**Jakich danych nie podawać w sieci? Scenariusz lekcji**

 **Cele operacyjne:**

Uczniowie:

 - potrafią podać przykłady naruszania prywatności z użyciem nowych technologii;

- rozumieją, dlaczego nowe technologie są wyzwaniem dla prywatności;

-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.

- są świadomi, że działania online są często monitorowane.

- są świadomi, że firmy wyświetlają reklamy i propozycje produktów w oparciu o nasze wcześniejsze zachowania w Internecie.

**Metoda:** wykład, rozmowa kierowana, dyskusje, omówienie

**Formy pracy:** indywidualna, grupowa

**Przebieg lekcji**

**Faza wprowadzająca**

Nauczyciel podkreśla, że cokolwiek zostanie upublicznione w Internecie zostaje tam na

zawsze. Zadaje uczniom pytanie jakie informacje umieszczają o sobie w Internecie? A jakie informacje są o nas zbierane? Czy można te informacje wykorzystać przeciwko nam? Uczniowie odpowiadają na pytanie

**Faza realizacyjna**

Nauczyciel systematyzuje odpowiedzi uczniów.

Podczas korzystania z Internetu zostawiamy mnóstwo swoich danych osobowych – świadomie i automatycznie.

Te **świadome ślady** to np. :

- imię i nazwisko,

- płeć

- adres e-mail,

- numer telefonu wpisywane np. podczas zakupów internetowych,

- zainteresowania,

- uprawiane sporty,

- krąg znajomych,

- komentarze,

- polubienia,

- statusy,

- zdjęcia, wizerunek

- filmiki,

 - informacje o pracy czy szkole czy o ukończonych szkołach, wykształcenie,

**Informacje zamieszczane automatycznie**:

- o systemie operacyjnym,

- przeglądarce internetowej,

- zestawie zainstalowanych czcionek,

- numerze IP,

- język, którego używamy

- czy korzystamy z określonej aplikacji lub usługi.

- preferencje wyszukiwania potencjalnych znajomych,

- lokalizacje każdej z rozmów online

**Informacje zamieszczane półautomatycznie:**

**-** geolokalizacja,

**-** informacje w plikach zdjęciowych o godzinie wykonania zdjęcia i modelu aparatu fotograficznego,

**-** statusy na portalach społecznościowych – np. czy jesteśmy w związku

**-**miejsce pracy,

**-** upodobania muzyczne,

**-** ulubione potrawy,

**-** najczęściej używane słowa,

**-** poglądy polityczne

- zamożność, status społeczny

**-** odwiedzane miejsca,

**-** dokonywane zakupy – co kupujemy, gdzie i kiedy i o której godzinie -jeśli płacimy kartą

- trasy spacerów

- jak zmienia się nasza lokalizacja,

- co robiliśmy w nocy z piątku na sobotę,

- dostęp do rzeczy takich, jak mikrofon w telefonie,

- sposób odżywiania

Nauczyciel podkreśla, że

narzędzia do śledzenia aktywności w internecie stały się coraz bardziej wyrafinowane. To już nie tylko pliki **cookies ciasteczka**, czyli pliki zapisywane na komputerze użytkownika. Większość z nich działa w ten sposób, że umożliwia w ogóle prawidłowe wyświetlanie strony czy rejestrację i logowanie się w serwisie. Istnieje jednak równie wiele takich, które pozyskują informacje przydatne dla właściciela strony internetowej, przykładowo umożliwiając zautomatyzowanemu oprogramowaniu dostosowywanie wyświetlanych reklam dla danego użytkownika. Niebezpieczny jest zwłaszcza tzw**. browser fingerprinting**, czyli **odcisk palca** tworzony dla każdej **przeglądarki**, dzięki któremu można zidentyfikować nie tylko urządzenie, lecz także konkretnego użytkownika. Pozyskane w ten sposób dane wykorzystywane są głównie w celach marketingowych, co może skutkować tym, że np. użytkownik komputera Mac za ten sam produkt zapłaci nawet 30 proc. więcej od użytkownika PC.. Osoby wyszukujące bilety lotnicze wiedzą to najlepiej – po kilku sprawdzeniach połączeń do danego miejsca, na stronie pojawiają się znacznie wyższe ceny biletów. Odcisk palca przeglądarki, zbiera informacje nawet przy wyłączonych plikach cookies. Do odwiedzanej witryny przesyłane są informacje o przeglądarce i na podstawie różnych danych stworzyć portret użytkownika. W ten sposób obecność w sieci nigdy nie jest anonimowa, choć jeszcze stosunkowo niedawno panowało przekonanie, że w sieci każdy z nas jest całkowicie bezpieczny, a ekran komputera skutecznie chroni naszą tożsamość. Jedynym rozwiązaniem, by możliwie jak najbardziej ochronić dane, jest korzystanie z zaszyfrowanej sieci czy specjalnych rozszerzeń i aplikacji

