MAKE IT HARDER TO FOOL YOU.

Phishing isn't just a suspicious email anymore. Attackers impersonate coworkers, IT support, and trusted organizations through email, texts, calls, QR codes, and collaboration tools. Don't fall for the act. Pause, verify, and report.



IT-ISAC.ORG

THE FUNDAMENTALS

01
EXPECT MORE THAN EMAIL

Phishing comes through texts, calls, QR codes, fake websites, and workplace chat. A familiar name, logo, or communication channel doesn't guarantee legitimacy.

02
PAUSE & VERIFY

Question urgent requests for credentials, payments, sensitive information, or account changes. Verify through a trusted channel using known contact information.

03
DON'T FALL FOR THE "FIX"

Fake security alerts may tell you to download software, run commands, or sign in. Stop and contact your IT team directly.

04
REPORT IT FAST

Report suspicious activity through approved channels. If you clicked, entered credentials, or shared information, speak up immediately. Early reporting helps contain threats.

BEYOND THE FUNDAMENTALS

05
SECURE HIGH-RISK ASKS

Require independent verification for password resets, MFA changes, financial transactions, and privileged access. Strengthen help desk procedures against impersonation.

06
PROTECT IDENTITIES & SESSIONS

Deploy phishing-resistant MFA, monitor suspicious sign-ins and session activity. Be ready to revoke compromised sessions and credentials quickly.

07
TURN REPORTS INTO INTEL

Make phishing easy to report. Analyze suspicious messages, links, and impersonation attempts to identify patterns, block threats, alert employees, and share actionable intelligence.

08
TEST YOUR RESPONSE

Run realistic phishing and impersonation exercises. Test how quickly teams verify requests, escalate reports, and contain compromised accounts.

PRO TIPS

- QR codes can phish too. Make sure to check the destination before scanning or sharing information.
- Don't trust the voice alone. AI can impersonate familiar voices. Verify unusual requests independently.

IT ISAC
CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING