edukacja medialna

Jak wzmocnić swoją prywatność?

WIEDZA W PIGUŁCE

Współczesne media społecznościowe nieustannie zachęcają użytkowników do porzucenia własnej prywatności na rzecz dzielenia się wszystkim z innymi. Nowe pokolenie celebrytów, robiące karierę za pośrednictwem Snapchata i Instagrama, udostępnia zapisy niemal każdej chwili swojego życia. Co ryzykujemy, rezygnując z dbania o prywatność?

Anonimowość jest jedną ze strategii ochrony naszej wolności i swobody. Im więcej podajemy o sobie informacji, tym większe prawdopodobieństwo, że ktoś wykorzysta je przeciwko nam. Nasze dane mogą się stać przedmiotem handlu i zostać wykorzystane w celach marketingowych. Nieraz konsekwencje niedbania o prywatność bywają bardzo niebezpieczne – takie działania prowokują cyberprzestępstwa, np. podszywanie się czy stalking.

Materiał raz udostępniony w sieci, nigdy w niej do końca nie ginie. Filmik dokumentujący zabawę ze znajomymi może być dla ciebie teraz świetną pamiątką, ale za kilka lat może zniechęcić potencjalnego pracodawcę do zatrudnienia cię. Udostępnione przez nas informacje mogą również łatwo trafić w niepowołane ręce – nie da się mieć pełnej kontroli nad tym, kto się na nie natknie i jak ich użyje.

Prywatność jest ważną wartością, jednak trudno ją chronić. Zwłaszcza że komunikacja w internecie zawsze narażona jest na nadzór – żadna metoda kontaktu za pomocą mediów nie daje nam stuprocentowej gwarancji prywatności. Warto jednak wyrobić sobie przyzwyczajenia, które pomogą ci na co dzień o nią dbać.

Przede wszystkim staraj się nie dzielić większą ilością informacji, niż jest to potrzebne. Nie wyrażaj zgody na przesyłanie ofert marketingowych czy newsletterów, na które nie masz ochoty. Zachowuj dystans w stosunku do proponowanych ci usług, zwłaszcza jeśli korzystanie z nich wiąże się z koniecznością udostępnienia twoich danych. Miej zwyczaj wylogowywania się z serwisów, które wymagają logowania, oraz korzystaj z bezpiecznych haseł.

Zadbaj również o to, aby stałe ustawienia twojego sprzętu gwarantowały ci maksymalną prywatność w sposób automatyczny. Aktualizuj swoje oprogramowanie i posiadaj sprawdzony program antywirusowy. Zachowaj umiar w korzystaniu z programów opartych na geolokalizacji i zawsze ją wyłączaj, jeśli jej rzeczywiście nie potrzebujesz. Zapewnia ona ciągły przesył danych o tym, gdzie się znajdujesz, przez co przekazujesz internetowym gigantom całą historię twojego przemieszczania się.

Wreszcie, jeśli potrzebujesz przekazać komuś poufne informacje o sobie, korzystaj ze sposobu komunikacji o dużym stopniu prywatności. Najlepiej zrób to osobiście lub telefonicznie, przebywając poza przestrzenią publiczną. Możesz również skorzystać z szyfrowanego maila lub innego sposobu szyfrowanej komunikacji. Należy w tym celu posiadać dodatkowe oprogramowanie, a także udostępnić odbiorcy metodę na odkodowanie twojej wiadomości. Klasyczny mail czy komunikacja przez Skype'a nie zapewniają wystarczającej prywatności – ich treści są automatycznie skanowane. Najmniej bezpieczne są czaty na portalach społecznościowych (również w formie osobnych aplikacji, takich jak Messenger Facebooka) i otwarte fora internetowe.

Nie rezygnuj ze swojej prywatności z lenistwa lub tylko dlatego, że panuje taka moda. Nigdy nie wiesz, w jaki sposób może się to obrócić przeciwko tobie.

