Phishing Prevention in 2025

28-March-25

Why Phishing is Everyone’s Problem

- What is phishing?
  Phishing is a cyberattack where criminals impersonate trusted entities (like companies or colleagues) to trick victims into revealing sensitive data—often through fake links, fraudulent emails, or malicious attachments designed to steal login credentials, payments, or personal information.
- 91% of cyberattacks start with phishing.
- This session will show you real attack examples and simple defenses—tailored to your daily work

Why You’re A Target

Department-Specific Risks

Team	What Hackers Want	How they Attack
Marketing	Vendor payments, ad accounts	Fake invoice PDFs with malware
IT	Network access	"Urgent patch" credential scams
Operations	Supply chain data	Fake shipping links
Sales	Client contracts	Malware disguised as lead attachments

Sneakiest Attacks in 2025

What’s New in Phishing

- AI Phishing: Emails mimicking your CEO’s writing style.
- QR Code Scams: "Scan to approve the budget" → Fake login.
- Chatbot Traps: "Hi [Your Name], your VPN access expired."

Spot the Red Flags

‘Test your eye’

1. Urgency: "Action required in 1 hour!" ❌
2. Mismatched Links: "company.com" → company-login.xyz ❌
3. Strange Attachments: "Contract_2025.pdf.exe" ❌

Interactive Quiz:
"Which email is real?"
A. "Marketing report (click here)" → marketing.yourcompany.com ✅
B. "Marketing report (click here)" → marketing-yourcompany.xyz ❌

"Let’s break down real examples..."

Urogeddomanm <forged@domain.com>
April 23, 2024, 10:45 AM

Subject: **Marketing Department Update**

Hello Marketing Team,

I've attached a document with the latest project plans and deadlines. Please review it as soon as possible.

Visit our updated website at http://intranet.example.com for important news and resources.

Quarterly_Report.exe
532 KB

30-Second Defense

1. Pause:

- Hover over links. Check sender emails ("security@company.com" vs. "security@company-support.net").

2. Verify:

- Call the sender (use your contacts, not the email’s number).

3. Report:

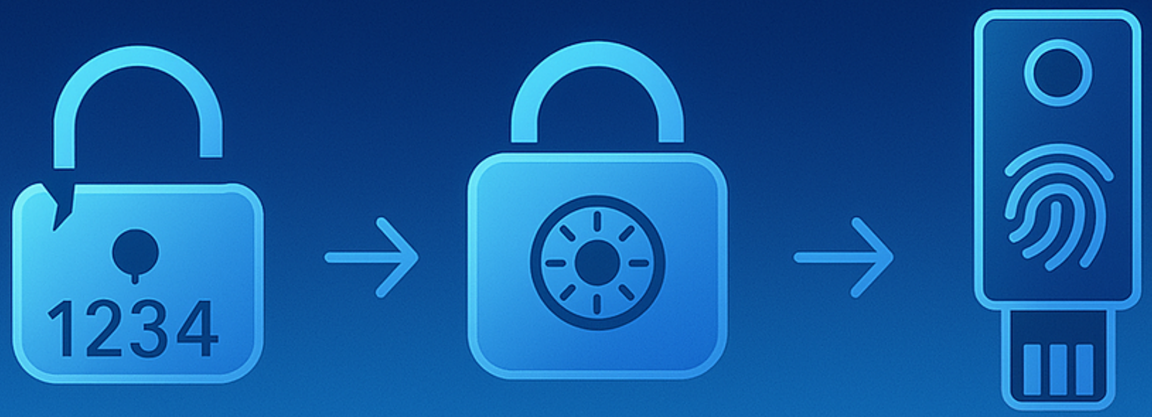
- Use the "Report Phishing" button or forward to IT.

Quote:
"The most secure teams report 10x more phishing attempts than others."

2025 Security Upgrades

Recommended for all departments

- FIDO2 Keys: No more SMS codes ("Unhackable logins").
- Password Managers: "One unique password per site”.
- DMARC: Stops email spoofing ("IT can set this up").



Our Phishing Test Results

Key Statistics

- 66.7% clicked phishing links (Marketing: 72%).
- 16.7% entered credentials (IT: 9%, Sales: 21%).

Takeaway:
"Even cautious teams can improve. Reporting is the first step."

Report —> Reward

New Policy

1. Forward phishing to IT (even if unsure).
2. Win a coffee card for first reports.
3. 3. Earn a "Phishing Hunter" badge in Slack after the first 3 accurate phishing reports.

Remember: Security Starts With YOU

- Spot the fake: Scrutinize links and senders.
- Never share secrets: Emails asking for passwords = red flag.
- Lock it down: Password managers = no repeats, no regrets.
- Trust, but confirm: A quick call can stop a scam.

Thank you for phishing with us!