PHISHING AWARENESS TRAINING

Presentation by:DHARSHINI K

WHAT IS PHISHING ?

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.

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.

PHISHING

Email Phishing

- Fake Emails
- Ask for Passwords

Spear Phishing

- Targeted Attacks
- Uses Personal Info

Smishing

- SMS Messages
- Fake Links

Vishing

- Phone Calls
- Pretend to be Bank/Official

Clone Phishing

- Copy of Real Email
- Malicious Attachment

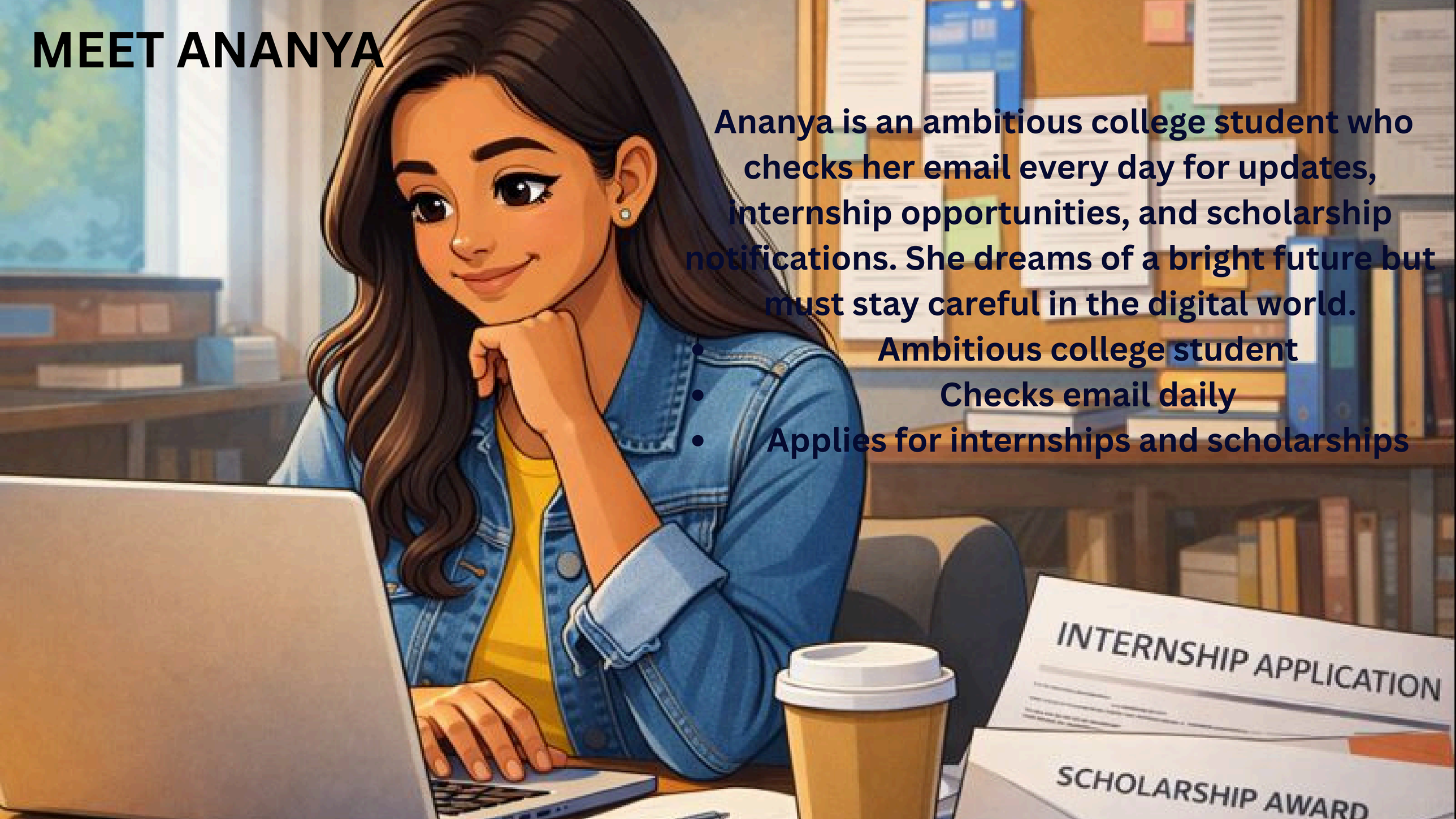
Website Phishing

- Fake Login Pages
- Steals Credentials

COMMON TYPES OF PHISHING:

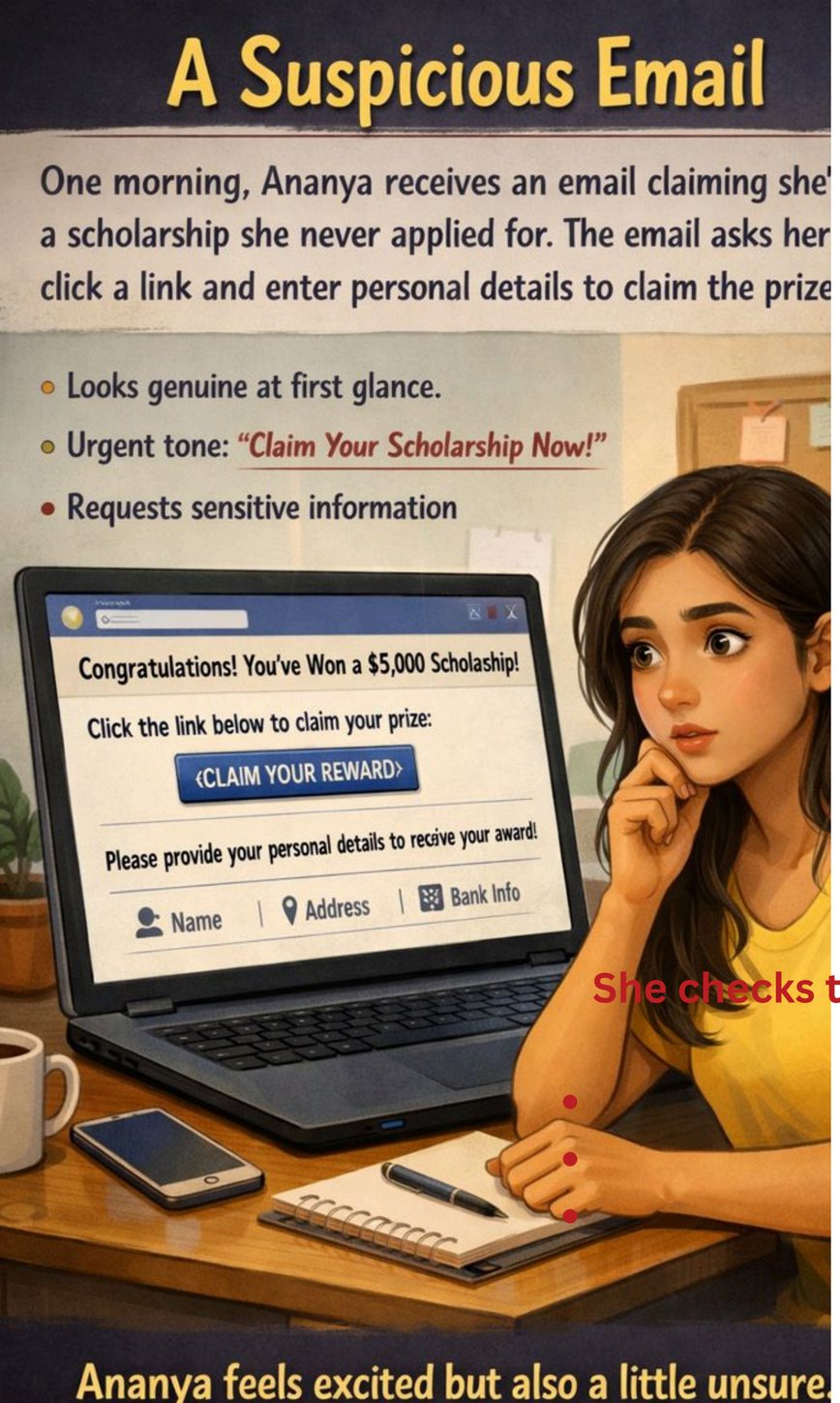
- **Email phishing – Fake emails pretending to be from banks, companies, or colleges, asking for passwords or personal details.**
- **Spear phishing – Targeted phishing aimed at a specific person or organization using personal information.**
- **Smishing – Phishing through SMS/text messages with fake 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



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

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

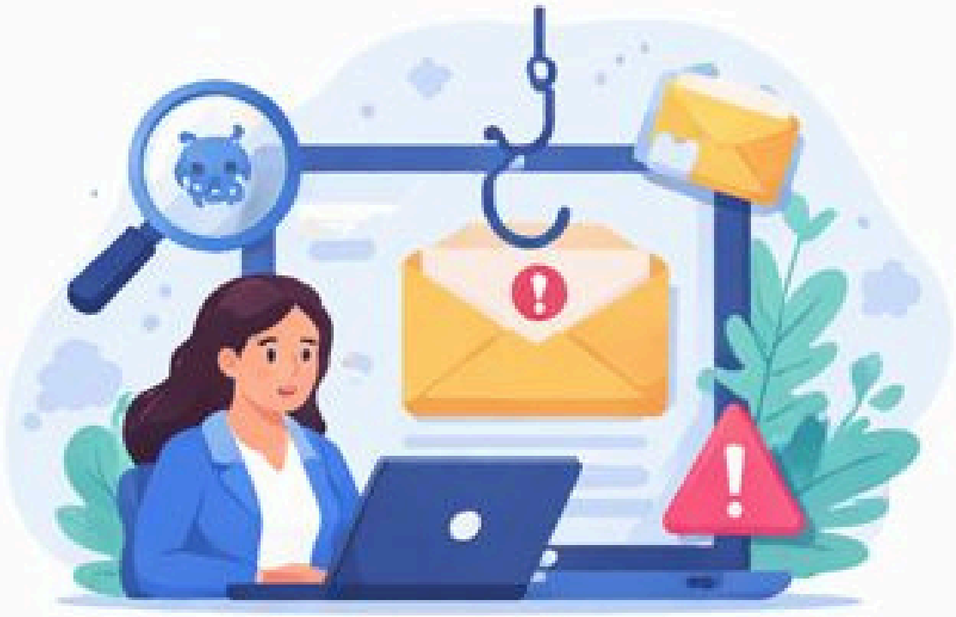
conclusion

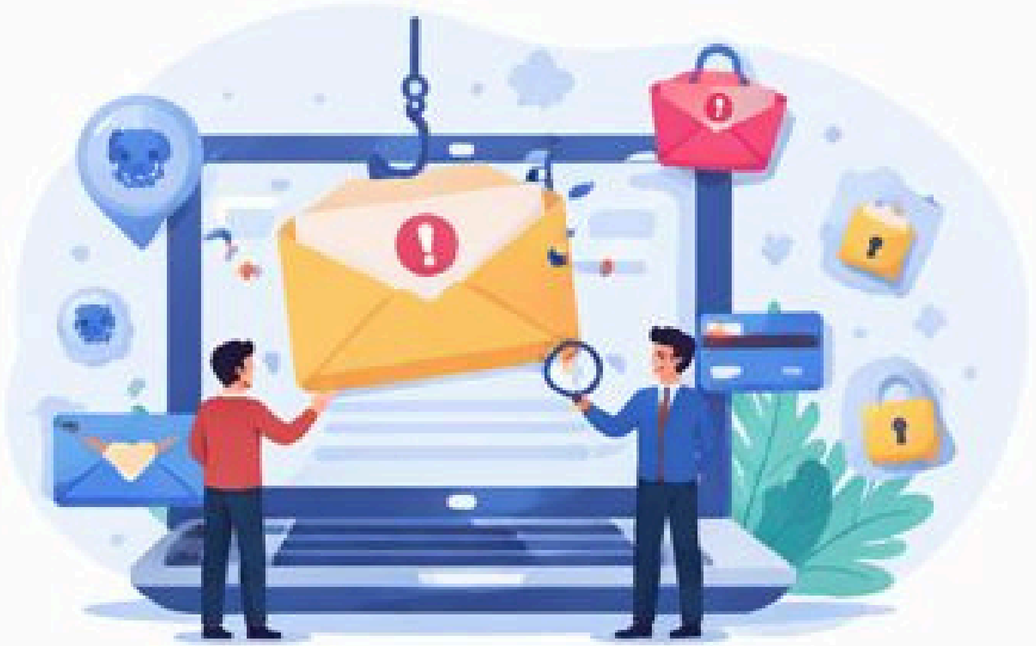
To conclude, remember that phishing attacks target people, not just technology. One careless click can lead to serious consequences, but most attacks are preventable with awareness.

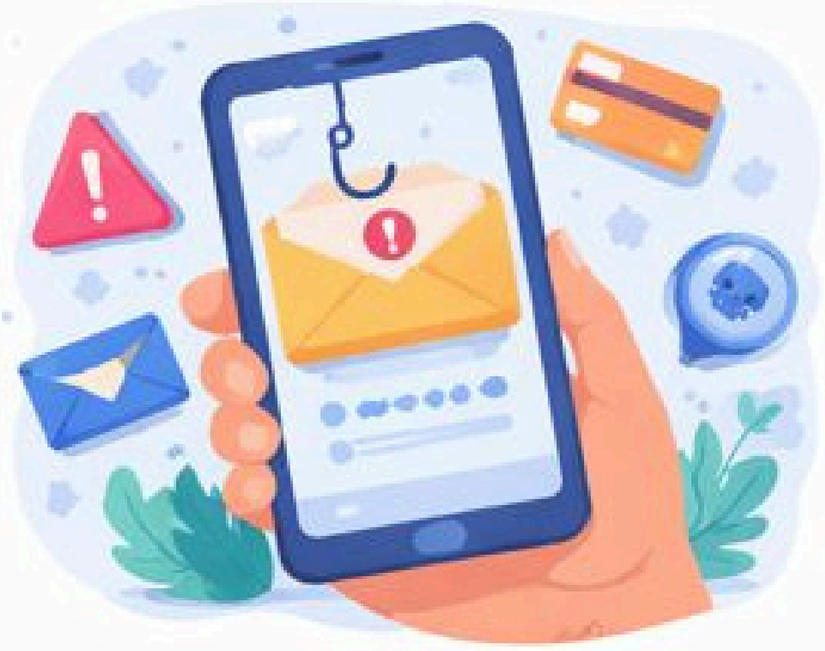
Always think before you click, verify before you trust, and report anything suspicious. If a message creates urgency or asks for personal information, pause and check.

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