POMYSŁ NA LEKCJĘ

Lekcja pokazuje, że prywatność jest wartością, o którą należy dbać. Warto zatem świadomie nią zarządzać i wybierać adekwatne kanały przekazu informacji na swój temat lub na temat innych. Podczas zajęć uczestnicy i uczestniczki odkrywają, że tak naprawdę trudno jest w pełni zachować prywatność w internecie, ale istnieją sposoby, dzięki którym można ją wzmocnić.

Cele operacyjne

Uczestnicy i uczestniczki:

- wiedzą, czym jest prywatność i dostrzegają w niej wartość;
- umieją zdecydować, czy w danej sytuacji komunikacja powinna być prywatna czy publiczna;
- potrafią dopasować kanał komunikacji do przekazu;
- znają podstawowe sposoby zapewnienia prywatności w komunikacji.

Przebieg zajęć

1.

Czas: 10 min
Forma: burza mózgów, praca wgrupach
Pomoce: tablica, kreda lub marker, karteczki samoprzylepne

Podziel uczestników i uczestniczki na dwie grupy. Poproś o wypisanie na karteczkach samoprzylepnych przychodzących im do głowy skojarzeń ze słowem „prywatność" oraz o stworzenie mapy pojęciowej. Zwróć uwagę, aby tworząc mapy, uczestniczki i uczestnicy przyklejali obok siebie skojarzenia o podobnym znaczeniu lub odnoszące się do jednego obszaru. W taki sposób utworzą się logicznie uporządkowane zbiory. Poproś o zaprezentowanie map. Dodaj, że każdy ma swoją granicę prywatności, której nie można przekraczać. Możemy mówić o prywatności w obrębie naszego ciała, naszej przestrzeni domowej, informacji na nasz temat oraz komunikacji.

2.

Czas: 10 min
Forma: praca wparach, burza mózgów
Pomoce: długopisy, **karta pracy "Komunikaty"**

Powiedz, że komunikacja w internecie nigdy nie jest na sto procent prywatna, ponieważ zawsze występuje pośrednik, który przekazuje nasz komunikat, np. administrator strony. Dlatego ważne jest dopasowanie odpowiedniego kanału komunikacyjnego do treści, które chcemy przekazać; istotne jest też określenie rangi sprawy. Powinniśmy świadomie decydować, czy ma to być przekaz osobisty, rozmowa telefoniczna, szyfrowany mail, komunikacja przez Skype, mail tradycyjny, portal społecznościowy typu Facebook czy też otwarte forum. Rozdaj uczestnikom **kartę pracy „Komunikaty"**. Poproś, aby w parach dopasowali

rodzaj komunikatu do kanału przekazu. Zachęć także do przygotowania własnych przykładów komunikatów odpowiednich dla każdego kanału. Odczytaj wspólnie odpowiedzi oraz poproś o wskazanie możliwych konsekwencji w przypadku przekazania informacji w inny sposób.

3.

Czas: 20 min
Forma: debata
Pomoce: tablica, kreda lub marker, **materiał pomocniczy „Wykorzystywanie danych"**, kropki samoprzylepne

Zaproś uczestników i uczestniczki do mini debaty na temat „Czy prywatność w mediach jest wartością, którą należy chronić?". Podziel klasę na dwie grupy. Jedną poproś o wypracowanie argumentów za tym, że prywatność należy chronić, zaś drugą o zebranie zdań przekonujących, że jest to niekonieczne. Rozdajmateriał pomocniczy „Wykorzystywanie danych" zawierający opisy rożnych sytuacji pokazujące, jak nasze dane mogą być wykorzystywane w dobrych lub niekorzystnych dla nas celach. Poproś o przedstawienie argumentacji naprzemiennie oraz w taki sposób, aby argumenty jednej grupy nawiązywały do argumentów drugiej. Spisuj wnioski na bieżąco. Następnie poproś, aby każdy wybrał trzy najbardziej przekonujące argumenty i zaznaczył je, naklejając kropkę przy swoim wyborze. W podsumowaniu zwróć uwagę na to, które argumenty okazały się najsilniejsze (te z największą ilością kropek), najbardziej trafiające do przekonania grupie oraz, co za tym idzie, do której argumentacji – za lub przeciw – uczestnicy i uczestniczki są skłonni się przychylać.

