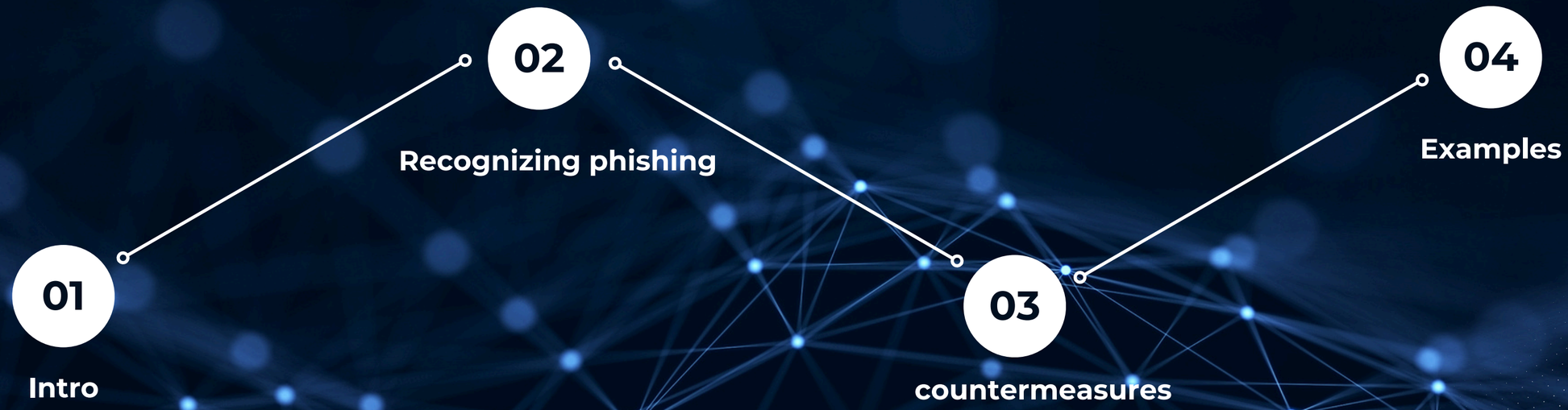
PHISHING AWARENESS

EXECUTIVE SUMMARY



Never click, never trust, always verify

INTRO

Phishing is a type of cyberattack where criminals pretend to be trusted people or organizations (like banks, companies, or friends) to trick you into giving them sensitive information such as passwords, bank details, or personal data.

happens through:

- Emails that look official but are fake
- Text messages with malicious links
- Fake websites that copy real ones

TYPES OF PHISHING

EMAIL & ONLINE-BASED

EMAIL PHISHING – GENERIC FAKE EMAILS.

SPEAR PHISHING – TARGETED AT SPECIFIC INDIVIDUALS.

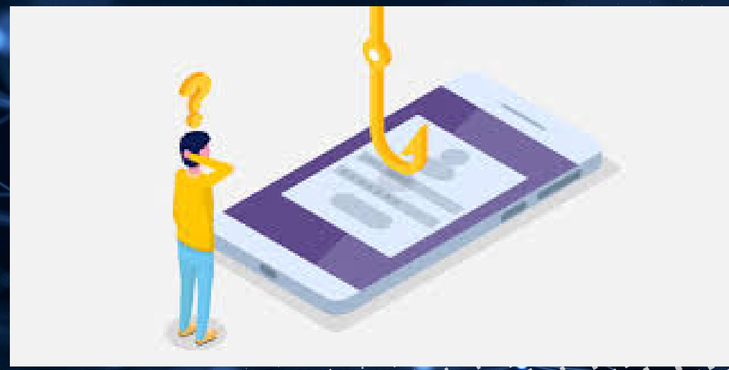
WHALING (CEO FRAUD) – TARGETS TOP EXECUTIVES.

CLONE PHISHING – USES A COPIED LEGITIMATE EMAIL.

CREDENTIAL HARVESTING PHISHING – FAKE LOGIN FORMS/WEBSITES.

MALWARE-BASED PHISHING – ATTACHMENTS/LINKS WITH MALWARE.

PHARMING – REDIRECTS USERS TO FAKE WEBSITES.



PHONE & MESSAGE-BASED

SMISHING – PHISHING VIA SMS/TEXT MESSAGES.

