Skillmine
Technology • Consulting • Services

Heat Attacks

When Everything Looks Completely Normal

You open a document link shared through a trusted platform.
The page asks you to sign in again — which feels routine.
You enter your credentials. Nothing looks suspicious.
But in the background, hidden browser scripts quietly capture your login details.
This is called a HEAT attack.

HEAT (Highly Evasive Adaptive Threat) is a modern attack technique that uses trusted websites, cloud services, and normal browser activity to steal credentials or session data.

There are:

- No infected files
- No malware alerts
- No obvious warning signs

The attack starts only after you interact with the page.

Where You May Encounter It

HEAT attacks often appear during daily work:

- Shared cloud documents
- Login prompts on familiar platforms
- Links from email, chat, or collaboration tools
- Trusted-looking websites

Routine actions become the entry point.

Pause Before You Sign In

Before entering credentials, ask:

- Was I expecting to sign in again?
- Does the website address look exactly correct?
- Did I reach this page through an official bookmark or portal?

A 5-second pause can prevent a major incident.

How to Stay Safe

- Use bookmarks or official portals for login
- Avoid signing in through unexpected links
- Verify access requests before proceeding
- Keep your browser and device updated
- Report suspicious pages to the IT/Security team

Key Message HEAT attacks do not look dangerous — that's why they work.

Trusted does not always mean safe.
Verify before you act.