

Prywatność i Śledzenie w Sieci

Warsztaty

Prowadzący: prof. dr hab. Maciej Rybczyński

Jakie dane zbierają o nas strony internetowe?

1. Adres IP i lokalizacja.
2. Historia przeglądania i aktywność online.
3. Dane z ciasteczek (cookies).
4. Dane logowania i identyfikatory urządzeń.
5. Informacje o sprzęcie i systemie operacyjnym.

Czym są cookies i jak działają?

1. Pliki zapisywane przez strony internetowe na Twoim urządzeniu.
2. Mogą być używane do zapamiętywania preferencji i logowania.
3. Ciasteczka śledzące (tracking cookies) zbierają informacje o Twojej aktywności online.
4. Jak zarządzać cookies? – ustawienia przeglądarki i rozszerzenia.

Zarządzanie Cookies w popularnych przeglądarkach

Google Chrome

1. Otwórz **Chrome** i kliknij ikonę **trzech kropek** (⋮) w prawym górnym rogu.
2. Wybierz **Ustawienia**.
3. Przejdź do sekcji **Prywatność i bezpieczeństwo**.
4. Kliknij **Pliki cookie i inne dane witryn**.
5. W tym miejscu możesz:
 - 1) **Zezwalać na wszystkie pliki cookie** (domyślne ustawienie),
 - 2) **Blokować pliki cookie innych firm** (zalecane dla większej prywatności),
 - 3) **Blokować wszystkie pliki cookie** (może powodować problemy z logowaniem na stronach),
 - 4) **Usuwać pliki cookie po zamknięciu przeglądarki**.

Usuwanie cookies

1. W sekcji **Prywatność i bezpieczeństwo** wybierz **Wyczyść dane przeglądania**.
2. Wybierz **Pliki cookie i inne dane witryn** i kliknij **Wyczyść dane**.

Zarządzanie Cookies w popularnych przeglądarkach

Mozilla Firefox

1. Otwórz **Firefox** i kliknij ikonę **trzech kresek** (≡) w prawym górnym rogu.
2. Przejdź do **Ustawienia** → **Prywatność i bezpieczeństwo**.
3. W sekcji **Cookies i dane witryn** możesz:
 - 1) **Zezwalać na wszystkie pliki cookie**,
 - 2) **Blokować pliki cookie innych firm** lub wszystkie cookies,
 - 3) **Ustawić automatyczne usuwanie cookies po zamknięciu przeglądarki**.

Usuwanie cookies

1. Przejdź do **Ustawienia** → **Prywatność i bezpieczeństwo**.
2. W sekcji **Cookies i dane witryn** kliknij **Wyczyść dane**.
3. Wybierz **Cookies i dane witryn**, a następnie **Wyczyść**.

Zarządzanie Cookies w popularnych przeglądarkach

Microsoft Edge

1. Kliknij ikonę **trzech kropek** w prawym górnym rogu.
2. Wybierz **Ustawienia** → **Pliki cookie i uprawnienia witryny**.
3. W sekcji **Pliki cookie i dane przechowywane** możesz:
 - 1) **Zezwalać na wszystkie pliki cookie**,
 - 2) **Blokować pliki cookie innych firm**,
 - 3) **Zarządzać wyjątkami** dla wybranych stron.

Usuwanie cookies

1. W sekcji **Prywatność, wyszukiwanie i usługi** wybierz **Wyczyść dane przeglądania**.
2. Wybierz **Pliki cookie i inne dane witryn** i kliknij **Wyczyść teraz**.

Zarządzanie Cookies w popularnych przeglądarkach

Safari (macOS, iOS)

1. Otwórz **Safari** i przejdź do **Preferencje**.
2. Wybierz zakładkę **Prywatność**.
3. W sekcji **Cookies i dane witryn** możesz:
 - 1) **Blokować wszystkie cookies**,
 - 2) **Zezwalać tylko na cookies odwiedzanych stron**,
 - 3) **Usuwać cookies przy zamykaniu przeglądarki**.

Usuwanie cookies

1. Otwórz **Preferencje** → **Prywatność**.
2. Kliknij **Zarządzaj danymi witryn**, wybierz strony i kliknij **Usuń**.

Zarządzanie Cookies w popularnych przeglądarkach

Rozszerzenia do zarządzania cookies

Jeśli chcesz uzyskać bardziej zaawansowaną kontrolę nad plikami cookies, warto zainstalować odpowiednie rozszerzenia do przeglądarek.

Najlepsze rozszerzenia do zarządzania cookies

1. Cookie AutoDelete (Chrome, Firefox, Edge)

- 1) Automatycznie usuwa cookies po zamknięciu karty lub przeglądarki.
- 2) Możliwość konfiguracji wyjątków dla wybranych stron.

