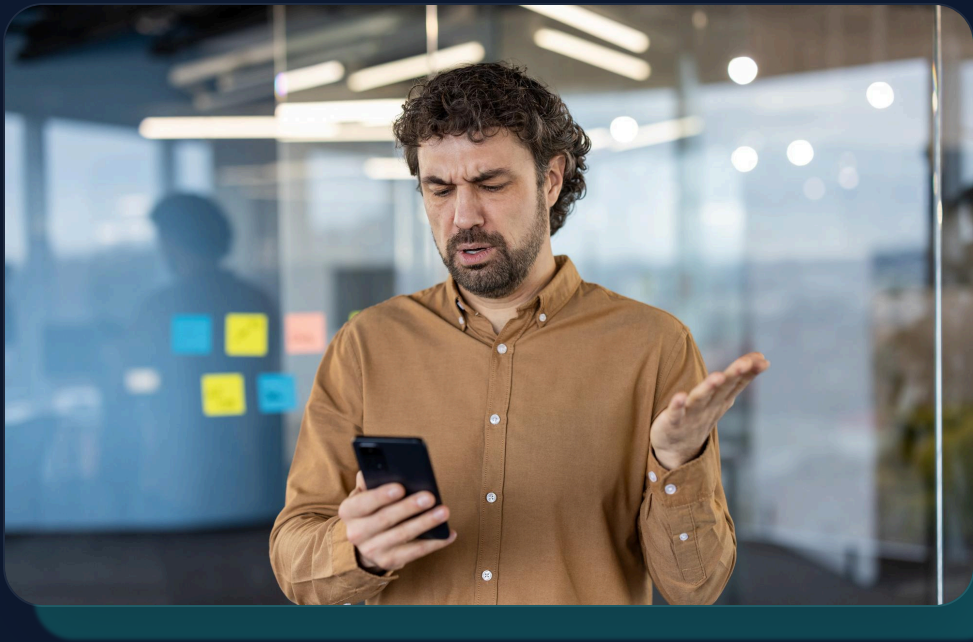


INFOGRAPHIC

How AI Scams Manipulate You

AI makes scams look, sound, and feel real. Attackers target your trust and emotions to make you act before you think.



THE THREATS

Modern AI-Enabled Scams



Cloned Voice Scams

EMOTIONS TARGETED: URGENCY, AUTHORITY

How it works: AI clones voices using short audio clips from calls, videos, or voicemails.

How attackers exploit it: They pressure you to act quickly without verifying the request.



Fake Support Scams

EMOTIONS TARGETED: FEAR, ANXIETY

How it works: AI powers fake chatbots, websites, or call center agents that seem legitimate.

How attackers exploit it: They make you believe something is wrong and push you to share information or grant access.



Deepfakes & Video Scams

EMOTIONS TARGETED: TRUST, FAMILIARITY

How it works: AI creates realistic videos or lip-syncs to impersonate people you know.

How attackers exploit it: They impersonate leaders, colleagues, or partners to request payments, data, or access.



AI-Written Phishing Emails

EMOTIONS TARGETED: CURIOSITY, HELPFULNESS

How it works: AI writes polished, personalized emails with real-looking context.

How attackers exploit it: They make messages feel routine so you click links, open attachments, or enter credentials.



Impersonation Attacks

EMOTIONS TARGETED: TRUST, AUTHORITY

How it works: AI creates fake profiles, identities, and histories.

How attackers exploit it: They build trust over time, then ask for data, payments, credentials, or access.

THE RESPONSE

Protect Yourself

1 Pause

Stop and think before you click, respond, approve, or share.

2 Verify

Use a trusted channel to confirm the person, request, or information.

3 Report

Report suspicious requests, messages, calls, or incidents to your security team.