Phishing Awareness Training

Learn how to identify and avoid phishing attacks.

Created by: *Kabir Rathod*
Code Alpha Internship -Task 2

What is Phishing?

Definition:

Phishing is a cyber attack technique where attackers trick users into revealing sensitive information like passwords, credit card numbers, or OTPs.

Goal:

Gain access to personal or company accounts by pretending to be a trusted source.

Example:
You receive an email claiming to be from your bank asking to “verify your account.”

Common Types of Phishing

- **Email Phishing** - Fake emails pretending to be from trusted organizations.
- **Spear Phishing** - Targeted emails toward specific individuals.
- **Smishing** - Phishing through **SMS messages**.
- **Vishing** - Voice phishing via **phone calls**.
- **Clone Phishing** - Duplicate of a real email with malicious links.

How to Recognize Phishing Emails

⚠️ **Red Flags to Look For:**

- Suspicious or misspelled sender address
- Poor spelling/grammar
- Urgent tone (“Your account will be locked!”)
- Links that look slightly different (paypa1.com instead of paypal.com)
- Unexpected attachments

Phishing Example

Fake Website Example:

Real: https://www.google.com
Fake: https://www.go0gle.com

Always check:

The domain name (not just the logo!)
HTTPS lock icon
URL spelling

Social Engineering Tactics

Phishing relies on **manipulating human behavior**.

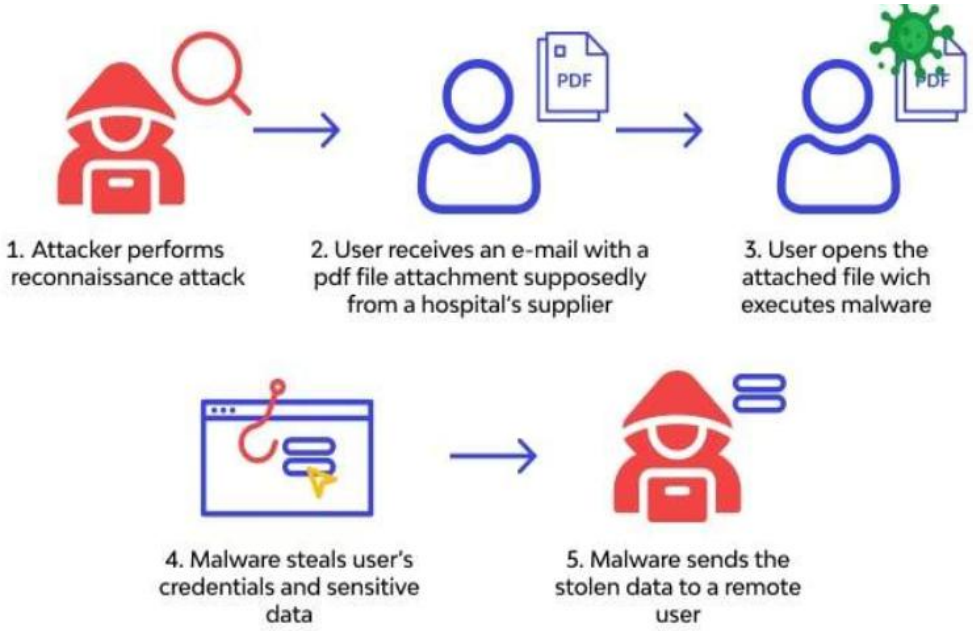
Common tactics:

Pretexting: Fabricating a believable story (ex. fake HR message)

Baiting: Offering something free to lure victims

Impersonation: Pretending to be a trusted person

Fear or urgency: “Immediate action required!”



Real-World Examples

- **Fake Bank Alerts** — Your account is blocked. Click here to verify.
- **Job Offer Scams** — Fake recruiters requesting personal details.
- **Delivery Notifications** — Your parcel is held. Pay ₹50 to release.
- **Password Reset Emails** — Sent from lookalike domains.

From: authenticationmail@trust.ameribank7.com
To: johnsmith@email.com
Subject: **A new login to your bank account**

Bank of America

Dear account holder,

There has been a recent login to your bank account from a new divice:

IP address: 192.168.0.1

Location: Miami, Florida

4 new transactions have been made with this account since your last login.

If this was not you, please reset your password immediately with this link:

https://trust.ameribank7.com/reset-password

Thank you,

Bank America

How to Protect Yourself

Best Practices:

- Verify the sender before responding.
- Do not share OTPs or passwords.
- Use **multi-factor authentication (MFA)**.
- Keep your system and antivirus updated.
- Report suspicious emails to IT/security teams.

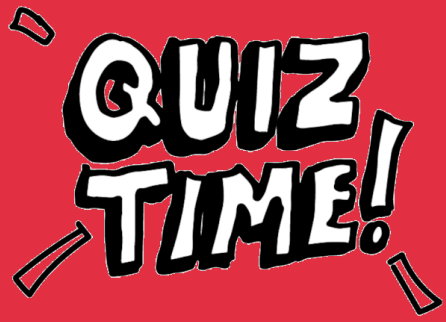
Do’s and Don’ts

Do’s

- Check URLs carefully
- Report suspicious messages
- Keep your browser and software updated
- Use strong, unique passwords

Don’ts

- Don’t click unknown links
- Don’t download random attachments
- Don’t enter credentials on unknown sites
- Don’t trust urgent scare tactics



Quiz Time

Quiz Link : https://forms.gle/5j8rPtAde9V3rde19

No login required — responses are anonymous.

Conclusion

🎯 **Key Takeaways:**

Think before you click.
Always verify the source.
Awareness is your best defense.

🔐 Stay smart. Stay safe.