PHISHING AWARENESS TRAINING

CODE ALPHA

Cyber Security Internship Task 2

Title: Phishing Awareness Training

Subtitle: Stay Smart. Stay Safe.

Presented by: Saira Arshad

Internship Name: Cyber security

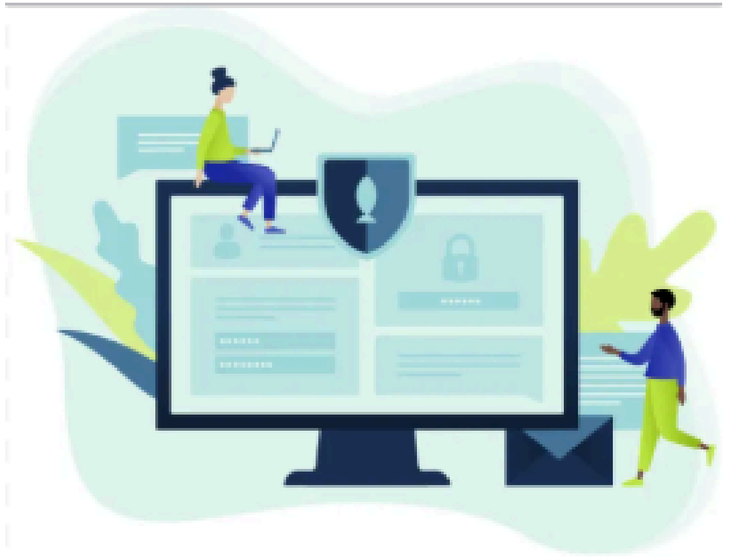
Company Name : Code Alpha

Phishing Awareness Training Introduction

In today's digital world, cyber threats are becoming increasingly sophisticated, with phishing attacks being one of the most common and dangerous. Phishing is a deceptive technique used by cybercriminals to trick individuals into revealing sensitive information such as passwords, credit card numbers, and personal data. These attacks are usually carried out through emails, messages, or fake websites that appear to be from legitimate sources.

The purpose of this phishing awareness training is to educate individuals on how phishing works, what forms it takes, and how to identify and avoid falling victim to it. As cybercriminals continuously refine their strategies, it becomes essential for users—whether students, employees, or general internet users—to stay informed and cautious.

This training covers different types of phishing attacks, common signs of phishing attempts, real-life examples, and effective best practices to enhance digital security. By understanding phishing and its tactics, individuals can play an active role in protecting not only their personal data but also the broader digital environment.



Importance of Phishing Awareness Training

Phishing awareness training holds significant importance in today's digitally connected world, where cyberattacks are increasingly sophisticated and frequent. Phishing is not merely a technical threat—it exploits human psychology, trust, and urgency to deceive individuals into revealing sensitive information. Therefore, awareness and education serve as the most effective first line of defense against such attacks.

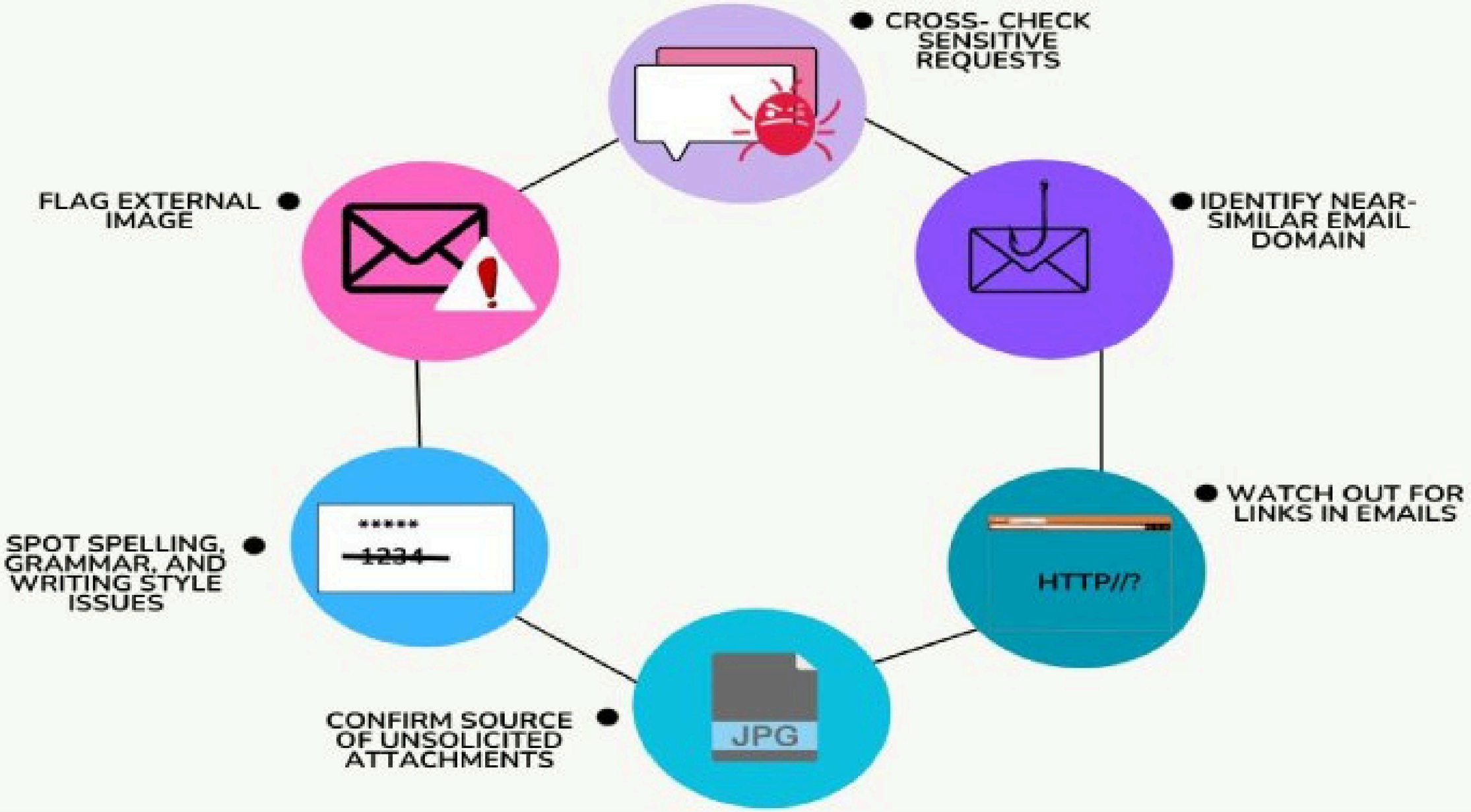
The key reasons why phishing awareness training is important include:

- Improves Digital Security
  Individuals learn how to identify and respond to phishing threats, thereby protecting their personal and organizational data.
- Increases Awareness and Vigilance
  Users become more cautious and critical when interacting with emails, websites, or messages, reducing the chance of falling for scams.
- Prevents Financial Loss
  Many phishing attacks aim to steal banking credentials or credit card information. Training helps users avoid these traps and secure their finances.
- Essential for Organizations
  One employee's mistake can lead to large-scale data breaches. Phishing training at the workplace is crucial for maintaining cybersecurity across the organization.
- Reduces Cybercrime
  As awareness spreads, fewer people fall victim to scams, which discourages attackers and helps reduce the overall success rate of phishing campaigns.
- Promotes a Culture of Cyber Awareness
  Individuals who understand phishing tactics are more likely to educate others, building a safer online environment for all.

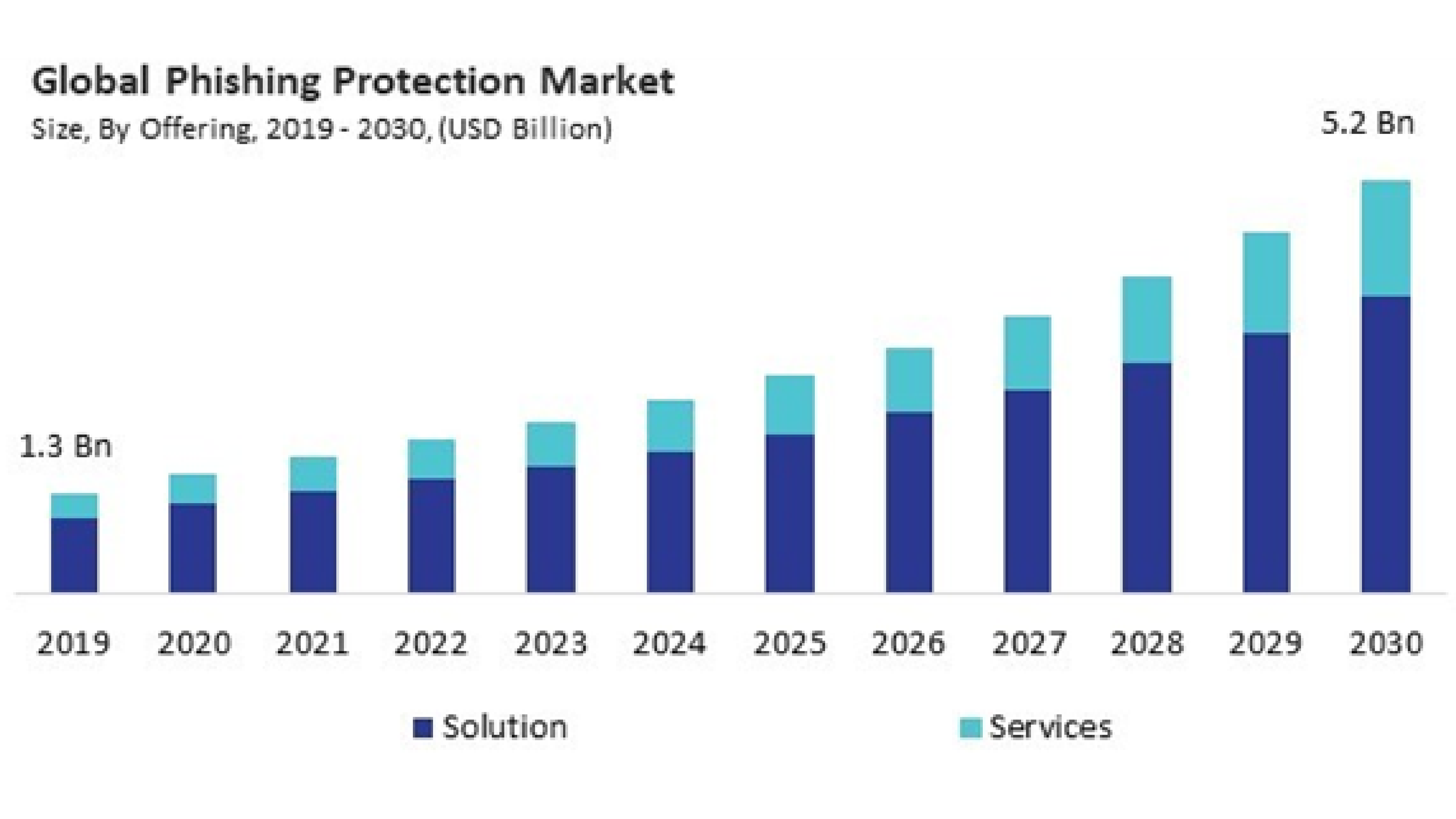
Types of Phishing Attacks

