Tracking Cookies

Privacy Risks and Data Exposure

Submitted by:

- AbdAelrahman Mostafa
- Omar yehia
- Hussein Mohammed
- Ahmed Alaa

Supervised by: Eng. Sarah Refaie

CONTENTS

INTRODUCTION

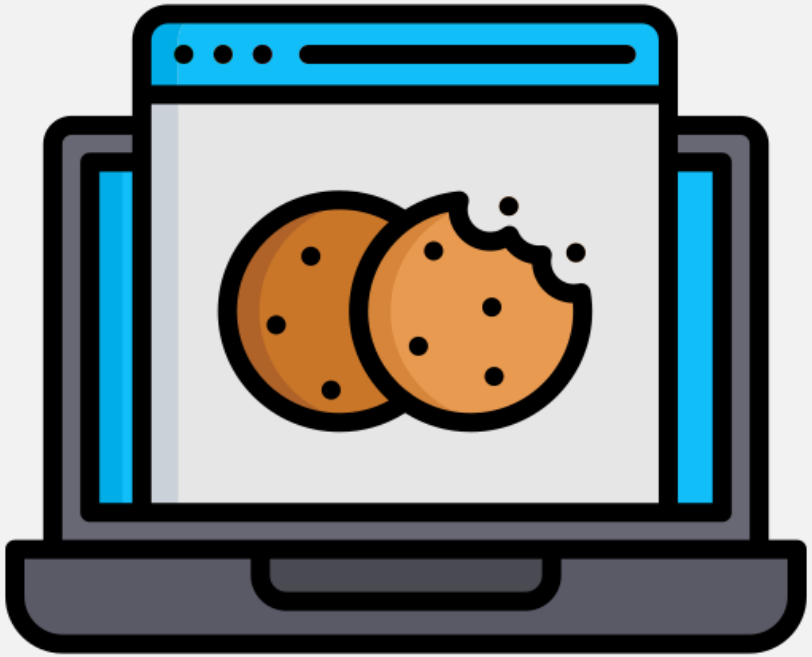
In today's digital world, our online activity is constantly tracked—often without our knowledge. One of the most common tools used for this is tracking cookies: small files stored by websites to monitor user behavior.

While some cookies improve user experience, others raise serious concerns about privacy, data sharing, and unauthorized profiling. This Research explores what tracking cookies are, how they work, their impact, and how users can protect themselves from unwanted tracking.

WHAT ARE TRACKING COOKIES?

- Cookies are small files that websites save on your device to remember information and improve your experience.

- Tracking cookies are a type of cookie used by third parties to follow your activity across different websites. They collect data about your interests and behavior for advertising and profiling.



WHAT ARE TRACKING COOKIES?

- Their main function is to store information about a user's browsing activity, such as visited pages, clicked links, and search terms. This data helps build a profile of user behavior, which can be used for targeted advertisements or behavior analysis.

- Unlike regular session cookies (which help websites remember user preferences or login sessions), tracking cookies can monitor users across multiple websites and persist for a long time even after the browser is closed.

HOW TRACKING COOKIES WORK

- When you visit a website, tracking cookies are saved on your device by the browser. These cookies store information about your visit, like the pages you view or links you click.

- When you visit other websites that use the same tracking companies, these cookies send data back to the trackers. This lets them follow your activity across multiple sites and build a profile of your interests and habits.

PRIVACY CONCERNS AND RISKS

Tracking cookies collect personal data without clear permission. This can lead to:

- Unauthorized data collection: Your browsing habits are recorded without clear consent.
- Targeted advertising: You may see ads based on detailed profiles built from your online behavior.
- Data security risks: If the data collected is leaked or hacked, your personal information could be exposed.

