okta

Keep off of my cookies!

Widespread adoption of multifactor and passwordless authentication is slowly diminishing the value of a stolen password to an attacker.

So what's the next best thing to a stolen password? A stolen *session cookie*.

Here are 8 ways to prevent account takeovers from stolen session cookies.

What are Session Cookies ?

Session cookies are small blocks of data stored in a user's browser after they sign-in to a web application. The cookie includes an identifier generated by the app that helps keep track of a signed-in user, ensuring they won't need to sign-in again until the session expires or the user logs out. If an attacker steals a session cookie and injects it into their browser, they can often access the same session as the legitimate user.

1 Endpoint protection

Endpoint protection software can protect user devices against malware that extracts session cookies from the user's browser. Bonus points if your EDR integrates with Okta to deny sign-ins from vulnerable devices!

Cookie-hungry malware

A number of malware families include modules that extract cookies from browser sessions running on an infected machine.

2 Strong authenticators

Authenticators that rely on "shared secret" factors such as SMS, email, or authenticator apps can be bypassed by phishing attacks that proxy legitimate requests via attacker infrastructure. Our suggestion? Protect access to high value accounts using strong authenticators such as WebAuthn, U2F keys and smart cards.

Phishing for cookies

Phishing sites are often configured as reverse proxy servers, relaying requests between a targeted user and an impersonated web application. If a user is tricked into signing in to the legitimate web application via one of these malicious sites, the attacker can access the user's credentials and the session token returned to the browser.

3 Device context

Authentication policies can be used to restrict access to applications to devices based on if they are registered with Okta FastPass, if they are fully managed, if they are assessed to have a strong security posture. All can play a role in thwarting cookie thieves!

Go Passwordless!

Okta FastPass uses a device-bound authenticator to enable sign-in to applications from any device without a password.

4 Define your perimeter

Where possible, block or perform step-up authentication on connections from rarely-used networks. With Okta Network Zones, access can easily be controlled by network location, ASN (Autonomous System Number), IP, and IP-Type (which identifies known anonymizing proxies).

Same, same

Reverse proxies used in phishing are also known as:
"Transparent HTTP proxies"
"In-line phishing proxies"
"MITM proxies"
"Adversary-in-the-middle proxies"

5 Behavior Detection

An attacker's sign-in behavior will very often differ from a user's typical behavior. Okta's Behavior Detection can be used to act (via step-up authentication) or alert (via System Log) when a user's sign in behavior deviates from a previous pattern of activity.

6 Security awareness

No matter how advanced the attacker's infrastructure, most cookie thieves rely on social engineering. Train users to identify signs of untrustworthy domains in the browser and the tricks attackers use to prompt user action.

Make it easy for users to report potential issues by configuring End User Notifications and Suspicious Activity Reporting.

Colour me unimpressed
Common phishing flags include:

Using domains with misspelled company names
Messages from executives asking you to act with urgency
Unexpected notification of packages or documents

7 Sensible sessions

Application session time-outs should, be fine-tuned based on the risk that unauthorized access to the SaaS application poses to the organization. We recommend expiring Okta sessions within two hours.

Continuous authentication refers to an ability to check for any changes in user context after a session is established (post-authentication). Okta is participating in efforts to standardize how risk signals are shared between identity providers and app providers.

8 Monitoring and Response

Application Logs often contain the first signs of cookie theft. Requests to Okta are logged in Okta System Log, which can be viewed in the admin console, streamed to security analytics tools or programmatically requested using the System Log API.

For more advice on common avenues for detection, check out this resource from Okta.