Phishing Red Flags 2026 Edition

AI killed the old advice. Here's what actually works.

The Rules Changed

DEAD ADVICE (STOP TEACHING)

- Look for spelling errors
- Watch for generic greetings
- Grammar mistakes = phishing
- Obvious urgency language

WHAT STILL WORKS (TEACH THIS)

- Verify context — did they mention the RIGHT project details?
- Check reply-to address matches
- Confirm via known channel first

5 Flavors to Know

PHISHING	SPEAR	WHALING	VISHING	SMISHING
Mass email blasts	Targeted, researched	Executives, C-suite $3B/yr	Voice + AI clones	SMS + QR codes

SOC Analyst Investigation Checklist

EMAIL HEADERS

- ☐ SPF result
- ☐ DKIM signature
- ☐ DMARC verdict
- ☐ Actual send server

URL ANALYSIS

- ☐ Hover — real URL
- ☐ urlscan.io check
- ☐ Domain age <30d?
- ☐ Certificate mismatch

SIEM CORRELATION

- ☐ Impossible travel
- ☐ New OAuth grants
- ☐ MFA anomalies
- ☐ Odd geo logins

SOCIAL SIGNALS

- ☐ Urgency pressure
- ☐ Authority claims
- ☐ Money requests
- ☐ Reply-to mismatch

Defense in Depth — 5 Layers

1. **Email Gateway** — Proofpoint / Mimecast / Defender for O365
2. **DMARC Enforce** — Publish + enforce reject policy (not p=none)
3. **MFA Everywhere** — Authenticator apps or YubiKeys — NOT SMS
4. **Continuous Training** — Simulated phishing + immediate feedback
5. **Incident Response** — Isolate, reset creds, revoke OAuth, trace lateral