PHISHING AWARENESS

DEFEND THE PERIMETER

Interactive Security Training Module 1.0

THE SILENT THREAT

What is Phishing?

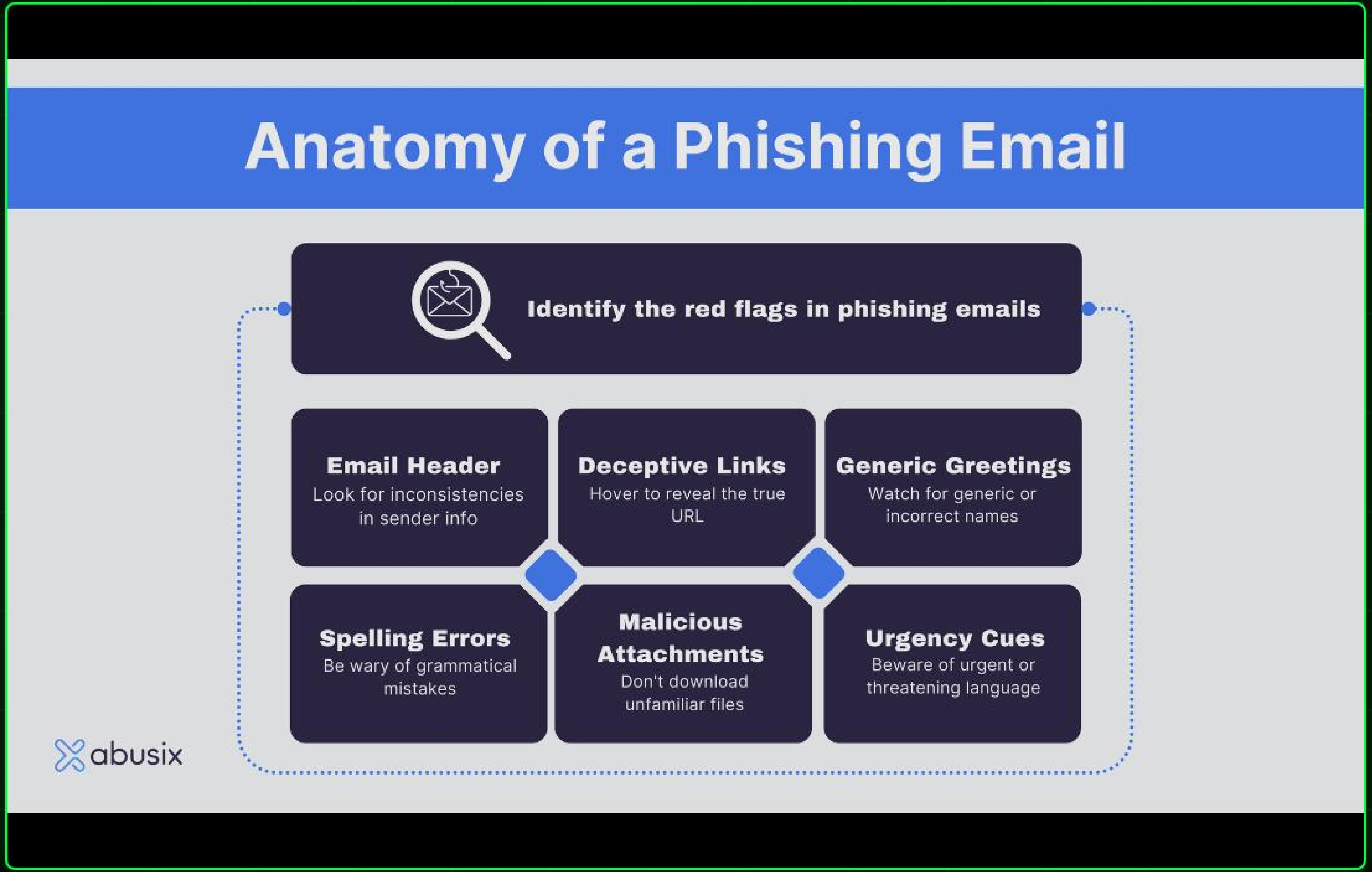
A deceptive cyber attack where attackers impersonate trusted entities to steal sensitive data like login credentials and credit card numbers.

> 90% of all cyber attacks start with phishing.

> Human error is the biggest vulnerability.

> Attacks are evolving: Email → SMS → Voice → QR.