VISHING – PHISHING VIA VOICE/PHONE CALLS.

QRISHING (QR CODE PHISHING) – MALICIOUS QR CODES LEADING TO FAKE SITES.

TYPES OF PHISHING

SOCIAL MEDIA & OTHER PLATFORMS

ANGLER PHISHING – FAKE CUSTOMER SUPPORT/SOCIAL MEDIA ACCOUNTS.

SOCIAL MEDIA PHISHING – FAKE LOGIN PAGES ON PLATFORMS (FACEBOOK, INSTAGRAM, ETC.).

SEARCH ENGINE PHISHING – FAKE WEBSITES PROMOTED IN SEARCH RESULTS.

EVIL TWIN PHISHING – FAKE WI-FI HOTSPOTS CAPTURING DATA.

ADVANCED/MODERN TECHNIQUES

BUSINESS EMAIL COMPROMISE (BEC) – HACKED/SPOOFED COMPANY EMAILS.

MAN-IN-THE-MIDDLE (MITM) PHISHING – INTERCEPTS COMMUNICATION BETWEEN USER AND SERVICE.

POP-UP PHISHING – MALICIOUS POP-UP WINDOWS ASKING FOR CREDENTIALS.

TABNABBING – INACTIVE TABS REDIRECTING TO FAKE LOGIN PAGES.

WATERING HOLE ATTACK – INFECTING WEBSITES FREQUENTLY VISITED BY A TARGET GROUP.

PHISHING-AS-A-SERVICE (PHAAS) – READY-MADE PHISHING KITS SOLD TO ATTACKERS.

RECOGNIZING PHISHING EMAILS

BY GRAMMAR AND SPELLING

emails often contain errors in grammar and spelling, unlike legitimate business communications

BY GENERIC GREETINGS

They may use generic greetings like "Dear Customer" instead of your name.

BY SUSPICIOUS SENDER ADDRESS

Check the sender's email address for typos, unusual domains, or public email addresses like Gmail instead of a company's official domain.

BY URGENCY AND THREATS

Phishing emails often create a sense of urgency or threaten account suspension if you don't act immediately.

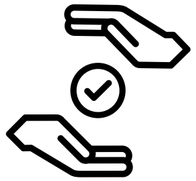
BY REQUESTS FOR PERSONAL INFORMATION

Be wary of emails asking for sensitive information like passwords, credit card details, or social security numbers

BY UNUSUAL LINKS OR ATTACHMENTS

Hover over links to check the destination URL. If it looks suspicious or doesn't match the email's context, don't click it. Avoid opening attachments from unknown senders

COUNTERMEASURES FOR PHISHING



Protect your computer by using security software

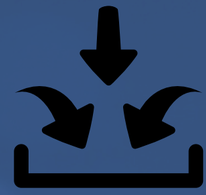
Set the software to update automatically so it will deal with any new security threats.

Protect your cell phone by setting software to update automatically

These updates could give you critical protection against security threats.

Protect your accounts by using multi-factor authentication

Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication.



Protect your data by backing it up

Back up the data on your computer to an external hard drive or in the cloud. Back up the data on your phone, too.

REAL-WORLD EXAMPLE OF A PHISHING EMAIL:

Imagine you saw this in your inbox. At first glance, this email looks real, but it's not. Scammers who send emails like this one are hoping you won't notice it's a fake.

Here are signs that this email is a scam

- The email has a generic greeting.
- The email says your account is on hold because of a billing problem.
- The email invites you to click on a link to update your payment details.

While real companies might communicate with you by email, legitimate companies won't email or text with a link to update your payment information. Phishing emails can often have real consequences for people who give scammers their information, including identity theft. And they might harm the reputation of the companies they're spoofing.

SOME SOCIAL ENGINEERING TACTICS USED BY THE ATTACKER

Impersonation

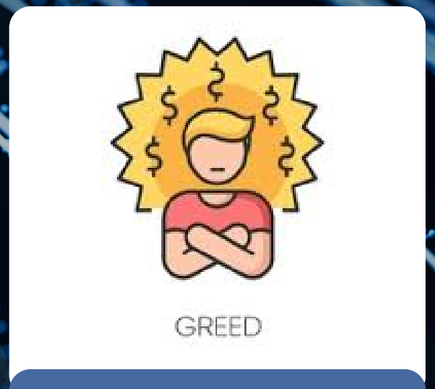
- Pretending to be a trusted entity (bank, company, government, colleague, or even a friend)
- Example: An attacker posing as IT support asking for your login to “fix an issue.”

Urgency and Fear

- Creating a sense of urgency so the victim acts quickly without thinking.
- Example: “Your account will be suspended in 24 hours unless you verify your identity.”

Authority Exploitation

- People are more likely to follow instructions from someone who appears to be in power.
- Example: A phishing email appearing to come from a CEO asking for immediate fund transfer



Greed or Curiosity

- Exploiting curiosity or desire for rewards.
- Example: “You have won a prize—click here to claim it.”

Reciprocity (Fake Help)

- Offering fake “help” in exchange for information.
- Example: “We noticed unusual activity on your account, verify here to secure it.”

PRACTICES AND TIPS TO AVOID FALLING VICTIM TO PHISHING ATTACKS

Security Tools

- Install anti-phishing filters (many browsers and email services have them).
- Use antivirus/antimalware software with real-time protection.
- Enable spam filters in your email account.
- use private networks like VPN

Account Protection

- Use strong, unique passwords for different accounts.
- Enable multi-factor authentication (MFA/2FA) wherever possible – this adds a strong layer of protection even if your password is compromised.
- Update software and browsers regularly – security patches close vulnerabilities attackers may exploit.

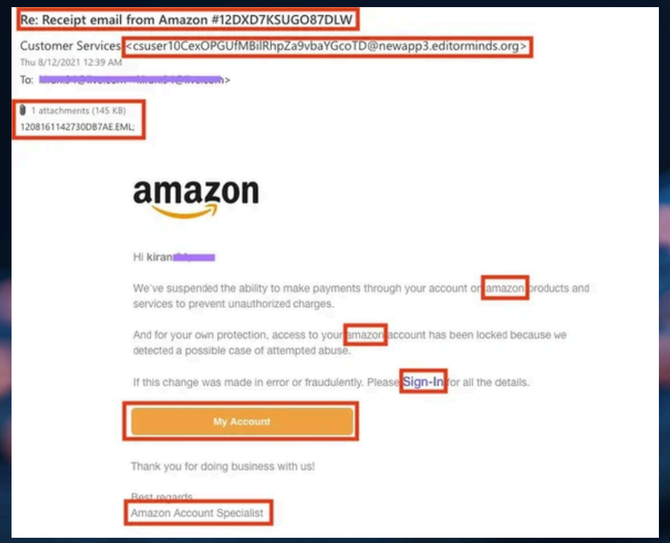
Behavioral Habits

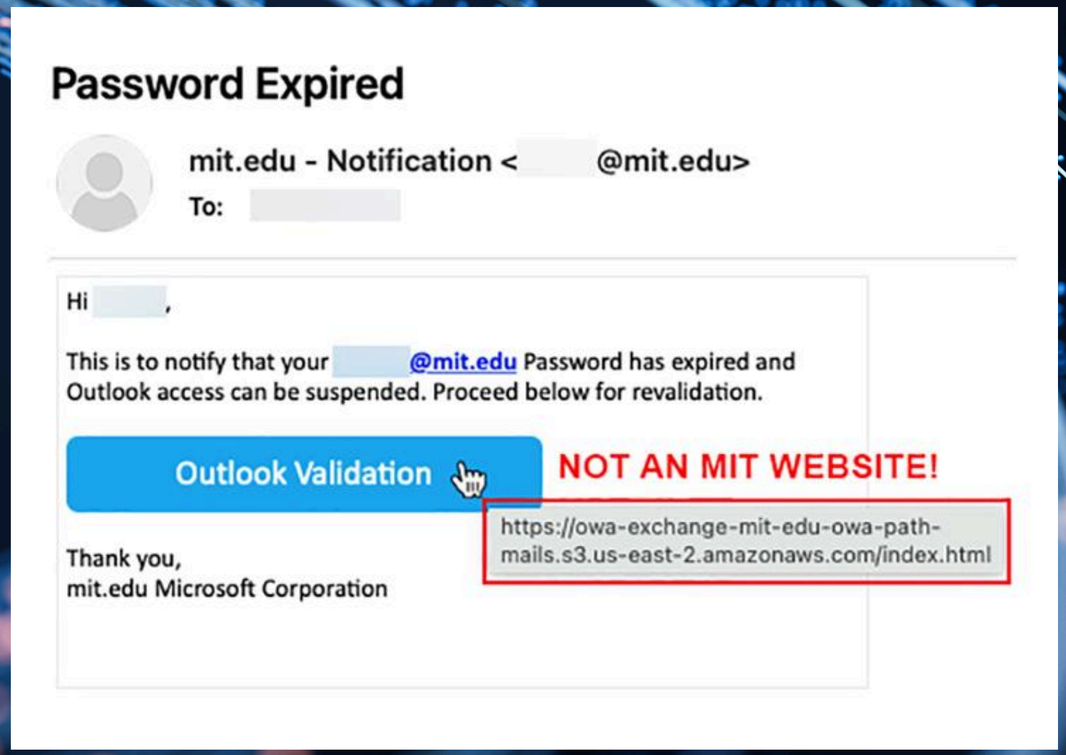
- Slow down before reacting – attackers rely on urgency.
- Verify requests through a second channel – if your “bank” emails you, call them directly.
- Educate yourself and others – awareness is the best defense.

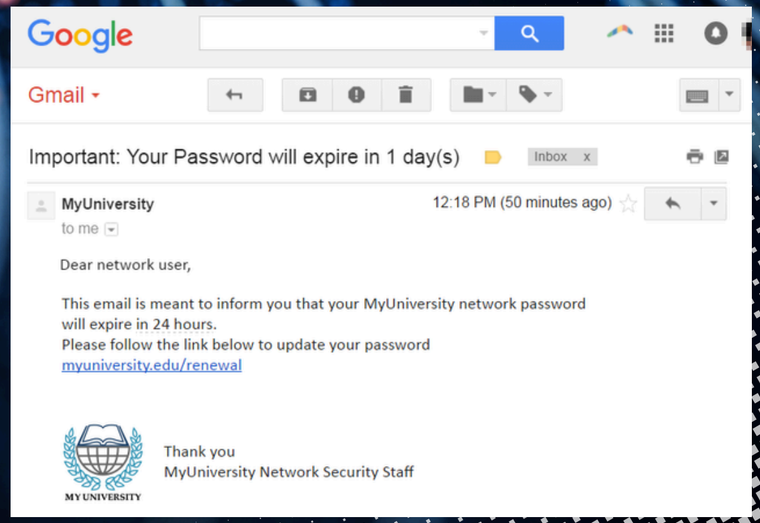
General Awareness

- Be skeptical of unsolicited emails, texts, or calls, especially those asking for personal information, money, or urgent action.
- Check for urgency or fear tactics ("Your account will be suspended," "Immediate action required") — these are common red flags.

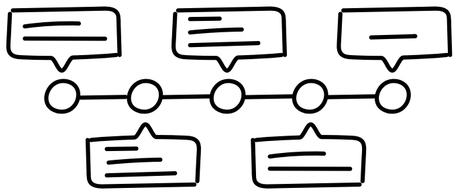
real world Examples for phishing emails and websites



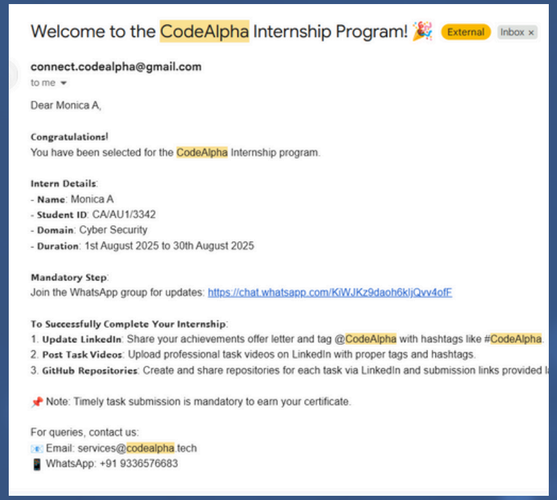




Quiz



which type of network will you use for safety measures



check whether it is phishing mail

how many types of phishing totaly