

PHISHING AWARENESS TRAINING

Presentation by:DHARSHINI K

WHAT IS PHISHING ?

PHISHING ATTACK!

Phishing is a type of cyber attack in which attackers pretend to be trusted organizations or individuals to trick users into revealing sensitive information such as passwords, OTPs, or bank details through fake emails, messages, or

websites.

Secure Your Information



LOGIN

Passwd

Sign In



WHY PHISHING IS DANGEROUS?

Phishing is dangerous because it deceives people into revealing personal and financial information.

Attackers use fake emails or messages that appear trustworthy.

This can result in identity theft, financial loss, and account hacking.





Email Phishing

- Fake Emails
- Ask for Passwords



Smishing

- SMS Messages
- Fake Links



Spear Phishing

- Targeted Attacks
- Uses Personal Info



Vishing



- Phone Calls
- Pretend to be Bank/Official



Clone Phishing

- Copy of Real Email
- Malicious Attachment



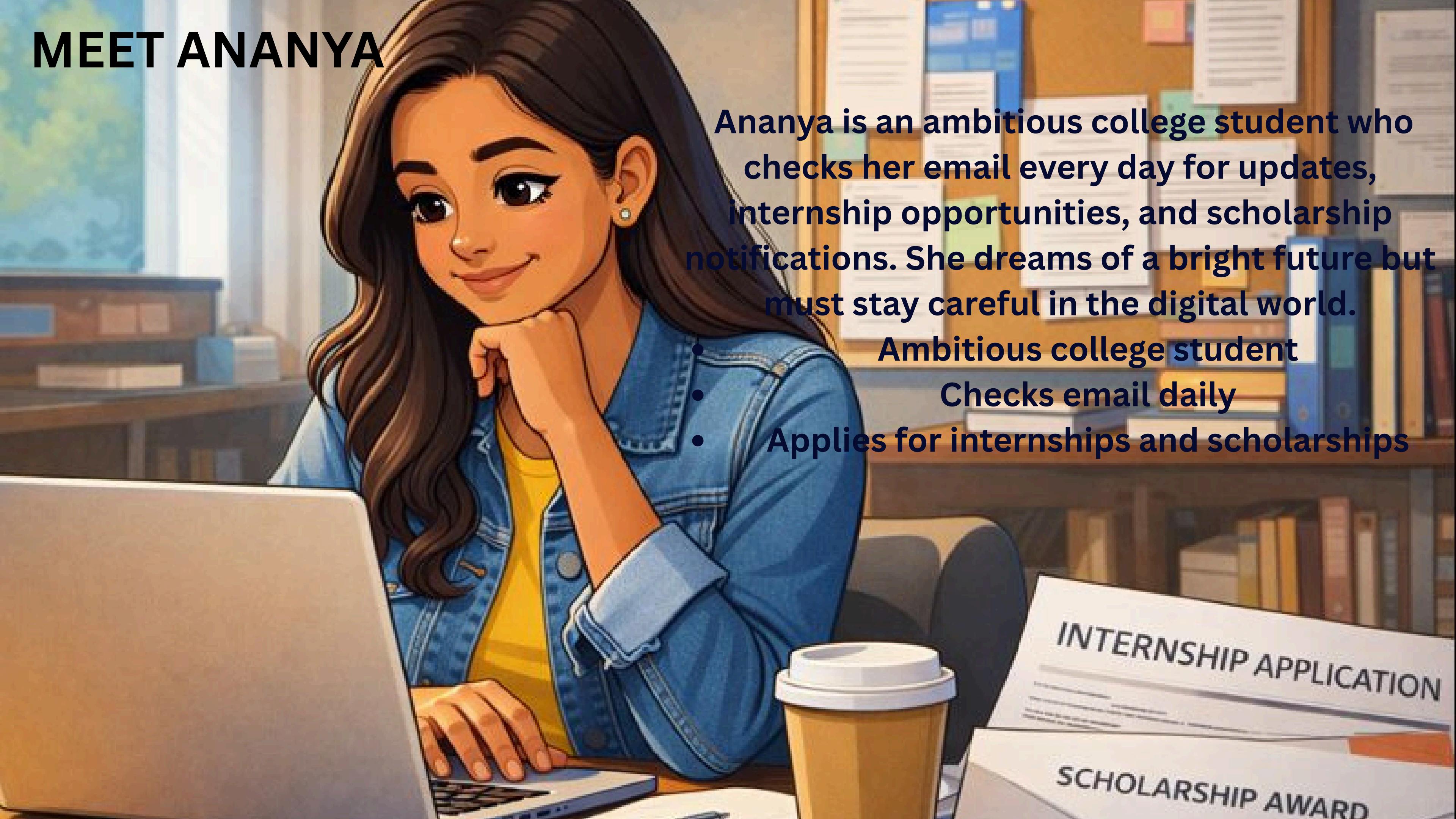
Website Phishing

- Fake Login Pages
- Steals Credentials

COMMON TYPES OF PHISHING:

- **Email phishing** – Fake emails pretending to be from banks, companies, or colleges, asking for passwords or personal details.
- **Spear phishing** – Targeted phishing aimed at a specific person or organization using personal information.
- **Smishing** – Phishing through SMS/text messages with fake links or urgent alerts.
- **Vishing** – Phishing through phone calls, where attackers pretend to be officials or customer care.
- **Clone phishing** – A real email is copied, but the link or attachment is replaced with a malicious one.
- **Website phishing** – Fake websites that look real and steal login details.

MEET ANANYA



Ananya is an ambitious college student who checks her email every day for updates, internship opportunities, and scholarship notifications. She dreams of a bright future but must stay careful in the digital world.

Ambitious college student

Checks email daily

Applies for internships and scholarships

INTERNSHIP APPLICATION

SCHOLARSHIP AWARD

A Suspicious Email

One morning, Ananya receives an email claiming she's won a scholarship she never applied for. The email asks her to click a link and enter personal details to claim the prize.

- Looks genuine at first glance.
- Urgent tone: **"Claim Your Scholarship Now!"**
- Requests sensitive information



Story Continues

A Suspicious Email

One morning, Ananya receives an email claiming she's won a scholarship she never applied for. The email asks her to click a link and enter personal details to claim the prize.

- Looks genuine at first glance
 - Urgent tone pressures her to act quickly
 - Requests sensitive information
- Ananya feels excited but also a little unsure...

Ananya Thinks Before Clicking

**Instead of clicking the link immediately,
Ananya pauses and thinks.**

She checks the sender's email address and notices small spelling mistakes and an unknown domain.

She does not click the link

She avoids sharing personal details

She realizes it could be a phishing email

Her careful thinking helps her stay safe online ✓

Ananya's story teaches us that being alert online is essential for safety. Phishing emails often look real and create urgency, but a moment of careful checking can prevent serious loss. Never click unknown links or share personal information without verification.



COMMON PHISHING EXAMPLES

- Fake Bank Emails
- Urgent Account Alerts
- Prize or Lottery Scams
- Fake Internship / Job Offers
- Social Media Messages
- Phishing Websites
- Government or Company Impersonation



Best Practices to Prevent Phishing

 Always verify the sender's identity

 Hover over links before clicking

 Do not share OTPs or passwords

 Avoid opening unknown attachments

 Use strong, unique passwords

 Enable Multi-Factor Authentication (MFA)

 Keep systems and software updated

1. Verify the Sender  <ul style="list-style-type: none">Check the sender's email carefully.	2. Inspect Links Before Clicking  <ul style="list-style-type: none">Hover over links to check the URL.	3. Never Share Sensitive Information  <ul style="list-style-type: none">No passwords, OTPs, or PINs.
4. Be Cautious with Attachments  <ul style="list-style-type: none">Beware of suspicious files.	5. Enable Multi-Factor Authentication (MFA)  <ul style="list-style-type: none">Use MFA for extra security.	6. Use Strong & Unique Passwords  <ul style="list-style-type: none">Create complex passwords.
7. Keep Systems Updated  <ul style="list-style-type: none">Install updates regularly.	8. Watch for Urgency Tactics  <ul style="list-style-type: none">Avoid 'Act Now!' messages.	9. Report Suspicious Messages  <ul style="list-style-type: none">Report to IT or Security.
10. Stay Educated & Aware  <ul style="list-style-type: none">Attend cybersecurity training.	STOP. THINK. VERIFY. One cautious click can prevent a major cyber incident.	

What you should do immediately

- Do NOT click on links or attachments
- Do NOT reply to the email or message
- Verify the sender using official websites or contacts
- Report the message to IT / security team
- Delete the email or message after reporting

Suspecting a Phishing Attack – What to Look For

Common Warning Signs

 Unexpected emails or messages

 Suspicious sender address @fakebank.com

 Generic greetings like "Dear User"

 Links that don't match when hovered

 Suspicious sender address

 Generic greetings like "Dear User"

 ABC Spelling and grammar mistakes

 Links that don't match when hovered

High-Risk Messages Often Claim:



Account Locked



Prize or Refund



Urgent Action Needed



Unexpected Invoice

What You Should Do Immediately:

 Do NOT click links or attachments

 Do NOT reply to the message

 Verify the source independently

 Report it to IT or security team

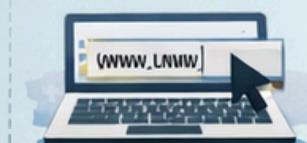
 Delete the email/message



Safe Habits to Prevent Phishing:



Check the Sender



Type URLs Manually



Use Two-Factor (2FA)



Keep Software Updated

 Remember: If a message creates fear, urgency, or excitement — stop and think before you click.

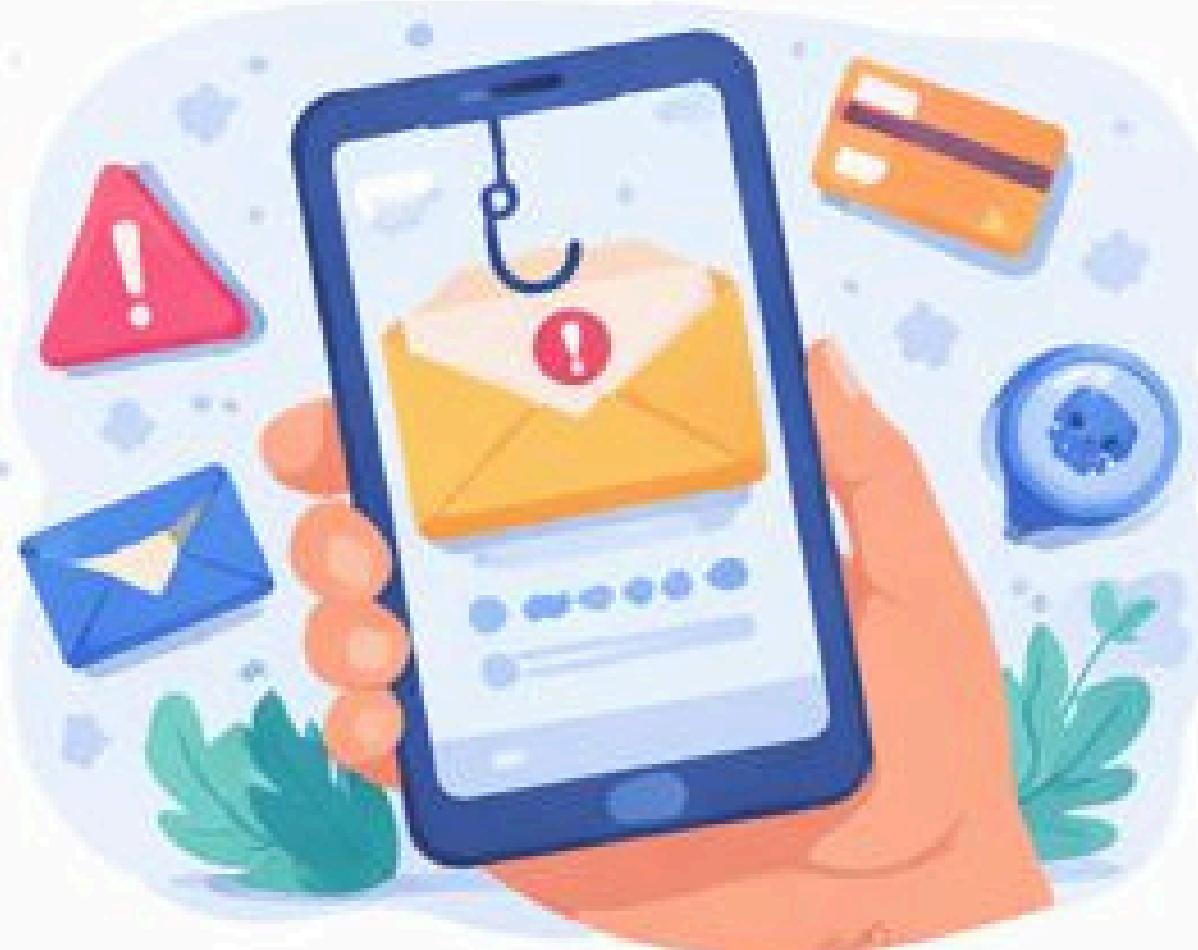
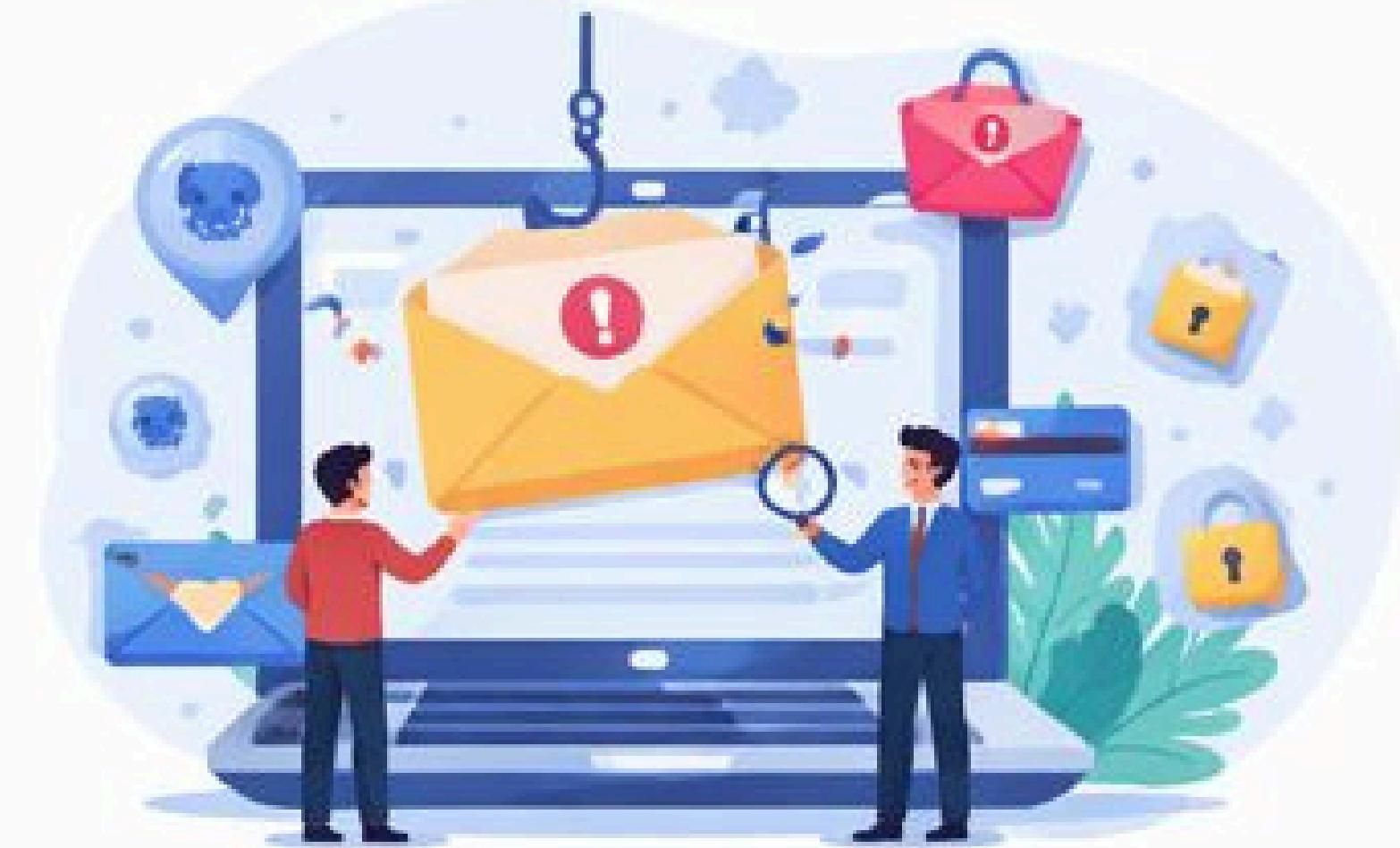
conclusion

To conclude, remember that phishing attacks target people, not just technology. One careless click can lead to serious consequences, but most attacks are preventable with awareness.

Always think before you click, verify before you trust, and report anything suspicious. If a message creates urgency or asks for personal information, pause and check.

Your awareness is your strongest defense.

Stay alert, stay informed, and stay cyber-safe. 





Test your knowledge and interact with us!

- 1. Scan the QR code with your phone.**
- 2. Answer the questions in the Google Form.**
- 3. Submit your answers**

Thank You
