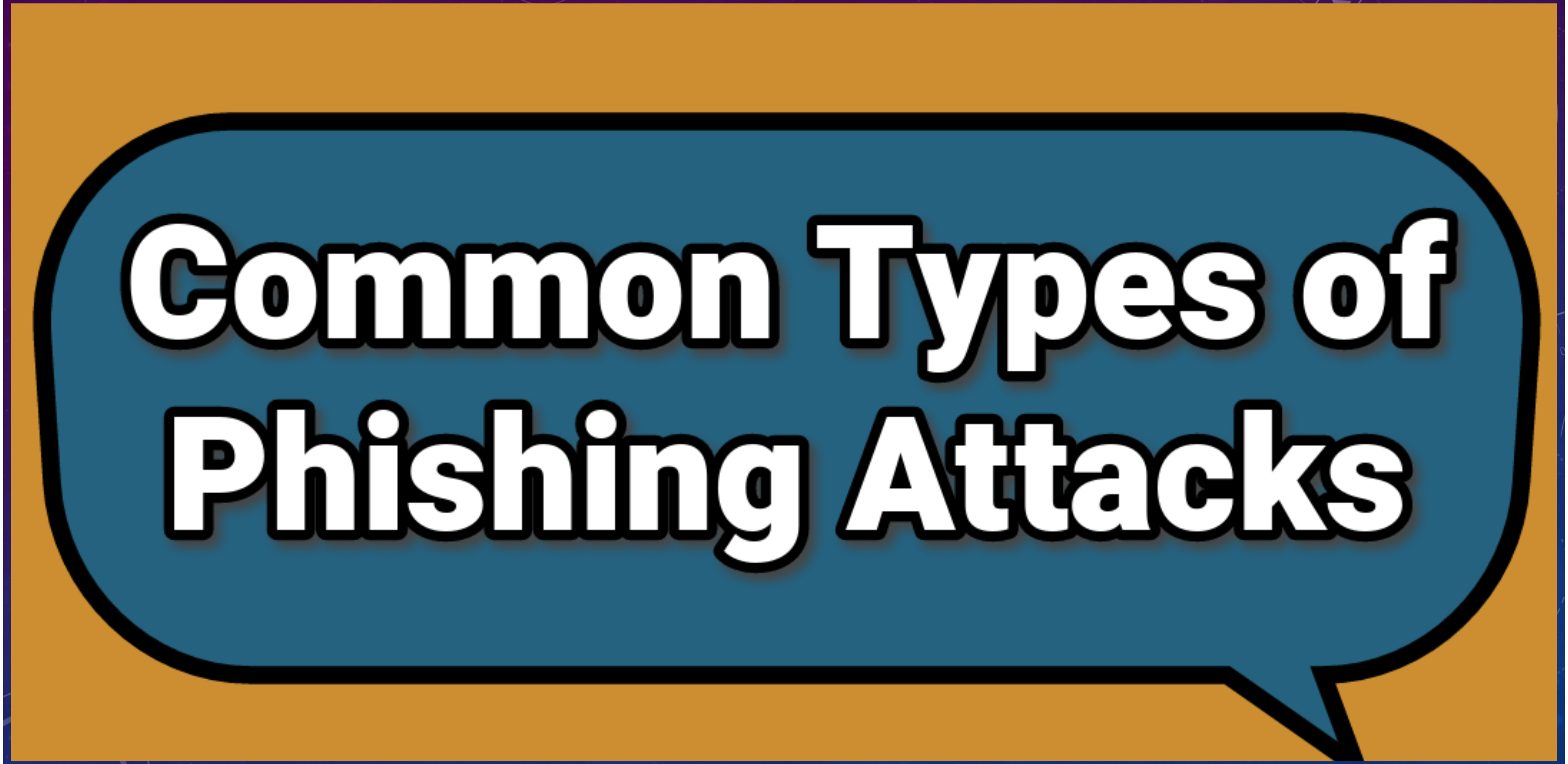
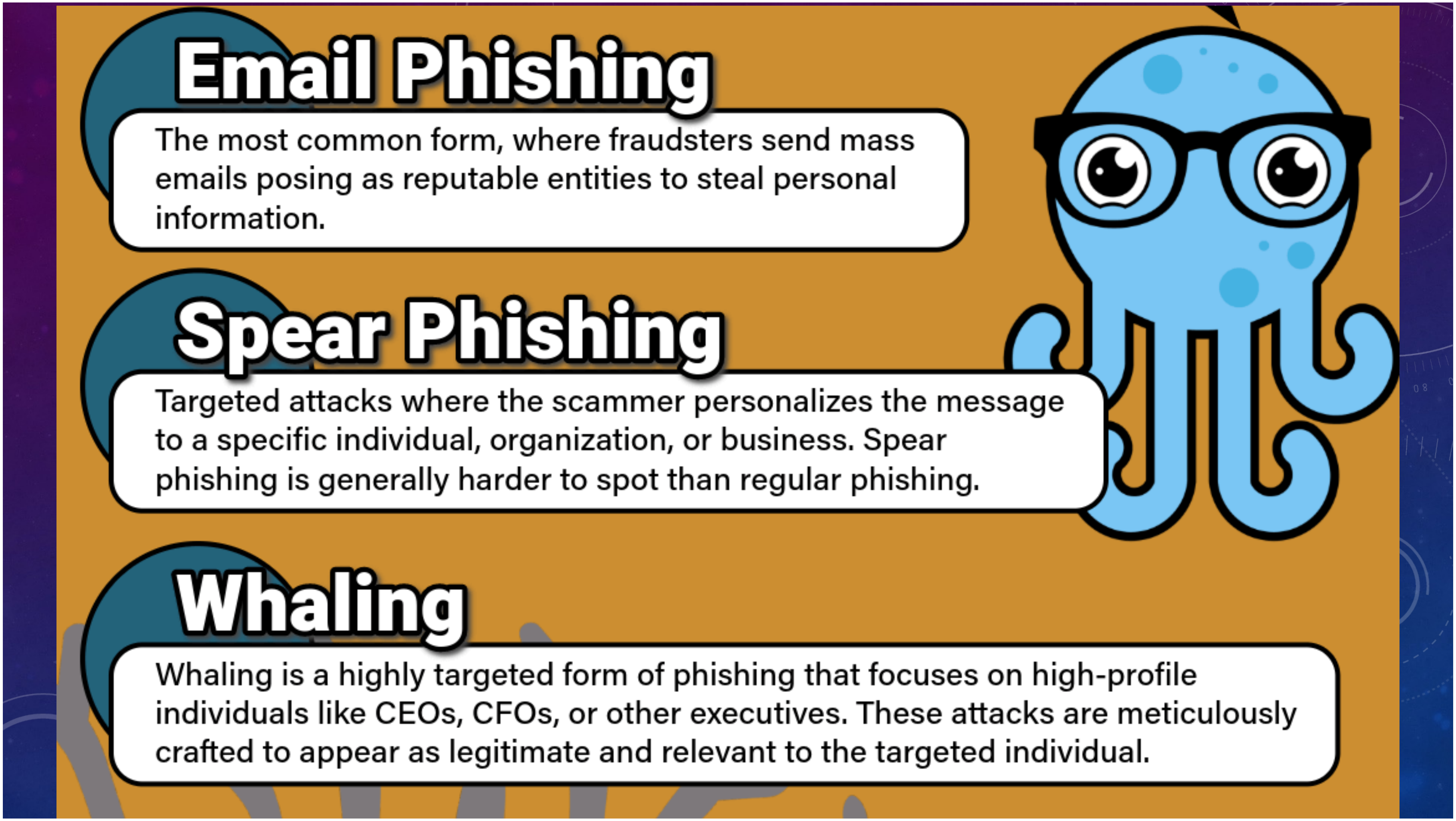
STAYSAFEONLINE.ORG


Common Types of
Phishing Attacks



Email Phishing

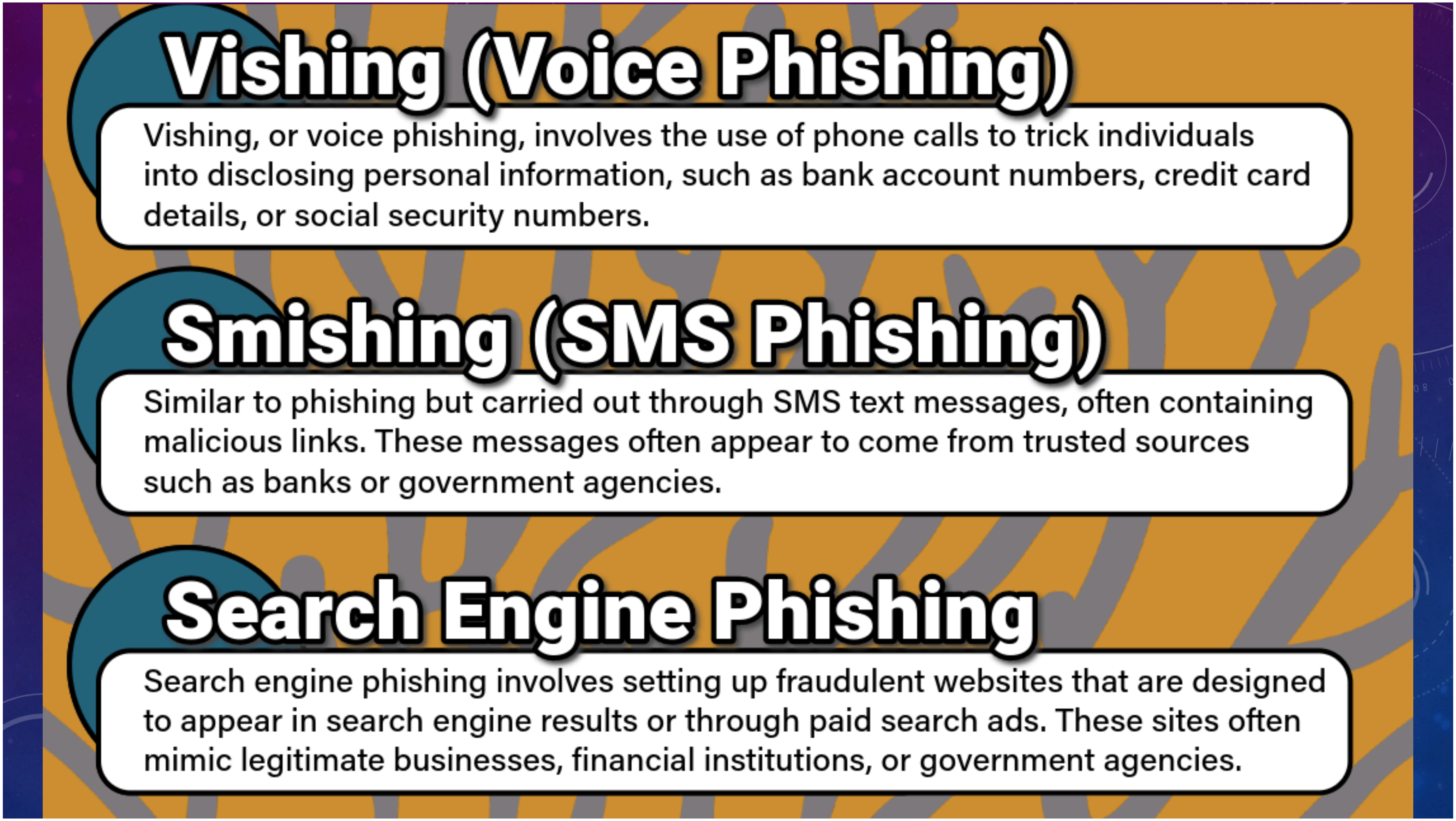
The most common form, where fraudsters send mass emails posing as reputable entities to steal personal information.

Spear Phishing

Targeted attacks where the scammer personalizes the message to a specific individual, organization, or business. Spear phishing is generally harder to spot than regular phishing.

Whaling

Whaling is a highly targeted form of phishing that focuses on high-profile individuals like CEOs, CFOs, or other executives. These attacks are meticulously crafted to appear as legitimate and relevant to the targeted individual.



Vishing (Voice Phishing)

Vishing, or voice phishing, involves the use of phone calls to trick individuals into disclosing personal information, such as bank account numbers, credit card details, or social security numbers.

Smishing (SMS Phishing)

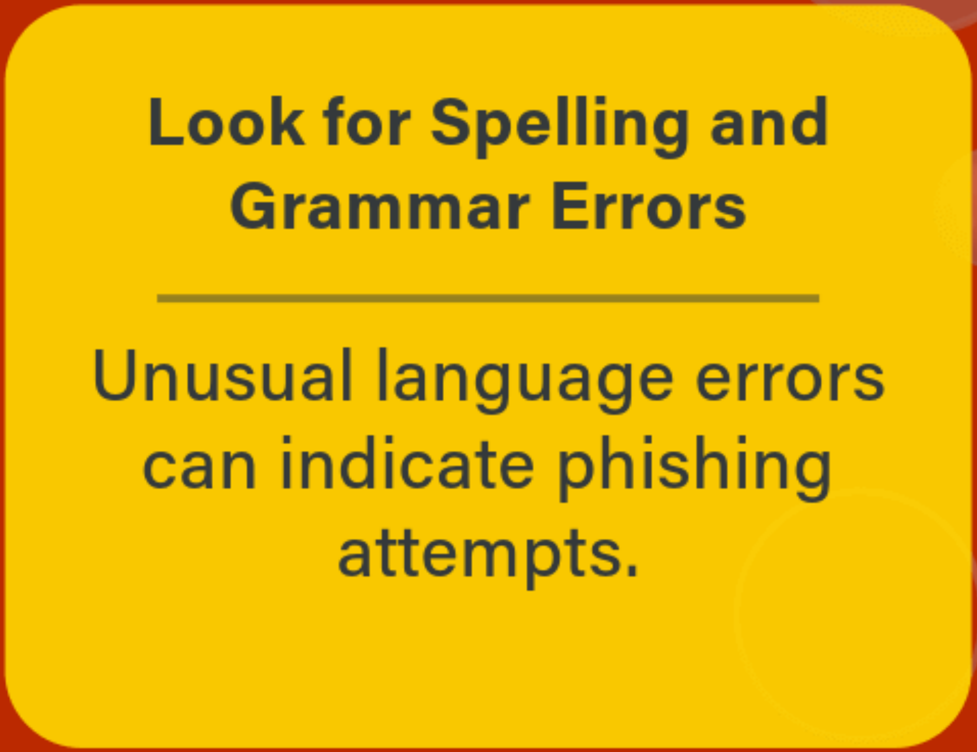
Similar to phishing but carried out through SMS text messages, often containing malicious links. These messages often appear to come from trusted sources such as banks or government agencies.

Search Engine Phishing

Search engine phishing involves setting up fraudulent websites that are designed to appear in search engine results or through paid search ads. These sites often mimic legitimate businesses, financial institutions, or government agencies.

Learn How to Spot the Phish!

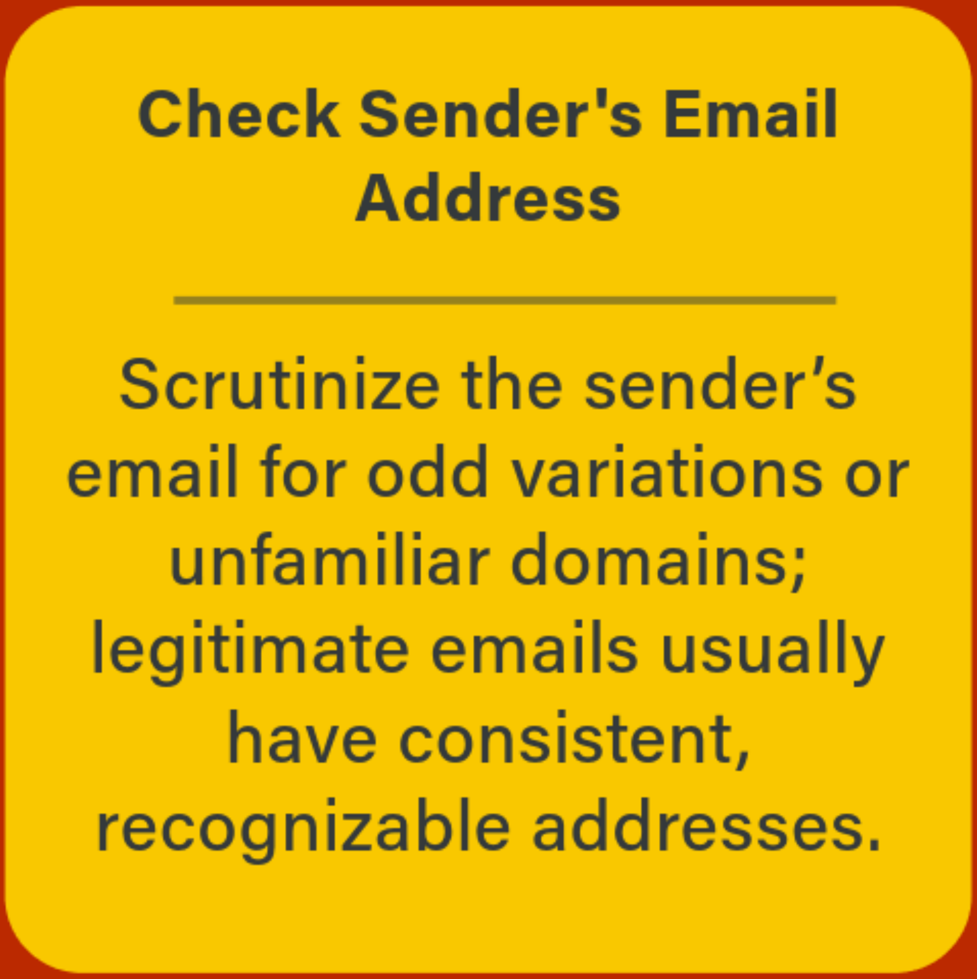
Learn How to Spot the Phish!



Look for Spelling and Grammar Errors

Unusual language errors can indicate phishing attempts.

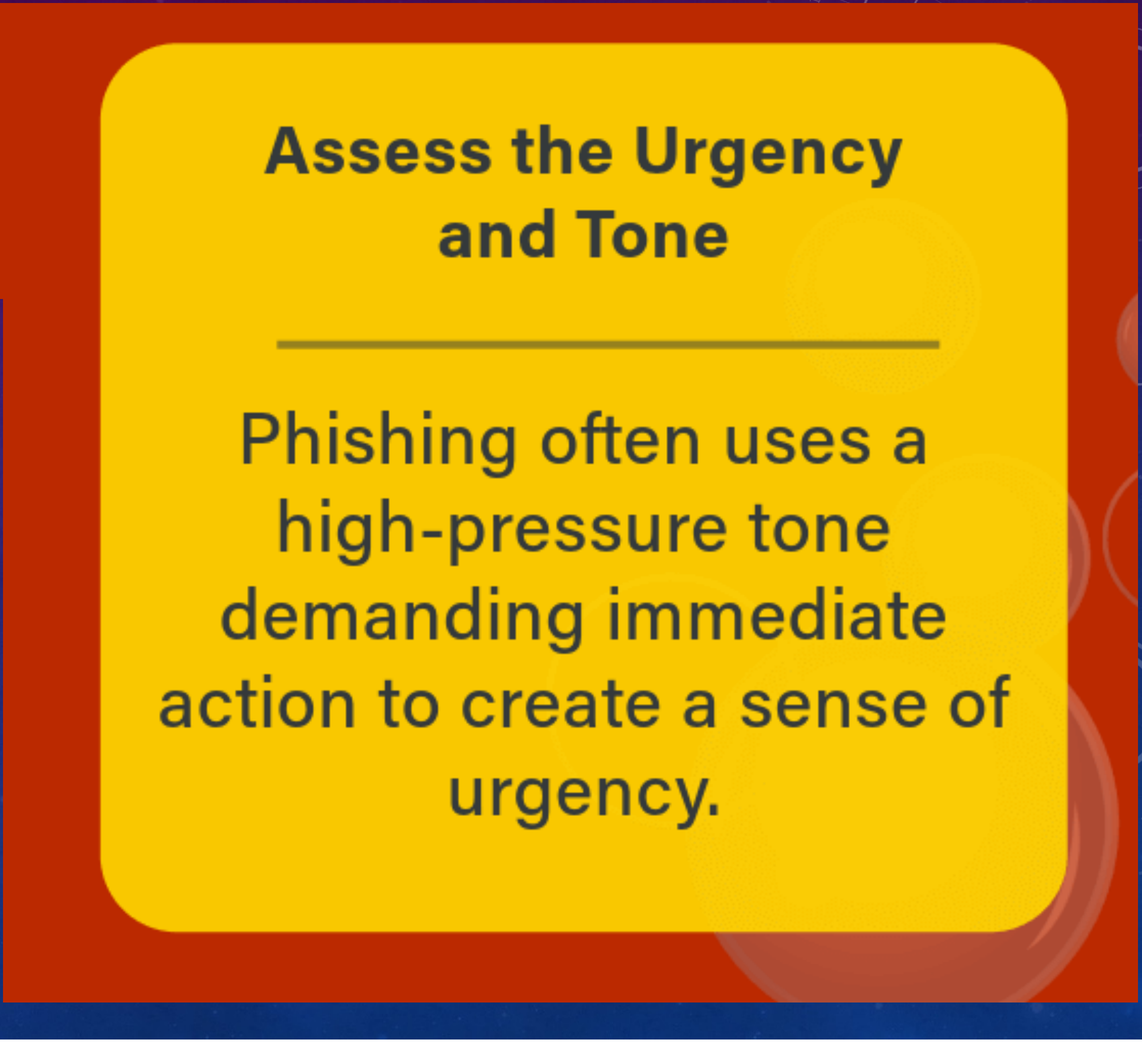
Learn How to Spot the Phish!