Type	Description	Example
Email Phishing	Generic emails sent to many users, appearing to be from trusted sources	Email from “bank” asking you to verify login info via a fake link
Spear Phishing	Targeted attack using personal info to trick a specific person	Fake email from “manager” requesting urgent access to internal documents
Whaling	Targets executives or senior leaders in organizations	Email posing as CEO requesting a wire transfer
Smishing	SMS-based phishing using fake texts and malicious links	“Your package is delayed. Click this link to reschedule delivery.”
Vishing	Voice call phishing, often pretending to be bank or government	Caller claims your bank account is compromised and asks for verification
Clone Phishing	A replica of a previous legitimate email, but with malicious attachments/links	Fake resend of an old invoice that now includes malware
Angler Phishing	Phishing via social media, using fake support accounts to deceive users	Fake customer service profile replies to a complaint on Twitter with a link

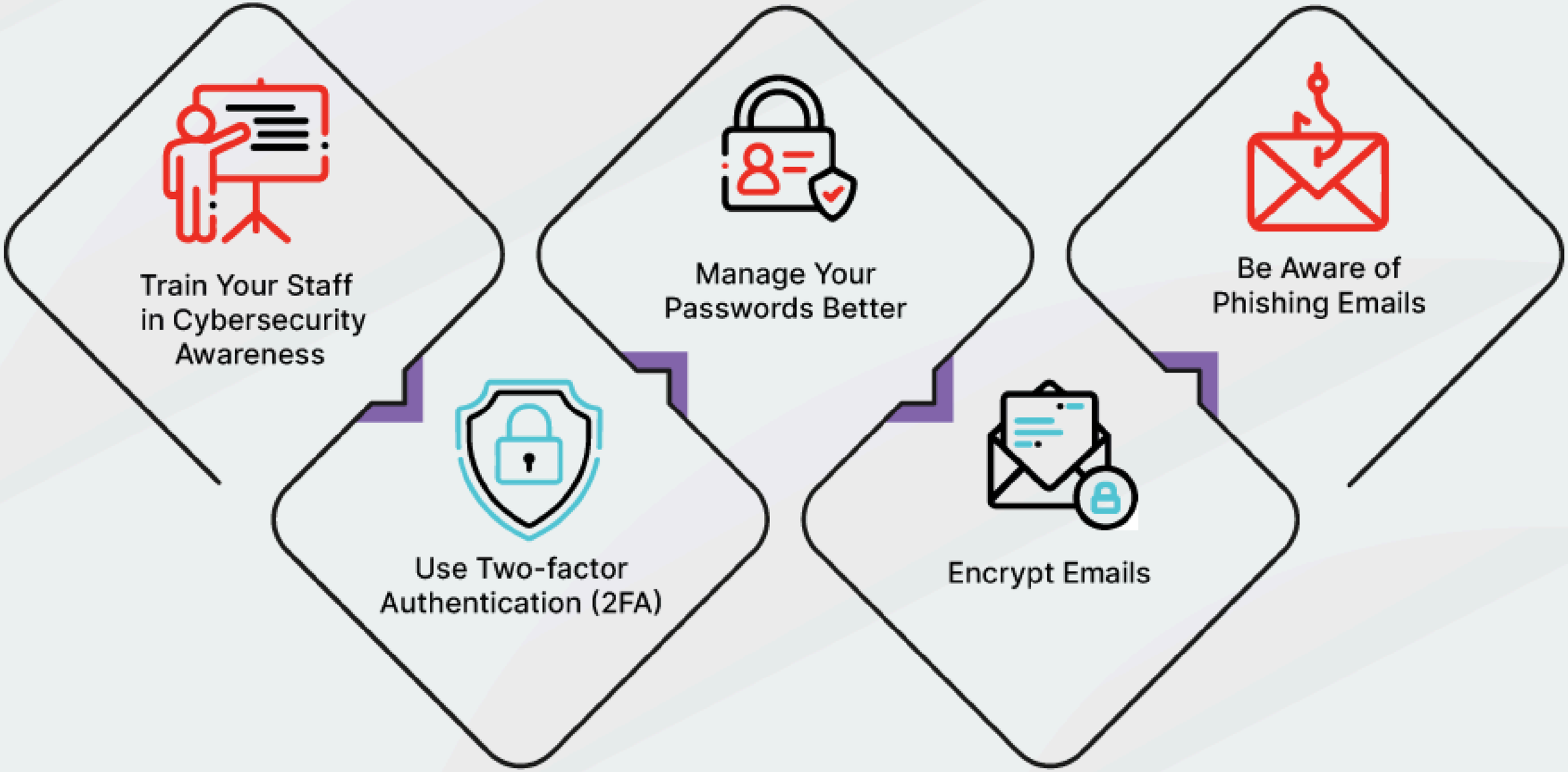
WAYS TO IDENTIFY A WHALING PHISHING ATTACK



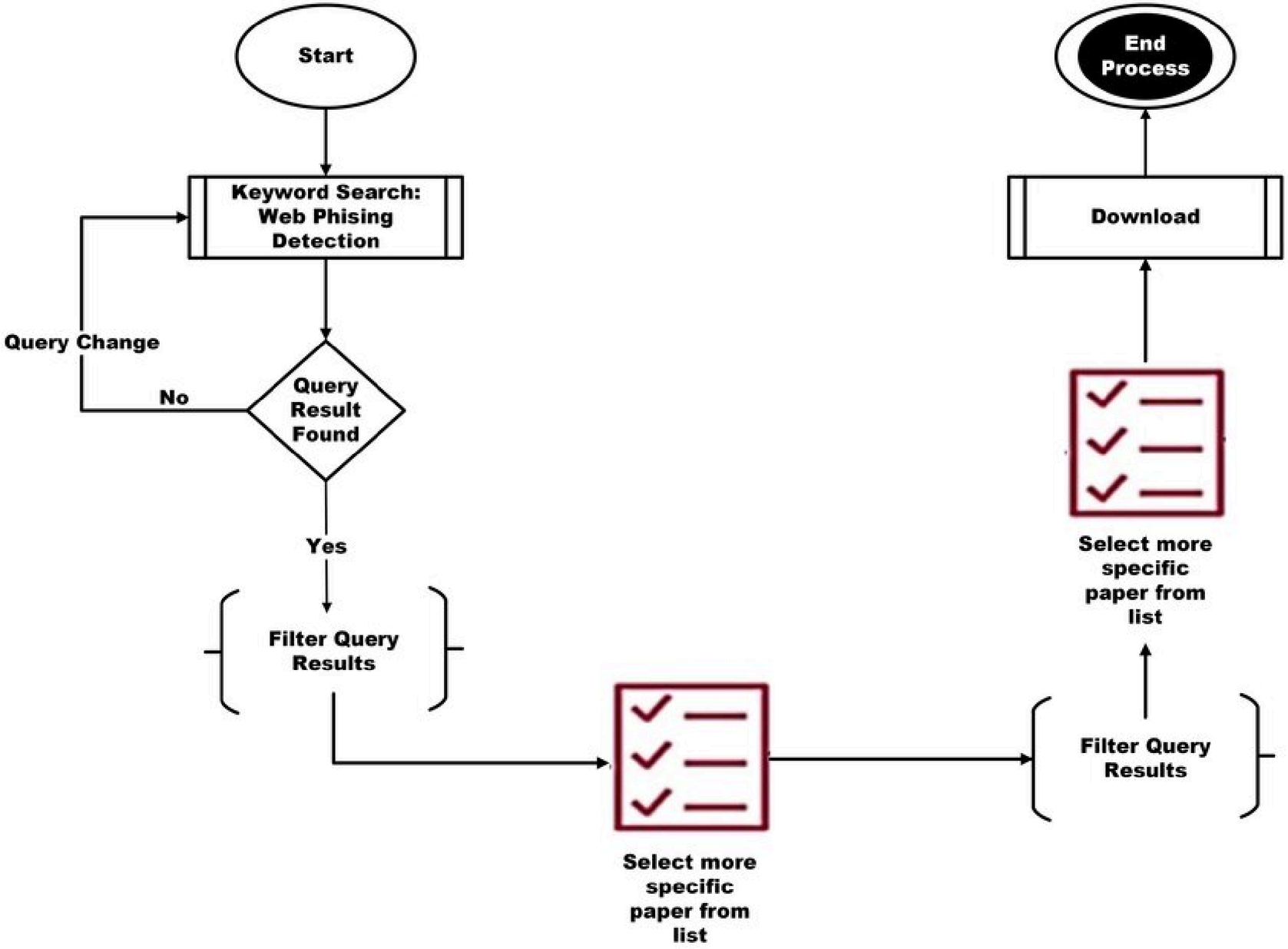
Common Types of Phishing Techniques


Global Phishing Protection Market
Size, By Offering, 2019 - 2030, (USD Billion)
5.2 Bn
1.3 Bn
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
Solution
Services

Top 5 Practices To Strengthen Your Email Security



Web Phishing Detection



Basic Rules for creating passwords

1 **NEVER RESUSE A PASSWORD**
Don't use the same password for all accounts

2 **DON'T USE PERSONAL INFORMATION**
Using versions of your name, family members or DOB

3 **MIX IT UP**
Use uppercase, lowercase, characters, and numbers.

4 **MAKE IT LONG**
The longer the password the harder it is to guess

5 **CHANGE THEM FREQUENTLY**
Set reminders to change them once a month

6 **DON'T SHARE THEM**
This may be tricky to manage but important to teach

7 **USE A PASSWORD MANAGER**
NordPass was rated the top password manager in Australia

8 **USE TWO-FACTOR AUTHENTIFICATION**
Where possible this will add another layer of protection

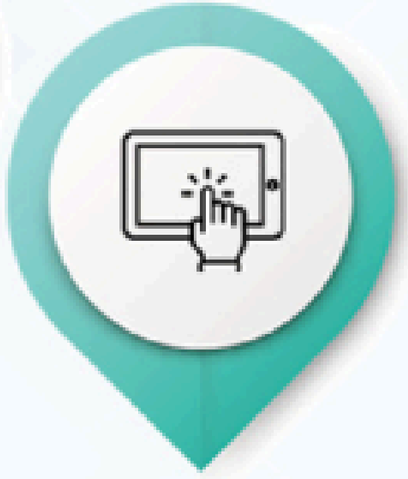
BENEFITS OF MULTI-FACTOR AUTHENTICATION

Provides increased security

Lessens the impact of password offenses

Addresses compliance regulations

Improves usability



Reduces legal risks

Helps take a step toward a zero trust model

Where Should You Report A Cyber Incident?

Internally

Regulatory authorities

Online platforms like Internet Crime Compliant center (IC3)

National cybersecurity agencies

Other affected or relevant parties such as customers, insurance providers etc.

7 Phishing Awareness Training Methods

Simulated Phishing Campaigns with Technical Feedback

Email Header Analysis Workshops

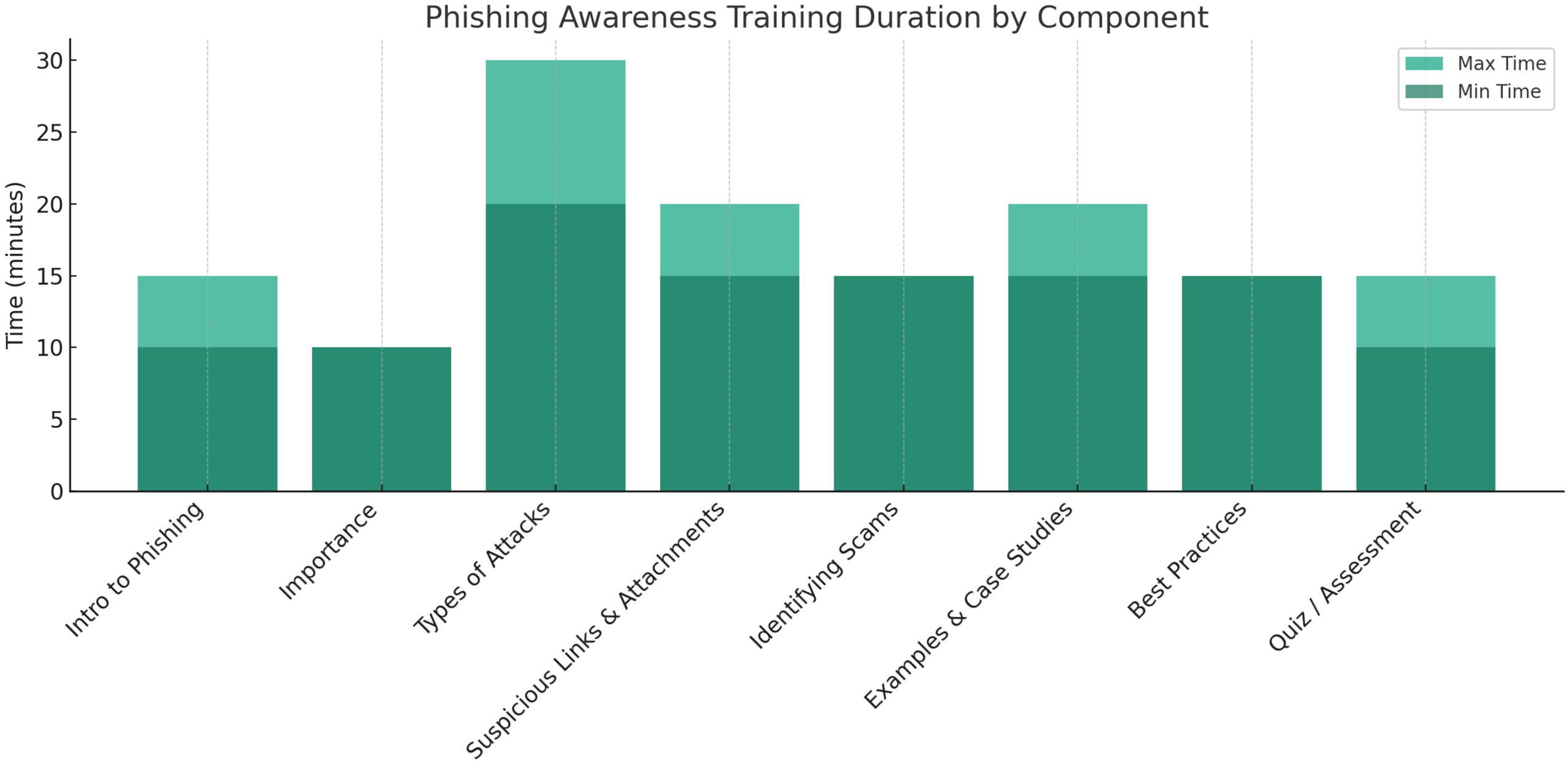
Advanced Social Engineering Recognition

Open-Source Intelligence (OSINT) for Threat Hunting

Technical Deep Dives into Malware

Incident Response Simulations

Data-Driven Training Adaptation


Phishing Awareness Training Duration by Component
Time (minutes)
0
5
10
15
20
25
30
Max Time
Min Time
Intro to Phishing
Importance
Types of Attacks
Suspicious Links & Attachments
Identifying Scams
Examples & Case Studies
Best Practices
Quiz / Assessment

How to prevent phishing attacks: best strategies

#1 Educate your employees

#2 Implement advanced email filtering

#3 Enforce MFA

#4 Regularly update and patch systems

#5 Conduct phishing simulation exercises

#6 Develop a response plan

#7 Use Secure Web Gateways and DNS Filtering

#8 Hold regular security checks and assessments

#9 Build a culture of reporting

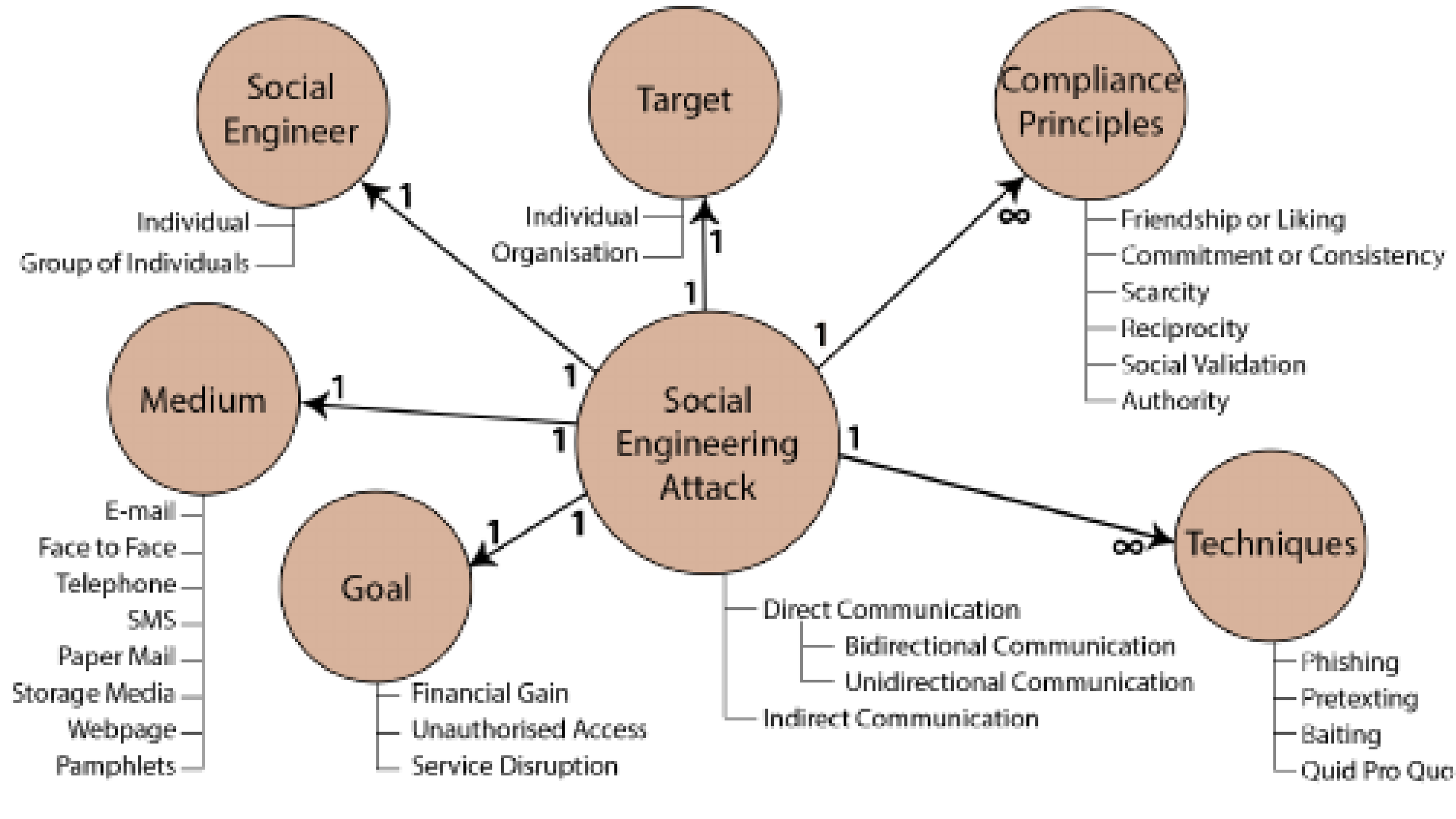
How Does A Phishing Simulation Work?