ANATOMY OF A PHISH



Anatomy of a Phishing Email

Identify the red flags in phishing emails

Email Header
Look for inconsistencies in sender info

Deceptive Links
Hover to reveal the true URL

Generic Greetings
Watch for generic or incorrect names

Spelling Errors
Be wary of grammatical mistakes

Malicious Attachments
Don't download unfamiliar files

Urgency Cues
Beware of urgent or threatening language

RED FLAGS TO WATCH

> **Suspicious Sender:** Mismatched domains (e.g., support@amazon-security-update.com).

> **Generic Greetings:** "Dear Customer" instead of your name.

> **Urgency & Fear:** "Account Suspended", "Immediate Action Required".

> **Suspicious Links:** Hover text doesn't match the URL.

> **Unexpected Attachments:** Invoices or receipts you didn't request (.zip, .exe).

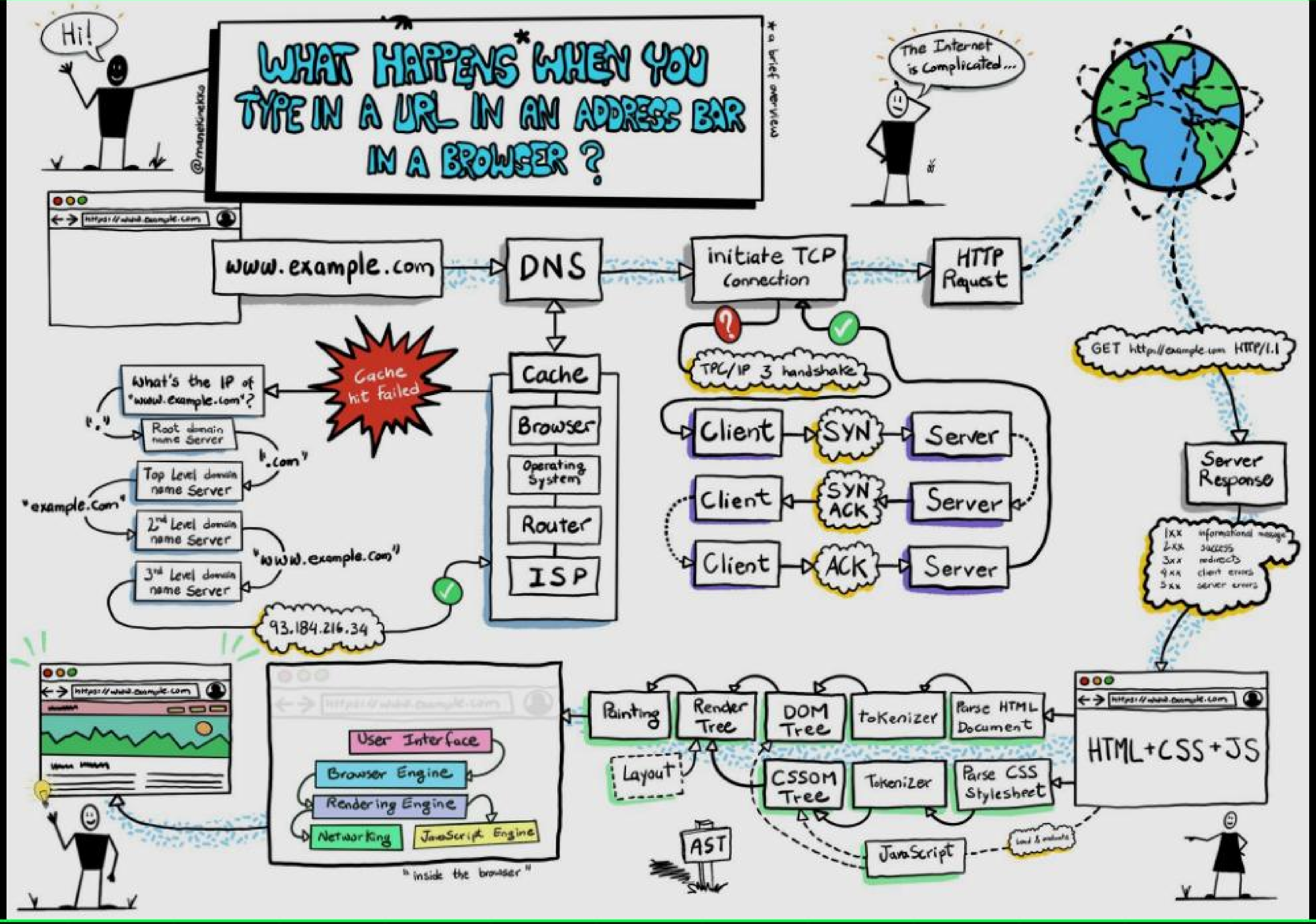
SPOTTING FAKE WEBSITES

URL INSPECTION

Attackers create look-alike sites to harvest credentials. Always check the address bar.

❌ http://paypal-secure-login.com
// Wrong domain, no HTTPS

✅ https://www.paypal.com
// Correct domain, Secure Lock



SOCIAL ENGINEERING TACTICS

VISHING

Voice Phishing. Attackers call pretending to be IT support or your bank to get you to hand over access codes.

SMISHING

SMS Phishing. Texts claiming "Delivery Failed" or "Bank Alert" with malicious links.

PRETEXTING

Creating a fabricated scenario (the pretext) to build trust. E.g., "I'm the CEO and I lost my phone, buy me gift cards."

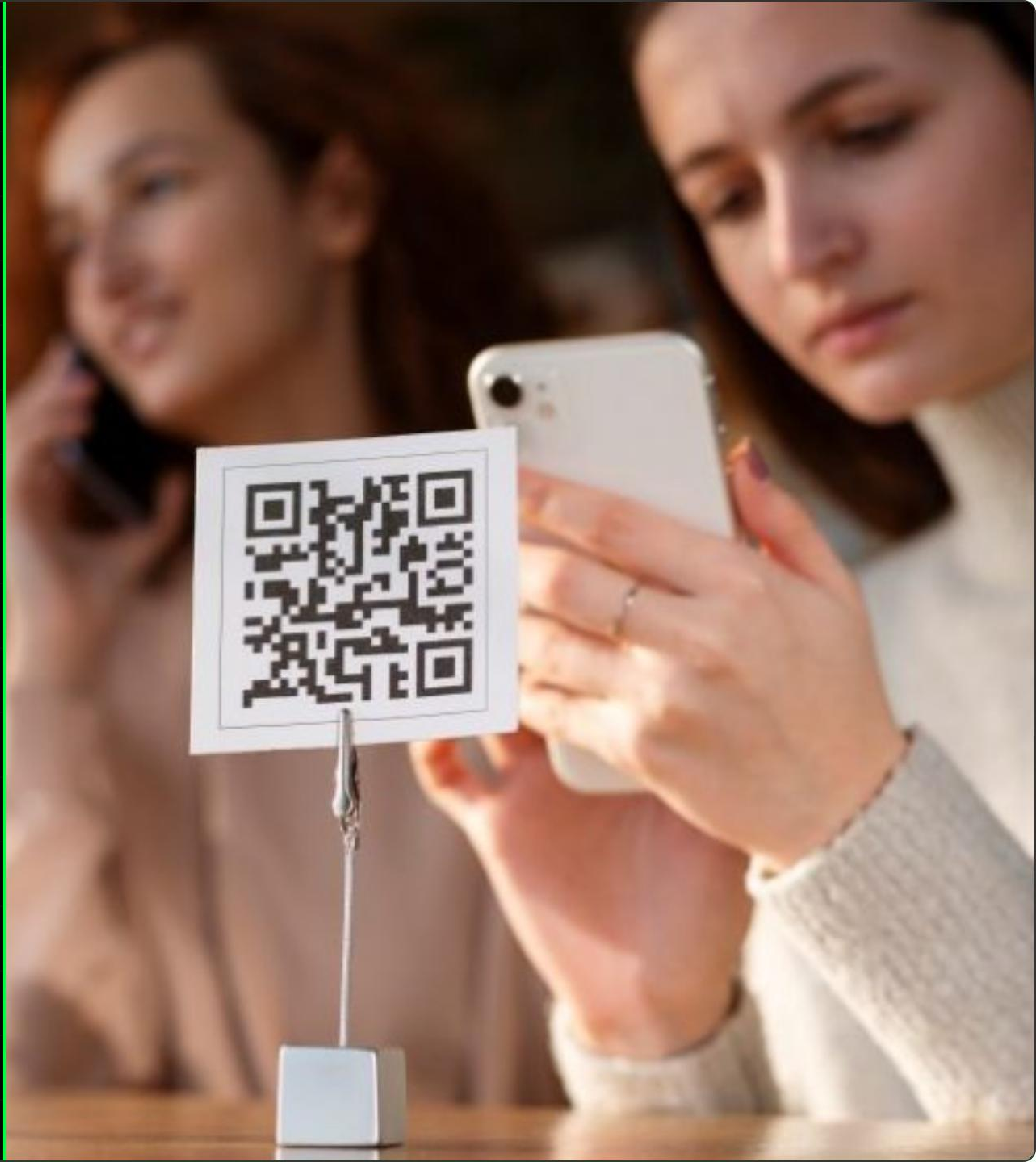
EMERGING THREATS (2024-25)

