

Phishing Awareness Training

Stay Safe. Stay Alert. Stay Aware.



What is Phishing?

- ▶ Phishing is a cyber attack that tricks you into giving up sensitive information by pretending to be a trustworthy source.
- ▶ Example: “You’ve won a free iPhone! Click here to claim.”

Why is Phishing Dangerous?

- ▶ • 91% of cyber attacks start with a phishing email.
- ▶ • Can lead to identity theft, financial loss, or system compromise.
- ▶ • Both individuals and companies are targets.

How to Recognize Phishing Emails

- ▶  **Red Flags:**
- ▶ - Urgent or threatening language: “Act now or your account will be locked.”
- ▶ - Suspicious sender address: support@paypall-secure.com
- ▶ - Spelling and grammar mistakes.
- ▶ - Unfamiliar links or attachments.
- ▶  Hover over links before clicking – check the actual URL.

Spotting Fake Websites

- ▶ • URL tricks: www.faceboook.com,
<https://bank.secure-login.com>
- ▶ • No HTTPS or invalid certificate warning.
- ▶ • Visual copying of legitimate sites.
- ▶ • Always type the website URL manually or use bookmarks.

Social Engineering Tactics

- ▶ • Impersonation: Pretending to be a friend, boss, or IT support.
- ▶ • Emotional Manipulation: Fear, urgency, curiosity.
- ▶ • Pretexting: Creating a fake situation to gain trust.
- ▶ Real Case: "CEO fraud" where attackers spoof a CEO's email to instruct employees to transfer money.

Best Practices to Avoid Phishing

- ▶ • Do not click on suspicious links or open unexpected attachments.
- ▶ • Use multi-factor authentication (MFA).
- ▶ • Regularly update your passwords and don't reuse them.
- ▶ • Verify directly with the sender via phone or known contacts.
- ▶ • Keep your devices and antivirus software updated.

Real-World Examples

- ▶ • **Target (2013):** 110 million customers' data stolen due to phishing email to a third-party vendor.
- ▶ • **Google & Facebook (2013-2015):** Lost over \$100M to fake invoices sent by a hacker posing as a vendor.

Quiz Time!

- ▶ **Q1: Which of the following is a phishing indicator?**
- ▶ A. Email from admin@google.com
- ▶ B. “Your account is suspended! Click now!” ✓
- ▶ C. Correct spelling and professional tone
- ▶ D. None of the above

- ▶ **Q2: What should you do if you suspect a phishing email?**
- ▶ A. Delete it
- ▶ B. Forward it to IT/Security
- ▶ C. Click the link to test
- ▶ D. Both A & B ✓

What to Do If You Fall for It

- ▶ • Disconnect from the internet immediately.
- ▶ • Change all compromised passwords.
- ▶ • Report to your IT/Security department or CERT-In (India).
- ▶ • Monitor accounts for suspicious activity.

Key Takeaways

- ▶ • Phishing relies on human error — awareness is the best defense.
- ▶ • Always pause, verify, and think before clicking.
- ▶ • Stay updated on current phishing trends.

Questions & Discussion

- ▶ Open the floor for real experiences or questions.
- ▶ Optional: Live demo of a phishing simulation or fake website inspection.

Bonus Tip for Daily Practice

- ▶ Use tools like:
- ▶ • Google Phishing Quiz
(<https://phishingquiz.withgoogle.com>)
- ▶ • HaveIBeenPwned (<https://haveibeenpwned.com>)