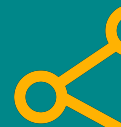


Bezpieczeństwo w sieci

Prowadząca:

Katarzyna Górkwicz



Podczas tego modułu:

- Nauczycie się, jak zadbać o swoje bezpieczeństwo i prywatność w sieci,
- poznacie i przećwiczycie dobre nawyki korzystania z sieci i nauczycie się wdrażać je w swoim codziennym życiu,
- przekonacie się, dlaczego temat higieny cyfrowej jest coraz bardziej aktualny i jak skutecznie ją praktykować,
- przyjrzycie się swojemu cyfrowemu wizerunkowi i dostaniecie narzędzia do jego świadomego kształtowania,
- nauczycie się rozpoznawać mechanizmy wykorzystywane w internecie do reklamy, profilowania, zarabiania pieniędzy i wpływania na opinie.





Kilka słów o mnie

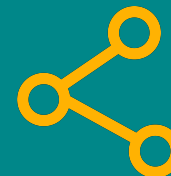
- Jestem trenerką, producentką i autorką materiałów edukacyjnych.
- Współpracuję z organizacjami pozarządowymi i instytucjami kultury. Realizuję projekty z pogranicza edukacji kulturalnej, medialnej i cyfrowej, nauk przyrodniczych i społecznych.
- Jestem autorką publikacji dla nauczycieli oraz materiałów edukacyjnych, w tym licznych materiałów filmowych - animacji i reportaży.
- Interesują mnie relacje pomiędzy człowiekiem a technologią – to, co dzięki nim zyskujemy i to, w czym powinniśmy być szczególnie ostrożni.





Spotkanie 1.

Nasze nawyki korzystania z sieci



A. są krótkie i proste, żeby łatwo mi było je zapamiętać

(np. takie same jak login, data urodzenia, drugie imię, imię zwierzęcia, prosta kombinacja cyfr, pojedyncze słowo ze słownika, to samo hasło z różną cyfrą na końcu),

używam tego samego hasła do wielu kont,

pozwalam je zapamiętać przeglądarce internetowej, mam też je zapisane przy komputerze lub na kartce, którą noszę przy sobie

A. są średniej długości i średnio skomplikowane

używam kilku haseł do wielu kont

A. są długie i jak najbardziej skomplikowane

składają się z małych i dużych liter, a także cyfr i znaków niealfanumerycznych albo długiej frazy (nawet jeśli jest łatwa do zapamiętania)

używam innego hasła do każdego konta,

pilnuję zwłaszcza, by hasła do ważnych kont (bank, e-mail) były wyjątkowe i skomplikowane, znane tylko mnie



1. Moje hasła do kont i profili:

***w komputerze, poczcie
e-mail, serwisach
społecznościowych, sklepach
internetowych***



2. Podaję swoje prawdziwe dane:

- A. zawsze, gdy strona internetowa o to pyta (np. biorąc udział w konkursach, badaniach czy quizach)
- A. czasem, np. rejestrując się w różnych serwisach nawet jednorazowo
- A. tylko, gdy jest to konieczne (np. zakupy)



3. Gdy widzę bannery reklamowe lub linki, które zachęcają do skorzystania z promocji, oferty specjalnej, konkursu czy odbioru nagrody, którą się wygrało:

- A. klikam w najciekawsze, jeśli mnie dotyczą
- A. czasem klikam, ale czasem wydaje mi się to niebezpieczne
- A. omijam z daleka, chyba, że widzę, że reklama jest związana z zaufaną instytucją





4. Kiedy loguję się w miejscu publicznym na któreś ze swoich kont, zwracam uwagę na bezpieczne połączenie (np. https, czy certyfikat jest bezpieczny) i czy nikt niepowołany nie patrzy na klawiaturę:

A. nigdy

B. czasem

C. zawsze



A. **zawsze i od każdego**

A. **czasem, ale tylko wtedy, gdy mnie dotyczy**

A. **tylko, gdy przesyła go znajomy i wygląda wiarygodnie**

np. temat wskazuje, że to rzeczywiście do mnie

jeśli mam wątpliwość, upewniam się, że przesyłający świadomie mi go wysłał

5. Gdy ktoś przesyła mi link lub załącznik e-mailem albo za pośrednictwem komunikatorów, np. WhatsApp, czy Messenger, otwieram go:



6. Publikuję swoje zdjęcia w internecie:

- A. **wszystkie, którymi mam ochotę się podzielić**
- A. **wybieram najciekawsze, nie analizując potencjalnych konsekwencji ich publikacji**
- A. **ze świadomością, że odtąd jest możliwe, że każdy będzie mógł je zobaczyć**
m.in. rodzina, znajomi, potencjalni pracodawcy
mimo ustawień prywatności, ktoś niepowołany może dostać do nich dostęp



A. **wszystkie, którymi mam ochotę się podzielić**

A. **wybierając najciekawsze, które pozytywnie pokazują te osoby, ale nie pytam ich o zgodę i nie analizuję potencjalnych konsekwencji ich publikacji**

A. **tylko za zgodą osób, które są na zdjęciach (lub ich prawnych opiekunów)**

ze świadomością, że odtąd jest możliwe, że każdy będzie mógł je zobaczyć, w tym rodzina, znajomi, potencjalni pracodawcy

mimo ustawień prywatności, ktoś niepowołany może dostać do nich dostęp

7. Publikuję w internecie zdjęcia dotyczące innych osób:



8. Co widzą w moich profilach w serwisach społecznościowych moi znajomi, a co nieznajomi?

- A. **nie wiem / każdy widzi wszystko**
np. e-mail, telefon, adres zamieszkania, wszystkie moje zdjęcia i wpisy
- A. **część danych (jak e-mail, telefon, adres zamieszkania czy zdjęcia) jest widoczna dla nieznajomych**
- A. **ustawiam różne dostępy dla różnych grup znajomych, członkowie każdej widzą co innego, nieznajomi widzą tylko nazwisko i zdjęcie**





9. Do grona znajomych w serwisach społecznościowych zapraszam:

- A. każdego kto zapyta, nawet jeśli nic o nim nie wiem
- A. różnie, zdarza się, że przyjmuję nieznajomych, a potem ich weryfikuję
- A. tylko znajomych, ew. osoby ostatnio poznane, które są w gronie znajomych moich znajomych



- A. wpisuję interesujące mnie hasło w wyszukiwarke i zapoznaję się z pierwszymi wynikami
- A. szukam nie tylko poprzez wyszukiwarke, ale i w Wikipedii i w różnych serwisach
- A. szukam korzystając z zaawansowanych narzędzi w wyszukiwarce (np. ustawienie daty, czy wyszukiwanie zaawansowane)
korzystam z Wikipedii i wiarygodnych serwisów specjalistycznych
eksperymentuję z Chatem GPT
każdą istotną informację weryfikuję w co najmniej dwóch różnych źródłach



10. Kiedy szukam informacji w sieci:

11. Kiedy robię zakupy:

A. **zawsze stacjonarnie i zawsze płacę gotówką – nie ufam wszystkim cyfrowym wynalazkom**

A. **chętnie przez internet, to wygodne i zawsze mogę znaleźć dokładnie to, czego szukam w najlepszej cenie;**

obawiam się jednak płatności online i wybieram opcję płatności przy dostawie

A. **uwielbiam zakupy w sieci – kupuję w ten sposób większość rzeczy;**

to komfort wyszukiwania, dostępności, lepsze ceny i bezpieczeństwo transakcji online, poza tym, jako klient mam większe prawa niż kupując stacjonarnie



- A. jest niewielka – raczej za namową bliskich czy znajomych przełamuję się żeby choć trochę nie odstawać i znać nowe technologie
- A. nowe technologie – strony www, aplikacje, media społecznościowe, smartfon czy platformy streamingowe to moje wielkie odkrycia
- poznałem dzięki nim wielu nowych znajomych, dużo dowiedziałem/am się o świecie
- to dla mnie rozrywka, praca i edukacja
- A. wiele zawdzięczam nowym technologiom, ale w pewnym momencie poczułem się ich niewolnikiem – ciągle nowe powiadomienia, komunikaty, śledzenie wielu tematów i ciągła chęć bycia na bieżąco...
- w pewnym momencie mnie to przytłoczyło i teraz świadomie kontroluję czas z nowymi technologiami i ustawiam blokady powiadomień, żeby nie rozpraszać się w czasie, gdy zajmuję się czymś innym



12. Moja aktywność w sieci:

***z wykorzystaniem telefonu/
komputera/ tabletu/ laptopa***

ZADANIE DOMOWE

Moja prywatność w serwisach społecznościowych

Przeanalizuj swoje ustawienia prywatności w serwisie społecznościowym Facebook. Sprawdź, kto i co może dowiedzieć się na Twój temat.

Weź pod uwagę min. treści postów, zdjęcia, lokalizacje, polubione profile czy aplikacje, które mają dostęp do Twojego profilu.

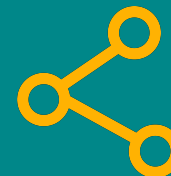
Przemyśl i zrealizuj dwie zmiany w swoich ustawieniach, które lepiej będą chroniły Twoją prywatność.





Spotkanie 2.

Mój cyfrowy ślad





Jakie informacje przekazujemy publikując zdjęcia w sieci?





Jakie informacje przekazujemy publikując zdjęcia w sieci?





Jakie informacje przekazujemy publikując zdjęcia w sieci?



- Pierwszy sposób na zacieranie za sobą śladów ;)
- Podczas korzystania z trybu incognito odwiedzane strony nie są zapisywane w historii. Zapisywane nie są również frazy wpisywane w wyszukiwarce, wprowadzane loginy i hasła, informacje podawane w formularzach czy też pliki cookies (czyli „ciasteczka”).
- Aby włączyć tryb INCOGNITO wchodzimy w ustawienia przeglądarki (najczęściej w prawym górnym rogu – trzy kropki lub kreski) i wybieramy opcję „otwórz nową kartę prywatną/incognito”.

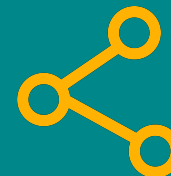
Tryb incognito/ prywatny





Podstawowe zasady bezpieczeństwa i prywatności w sieci

Terminy, które warto znać



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.

Określenie fizycznego położenia geograficznego osoby i urządzenia telekomunikacyjnego za pomocą systemu GPS lub adresu IP.

GEOLOKALIZACJA

Wszelkie informacje dotyczące określonej osoby fizycznej (czyli zidentyfikowanej lub możliwej do zidentyfikowania). Podlegają ochronie i nie mogą być zbierane bez odpowiedniej podstawy prawnej (np. zgody osoby, której dotyczą).

DANE OSOBOWE

CIASZTECZKA

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). Mogą narażać użytkownika na wiele zagrożeń, gdyż działają w sposób niewidoczny i mogą zapamiętywać wiele wrażliwych informacji.

DANE WRAŻLIWE

Dane osobowe, które podlegają szczególnej ochronie. Należą do nich informacje o rasie, pochodzeniu etnicznym, poglądach politycznych, przekonaniach religijnych, stanie zdrowia, przynależności partyjnej, związkowej lub wyznaniowej, kodzie genetycznym, nałogach, życiu seksualnym, skazaniach i orzeczeniach dotyczących mandatów i kar.

Jakie informacje zbierają o nas strony www i aplikacje?

Dane osobowe i wrażliwe:

Imię, nazwisko, adres e-mail, data urodzenia, płeć, a także bardziej szczegółowe informacje, takie jak wyznanie, orientacja seksualna, czy poglądy polityczne.

Lokalizacja:

Aplikacje mogą śledzić i gromadzić dane o lokalizacji użytkownika za pomocą GPS, co pozwala na ustalenie miejsc, które odwiedza, oraz ścieżek poruszania się.

Historia przeglądania i wyszukiwania:

Dane o stronach internetowych odwiedzanych przez użytkownika, zapytania wyszukiwane w wyszukiwarkach, oraz aktywność w mediach społecznościowych.



Uprawnienia do kontaktów, kalendarza, aparatu:

Aplikacje mogą prosić o dostęp do listy kontaktów, kalendarza, aparatu i mikrofonu, co pozwala im na gromadzenie informacji o kontaktach, wydarzeniach w kalendarzu, zdjęciach, nagraniach audio i wideo.

Biometria:

Niektóre aplikacje mogą zbierać dane biometryczne, takie jak odciski palców, skany twarzy, czy rozpoznawanie głosu.

Dane zdrowotne:

Aplikacje związane ze zdrowiem mogą zbierać informacje o stanie zdrowia, aktywności fizycznej, diecie, a nawet danych medycznych.



Dane o urządzeniu:

Informacje o modelu telefonu, producencie, systemie operacyjnym, adresie IP, a także unikalne identyfikatory urządzenia.

Dane z mediów społecznościowych:

Aplikacje mogą integrować się z portalami społecznościowymi i pozyskiwać informacje udostępniane przez użytkowników, w tym posty, komentarze, polubienia i udostępnienia.

Dane z zakupów:

Aplikacje mogą śledzić historię zakupów i preferencje zakupowe użytkowników.



Do czego te informacje są wykorzystywane?

Personalizacja treści:

Dostarczanie spersonalizowanych reklam, rekomendacji produktów, oraz treści dopasowanych do zainteresowań i preferencji użytkownika.

Analiza rynku i zachowań użytkowników:

Tworzenie profili użytkowników, grup docelowych dla reklamodawców, oraz badanie trendów rynkowych.



Usprawnienie działania stron i aplikacji:

Ułatwienie wyszukiwania, personalizacja ustawień, oraz dostosowanie funkcji do indywidualnych potrzeb użytkownika.

Zarządzanie kontem:

Uwierzytelnianie tożsamości, odzyskiwanie dostępu do konta, oraz personalizacja ustawień konta.

Bezpieczeństwo:

Wykrywanie oszustw, zapobieganie nadużyciom, oraz ochrona przed nieautoryzowanym dostępem do konta.



- Sprawdzając ustawienia prywatności na platformach społecznościowych i w usługach Google.
- Analizując ustawienia przeglądarki i uprawnienia aplikacji.
- W ustawieniach telefonu można sprawdzić, jakie uprawnienia posiada dana aplikacja i jakie dane może zbierać.
- Czytając politykę prywatności aplikacji, aby dowiedzieć się, jakie dane są zbierane i w jaki sposób są wykorzystywane.

**Jak sprawdzić,
jakie
informacje o
nas są
zbierane?**



ZADANIE DOMOWE

Bezpieczeństwo moich haseł

Przeanalizuj i spróbuj spisać wszystkie miejsca w sieci, w których utworzyłeś/aś konto i do których posiadasz hasło.

Zastanów się, czy twoje hasła są bezpieczne.

Ilością kont i przemyśleniami o ich bezpieczeństwie podziel się na naszej Facebookowej grupie.

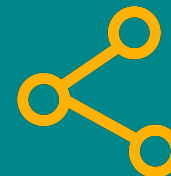
Wypróbuj menedżera haseł w przeglądarce, której używasz i uporządkuj swoje konta w sieci.





Spotkanie 3.

**Dlaczego nowe technologie
nami manipulują?**



- Inaczej nazywany błędem konfirmacji lub strategią konfirmacyjną.
- Tendencja do preferowania informacji, które potwierdzają wcześniejsze oczekiwania i hipotezy, niezależnie od tego, czy te informacje są prawdziwe.
- Powoduje, że ludzie poszukują informacji i zapamiętują je w sposób selektywny, interpretując je w błędny sposób.
- Efekt ten jest szczególnie silny w przypadku zagadnień wywołujących silne emocje i dotyczących mocno ugruntowanych opinii.
- Wiąże się z interpretowaniem niejednoznacznych dowodów jako potwierdzających ich własne zdanie.

Efekt potwierdzenia



Jak na nas wpływa efekt potwierdzenia?

- Poszukujemy i preferujemy dowody potwierdzające nasze poglądy.
- Skuteczniej zapamiętujemy informacje zbieżne z naszymi poglądami.
- Interpretujemy dowody na korzyść konkretnej tezy (szczególnym przypadkiem jest stosowanie absurdałnego wyjaśnienia, że wyjątek potwierdza regułę).
- Unikamy sytuacji, które mogą zagrozić naszym przekonaniom („Nie będę z Tobą o tym dyskutował”).
- Ignorujemy dane nie pasujące do naszego światopoglądu.



Konsekwencje efektu potwierdzenia

- Szczególnie podatna na efekt potwierdzenia jest nauka. Wielokrotnie zauważono, że naukowcy oceniają korzystniej badania, których wyniki są zbieżne z ich wcześniejszymi przekonaniami.
- Psycholodzy społeczni zauważyli dwie skłonności w sposobie poszukiwania i interpretowania przez ludzi informacji na swój temat. Po pierwsze dążymy do wzmocnienia obrazu siebie; po drugie, poszukujemy pozytywnej informacji zwrotnej na swój temat.
- Media społecznościowe tworzą bańki informacyjne, do których nie docierają (lub docierają w zubożonej formie) informacje z zewnątrz.



Wierz, w co chcesz!



Słyszysz tylko to,
co chcesz!

Żaden argument,
nie przekona mnie, że....



Bańka informacyjna/ filtrująca

- Osobista i spersonalizowana przestrzeń każdej osoby, która nie jest współdzielona z innymi.
- Składa się ona w dużym stopniu z elementów, które lubimy i dobrze znamy, są wariantami znanych rzeczy i które są nieustannie dopasowywane przez podmioty działające w sieci.
- Termin stworzony przez działacza internetowego - Eliego Parisera, opisany w wydanej w 2010 roku książce „*The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*”



Konsekwencje funkcjonowania w zamkniętych w bańkach

- Nasza aktywność w sieci jest zapamiętywana i analizowana.
- Wiedza na temat naszych działań w sieci służy różnym podmiotom do różnych celów:
 - e-marketerzy interesują się tym, z jakich korzystamy usług i produktów, by dopasowywać określone reklamy;
 - pracownicy banku, ubezpieczyciele czy potencjalny pracodawca przeglądają zawartość naszych kont w portalach społecznościowym, by sprawdzić naszą wiarygodność;
 - państwo interesuje się tym, czy możesz stanowić zagrożenie dla bezpieczeństwa publicznego.



Mechanizm, który polega na kategoryzowaniu ludzi według cech i zachowań.

- Facebook, YouTube i inne platformy społecznościowe (lajki, co obserwujemy, ile czasu poświęcamy danemu postowi, czy bierzemy udział w dyskusji itp.)
- Wyszukiwarka internetowa (indywidualne dopasowanie wyników, historia wyszukiwania, wybrane przez nas odpowiedzi)

Profilowanie



Higiena cyfrowa

Zachowania chroniące zdrowie związane z używaniem internetu i urządzeń ekranowych. Potrzebna jest każdemu, dlatego uczymy jej bez względu na wiek.

Źródło: Instytut Cyfrowego Obywatelstwa



Zadanie domowe

Stwórzmy wspólnie mapę dobrych nawyków w sieci

Zastanów się, jakie zachowania i nawyki pomogą Ci bezpiecznie i odpowiedzialnie korzystać z internetu i nowych technologii. Wykorzystaj wiedzę zdobytą na naszych zajęciach. Możesz też dodać od siebie kwestie, o które dbasz od jakiegoś czasu i chcesz podzielić się swoim doświadczeniem.

Wasze odpowiedzi zbiorę we wspólną pracę, która zostanie z Wami po kursie, jako lista rzeczy, o których warto pamiętać!



Dziękuję!

MATERIAŁ DOSTĘPNY NA LICENCJI:

CC BY-NC-SA 4.0



Projekt „Dojrzała sieć” powstaje jako część programu “Countering Disinformation among Vulnerable Populations in Central Europe” realizowanego w 4 krajach: Polska (Towarzystwo Inicjatyw Twórczych “ę”), Czechy (Transitions), Słowacja (Memo98), Węgry (Center of Independent Journalism).

Organizator:



Partnerzy:

