Mandar Kajbaje

Phishing Awareness

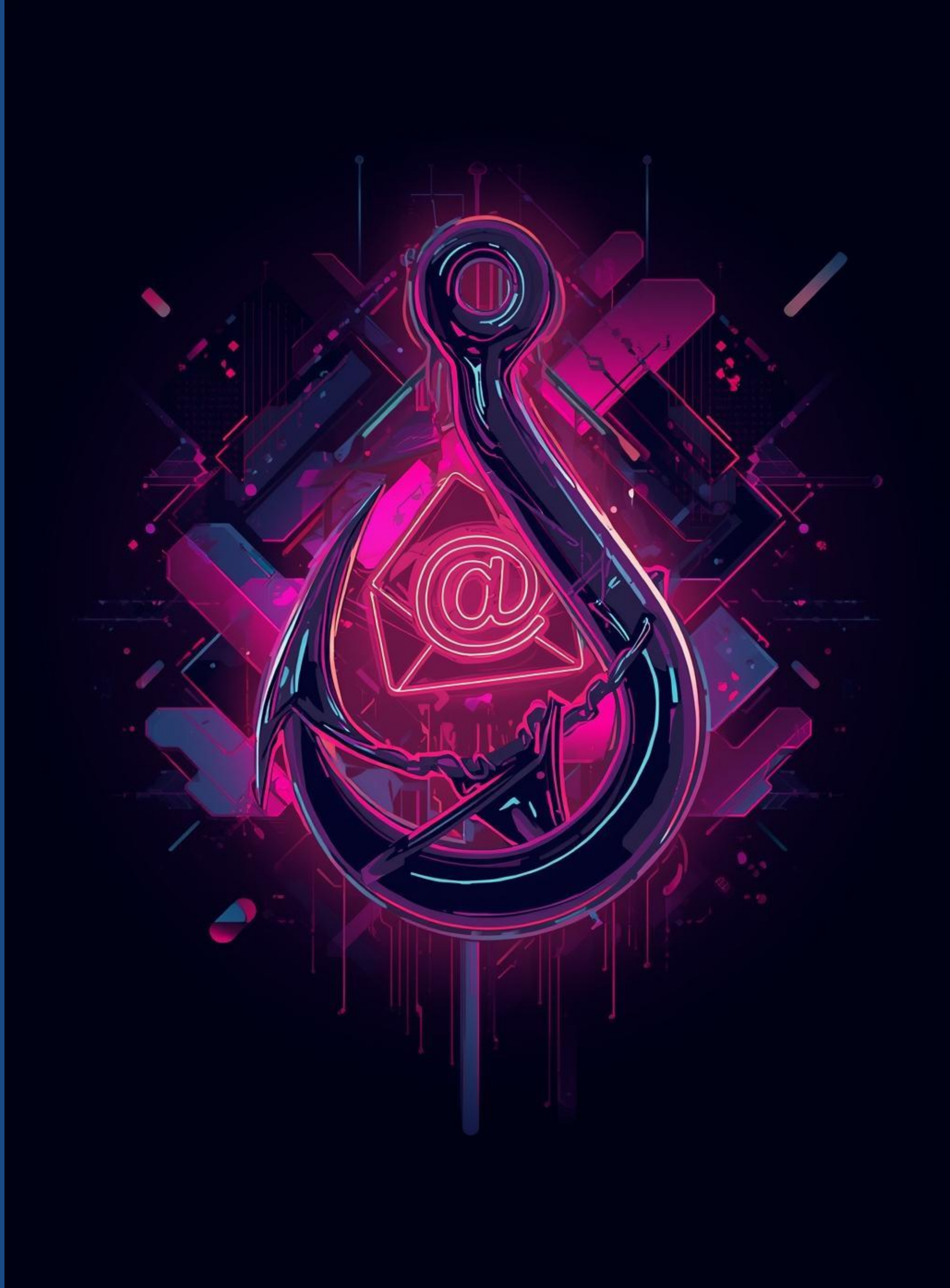
BSC CS Student Training

PRESENTED BY

Mandar Kajbaje

What is Phishing?

Phishing is a form of **cyber deception** where attackers manipulate individuals into revealing sensitive information, often through fake emails or websites designed to appear legitimate.



Types of Phishing Attacks Explained

EMAIL PHISHING

Email phishing involves deceptive emails that appear legitimate, aiming to trick recipients into revealing sensitive information or downloading malware. This is one of the **most common attack** methods.

SMISHING

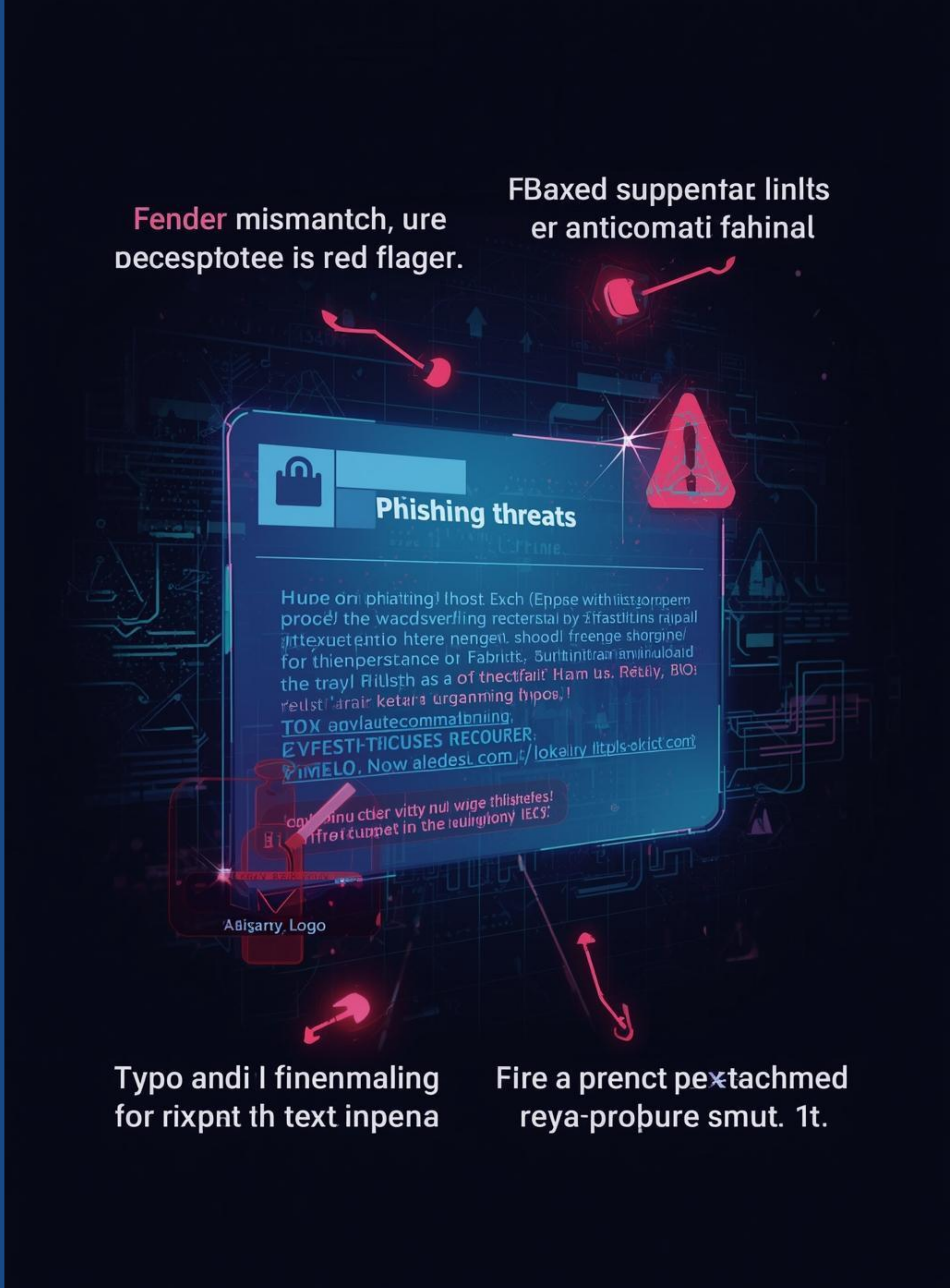
Smishing utilizes SMS messages to lure victims into providing personal information or clicking malicious links. This technique exploits the trust people place in text messages, often appearing urgent.

VISHING

Vishing, or voice phishing, involves phone calls where scammers impersonate legitimate entities to extract sensitive data. This tactic relies heavily on **manipulating the victim's trust** and emotions.

Recognizing Phishing Emails

Identifying phishing emails is crucial for online safety. Look for **red flags** like sender mismatches, urgency, typos, and suspicious links to protect your data.

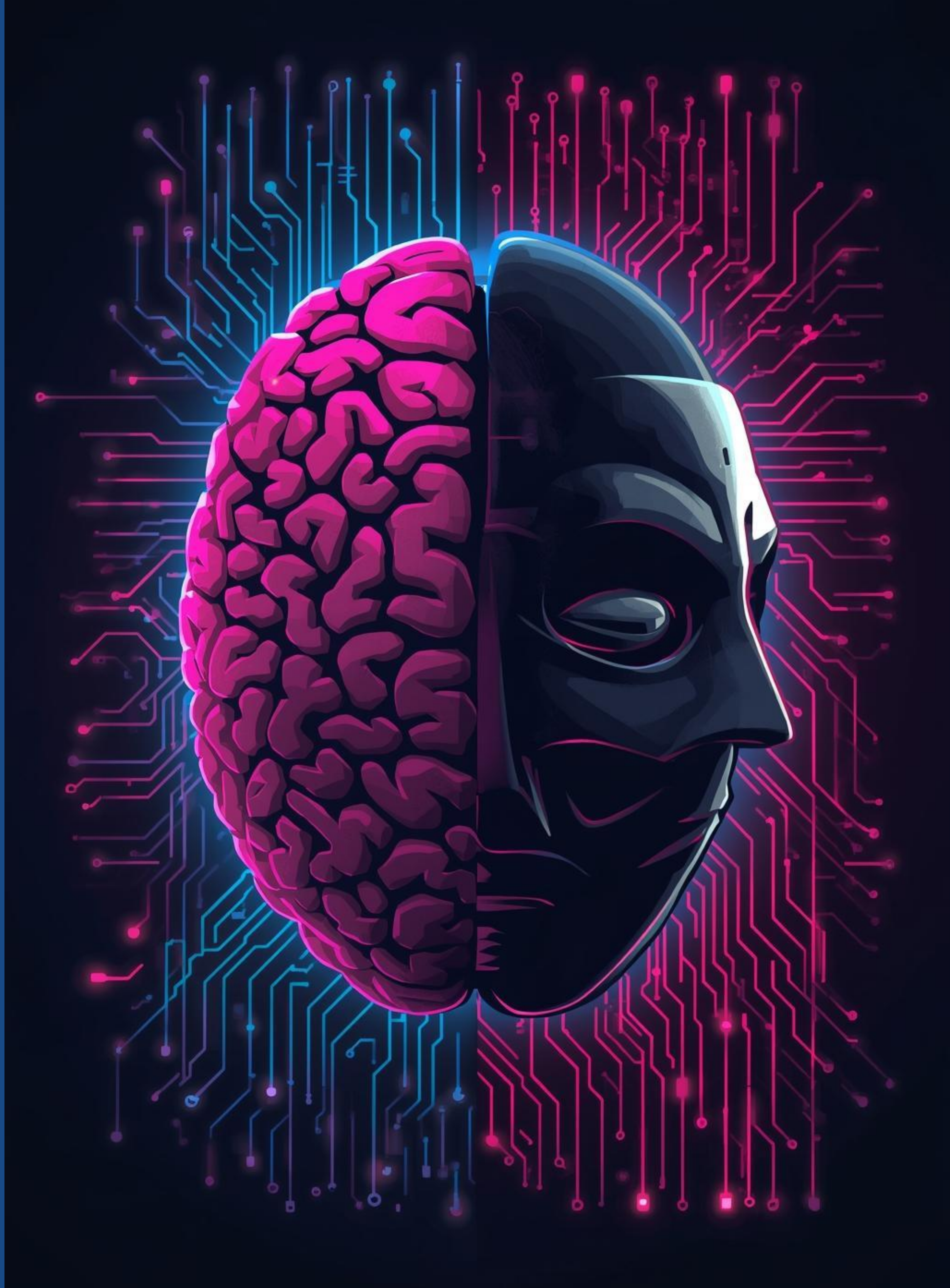

Fender mismantch, ure
ᴅecesptotee is red flager.
FBaxed suppentaɪ linlts
er anticomati fahinal
Phishing threats
Hupe on phiatting! lhost Exch (Enpse withiist:ompern
proce! the wacdsverfling rectersial by 1fastlitins raipall
ittexuetentio htere nengel. shoodl freenge shorgine/
for thienperstance or Fabritt, 5urltinitran anjinuloaid
the trayl Fitlsth as a of tnectfait' Ham us. Rebly, BIO!
reilst' arair ketara urganming fnpos.!
TOX aovlautecommatbniing
EVFESTI-TIICUSES RECOURER
YIMELO. Now aledesl com t/lokairy litpls-okict com
Abisarty Logo
Typo andi I finenmaling
for rixpnt th text inpena
Fire a prenct pextachmed
reya-probure smut. 1t.

Fake Websites

Recognizing fake websites is crucial in preventing online fraud. Look for **URL traps** and deceptive practices that can easily lead to data theft and malware.

How Social Engineering Works

Social engineering exploits **human psychology** to manipulate individuals into divulging confidential information. It leverages emotions like fear, urgency, and trust to achieve its aims.



Spear Phishing

Spear phishing targets specific individuals or organizations, using personalized tactics to deceive victims. These attacks often involve custom emails that appear legitimate, making them more dangerous.

Business Email Compromise

Business Email Compromise (BEC) is a sophisticated scam where attackers impersonate executives to defraud organizations through deceitful emails, often leading to significant financial losses.

Ransomware Threats

Ransomware delivered through phishing attacks can **encrypt critical files**, demanding payment for access. Understanding this risk is essential for protecting personal and organizational data from malicious actors.

Best Practices

Staying safe online requires vigilance and proactive measures. Familiarize yourself with essential practices to protect against phishing and ensure your digital security effectively.

CHECKLIST
Verify URLs
Reace larant the consefr iryed ityars and actiiynors us for hera arpenvery aducasty.
Manuees 4n stom
Caldan gundslaige srress uber afer to uckest svirces or safes, inyers-uen a forn. cnviping acturting.
Enable & Factuber
Rrecvio andrelltailrytaciogrant anf perted eift vence wih dites to reglaser nour wark and yay pelder visiltms.
Eigallert Supicautton
Onemonikig-ace perfectars.fo artohoo y tyli frrn do unielopesrate a aprotrance gnoderparveraderlfit.
Regularry & software
Can fotillists asd mouse is are chippeer implegence whange or ancyewewar'z undacsment, forole te'jordens.

What to Do

If you clicked on a suspicious link, it's crucial to take immediate action to **protect your information** and minimize potential damage.

Interactive Quiz

SCENARIO QUESTION 1

An email claims you've won a prize. What should you do first?

SCENARIO QUESTION 3

A link directs you to a login page that looks familiar. How do you verify?

SCENARIO QUESTION 5

A colleague asks for sensitive information via email. What is your next step?

SCENARIO QUESTION 2

You receive a call asking for your bank details. What action is best?

SCENARIO QUESTION 4

You see a message with urgent language demanding immediate action. What’s your response?

SCENARIO QUESTION 6

You clicked a suspicious link. What should you do immediately to stay safe?

Key Takeaways

Understanding phishing is vital for **staying safe online**. Remember to stop, think, and verify communications, as awareness and reporting are crucial in combating cyber threats.

Report Cybercrime

It's essential to report any cybercrime incidents to protect yourself and others. Utilize the official channels for assistance and guidance in handling these threats effectively.

THANK YOU

Stay Safe Online

Mandar Kajbaje