edukacja medialna

Nadzór w sieci

WIEDZA W PIGUŁCE

Pewnie nieraz w internecie pokazał ci się baner reklamowy proponujący zakupy w sklepie niedawno przez ciebie odwiedzanym. To powszechne zjawisko jest efektem tzw. cyfrowego śladu, pozostawianego przez każdego użytkownika sieci. Składają się na niego nie tylko informacje świadomie przez nas udostępniane, lecz także przekazywane automatycznie (np. ciasteczka, informacje o adresie IP hosta odwiedzającego stronę itp.).

Bardzo często nie uświadamiamy sobie skali przepływu informacji o naszej aktywności w sieci. Wystarczy być zalogowanym do Facebooka lub do serwisów Google (np. Gmaila lub YouTube), aby historie naszych wyszukiwań i odwiedzanych stron z innych kart były udostępniane tym przedsiębiorstwom. Nie musisz nawet mieć otwartej strony Facebooka – wystarczy, że nie wylogowałeś się po ostatnich odwiedzinach.

Niektórzy w trosce o bezpieczeństwo informacji o sobie unikają portali społecznościowych. Zwykle jednak nawet i oni nie są zupełnie anonimowi dla Facebooka. Osoby korzystające z aplikacji Facebooka na smartfony udostępniają mu wszystkie swoje kontakty – numery telefonów i nazwiska swoich znajomych, w tym również tych, którzy nie mają konta na portalu.

Nigdy nie mamy pełnej kontroli nad informacjami, które udostępniliśmy – a często, gdy trafiają one w niepowołane ręce, prowokują do popełnienia przestępstwa. Na przykład o charakterze finansowym: niebacznie udostępniony numer dowodu wraz z naszym imieniem i nazwiskiem wystarczą, aby ktoś obciążył nas kredytem. Z drugiej strony łatwy dostęp do naszych danych może ułatwić wielokanałowy stalking. Umożliwia też przestępcom podszywanie się, które może służyć m.in. wyłudzaniu pieniędzy czy informacji o tobie od członka twojej rodziny.

Informacje o aktywności użytkowników w sieci mogą w mocy prawa być pozyskiwane przez instytucje państwowe. Zwykle służy to tropieniu cyberprzestępców. Często jednak masy informacji zagarniane przez oddziały śledcze dotyczą nie tylko przestępców, lecz także obejmują wielką ilość przypadkowych osób. Na przykład ABW ma prawo zażądać od administratora obserwowanej strony wszystkich treści oraz danych o użytkownikach czy listy adresów IP odwiedzających stronę. Może nawet uzyskać zdalny, bieżący dostęp do wszystkich aktywności dziejących się na niej. Zatem nawet jeśli nie jesteś internetowym przestępcą, możesz być obserwowany.

Pewnie zastanawiasz się, czy można jakoś zaradzić niekontrolowanemu przepływowi informacji o tobie? Podczas twojej sieciowej aktywności warto kierować się zasadą informacyjnego minimalizmu: im mniej możesz przekazać informacji, tym dla ciebie lepiej. Za każdym razem zastanów się, czy na pewno coś zyskasz, udostępniając kolejne zdjęcie czy materiał o sobie. Pomyśl, czy ktoś mógłby wykorzystać je jakoś wbrew twojej woli. Możesz również zrezygnować z wielu usług, które wymagają przekazywania zbyt wielu danych. Wybierz raczej podobne, ale o mniejszych wymaganiach. Rozważ również podawanie fikcyjnych danych, jeśli uważasz, że to uzasadnione.

POMYSŁ NA LEKCJĘ

W świecie wirtualnym nie jesteśmy anonimowi: świadomie lub nie pozostawimy informacje, które mogą być wykorzystywane również przeciwko nam. Uczestnicy i uczestniczki podczas lekcji będą mogli zobaczyć, do jakich celów może być użyta ich indywidulana aktywność w internecie oraz jak można chronić swoje dane.

Cele operacyjne

Uczestniczki i uczestnicy:

- rozumieją, że w sieci nie jesteśmy anonimowi;
- wiedzą, że informacje pozostawiane o nas w sieci są gromadzone i mogą być wykorzystane do różnych celów;
- wiedzą, w jaki sposób mogą chronić swoje dane.

Przebieg zajęć

1.

Czas: brak min
Forma: praca indywidualna
Pomoce: **karta pracy „Dziennik aktywności w internecie"**

Kilka dni przed lekcją wydrukuj i rozdaj **kartę pracy „Dziennik aktywności w internecie".** Poproś, aby uczestniczki i uczestnicy wypełnili ją, zaznaczając z jakich stron korzystają i jednocześnie jakie informacje o sobie tam zostawiają. Zapowiedz, że karty pracy będą pomocne w lekcji, będą służyły do pracy indywidulanej i nie będą przekazywane innym osobom.

2.

Czas: 5 min
Forma: rozmowa, praca indywidualna
Pomoce: tablica, kreda lub marker, długopisy, wypełniona **karta pracy „Dziennik aktywności w internecie"**

Zapowiedz uczestnikom i uczestniczkom, że lekcja będzie dotyczyła nadzoru w sieci oraz możliwych sposobów wykorzystywania informacji, które po sobie zostawiamy w internecie. Zapytaj o skojarzenia ze słowem „nadzór"; podane odpowiedzi wypisz na tablicy. Wyjaśnij, że korzystając z internetu, nie jesteśmy anonimowi, a to, jakie infomacje zostawiamy stronach, tworzy nasz profil użytkownika. Informacje te mogą być wykorzystane do różnych celów. Poproś uczestniczki i uczestników o przyjrzenie się swoim kartom pracy, które są dziennikami jednego dnia aktywności w sieci. Podkreśl, że podczas lekcji każdy będzie mógł się przekonać, jaki indywidulany profil pozostawia po sobie w internecie i zastanowić się, do czego może on być wykorzystany. Zapytaj, czy uczestniczki i uczestnicy widzą w swoich dziennikach, z jakich stron najczęściej korzystają i co zamieszczają: np. filmy, zdjęcia, komentarze, swoje dane. Poproś o zakreślenie najczęściej pojawiających się stron i danych.

3.

Czas: 15 min
Forma: Jigsaw
Pomoce: kartki A4, długopisy, **instrukcja dla grup "Stoliki ekspertów"**, materiał „Wiedza w pigułce"

Zapowiedz, że teraz zobaczymy, do jakich celów mogą być wykorzystywane informacje pozostawiane w internecie. Podziel uczestników i uczestniczki na 3 grupy. Pierwsza grupa zajmie się wykorzystaniem informacji w celach komercyjnych, druga w celu popełnienia przestępstwa, trzecia wykorzystaniem danych przez państwo. Pomocniczo rozdaj grupom **instrukcje „Stoliki ekspertów"** oraz materiał „Wiedza w pigułce". Zaproś grupy do dyskusji (ok. 5 min) na wyznaczone tematy oraz do spisania refleksji i pomysłów. Następnie poproś o wybranie jednej osoby z każdej grupy, która jako ekspert przekaże informacje innym grupom. Eksperci pozostają na swoich miejscach, reszta osób z grupy zmienia miejsce, przesiadając się do eksperta z innej grypy. Poproś, aby eksperci przekazali informacje i wnioski, które powstały w pierwszej części zadania. Dokonaj jeszcze jednej zamiany grup, następnie poproś, aby wszyscy wrócili na swoje pierwotne miejsca i podsumowali to, czego dowiedzieli się od innych (reszta osób z grupy przejmuje rolę eksperta). Upewnij się, czy podczas dyskusji pojawiły się jakieś dodatkowe wnioski lub pytania.

1.

4.

Czas: 20 min
Forma: praca wgrupach
Pomoce: flamastry, papier kolorowy, klej, nożyczki, kartki A2 dla każdej grupy (lub dostęp do komputerów z programami graficznymi)

Zaproś uczestniczki i uczestników do przygotowania w zespołach liczących po 3–4 osoby infografik, które przedstawią problem nadzoru w sieci. Można je przygotować, korzystając z komputerów, jeśli jest taka możliwość, lub przy pomocy materiałów plastycznych. Zachęć do prostej, czytelnej formy, pokazującej związki przyczynowo-skutkowe. Infografiki mogą wskazywać na takie aspekty jak: przepływ informacji o naszej aktywności w sieci, cele wykorzystywania informacji, zasady bezpiecznego korzystania z internetu podporządkowane zasadzie minimalizmu, tzn. sprzyjające temu, aby pozostawionych informacji było jak najmniej. Możesz skorzystać z linków do materiałów dostępnych w czytelni na końcu scenariusza. Na zakończenie poproś o przedstawienie prac przez zespoły.

5.

Czas: 5 min
Forma: rozmowa, praca indywidualna
Pomoce: tablica, kreda lub marker, długopisy, postity

Poproś, aby na zakończenie każdy na karteczce napisał, co było dla niego najważniejsze z lekcji i o czym chce pamiętać przy następnym wejściu na stronę WWW. Zbierz kartki, przylep do tablicy wokół słowa „podsumowanie" i odczytaj odpowiedzi.

Ewaluacja

Czy po przeprowadzeniu zajęć ich uczestnicy i uczestniczki:

- rozumieją, że w sieci nie jesteśmy anonimowi;
- wiedzą, że informacje pozostawiane o nas w sieci są gromadzone i mogą być wykorzystane do różnych celów;
- wiedzą, w jaki sposób mogą chronić swoje dane?

Opcje dodatkowe

Jeśli masz więcej czasu, poproś o przygotowanie komiksów (aktywność można przeprowadzić grupowo) z historyjkami dotyczącymi sytuacji, w których mogą być użyte dane pozostawione przez nas w internecie np. do celów komercyjnych czy podszywania się pod kogoś. Zachęć do umieszczania ciekawych dialogów, zachowania lekkiej formy przekazu oraz wymyślenia trafnej puenty pokazującej cele wprowadzania nadzoru w sieci. Prace mogą zostać umieszczone w gazecie szkolnej lub na tablicy ogłoszeń.

MATERIAŁY

- **karta pracy „Dziennik aktywności w internecie"**
- **instrukcja dla grup „Stoliki ekspertów"**

ZADANIE DLA UCZNIA

Zadanie 1.

1. Przestępstwa popełnianie w sieci nazywamy _____ [rozwiązanie: cyberprzestępstwami].
2. _____ [rozwiązanie: Stalking] to uporczywe i trwałe nękanie jakiejś osoby, którego celem jest upokorzenie lub dezorganizacja życia. Może być osobiste lub wirtualne.
3. Najlepszym sposobem na to, aby nasze dane nie zostały wykorzystane jest _____ [rozwiązanie: minimalizm], czyli pozostawianie po sobie w internecie jak najmniejszej ilości informacji.

- Stalking
- cyberprzestępstwami
- minimalizm

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.
- **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.
- **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.

- **host**: dowolna maszyna (np. komputer), która posiada własny adres IP oraz uczestniczy w wymianie danych lub udostępnia usługi sieciowe poprzez sieć komputerową.

CZYTELNIA

- Szumańska Małgorzata, Obem Anna, **Jak bezpiecznie komunikować się w sieci**, Fundacja Panoptykon, dostępny w internecie [dostęp 14.11.2016]: http://cyfrowa-wyprawka.org/teksty/jak-bezpiecznie-komunikowac-sie-w-sieci
- Obem Anna, Czyżewski Michał „Czesiek", Szymielewicz Katarzyna, **Prywatność – zrób to sam!**, Fundacja Panoptykon, dostępny w internecie [dostęp 14.11.2016]: http://cyfrowa-wyprawka.org/teksty/prywatnosc-zrob-sam

---

Tekst: Urszula Dobrowolska, scenariusz: Monika Prus-Głaszczka, konsultacja merytoryczna: Wojciech Klicki. Materiał pochodzi z serwisu edukacjamedialna.edu.pl prowadzonego przez Fundację Nowoczesna Polska.

Źródło: http://edukacjamedialna.edu.pl/lekcje/nadzor-w-sieci/.

Publikacja zrealizowana w ramach projektu "Cybernauci - kompleksowy projekt kształtowania bezpiecznych zachowań w sieci", finansowanego ze środków Ministra Edukacji Narodowej.

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.

Wiedza o społeczeństwie, IV poziom edukacyjny
Cele kształcenia
II. Rozpoznawanie i rozwiązywanie problemów.

Nowa podstawa programowa:

Etyka, liceum i technikum
Treści nauczania
Podaje przykłady działań, które są wyrazem troski o własne zdrowie i życie; wyjaśnia, dlaczego należy odnosić się z szacunkiem do własnego ciała.
podaje przykłady właściwego i niewłaściwego wykorzystywania nowych technologii, w szczególności technologii informatycznych.
identyfikuje i analizuje wybrane problemy moralne związane z postępem naukowo-technicznym (np. problem ochrony prywatności, ochrony praw autorskich, cyberprzemocy, rozwój sztucznej inteligencji, transhumanizm).

Wychowanie do życia w rodzinie, liceum i technikum
Treści nauczania
rozumie, na czym polega prawo człowieka do intymności i ochrona tego prawa.

Język polski, liceum i technikum
Treści nauczania
rozróżnia pojęcia manipulacji, dezinformacji, postprawdy, stereotypu, bańki informacyjnej, wiralności; rozpoznaje te zjawiska w tekstach i je charakteryzuje.

Informatyka, liceum i technikum
Treści nauczania
bezpiecznie buduje swój wizerunek w przestrzeni medialnej.
stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji.