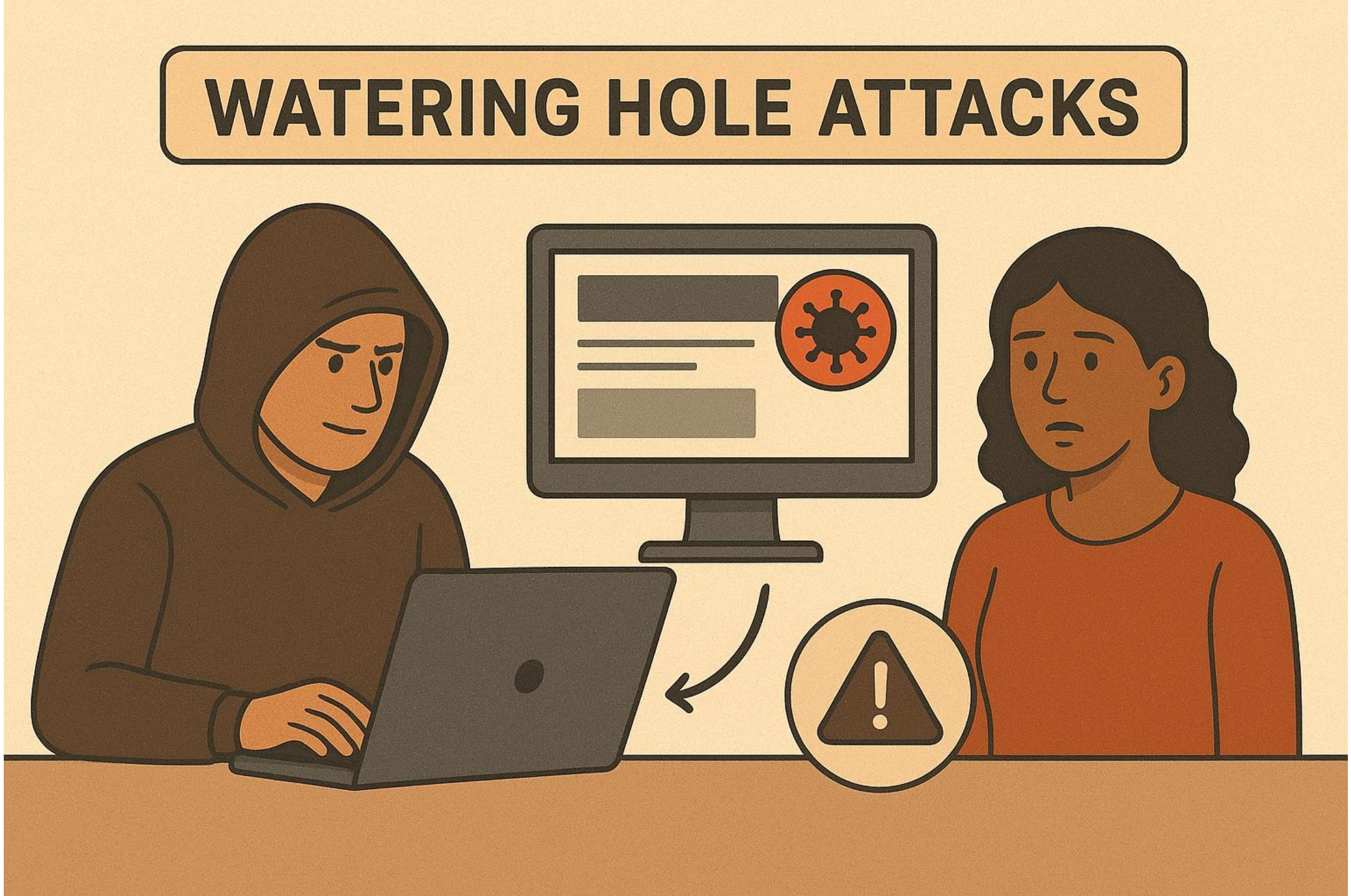
3. WATERING-HOLE ATTACKS

Attackers compromise a website that is frequently visited by a specific group, such as employees of a company or members of an industry. When visitors access the site, they may unknowingly download malware, have their browsers exploited, or get redirected to phishing pages, giving attackers a way to infiltrate their systems.


WATERING HOLE ATTACKS

Scenario: Hassan Visits an Industry Blog

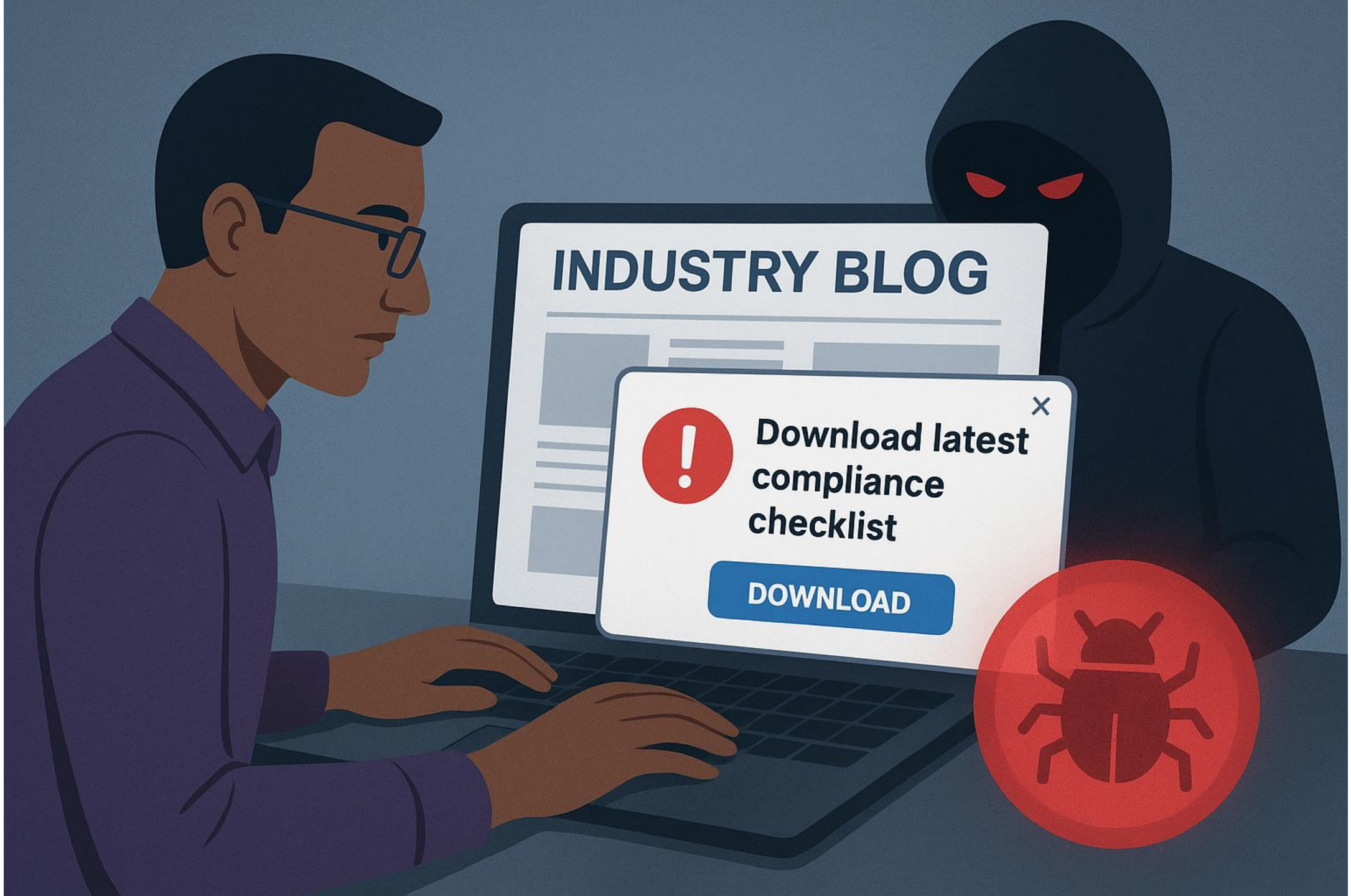
Hassan regularly reads a cybersecurity blog for updates.

Cybercriminals compromise the site and insert a fake pop-up: “Download latest compliance checklist.”

Hassan clicks it, unknowingly installing malware that can steal data or monitor his activities.

The attack leverages his trust in a familiar, frequently visited site.

Lesson: Always verify downloads from trusted sources. Keep antivirus and browser protections active to detect malicious content.


INDUSTRY BLOG
Download latest compliance checklist
DOWNLOAD

How Watering-Hole Attacks Work?

- Attackers study which sites employees visit
- Compromise those sites
- Inject malicious ads, pop-ups, redirects
- Wait for employees to visit naturally

Red Flags Hassan Should Notice

- Website suddenly behaves differently
- Unexpected downloads
- Pop-ups asking for credentials
- HTTPS missing on familiar pages

Prevention Tips

- Avoid downloads from external blogs
- Enable browser/endpoint protection
- Report suspicious site behavior
- Only download tools from official sources