edukacja medialna

Gdy ktoś wykorzysta moją nieuważność

WIEDZA W PIGUŁCE

Nasze dane osobowe są dobrem, które warto chronić. Współcześnie na każdym kroku rozmaici usługodawcy zachęcają nas do ich swobodnego udostępniania. Nie pomni konsekwencji, często godzimy się na to bez zastanowienia.

Tymczasem udostępnianie dużej ilości informacji o nas może być wykorzystywane przeciwko nam. Poważne konsekwencje może mieć podszywanie się, a więc kradzież tożsamości. Często przyświeca jej chęć kompromitacji lub wyśmiania. To jedno z oblicz cyberbullyingu. Twórcy fałszywych profili na portalach społecznościowych często wykorzystują je do różnych moralnie wątpliwych działań, co stawia poszkodowaną osobę w bardzo negatywnym świetle.

Jeśli zauważysz, że ktoś podszywa się pod ciebie:

- zgłoś to niezwłocznie do administratora strony i zażądaj odpowiednich kroków (np. usunięcia profilu);
- opowiedz o tym swoim przyjaciołom, rodzinie i wychowawcom – poproś o wsparcie w walce z podszywającą się osobą;
- staraj się uprzedzać możliwe działania gnębicieli. Jeśli domyślasz się, że ktoś podpisany twoim imieniem i nazwiskiem może np. obrazić w internecie nauczyciela, lepiej poinformuj go o tym problemie. W wypadku, gdy do tego dojdzie, będziesz w dużo lepszej sytuacji, niż jeśli tego nie zrobisz.

Podszywanie się może być też wykorzystywane do celów przestępczych, np. wyłudzeń czy kradzieży. Podszywanie się pod członka rodziny sprawia, że potencjalna ofiara staje się ufniejsza i wprost podaje potrzebne informacje lub wykonuje pożądane działania (np. przelew na wskazane konto).

Udostępnianie naszych danych na portalach społecznościowych to nie jedyne działanie, które powinniśmy kontrolować. Zwykle, aby w pełni korzystać z rozmaitych usług internetowych, należy założyć konto i podać nasze dane. Często, jeśli zależy nam na danej usłudze, jest to tzw. zło konieczne. Warto jednak pamiętać, że mamy prawo się wycofać z korzystania z tej usługi oraz unieważnić zgodę na wykorzystywanie naszych danych. Żaden usługodawca nie ma również prawa przekazywania naszych danych innym osobom bez naszej zgody.

Dane osobowe każdego obywatela Polski są chronione dzięki ustawie o ochronie danych osobowych. Powołała ona do życia specjalny organ, który stoi na ich straży – Generalnego Inspektora Ochrony Danych Osobowych, GIODO.

Jeśli staniemy się ofiarami wykorzystania naszych danych lub wizerunku wbrew naszej woli, rozważmy podjęcie oficjalnych kroków. Zgłoszenie się do GIODO jest ostatecznością – wcześniej powinniśmy zainterweniować u administratora danych i zażądać, aby nie przechowywał dłużej naszych danych.

Niestety, w przypadku wielu naruszeń naszych praw zakres działania GIODO jest zbyt ograniczony. Internet jest medium międzynarodowym, a władza określonych instytucji ma zasięg nieprzekraczający granic terytorium kraju. Jeśli siedziba lub serwery firmy, która narusza nasze prawa, są w innym państwie, będzie nam dużo trudniej ubiegać się o nasze prawa.

Dlatego też lepiej zapobiegać możliwym nadużyciom, niż mierzyć się z konsekwencjami nadużyć. Dbaj swoje dane i udostępniaj je w sposób przemyślany.

POMYSŁ NA LEKCJĘ

Uczestniczki i uczestnicy będą mieli okazję w nowy sposób spojrzeć na cyfrowy wizerunek, który budujemy lub chcielibyśmy zbudować w sieci. Okiem krytyka przyjrzą się przykładom rozmaitych publikacji, których autorzy nie zachowali należytej ostrożności, zanim zdecydowali się umieścić w sieci informacje czy swoje zdjęcia. Zastanowią się, jakie mogłyby ich czekać przykre konsekwencje i dowiedzą się, co można zrobić, gdy już ktoś znajdzie się w takiej trudnej sytuacji.

Cele operacyjne

Uczestnicy i uczestniczki:

- potrafią zarządzać swoim cyfrowym wizerunkiem,
- wiedzą, że należy świadomie podejmować decyzje o zakresie publikowanych danych umożliwiających odkrycie ich tożsamości,
- wiedzą, gdzie zwrócić się o pomoc w przypadku naruszeń praw związanych z korzystaniem z mediów.

Przebieg zajęć

1.

Czas: 7 min
Forma: rozmowa
Pomoce: tablica, kreda lub marker, **Materiał pomocniczy „Zachowaj ostrożność"**, **Karty pracy „Historia o radach"**, koperty

Przed zajęciami zapisz na tablicy i zakryj przykłady działań w sieci, które mogą spowodować sytuacje potencjalnie niebezpieczne dla użytkownika Internetu (**Materiał pomocniczy „Zachowaj ostrożność"**) oraz wydrukuj dla wszystkich uczestniczek i uczestników **Karty pracy „Historia o radach"**, a następnie rozdziel je nożyczkami i każdy zestaw rad włóż do osobnej koperty.

Zapytaj uczestników i uczestniczki, co to jest cyfrowy wizerunek osoby (wszystkie informacje, jakie zamieszczamy o sobie w sieci). Co mieści się w tym pojęciu? Czy swoim cyfrowym wizerunkiem można zarządzać – budować go tak, aby odzwierciedlał tylko to, co naprawdę chcemy upubliczniać? Czego przykładowo możemy dowiedzieć się o drugiej osobie, odwiedzając np. jej profil na portalu społecznościowym? Czy uczestniczki i uczestnicy założyli sobie konta na różnych dostępnych portalach? Do czego im one najczęściej służą (np. do rozmów z kolegami, udostępniania zdjęć i filmów, dzielenia się ciekawymi linkami, swoimi poglądami, twórczością, zainteresowaniami)?

2.

Czas: 10 min
Forma: praca indywidualna
Pomoce: tablica, kartki typu post-it, długopisy, **Materiał pomocniczy „Zachowaj ostrożność"**

Zwróć uwagę uczestniczek i uczestników, że portale społecznościowe, blogi, chaty i inne formy komunikacji internetowej mogą przynieść wiele korzyści. Podobnie jak budowanie swojego cyfrowego wizerunku. Dziś jednak porozmawiacie o drugiej stronie medalu, czyli możliwych zagrożeniach wynikających z niewiedzy lub nieostrożności, ale mogących wpływać na wizerunek danej osoby. Rozważycie także konsekwencje, jakie mogą wyniknąć z takiej niepożądanej ingerencji. Zajmiecie się więc wszystkim tym, na co warto zwrócić uwagę, zarządzając swoim cyfrowym wizerunkiem. Odsłoń zapisane wcześniej na tablicy opisy sytuacji potencjalnie niebezpiecznych (**Materiał pomocniczy „Zachowaj ostrożność"**). Przeczytaj je głośno, a następnie wręcz uczestniczkom i uczestnikom karteczki typu post-it oraz długopisy i poproś, by spróbowali napisać, jakie mogą być konsekwencje tych sytuacji. Ważne, by każda konsekwencja znalazła się na osobnej karteczce. Można odnieść się do wszystkich sytuacji albo tylko do jednej z nich. Gotowe kartki uczestniczki i uczestnicy powinni przykleić przy wybranych sytuacjach. Poproś chętną osobę (lub kilku chętnych) o przeczytanie głośno, co znajduje się na każdej z kartek. Zapytaj uczestników i uczestniczki, jakie refleksje nasuwają im się na myśl po tym ćwiczeniu. Podkreśl, że zawsze trzeba zachować ostrożność, publikując coś w sieci, tyczy się to także tworzenia naszego cyfrowego wizerunku.

3.

Czas: 15 min
Forma: praca indywidualna
Pomoce: **Karty pracy „Historia o radach"**, koperty

Co jednak zrobić, kiedy już dojdzie do niepożądanej sytuacji i ktoś, wykorzystując naszą nieuważność, posłuży się informacjami, które zamieściliśmy? Poproś uczestniczki i uczestników, by spróbowali podać kilka przykładów działań, które można w tej sytuacji podjąć. Odpowiedzi zapisz na tablicy. Następnie zaproponuj zadanie, które będzie uzupełnieniem widniejącej na tablicy listy. Powiedz, że kilka rad, które mogą być dobrą wskazówką w omawianej sytuacji, znajdą w **Kartach pracy „Historia o radach"**. Rozdaj uczestniczkom i uczestnikom koperty z zestawem rad i poproś, by ułożyli je w kolejności według kroków, które ich zdaniem podczas ewentualnej interwencji powinno się podjąć na początku, a które nieco później. Porozmawiajcie o tym, dlaczego wybrali taką kolejność.

4.

Czas: 13 min
Forma: rozmowa
Pomoce: tablica, kreda lub marker

Porozmawiajcie o samych radach, które znalazły się w kopertach. Czy uczestnicy i uczestniczki mają jakieś pytania z nimi związane? Czy wiedzieli wcześniej o tych możliwościach reakcji na zagrożenie, które zostały wskazane podczas zajęć? Czy teraz wiedzieliby, do kogo się zwrócić po pomoc? Zapytaj również, jakie najważniejsze wnioski dotyczące budowania swojego wizerunku w sieci nasuwają im się na myśl. Poproś, by odpowiadając wyobrazili sobie, że przekazują wiedzę, którą zdobyli, komuś, kto nie uczestniczył w dzisiejszych zajęciach. Zaproś chętnych do odegrania krótkich scenek, w których przekazują treść zajęć znajomej osobie (koledze, rodzicowi, młodszemu bratu lub siostrze) albo są wykładowcami, którzy muszą w krótki i przystępny sposób przedstawić temat swojemu audytorium. Wnioski, które wyłoniły się podczas tej rozmowy/scenek, zapisz na tablicy.

