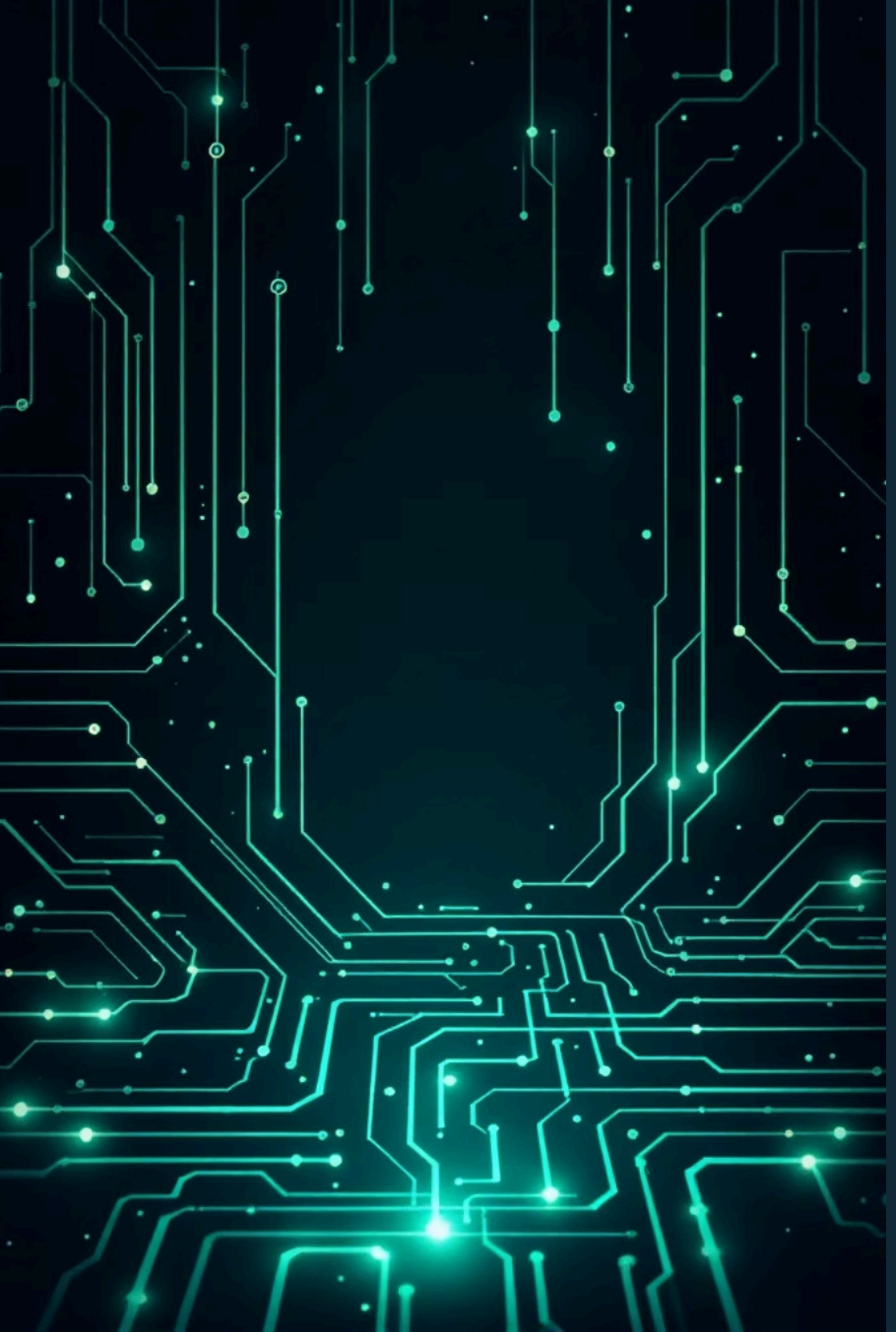
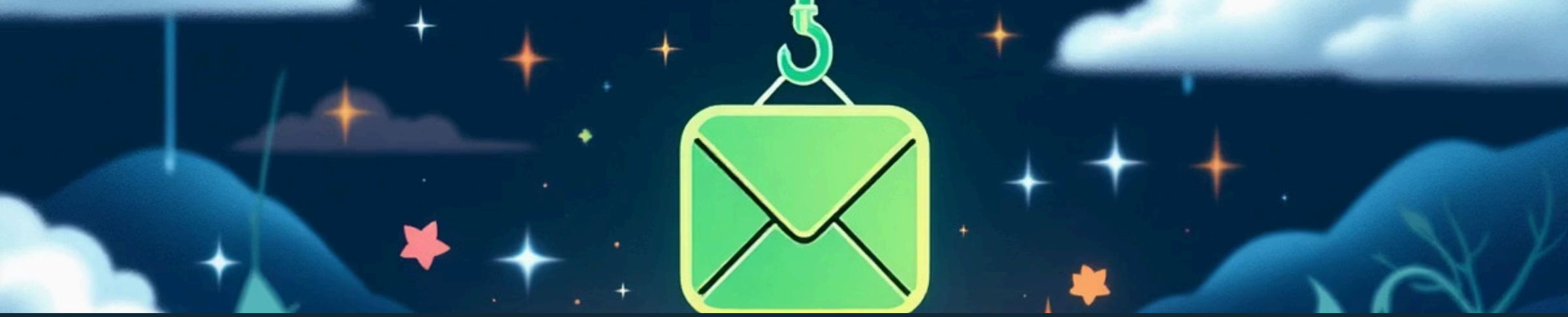