4.

Czas: 5 min
Forma: rozmowa
Pomoce: tablica, kreda lub marker

Zwróć uwagę, że choć trudno jest całkowicie zachować prywatność w internecie, jednak można wskazać szereg rzeczy, o które warto zadbać, aby ją wzmocnić. Zapytaj grupę, co może pomóc w zachowaniu naszej prywatności podczas korzystania z internetu. O czym należy pamiętać na co dzień? Zwróć uwagę, że ważne są nasze nawyki podczas korzystania z internetu, czyli m.in.: wylogowanie się z poczty, portalu, używanie bezpiecznych haseł, minimalizowanie ilości udostępnianych informacji na swój temat, niewyrażanie zgód marketingowych, czytanie regulaminów, korzystanie z bezpiecznej sieci bezprzewodowej, używanie programu antywirusowego, aktualizowanie oprogramowania.

Ewaluacja

Czy po przeprowadzeniu zajęć ich uczestniczki i uczestnicy:

- wiedzą, czym jest prywatność i dostrzegają w niej wartość;
- umieją zdecydować, czy w danej sytuacji komunikacja powinna być prywatna czy publiczna;
- potrafią dopasować kanał komunikacji do przekazu;
- znają podstawowe sposoby zapewnienia prywatności w komunikacji?

Opcje dodatkowe

Jeśli masz więcej czasu, możesz poprosić uczestników i uczestniczki o przygotowanie kampanii informującej inne klasy o problemie prywatności w internecie. Poproś o przygotowanie planu kampanii – mogą to być plakaty, spoty w szkolnym radiowęźle lub happeningi.

MATERIAŁY

- **karta pracy „Komunikaty"**
- **materiał pomocniczy „Wykorzystywanie danych"**

ZADANIE DLA UCZNIA

Zadanie 1.

1. Najbezpieczniejszym sposobem przekazania poufnych informacji w formie elektronicznej jest _____ [rozwiązanie: szyfrowanie] poczty elektronicznej.
2. Jeśli chcesz przekazać ważną informację drugiej osobie, najlepiej zrób to _____ [rozwiązanie: osobiście].
3. _____ [rozwiązanie: prywatność] to możliwość utrzymania informacji o sobie i swoich danych w tajemnicy; każdy ma do niej prawo.

- prywatność
- osobiście
- szyfrowanie

SŁOWNICZEK

- **geolokalizacja**: określenie fizycznego położenia geograficznego osoby i urządzenia telekomunikacyjnego za pomocą systemu GPS lub adresu IP.
- **szyfrowanie poczty elektronicznej**: metody szyfrowania treści komunikacji e-mail tak, by odczytać ją mogli tylko nadawca i adresaci.

CZYTELNIA

- Szumańska Małgorzata, **Co warto wiedzieć o śledzeniu i profilowaniu w sieci**, Fundacja Panoptykon, dostępny w internecie [dostęp 14.11.2016]: http://cyfrowa-wyprawka.org/teksty/co-warto-wiedziec-o-sledzeniu-profilowaniu-w-sieci
- Pryciak Marcin, **Prawo do prywatności**, Biblioteka Cyfrowa, dostępny w internecie [dostęp 14.11.2016]: http://www.bibliotekacyfrowa.pl/Content/37379/011.pdf

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/jak-wzmocnic-swoja-prywatnosc/.

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

Podstawa programowa:

Wiedza o społeczeństwie, III poziom edukacyjny
Treści nauczania
Życie społeczne
Życie społeczne

Nowa podstawa programowa:

Etyka, IV-VIII klasa
Treści nauczania
Uczeń podaje przykłady właściwego i niewłaściwego wykorzystywania nowoczesnych technologii informacyjnych.

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

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