Nasze ślady w sieci są przedmiotem handlu w celach reklamowych, np. portal Facebook, który na co dzień „szpieguje” nas głównie pod kątem informacji mogących przydać się w marketingu, ale nie tylko. 250 like'ów z Facebook'a jest wystarczającą porcją informacji do określenia z dużym prawdopodobieństwem wielu cech intymnych kim jest badana osoba. System będzie znał tę osobę lepiej niż jej/jego małżonek. Istnieją już algorytmy, które są w stanie odczytać cechy danej osoby tylko na bazie zdjęcia jej twarzy. Na podstawie analizy dostępnych w Internecie danych o nas samych, firmy prowadzą tzw. **profilowanie**, czyli odgadywanie naszych przyszłych zachowań dotyczących m.in. zainteresowań, dokonywanych zakupów czy miejsc spędzania urlopu - może to mieć poważne skutki społeczne. Spółka Cambrige Analiytica komercyjnie wykorzystała dane nawet 50 milionów ludzi zarejestrowanych na Facebooku. Specjaliści mówią, że spółka mogła wpłynąć na wynik wyborów prezydenckich w Stanach Zjednoczonych oraz w sprawie Brexitu.

Dzienniki "Washington Post" oraz brytyjski "Guardian" ujawniły w 2013 r. dokumenty na temat istniejącego od 2007 roku programu PRISM, w ramach którego NSA i FBI sprawdzają dane na serwerach czołowych firm internetowych. Opublikowane przez gazety dokumenty wymieniają dziewięć firm: Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube i Apple. Według tych dokumentów, agenci służb specjalnych mają dostęp do znajdujących się na serwerach tych firm plików audio i wideo, maili, czatów czy przesyłanych fotografii i dokumentów.

Stravy, to jedna z najpopularniejszych aplikacji sportowych, których używają np. Amerykanie. Wykorzystuje ona informacje GPS zamontowane w smartfonach i smartwatchach. Nanoszone są one na mapę z drogami, którymi najczęściej poruszają się użytkownicy tej aplikacji. W 2017 roku Strava udostępniła takie trasy, a użytkownicy Twittera nanieśli je na mapy Syrii czy Iraku. Niektóre z nich znajdowały się z dala od miast czy wiosek, pośrodku niczego. To z kolei pozwoliło zasugerować, że funkcjonują tam tajne bazy wojskowe, a żołnierze, którzy w nich służą, trenują w okolicy. Biegi wokół bazy wojskowej lub lotniska zdemaskowały z kolei żołnierzy w Somalii. Co więcej, niektórzy nie wyłączali aplikacji po skończonym treningu i używali jej podczas wykonywania codziennych obowiązków, co mogło doprowadzić choćby do ustalenia tras patrolu.

**Faza podsumowująca**

Uczeń zapisuje notatkę:

W korzystaniu z internetu najważniejsze jest, abyśmy :

- informacje o sobie zostawiali świadomie - tylko te dane, które są niezbędne;

- nie umieszczali zbyt wielu szczegółów dotyczących naszego życia osobistego w serwisach społecznościowych

- a także zbyt wielu danych określających nasze miejsce zamieszkania, pracy czy zarobków,

- nie udostępniali danych o innych osobach, bo mogą sobie tego nie życzyć

 - nie wszystkie konsekwencje zamieszczonych o nas informacji da się przewidzieć;

 - pamiętali o wyłączeniu zapamiętywania w wyszukiwarce lub skasowaniu

tego, co zostało już zapamiętane (zazwyczaj w menu „Narzędzia”).

- przy instalowaniu aplikacji na telefonie należy sprawdzić, do jakich informacji

chce ona mieć dostęp.

- spam (niechciane wiadomości mailowe), nie otwierać załączników – po prostu je zignorować. Mogą one zawierać linki do złośliwego oprogramowania.

- wybierali silne hasła w sposób, który pozwoli wam je zapamiętać.

Warto więc zabezpieczyć się przed rozmaitymi niekontrolowalnymi skutkami wykorzystania naszych danych przez różne podmioty. Możemy w tym celu:

- instalować różne wtyczki do naszych przeglądarek dbających o prywatność użytkownika,

- korzystać z zapewniających większą anonimowość specjalnych przeglądarek, jak TOR czy też korzystanie z anonimizujących wyszukiwarek internetowych – przykładowo duckduckgo.com.

- zacierać po sobie ślad w komputerze

**Każda nasza aktywność w sieci zostawia po sobie ślad; w Internecie nic nie ginie**

**Dla zainteresowanych**

**Profilowanie osobowości na podstawie śladów cyfrowych**

[**https://blog.zyjespox.com/it/internet/76-profilowanie-osobowosci-na-podstawie-sladow-cyfrowych-keynote**](https://blog.zyjespox.com/it/internet/76-profilowanie-osobowosci-na-podstawie-sladow-cyfrowych-keynote)

[**https://www.radiokrakow.pl/audycje/trendy-w-sieci/trendy-z-sieci-profilowanie-osobowosc-na-podstawie-sladow-cyfrowych/**](https://www.radiokrakow.pl/audycje/trendy-w-sieci/trendy-z-sieci-profilowanie-osobowosc-na-podstawie-sladow-cyfrowych/)