2. Privacy Badger (Chrome, Firefox, Edge)

- 1) Blokuje śledzące cookies i inne skrypty śledzące.

3. uBlock Origin (Chrome, Firefox, Edge)

- 1) Zaawansowany bloker reklam i trackerów, który także blokuje cookies śledzące.

4. EditThisCookie (Chrome)

- 1) Umożliwia ręczne edytowanie, dodawanie i usuwanie cookies.

5. Ghostery (Chrome, Firefox, Edge, Safari)

- 1) Blokuje śledzące cookies i skrypty analityczne.

Zarządzanie Cookies w popularnych przeglądarkach

Jak całkowicie wyłączyć cookies?

Jeśli chcesz całkowicie wyłączyć cookies w przeglądarce, wykonaj poniższe kroki:

- **Chrome** → **Ustawienia** → **Prywatność i bezpieczeństwo** → **Pliki cookie i inne dane witryn** → **Blokuj wszystkie pliki cookie.**
- **Firefox** → **Ustawienia** → **Prywatność i bezpieczeństwo** → **Pliki cookie i dane witryn** → **Zablokuj wszystkie pliki cookie.**
- **Edge** → **Ustawienia** → **Pliki cookie i uprawnienia witryny** → **Blokuj wszystkie pliki cookie.**
- **Safari** → **Preferencje** → **Prywatność** → **Blokuj wszystkie pliki cookie.**

Uwaga: Wyłączenie wszystkich cookies może powodować problemy z logowaniem się na stronach internetowych oraz brakiem zapamiętywania preferencji.

Podsumowanie

- **Pliki cookies można łatwo zarządzać w ustawieniach przeglądarki** – można je usuwać, blokować lub ustawić ich automatyczne usuwanie.
- **Zaawansowane zarządzanie cookies** oferują rozszerzenia, takie jak Cookie AutoDelete, Privacy Badger czy uBlock Origin.
- **Całkowite wyłączenie cookies** może wpłynąć na działanie stron internetowych.

Jak reklamodawcy śledzą nas w sieci?

1. Ciasteczka stron trzecich.
2. Fingerprinting przeglądarki.
3. Piksele śledzące w e-mailach.
4. Analiza zachowania użytkownika na stronach.

Piksele śledzące w emailach

Co to jest piksel śledzący?

Piksel śledzący (ang. *tracking pixel*) to niewidoczny obrazek o wielkości 1×1 piksela umieszczony w treści wiadomości e-mail. Jego główną funkcją jest monitorowanie interakcji użytkownika z wiadomością poprzez zbieranie określonych danych w momencie otwarcia e-maila.

Piksel może być wstawiony w formie:

- **Pliku graficznego (GIF, PNG, JPEG)** hostowanego na zewnętrznym serwerze.
- **Osadzonego obrazu w kodzie HTML** (np. ``).

Jak działają piksele śledzące w e-mailach?

1. Nadawca umieszcza niewidoczny obrazek w wiadomości e-mail.
2. Po otwarciu e-maila przeglądarka lub klient poczty (np. Gmail, Outlook) wysyła żądanie do serwera, na którym znajduje się obrazek.
3. Serwer rejestruje to żądanie, zapisując informacje o odbiorcy, czasie otwarcia, lokalizacji i innych parametrach.
4. Dane są następnie analizowane przez systemy marketingowe do śledzenia skuteczności kampanii e-mailowej.

Piksele śledzące w emailach

Jakie dane zbierają piksele śledzące?

Piksele śledzące mogą gromadzić różne informacje, w tym:

Rodzaj informacji	Opis
Czas otwarcia	Moment, w którym e-mail został otwarty.
Adres IP	Może sugerować lokalizację odbiorcy.
Rodzaj urządzenia	Desktop, tablet, smartfon.
System operacyjny	Windows, macOS, iOS, Android itp.
Klient pocztowy	Gmail, Outlook, Apple Mail itp.
Czy kliknięto linki?	Monitorowanie interakcji z treścią.

Piksele śledzące w emailach

Zastosowania pikseli śledzących

Piksele śledzące są szeroko stosowane w marketingu, analizie efektywności kampanii oraz cyberbezpieczeństwie.

Marketing i analityka

- **Śledzenie otwarć e-maili** – marketerzy mogą sprawdzać, jak skuteczne są ich kampanie.
- **Segmentacja odbiorców** – użytkownicy aktywnie otwierający e-maile mogą otrzymać dodatkowe wiadomości.
- **Optymalizacja czasu wysyłki** – analiza danych pozwala dostosować godziny wysyłania e-maili dla większej skuteczności.
- **Śledzenie konwersji** – analiza kliknięć w linki pomaga mierzyć skuteczność działań.