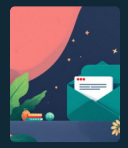
Phishing Awareness Training

Learn how phishing works, how to spot it, and simple steps to stay safe online.



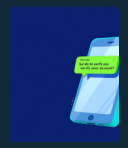
What is Phishing?

Phishing is a type of online scam where attackers pretend to be someone you trust (like a bank or coworker) to trick you into revealing passwords, personal data, or money. It often arrives as email, text, phone calls, or fake websites.



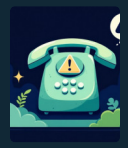
Email Phishing

Most common. Fake emails urging you to click links or open attachments.



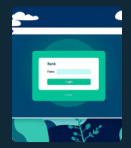
SMS (Smishing)

Text messages that prompt urgent actions or ask for codes.



Voice (Vishing)

Phone calls pretending to be support, banks, or government agencies.



Fake Websites

Lookalike sites made to steal your credentials or payment info.

How Phishing Attacks Work — Step by Step

Craft Message

Deliver Message

Click Link / Open

Data Stolen / Malware

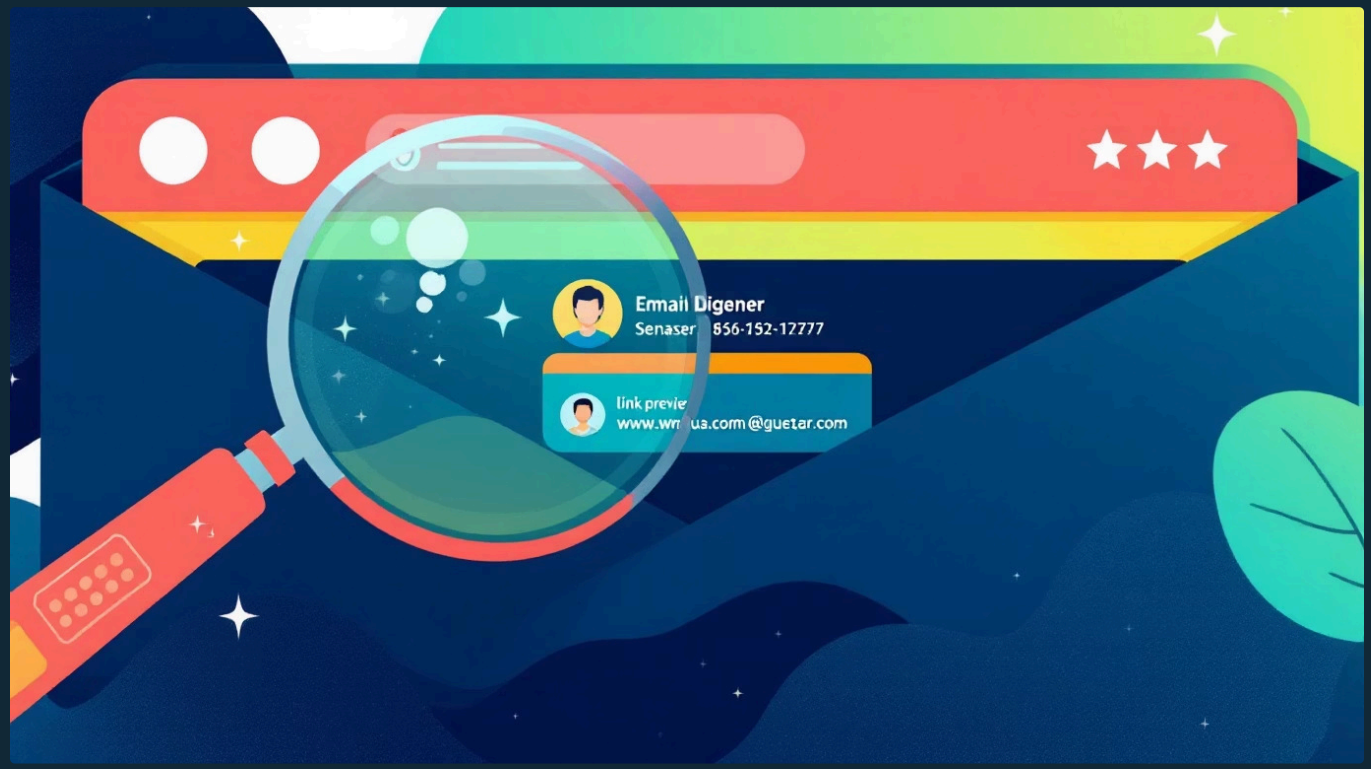
Attackers create convincing messages, deliver them, tempt you to act, then collect data or install malware. Small mistakes can lead to big breaches.

Example: A Phishing Message

Subject: Urgent — Verify Your Account Now

From: support@bank-secure.com (looks real but slightly off)

Message: "Your account will be locked. Click here to verify." — Link leads to a fake login page.



How to Identify Phishing

- Check the sender's address (look for small misspellings).
