threat level: human

The attack vector you can't patch.

Social Engineering Red Flags

The warning signs across the attacks that target people, and the one move that beats them.

60%
of breaches involve the human element
Verizon DBIR 2025

$2.77B
reported losses to business email compromise in 2024
FBI IC3 2024

21 sec
median time to click a phishing link
Verizon DBIR 2024

EMAIL AND MESSAGE LURES (PHISHING)

01 Urgency and pressure
Act now, this expires, do not tell anyone. Real requests survive a pause.

02 A sender that almost matches
Look-alike domains, a reply-to that differs, a display name that spoofs someone you know.

03 Verify your account links
A login page reached from a message, not from your own bookmark or typed address.

PHONE AND VOICE (VISHING)

04 A call that manufactures urgency
IT, a bank, or a manager who needs you to act before you have time to think.

05 Requests to read a code aloud
No legitimate caller ever needs the one-time code on your screen.

06 Pressure not to hang up and check
Discouraging a callback is the tell. Hang up and call a known number.

IMPERSONATION AND DEEPFAKES

07 A familiar face or voice pushing a transfer
A senior leader on video asking for an urgent, secret payment or login.

08 Audio and video that drift
Lip-sync that lags, odd blinking, flat lighting, or a voice slightly off.

09 Camera or mic problems on cue
Quality drops the moment you ask a hard or unexpected question.

AUTHENTICATION ATTACKS (MFA AND AITM)

10 An MFA prompt you did not start
Approving a push you did not request hands your live session to the attacker.

11 A login reached through a link
Adversary-in-the-middle pages relay your real login and steal the session token.

PAYMENT AND AUTHORITY

12 New payment details by message
Wire changes, gift cards, crypto, or new bank details that arrive in a message or call.

13 Requests to bypass process
Just this once, skip the second approver, keep it quiet.

14 Authority used to skip the check
A name, a title, or a logo deployed to make you waive the normal step.

THE ONE MOVE

The one move that beats most of them: stop and verify on a channel you chose. Call back on a known number, open the site from your own bookmark, confirm with the person directly. The attacker is counting on you not to pause.

Get a briefing like this every week, free.

threatlevelhuman.substack.com

youtube.com/@threatlevelhuman

Sources: Verizon Data Breach Investigations Report (2024, 2025); FBI IC3 2024 Annual Report. Figures as publicly reported.

How this is made: threat level: human is an AI-assisted production. A real person researches every story, checks each claim against primary sources, and is accountable for the facts.