QUISHING (QR PHISHING)

Attackers paste malicious QR codes on parking meters or send them in emails to bypass text scanners. Scanning leads to a credential theft site.

AI DEEPFAKES

Using AI to clone a CEO's voice in a vishing attack, authorizing urgent wire transfers. "The boss" sounds real, but it's a bot.



CASE STUDY: THE PAYROLL LURE

THE SCENARIO

Employees receive an email: *"Action Required: Update Direct Deposit Info before Payday."*

THE CATCH

> Creates financial urgency (fear of not getting paid).

> Link leads to a fake O365 login page.

> Result: Attackers hijack payroll to their own accounts.

DEFENSE BEST PRACTICES

STOP & LOOK

Don't click on impulse. Analyze the sender, subject, and link destination first.

ENABLE MFA

Multi-Factor Authentication stops 99.9% of account takeovers even if they get your password.

REPORT IT

Use the "Report Phishing" button in your email client. Don't just delete it; help the security team.

KNOWLEDGE CHECK: THE "CEO" REQUEST

You get a text from the CEO at 9 PM: "In a meeting, can't talk. Need you to buy 10 Google Play cards for a client gift ASAP. Will reimburse." What do you do?

A Buy the cards immediately to impress the CEO.

B Reply asking for the company credit card number.

[✓ C Do nothing/Verify. This is a classic "Gift Card" scam. Report to security.]

KNOWLEDGE CHECK: THE ATTACHMENT

You receive an email from "HR-Dept@company-updates.net" with an attachment named "Q3_Bonus_Structure.exe".

[✓ A] Flag as Phishing. The domain is wrong and .exe files are dangerous.

B Open it to see if you are getting a bonus.

C Forward it to your personal email to check it safely on your phone.

KNOWLEDGE CHECK: THE LOGIN PAGE

You clicked a link to update your password. The website looks identical to Microsoft 365, but the URL is "microsoft-security-auth.co".

A Enter your old password to test it.

[✓ B Close the tab immediately. This is a spoofed domain.]

C Enter your username but a fake password.

STAY VIGILANT

You are the first line of defense.

TRAINING COMPLETE

Cyber Security Internship Module

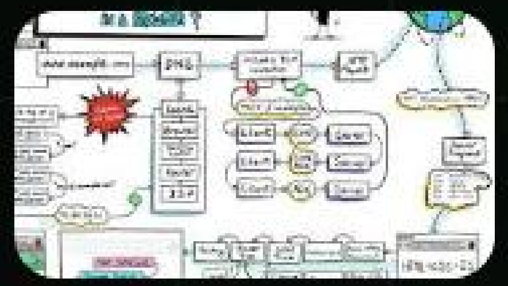
IMAGE SOURCES

https://png.pngtree.com/png-clipart/20250710/original/pngtree-cyber-security-shield-with-padlock-digital-protection-concept-png-image_21294701.png

Source: pngtree.com

https://abusix.com/wp-content/uploads/2023/09/1-anatomy-of-a-phishing-email_ec104ccad55dae1baa0c3044823a542d_2000.png

Source: abusix.com



https://blog.knowbe4.com/hubfs/How-The-Web-Works.jfif

Source: blog.knowbe4.com

https://www.quickheal.co.in/knowledge-centre/wp-content/uploads/2025/04/QR-Code-Scams-991x564.jpg

Source: www.quickheal.co.in

https://uit.stanford.edu/sites/default/files/images/Screenshot%202023-03-16%20at%2010.58.38%20AM.png

Source: uit.stanford.edu

https://easy-peasy.ai/cdn-cgi/image/quality=95,format=auto,width=800/https://media.easy-peasy.ai/27feb2bb-aeb4-4a83-9fb6-8f3f2a15885e/dc02123f-1706-4ce8-bdf0-678e7cd0dbd3.png

Source: easy-peasy.ai