- Hover over links to preview the real URL before clicking.
- Watch for urgent language, threats, or too-good-to-be-true offers.
- Look for spelling/grammar mistakes and odd greetings.
- Never give passwords, codes, or payments in response to unsolicited messages.

Prevention: Simple Daily Habits

Pause Before You Click

Think: Is this expected? If unsure, don't click links or open attachments.

Verify Requests

Contact the company or person using a known phone number or website—not the info in the message.

Use Strong Authentication

Enable multi-factor authentication (MFA) on important accounts.

Keep Software Updated

Install updates and use up-to-date antivirus and browser protections.

What to Do If You Think You Clicked a Phish

- Disconnect from the internet and change your passwords from a safe device.
- Enable MFA and review recent account activity for unauthorized access.
- Report the message to your IT/security team or the service provider.
- Run an antivirus/malware scan and monitor financial accounts closely.

Quick action reduces harm — act immediately and seek help.

Key Takeaways

Stay Skeptical

Verify unexpected requests — trust but verify.

Protect Accounts

Use MFA and strong, unique passwords.

Report Quickly

Report suspected phishing to reduce risk for everyone.

Prepared by

Rugwed Salunke

Email: salunkerugwed@gmail.com

Contact: 705-805-6176

This training gives basic steps to recognize phishing and reduce risk. For organizational policy or incident reporting, contact your IT/security team.