

INFOGRAPHIC

Modern Phishing at a Glance

Attackers have moved beyond suspicious emails. Modern phishing has one goal — to get you to act before you think. Here's where it hides now, and how to spot it before you click, scan, or approve.



THE THREAT

Where Phishing Hides Now

**AI-Written Emails**

Grammatically perfect, personalized, and referencing real projects. They pass every "does it look suspicious" test.

**QR Codes (Quishing)**

Fake meeting invites, parking notices, or document portals that redirect to credential-stealing pages.

**Teams & Slack Messages**

Impersonated colleagues or automated bots sending malicious links inside trusted platforms.

**Fake Browser Pop-Ups (ClickFix)**

Social engineering that tricks you into pasting hidden commands into your device — installing malware yourself.

**SMS & WhatsApp Messages**

Package delivery updates, bank alerts, and HR reminders — all designed to catch you on the move.

**Where It All Leads**

Most of these end at a fake login page — a pixel-perfect copy of Microsoft, Google, or Okta built to capture your password and MFA code in one go.

THE PATTERN

What They All Have in Common

However it reaches you, every phishing attempt leans on the same three levers.

**Urgency**

"Action required within 24 hours." "Your access will be suspended." Pressure removes your time to think.

**Authority**

It appears to come from a CEO, IT, HR, or your bank — someone you're inclined to trust and obey.

**A Small Ask**

Just approve, scan, click, or paste. Just this once. The request always feels minor.

THE RESPONSE

The 5-Second Phishing Check



Before you click, scan, or approve, ask yourself:

- 1

Did I expect this?

Unexpected requests deserve extra scrutiny, no matter who they appear to be from.
- 2

Am I being pushed to act now?

Real urgency is rare. Pressure to act immediately, with no time to check, is a red flag.
- 3

Is there a link, QR code, or attachment?

Anything asking you to click, scan, or open a file is the payload — treat it with caution.
- 4

Would they really ask this way?

Consider whether this person or organization would genuinely make this request through this channel.
- 5

Can I verify another way first?

Confirm through a known phone number or a fresh message — never by replying to the request itself.

IF IN DOUBT

What to Do If You're Not Sure

-  **Don't click, scan, or approve.** If something feels off, stop before you act.
-  **Report it** to your security team through your organization's reporting channel.
-  **Already acted? Report it anyway.** Fast reporting limits the damage.