Ewaluacja

Czy po przeprowadzeniu zajęć ich uczestnicy i uczestniczki:

- potrafią zarządzać swoim cyfrowym wizerunkiem;

- wiedzą, że należy świadomie podejmować decyzje o zakresie publikowanych danych umożliwiających odkrycie ich tożsamości;
- wiedzą, gdzie zwrócić się o pomoc w przypadku naruszeń praw związanych z korzystaniem z mediów?

Opcje dodatkowe

Jeśli masz więcej czasu, zaproponuj uczestniczkom i uczestnikom stworzenie plakatów, które mogłyby promować pozytywne zachowania w sieci (przykładowe hasła na plakat: „Świadomie buduję swój wizerunek w sieci"; „Nie używam internetu, aby szkodzić innym") lub przestrzegać przed lekkomyślnymi działaniami on-line (przykładowe hasło: „Nie szastam moimi danymi w sieci", „On-line mówię o sobie tylko tyle, ile chcę, by wiedział o mnie świat").

MATERIAŁY

- **Materiał pomocniczy „Zachowaj ostrożność"**
- **Karta pracy „Historia o radach"**

ZADANIE DLA UCZNIA

Zadanie 1.

Oznacz poniższe zdania jako prawdę lub fałsz.

- W sieci można zamieszczać, co tylko nam się podoba. W końcu to nasz wizerunek, więc możemy z nim zrobić, co chcemy. To tylko internet, a nie realna sytuacja, więc nie ma żadnego zagrożenia. [rozwiązanie: falsz] [Prawda/Fałsz]
- GIODO to skrót od Generalnego Inspektoratu Ochrony Danych Osobowych. [rozwiązanie: prawda] [Prawda/Fałsz]
- Gdy ktoś bezprawnie wykorzysta moje dane, nic nie da się na to poradzić. [rozwiązanie: falsz] [Prawda/Fałsz]
- Nie wolno na ogólnodostępnych stronach internetowych zamieszczać swojego adresu zamieszkania czy numeru telefonu. [rozwiązanie: prawda] [Prawda/Fałsz]

SŁOWNICZEK

- **cyberbullying**: (inaczej: cyberprzemoc, agresja elektroniczna) zachowania agresywne i przemoc, dokonywane za pośrednictwem mediów telekomunikacyjnych, zwłaszcza Internetu. Może przybierać formę: prześladowania, zastraszania, uporczywego wyśmiewania się i złośliwości, stalkingu itd.
- **GIODO**: Generalny Inspektor Ochrony Danych Osobowych. Organ powołany w celu ochrony danych osobowych. Do jego zadań należy m.in. kontrola zgodności przetwarzania danych z przepisami prawa oraz rozpatrywanie skarg w sprawach ich łamania. Jest powoływany na czteroletnią kadencję przez Sejm RP za zgodą Senatu.

CZYTELNIA

- **Materiały nt. ochrony danych osobowych**, Generalny Inspektor Danych Osobowych, [dostęp: 14.11.2016] dostępny w internecie: `http://www.giodo.gov.pl/473/j/pl/`
- **Ochrona prywatnośc**i, Polskie Centrum Programu Safer Internet, [dostęp: 14.11.2016] dostępny w internecie: http://www.saferinternet.pl/pl/ochrona-prywatnosci

- Zegarek Łukasz, **Kradzież tożsamości w Internecie**, Lex Artist, [dostęp: 14.11.2016] dostępny w internecie: http://blog-daneosobowe.pl/kradziez-tozsamosci-w-internecie/
- **Bezpieczeństwo dzieci online. Kompendium dla rodziców i profesjonalistów**, Polskie Centrum Programu Safer Internet, Warszawa 2014, [dostęp: 14.11.2016] dostępny w internecie: `http://edukacja.fdds.pl/?link=15187`

Tekst: Urszula Dobrowolska, scenariusz: Anna Walczak, konsultacja merytoryczna: Szymon Wójcik. Materiał pochodzi z serwisu edukacjamedialna.edu.pl prowadzonego przez Fundację Nowoczesna Polska.

Źródło: http://edukacjamedialna.edu.pl/lekcje/gdy-ktos-wykorzysta-moja-nieuwaznosc/.

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.
V. Ocena zagrożeń i ograniczeń, docenianie społecznych aspektów rozwoju i zastosowań informatyki.

Nowa podstawa programowa:

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.