji o Was?
- Do czego te informacje mogą zostać użyte?

Zwróć uwagę na to, że wiele osób traktuje smartfon jako narzędzie do uzyskania wolności. Tymczasem, zwłaszcza gdy lekkomyślnie się z niego korzysta, może stać się narzędziem kontroli.

Zapytaj:

- Jak myślicie, czy można tę sytuację odwrócić: czy zamiast pozwolić smartfonowi Was kontrolować, to Wy możecie świadomie dbać o prywatność, korzystając z niego?
- Jakie zasady mogą Wam w tym pomóc?

Odpowiedzi uczestników zapisuj na tablicy. Jeżeli brakuje pomysłów, możesz nakierowywać, posiłkując się „Wiedzą w pigułce".

Po wypisaniu wszystkich zasad poproś, żeby każdy z uczestników podszedł do tablicy i kredą lub markerem postawił kropkę przy tej, która jest dla niego najważniejsza.

Ewaluacja

Czy po przeprowadzeniu zajęć uczestnicy i uczestniczki:

- wiedzą, w jaki sposób, korzystając ze smartfona, udostępniają innym informacje o sobie?
- potrafią wskazać, kto może mieć dostęp do tych informacji?
- wiedzą, jak zabezpieczyć się przed udostępnianiem niepotrzebnych informacji?

Opcje dodatkowe

Opcją dodatkową może być puszczenie uczestnikom filmu *Wolność*, ilustrującego, jak korzystanie ze smartfona wpływa na ograniczenie prywatności i możliwości wyboru. Film można pobrać tutaj: filmy.panoptykon.org.

Materiały

- Karta pracy nr 1 „Wyobraź sobie kogoś, kto…"
- Karta pracy nr 2 „Smartfon, czyli kto"

Zadania sprawdzające

Zadanie 1

Prawda czy fałsz (P/F)?

1. _ Operator sieci komórkowej zna moją lokalizację tylko wtedy, kiedy do kogoś dzwonię.
2. _ Nie mam żadnego wpływu na to, że ile informacji o mnie gromadzi smartfon.
3. _ Nikt oprócz mnie nie ma dostępu do tego, co zapisuję na swoim smartfonie.
4. _ Korzystając ze smartfona, udostępniam więcej danych o sobie niż w przypadku używania tradycyjnego telefonu.
5. _ Gry, które ściągam na smartfona, nie mają żadnego wpływu na moją prywatność.

Słowniczek

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

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

1. Małgorzata Szumańska, Kamil Śliwowski, *Szpieg w wersji smart: co wie o Tobie Twój telefon*, Fundacja Panoptykon [dostęp: 14.12.2014]: http://cyfrowa-wyprawka.org/teksty/szpieg-w-wersji-smart-co-wie-o-tobie-twoj-telefon.

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

Projekt współfinansowany ze środków Ministra Kultury i Dziedzictwa Narodowego.