Cyberbezpieczeństwo i phishing

- **Ataki śledzące** – cyberprzestępcy mogą używać pikseli do śledzenia, kto otworzył złośliwy e-mail.
- **Potwierdzenie aktywności konta** – piksel może pomóc hakerom sprawdzić, czy adres e-mail jest aktywny.
- **Ataki ukierunkowane** – złośliwe e-maile mogą zbierać dane techniczne o systemie ofiary.

Piksele śledzące w emailach

Jak blokować piksele śledzące?

Ochrona przed śledzeniem w klientach pocztowych

Większość nowoczesnych klientów pocztowych oferuje opcje blokowania pikseli śledzących:

- **Gmail** (domyślnie blokuje automatyczne ładowanie obrazków, ale może je pobierać przez serwery Google).
- **Outlook** → Ustawienia > Automatyczne pobieranie obrazków > Wyłącz automatyczne pobieranie.
- **Apple Mail (iOS 15+)** → *Mail Privacy Protection* ukrywa adres IP i blokuje śledzenie.

Rozszerzenia przeglądarek do ochrony prywatności

- **uBlock Origin** – blokuje skrypty śledzące w e-mailach przeglądanych przez webmail.
- **Privacy Badger** – wykrywa i blokuje śledzące obrazy.
- **Trocker (dla Gmaila i Outlooka)** – automatycznie blokuje piksele śledzące.

Użycie alternatywnych klientów e-mail

Niektóre usługi e-mail koncentrują się na prywatności, np.:

- **ProtonMail** – domyślnie blokuje śledzenie.
- **Tutanota** – szyfrowana poczta e-mail bez zewnętrznych zasobów.

Ręczne blokowanie ładowania obrazów

W większości klientów pocztowych można wyłączyć automatyczne pobieranie obrazów:

1. **Gmail** → Ustawienia → Obrazy → "Pytaj przed wyświetlaniem obrazów".
2. **Outlook** → Opcje → Centrum zaufania → Automatyczne pobieranie obrazów → "Nie pobieraj obrazów automatycznie".
3. **Thunderbird** → Ustawienia konta → Prywatność i bezpieczeństwo → "Blokuj zdalne treści w wiadomościach".

Piksele śledzące w emailach

Czy piksele śledzące są legalne?

Piksele śledzące nie są nielegalne, ale ich stosowanie podlega przepisom o ochronie prywatności, takim jak:

- **RODO (UE)** – wymaga zgody użytkownika na śledzenie.
- **CCPA (USA, Kalifornia)** – użytkownicy mogą żądać rezygnacji ze śledzenia.
- **PECR (Wielka Brytania)** – firmy muszą informować użytkowników o pikselach śledzących.

Większość firm umieszcza informacje o śledzeniu w polityce prywatności, ale niewiele osób o tym wie lub świadomie akceptuje takie praktyki.

Podsumowanie

- **Piksele śledzące pozwalają na monitorowanie otwierania e-maili i interakcji użytkowników.**
- **Są szeroko stosowane w marketingu, ale mogą być wykorzystywane do śledzenia i ataków phishingowych.**
- **Można je blokować za pomocą ustawień poczty, rozszerzeń przeglądarek i klientów e-mail nastawionych na prywatność.**
- **Ich użycie w Unii Europejskiej podlega przepisom RODO, ale wciąż są stosowane bez wyraźnej zgody użytkownika.**

Jak chronić swoją prywatność w sieci?

1. Używaj przeglądarek zorientowanych na prywatność (np. Brave, Firefox).
2. Blokuj trackery za pomocą rozszerzeń (np. uBlock Origin, Privacy Badger).
3. Korzystaj z wyszukiwarek chroniących prywatność (np. DuckDuckGo).
4. Używaj VPN do ukrywania swojego adresu IP.

Interaktywne zadanie: Jak anonimowy jesteś w sieci?

1. Odwiedź stronę <https://www.whatismybrowser.com>.
2. Sprawdź, jakie informacje są widoczne o Twojej przeglądarce i systemie.
3. Zmodyfikuj ustawienia prywatności i zobacz, co się zmienia.

Zabezpieczanie prywatnych danych – podstawowe kroki

1. Unikaj logowania do nieznanych stron za pomocą kont Google/Facebook.
2. Regularnie usuwaj historię przeglądania i ciasteczka.
3. Korzystaj z trybu incognito, ale pamiętaj, że nie zapewnia on pełnej anonimowości.
4. Sprawdzaj uprawnienia aplikacji na telefonie.

Podsumowanie i pytania

1. Jakie dane są zbierane o nas w Internecie?
2. Jakie metody śledzenia stosują reklamodawcy?
3. Jak można poprawić swoją prywatność w sieci?
4. Jakie masz pytania?