HOW TO PROTECT YOURSELF FROM TRACKING COOKIES

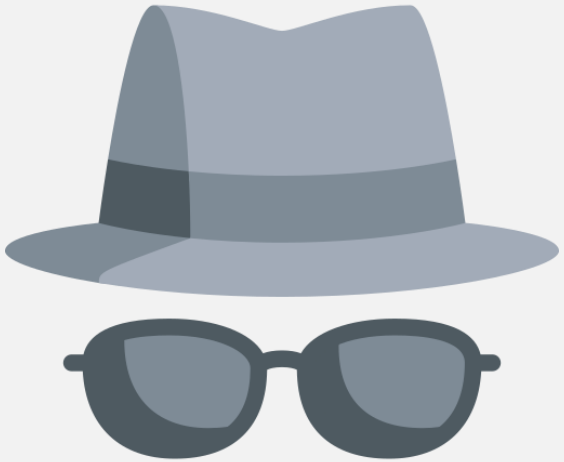
Tracking cookies can invade your privacy, but there are ways to protect yourself:

- Use Privacy-Focused Browsers:
  Browsers like Brave, Mozilla Firefox, or Tor have built-in features to block tracking cookies.
- Enable Do Not Track Settings:
  Most browsers offer a “Do Not Track” option that asks websites not to track your activity.

brave

HOW TO PROTECT YOURSELF FROM TRACKING COOKIES

- Install Anti-Tracking Extensions:
  Tools like uBlock Origin, Privacy Badger, and Ghostery block trackers and third-party cookies.
- Clear Cookies Regularly:
  Removing cookies often reduces how long tracking cookies can follow you.
- Use Private Browsing or Incognito Mode:
  This stops cookies from being saved after you close the session.



REAL-WORLD EXAMPLES OF TRACKING COOKIES IMPACT

Facebook & Cambridge Analytica Scandal (2018)

What happened?

Facebook allowed third-party apps to collect user data through cookies and APIs. Cambridge Analytica harvested data from over 87 million users to influence political campaigns, including the 2016 U.S. election.

Role of Tracking Cookies:

Tracking cookies helped gather user behavior across many websites, enabling precise micro-targeted political ads.

Aftermath & Response:

Facebook faced global backlash and was fined $5 billion by the FTC in 2019. The company updated privacy controls, limited third-party data access, and made cookie permissions clearer.

REAL-WORLD EXAMPLES OF TRACKING COOKIES IMPACT

Google's FLoC & Privacy Concerns (2021)

What happened?

Google introduced Federated Learning of Cohorts (FLoC) to replace third-party cookies by grouping users based on browsing habits rather than tracking individuals.

Public Reaction:

Privacy groups like the Electronic Frontier Foundation criticized FLoC for still enabling profiling and surveillance.

Outcome:

Google canceled FLoC and replaced it with the "Topics API," which shares broader interest categories to reduce invasiveness.

REAL-WORLD EXAMPLES OF TRACKING COOKIES IMPACT

Apple's App Tracking Transparency (ATT) Update (2021)

What happened?

Apple required apps to get user permission before tracking across apps and websites.

Impact on Industry:

Companies relying on tracking cookies, like Facebook, saw major revenue drops. Facebook reported a $10 billion loss in ad revenue.

Public Reaction:

The update was praised by privacy advocates and enhanced Apple's reputation as a privacy-focused company.

CONCLUSION

- Tracking cookies are widely used to collect data about users' online behavior.
- While they can improve user experience, they often raise serious privacy concerns.
- Tracking cookies enable targeted advertising but can lead to unauthorized data sharing and profiling.
- Many companies and governments are responding with new privacy rules and tools.
- Users can protect themselves by using privacy-focused browsers, anti-tracking tools, and managing cookie settings.
- Understanding tracking cookies helps us make better choices about our online privacy.

REFERENCES

- https://www.cookiebot.com/en/tracking-cookies/
- "Hacking: The Art of Exploitation" by Jon Erickson
- "Computer Security: Principles and Practice" by William Stallings & Lawrie Brown
- https://www.bbc.com/news/world-us-canada-48972327
- https://usefathom.com/blog/google-floc
- https://www.adjust.com/glossary/app-tracking-transparency/