1. **Setup:** Choose or customize a phishing template and target audience within the organization.

2. **Launch Simulation:** Distribute the simulated phishing emails to employees.

3. **Track:** Monitor interactions such as email opens, clicks, and credential entry attempts.

4. **Feedback & Analysis:** Provide immediate educational feedback to participants and analyze the results for insights into the organization's phish detection skills and potential vulnerabilities.


Social Engineer
Individual
Group of Individuals
Target
Individual
Organisation
Compliance Principles
Friendship or Liking
Commitment or Consistency
Scarcity
Reciprocity
Social Validation
Authority
Medium
E-mail
Face to Face
Telephone
SMS
Paper Mail
Storage Media
Webpage
Pamphlets
Social Engineering Attack
Goal
Financial Gain
Unauthorised Access
Service Disruption
Direct Communication
Bidirectional Communication
Unidirectional Communication
Indirect Communication
Techniques
Phishing
Pretexting
Baiting
Quid Pro Quo
1
∞

8 Measures to Counter Social Engineering

- Stay informed about the latest attacks
- Implement Multi-Factor Authentication
- Always verify identify & legitimacy
- Enable anti-spam filters

- Use firewalls & anti-virus software
- Update with latest security patches
- Conduct penetration testing
- Check SSL certificate on websites

Phishing attacks:
Defending your organisation

A multi-layered approach - such as the one summarised below - can improve your resilience against phishing whilst minimising disruption to user productivity. This approach provides multiple opportunities to detect a phishing attack and stop it before it causes major harm. The mitigations included are also useful against other types of cyber attack.

LAYER 1
Make it difficult for attackers to reach users.

- Implement anti-spoofing controls to stop your email addresses being a resource for attackers.
- Consider what information is available to attackers on your website and social media and help your users do the same
- Filter or block incoming phishing emails.

LAYER 2
Help users identify and report suspected phishing emails.

- Relevant training can help users spot phishing emails, but no amount of training can help them spot every email.
- Help users to recognise fraudulent requests by reviewing processes that could be mimicked and exploited.
- Create an environment that lets users seek help through a clear reporting method, useful feedback and a no-blame culture.

LAYER 3
Protect your organisation from the effects of undetected phishing emails.

- Protect your accounts: make authentication more resistant to phishing (such as setting up MFA) and ensure authorisation only gives privileges to people who need them.
- Protect users from malicious websites by using a proxy services and an up-to-date browser.
- Protect your devices from malware.

LAYER 4
Respond to incidents quickly.

- Define and rehearse an incident response plan for different types of incidents, including legal and regulatory responsibilities.
- Detect incidents quickly by encouraging users to report any suspicious activity.

