What is a refresh token, and why is losing one especially damaging?

Short answer: A refresh token is a long-lived credential used to silently obtain new access tokens without the user logging in again. It's what "remember me" relies on. Because it can keep minting fresh access indefinitely, a stolen refresh token can give an attacker durable access long after your session ends.

Access token vs. refresh token

- **Access token (session token):** short-lived, used on each request, expires in minutes or hours.
- **Refresh token:** long-lived, used only to request new access tokens. Sometimes valid for weeks or months.

A stolen access token eventually expires. A stolen refresh token can be used to generate new access tokens repeatedly — which turns a one-time theft into persistent access.

Why "remember me" is the trade-off

Staying signed in requires storing something durable on the device. That convenience is exactly what makes the stored token valuable to an attacker. Browser and app credential stores are standard, predictable locations, so automated tools go straight to them.

Reducing the damage

Revoking a refresh token invalidates the access it can mint — which is why "sign out of all devices" and token revocation matter after any suspected compromise. But revocation is a response *after* theft.

Cyber Crucible's approach is to prevent the read. The credential store is a protected location: a legitimate program overreaching there receives fake data or is denied, while an unknown or compromised one is rejected or suspended. The refresh token itself is never surrendered.

Revision #3
Created 2026-07-20 19:24:24 UTC by Dennis Underwood
Updated 2026-07-21 19:32:38 UTC by Dennis Underwood