GenZ, Cybersecurity, and New Security Measures on User-Facing Tech

an SNSI Security Summit

Jason Griffey

Director of Strategic Initiatives, NISO
User Facing Technology

Browsers &
Online Tracking

Passkeys
Browsers & Online Tracking
Non-transparent, uncontrollable tracking of users across the web needs to be addressed and prevented.
Browser vendors are being held accountable for tracking.

They will implement tech that breaks things in order to avoid legal action.
How Does Tracking Happen

- Third-Party Cookies
- IP Addresses
- Browser Fingerprinting
- Link Decoration
HTTP cookies (also called web cookies, Internet cookies, browser cookies, or simply cookies) are small blocks of data created by a web server while a user is browsing a website and placed on the user's computer or other device by the user’s web browser.

- **First-Party Cookies**
  - Accessible only by the domain that created it
- **Third-Party Cookies**
  - Accessible to any site at any domain
Sites use features like cookies for more than just authentication and authorization

- Storing user preferences
- Session information across frames
- Demographic info for targeted advertising / content
IP Addresses

Used to identify machines and/or services

- Tracking mitigations for Browser Fingerprinting often impact IP address information
- Often used to make authorization decisions in:
  - Libraries
  - Enterprise Resource Planning (ERP) systems
Browser Fingerprinting

Information collected about the software and hardware of a remote computing device for the purpose of identification

Includes capture of information such as
• Browser used
• Fonts used
• Add-ons used
• Browser security configuration
• IP address
• ...
•
Link Decoration

A method of adding extra information to the URL. Also known as “navigation-based tracking”

Used for:
• Query strings
• Some authentication tokens (i.e., “Front-channel”)
• Tracking information

https://2023alaannual.eventscribe.net/myplan.asp?mode=sessions&afp=MkMxMTc3MTUyNjc2MDpNc1N1SDVYYg
So now what?
What is happening Right Now?

- Library-focused groups are part of the conversation with Browser Vendors
- Seamless Access
- Changes are being made and rolled out
Timelines

- Apple’s timeline:
  - n/a (Apple started blocking third-party cookies by default in 2017 as part of Intelligent Tracking Protection)
  - With Safari 17, they are also removing known link decoration trackers in Private Browsing Mode.

- Mozilla’s timeline:
  - n/a (Mozilla also blocks third-party cookies by default as of June 2022 with Total Cookie Protection)

- Google’s timeline:
  - https://privacysandbox.com/timeline
  - “As developers adopt these APIs, we now intend to begin phasing out third-party cookies in Chrome in the second half of 2024.”
• Something you Know
• Something you Are
• Something you Have

• Password
• Fingerprint/Face Scan
• Key/Passkey/ Hardware Token
1. Users select their preferred authentication method.

2. User's device creates a new key pair:
   - **KEY PAIR C**
   - **Private**
   - **Public**

3. The device retains the private key and sends the public key to the online service.
Passwordless by default: Make the switch to passkeys

Oct 10, 2023
2 min read

For Cybersecurity Awareness Month we’re making it even easier for users to get started with passkeys

Sriram Karra
Senior Product Manager

Christiaan Brand
Group Product Manager
Passkey support on Android and Chrome

Passkeys can be synchronized across devices in the same ecosystem. For example, passkeys created on Android are stored in the Google Password Manager.

Note: Starting from Android 14, users will be able to opt to use third-party credential management apps to store their passkeys.

Passkeys are an emerging technology and supported environments are still evolving. As of August 2023, Chrome on macOS and Windows stores passkeys on the local device only.

Google Password Manager

Google Password Manager stores, serves, and synchronizes passkeys on Android and Chrome. Passkeys from Google Password Manager are available to all Android apps, including Chrome and other browsers. When the user creates a passkey on an Android device it’s stored and synchronized with their other Android devices, and their passkey secrets are encrypted end-to-end. This makes passkeys available to the user across all Android devices that use Google Password Manager and are signed in with the same Google account.

Google Password Manager on Chrome helps create and sign in with passkeys. Depending on the desktop operating system (e.g. ChromeOS, iOS, MacOS, Windows) users may be presented with a QR code to securely use a passkey stored on their mobile device, or a notification may be displayed prompting the user to unlock their phone to use the relevant passkey.
Passkeys

Passkeys can now be synced using external providers, and you can create groups to share passwords and passkeys. In managed environments, passkeys support Managed Apple IDs, including syncing via iCloud Keychain, and access controls let people easily restrict how passkeys are shared and synced.
Passkeys in Windows

Windows 11

Are you tired of constantly forgetting your passwords and having to type them in every time you want to access your favorite websites and applications? Say hello to passkeys! Passkeys provide a more secure and convenient way to sign in. With passkeys, you can use Windows Hello to sign in with a PIN, facial recognition, or fingerprint, making the authentication process faster and more convenient than ever before. And if you’re on the go, you can even use your phone or tablet to sign in by scanning a QR code or via Bluetooth!

Passkeys compared to passwords

Passkeys are the future of authentication, and for good reason! They’re incredibly easy to use and intuitive, eliminating the need for complicated password creation processes and the hassle of remembering them. Plus, they’re unique to each website or application, so you don’t have to worry about someone using your passkey to access other services. And unlike passwords, passkeys are resistant to phishing attempts, making them a much more secure option. Best of all, you can use your passkey across all your devices, so you never have to worry about forgetting your password again!

Note: the website or application you’re trying to sign into must support passkeys in order for them to work. The good news is that the industry is quickly adopting passkeys as an authentication mechanism, so more and more websites and applications are beginning to offer this feature.
Talk to your IT Department
Talk to your Vendors
Talk to your Users
Change is hard.
Jason Griffey
Director of Strategic Initiatives
NISO

jasongriffey.net
griffey@niso.org
griffey@gmail.com
@griffey@mastodon.social