10 Examples of Spear Phishing

1. Business Email Compromise (BEC)

2. Whaling

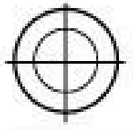
3. Fake Invoices

4. Stealing Login Credentials

5. Spear Phishing for Malware Delivery

6. Spear Phishing for Trade Secrets

7. Targeted Attacks on Suppliers



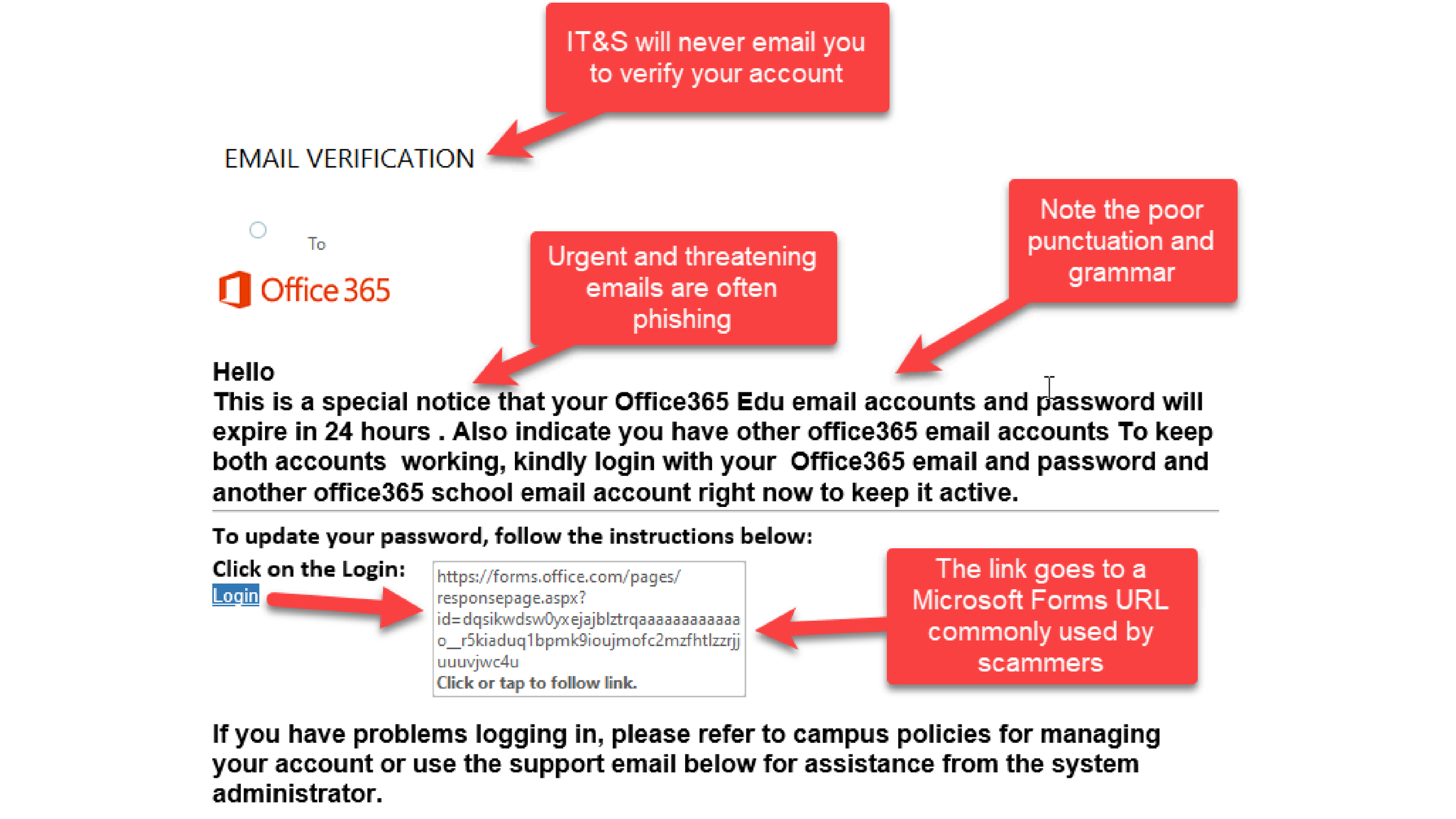
8. Tax-Themed Phishing

9. Fake Job Offers

10. Impersonation of Trusted Contacts

Real email

Cloned email


IT&S will never email you to verify your account
EMAIL VERIFICATION
To
Office 365
Urgent and threatening emails are often phishing
Note the poor punctuation and grammar
Hello
This is a special notice that your Office365 Edu email accounts and password will expire in 24 hours . Also indicate you have other office365 email accounts To keep both accounts working, kindly login with your Office365 email and password and another office365 school email account right now to keep it active.
To update your password, follow the instructions below:
Click on the Login:
Login
https://forms.office.com/pages/responsepage.aspx?id=dqsikwdsw0yxejajblztrqaaaaaaaaaaaaao__r5kiaduq1bpmk9ioujmofc2mzfhtlzzrjjuuuvjwc4u
Click or tap to follow link.
The link goes to a Microsoft Forms URL commonly used by scammers
If you have problems logging in, please refer to campus policies for managing your account or use the support email below for assistance from the system administrator.

Interactive Quiz (Phishing Awareness) ?

Question 1
You get an email from your bank asking you to "verify your password immediately." What do you do?
A) Click the link and log in
B) Reply to the email
C) Call the bank directly using the number on your bank card
D) Ignore it

Question 2
Which of the following is a common sign of a phishing email?
A) Personalized greeting with your full name
B) Urgent language like “Your account will be locked!”
C) Sent from your company’s internal domain
D) Signed by your known manager

Question 3
An email contains a link that says www.paypal.com but hovering over it shows www.pavpal.securelogin.ru. What should you do?
A) Click the link to confirm
B) Forward the email to friends
C) Do not click — report it as phishing
D) Reply to verify sender’s identity

Question 4
You receive a call from someone claiming to be your company’s IT department asking for your password. What should you do?
A) Give them your password to avoid delay
B) Ask for their employee ID
C) Refuse and report the call to your supervisor or IT
D) Hang up and ignore

Question 5
Which of the following is the BEST way to protect yourself from phishing?
A) Use the same password for all accounts
B) Enable Two-Factor Authentication (2FA)
C) Only use email during work hours
D) Download all attachments from your boss

Conclusion — Stay Vigilant

⚠️ Phishing attacks are evolving — and getting smarter every day.

✅ Key Takeaways:
Stay alert: Don’t trust emails or messages blindly.
Verify before you act: When in doubt, contact the source directly.
Think before you click: One wrong move can compromise your data.
Protect yourself & your organization: Report suspicious activity.

🔒 Awareness is your best defense.
“Cybersecurity is not just an IT issue — it's everyone's responsibility.”

💡 Tip: Add a soft background image like a lock, shield, or alert icon to visually reinforce the message.


Stay safe and help others stay informed!


Thank
you