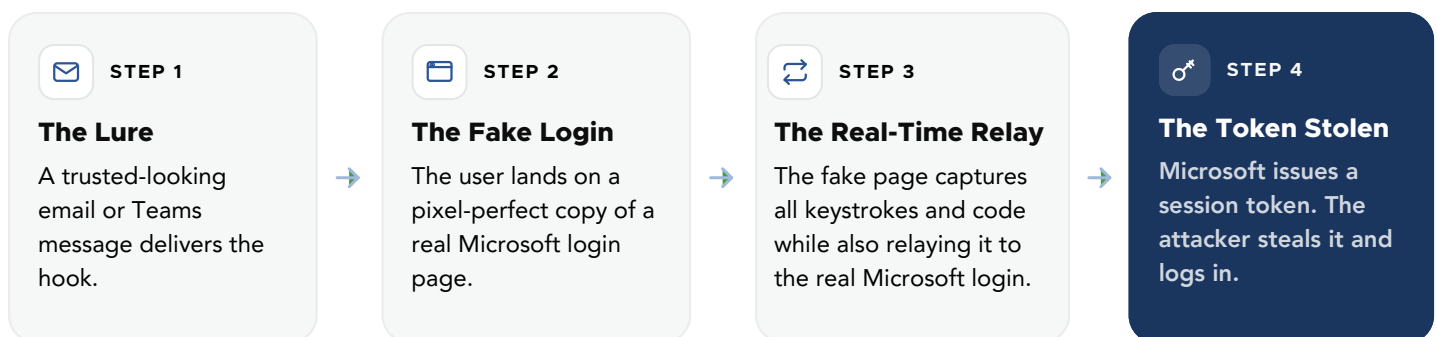


Attackers Are Bypassing MFA In Real Time.

The solution is **Phishing-Resistant MFA**.

How a modern attack slips past MFA:



How phishing-resistant MFA stops these attacks:

- Each credential is cryptographically bound to the real site's origin. A proxied login fails the binding, so the attacker **never receives a session token**.

\$130K+

average loss from a single business email compromise

- Wire fraud
- Vendor impersonation
- Email & identity theft
- Ransomware entry

Easy authentication methods:

Passkeys **MOST COMMON**

On your device or authenticator. Any platform — a tap or biometric.

Windows Hello **EASY WIN**

Built into Windows — face, fingerprint or PIN. No phone needed.

Certificate-Based **ENTERPRISE**

Organization-controlled PKI for regulated environments. Maximum control.

A baseline security requirement.



Now part of how we responsibly manage your environment. Clients below baseline may have the Cybersecurity Service Guarantee suspended for preventable incidents.

Book your MFA assessment

Talk to your vCIO about scope, timeline, and Entra ID P1 licensing.