Information Technology Services

Information and Cybersecurity Awareness

Email ithelp@up.ac.za | **www.up.ac.za/itsecurity

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Make today matter

Digital Fingerprinting

'Small actions, big difference—welcome to the digital neighbourhood'

Our digital fingerprints contain a set of data that identifies our browser setups and devices as unique. This allows internet users to be identified and tracked, even when they take evasive measures against cookies. These identifiers relate mainly to browser and devices, but can be used to pry into our personal data and internet browsing habits.

Digital fingerprinting has become extremely hard to control or regulate. The two main forms are browser fingerprinting, when this information is delivered through the browser when a user visits remote sites, and device fingerprinting, when the information is delivered through apps installed by users on their devices.

How does it work?

Digital fingerprints are saved server-side, so we cannot typically block them without taking considerable steps to do so, and many of these steps negatively impact our browsing experience. When we visit a website, a fingerprint tracking script (typically JavaScript) collects data from our browser and device. Once this data is rendered, it is processed, hashed and sent to a server for server-side storage.

However, there are browsers that do not allow digital fingerprinting to occur without consent, for example Brave.

SEE MORE

A Guide to Digital Fingerprints (YouTube)

READ MORE

What Is Fingerprinting? (eff.org)

DO MORE

Be aware of digital fingerprinting

How effective is tracking?

In order for fingerprinting to be effective for trackers, it must meet the following two criteria:

1. It must be persistent—if the user's fingerprint changes rapidly, it would be impossible for the tracker to tell one visit by a user from the next. This persistent identifier is used as a substitute for a cookie, which can be easily deleted by the user.
2. It must be unique—if two or more users have the same fingerprint, the tracker loses the ability to identify and pinpoint a single individual by using fingerprinting.

According to a Panopticlick study of user browsers, the vast majority of browsers satisfied these two criteria.

A digital fingerprint

Data points extracted from your browser or device are calculated to provide a digital fingerprint unique to you. The long list of data points that increase the probability of a unique digital footprint includes the following:

- IP address
- Device MAC address
- User-agent string
- Clock information and timestamp
- Web browser plugins
- Fonts installed on your device
- JavaScript objects
- Internal application programming interfaces (APIs)
- Device information (resolution, OS, language)
- Flash data
- Hypertext Transfer Protocol (HTTP) headers
- List of mime-types

Who uses digital fingerprinting?

- Marketing and advertising: Digital fingerprinting helps people responsible for marketing and advertising to send targeted ads and services to specific users without cookies.
- Anti-fraud and security: Digital fingerprinting is a powerful anti-fraud technique used, for example, to detect when one device is used to log into multiple payment accounts or uses several pieces of personal information.
- Validation services: Banking apps, for example, use fingerprinting as part of their authentication processes.