

INFOGRAPHIC

Your Login Is the Target

Attackers no longer need to break in — they just need your login, or your permission to use it. Identity attacks are now the number one way ransomware and account takeovers begin. Here's how they work, and what stops them.



THE THREAT

How Attackers Steal Identities



Phishing for Credentials

A link by email, chat, text, or QR code leads to a fake sign-in page identical to the real one. Type your password, and they've got it.



Session Theft

Malware — from a bad download, fake extension, or hacked site — steals the “already logged in” token from your browser, bypassing passwords and MFA entirely.



MFA Fatigue Attacks

You're bombarded with approval prompts at odd hours, hoping you'll approve one just to stop the noise.



Fake App Permissions

A convincing app or extension asks to connect to your work account. Approve once, and it can quietly read your email, calendar, and files from then on.



Credential Reuse

One breach exposes a password — attackers then try it on every other service you use.

THE PATTERN

Why Identity Attacks Work So Well

The hardest attacks to catch are the ones that don't feel like attacks at all.



They Bypass Security Tools

Legitimate logins from stolen credentials don't trigger alerts — the system sees a valid user.



They Exploit Trust

A colleague's compromised account messaging you *is* your colleague, as far as your inbox knows.



They Compound Fast

One stolen identity opens the door to email, files, financial systems, and more.

THE RESPONSE

How to Spot and Stop an Identity Attack



Before you approve a prompt, enter a password, or grant an app access, pause and ask:

- 1 Did I trigger this?**

A legitimate login, reset, or MFA prompt matches something you just did. If nothing on your end matches, something's wrong.
- 2 Am I where I think I am?**

Check the address bar before typing your password. Fake login pages look identical — the URL is usually the only tell.
- 3 Does this app really need this access?**

An app asking to read all your emails or files is asking for a lot. Approve only what genuinely makes sense.
- 4 Would they really contact me this way?**

Real IT teams don't ask for passwords by phone. Real colleagues don't send urgent login links out of nowhere.

IF IN DOUBT

If Anything Feels Off

Fast reporting is the difference between a near-miss and a real breach.



Stop. Don't approve the prompt, enter the password, or grant the access.



Report it to your security team through your organization's reporting channel.



Acted already? Report it anyway. Speed limits how far an attacker can get.