Check Sender's Email Address

Scrutinize the sender’s email for odd variations or unfamiliar domains; legitimate emails usually have consistent, recognizable addresses.

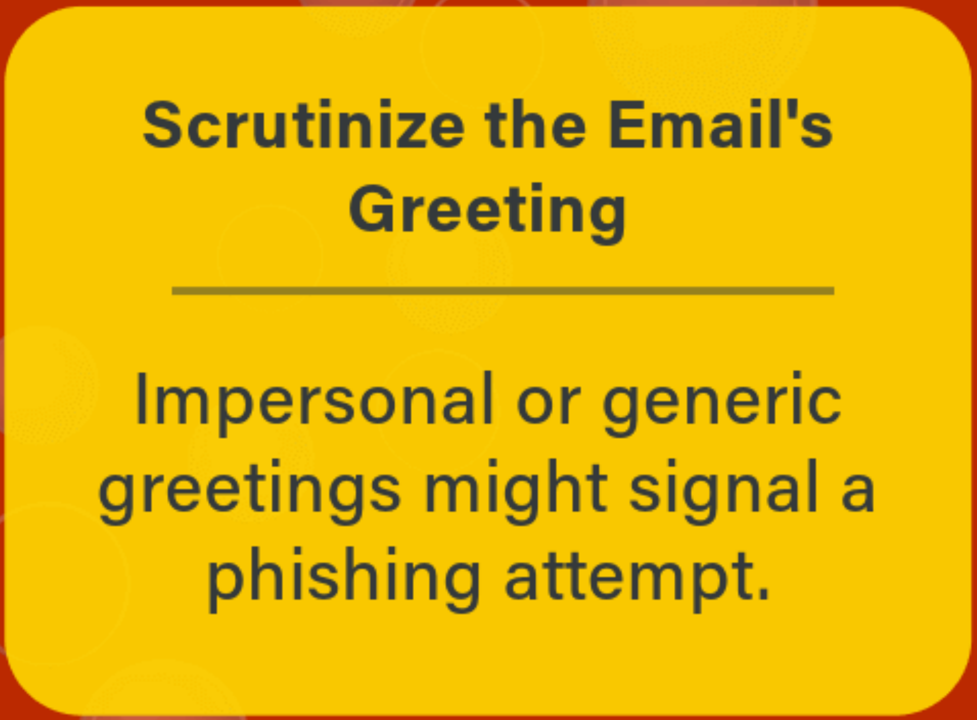
Learn How to Spot the Phish!



Assess the Urgency and Tone

Phishing often uses a high-pressure tone demanding immediate action to create a sense of urgency.

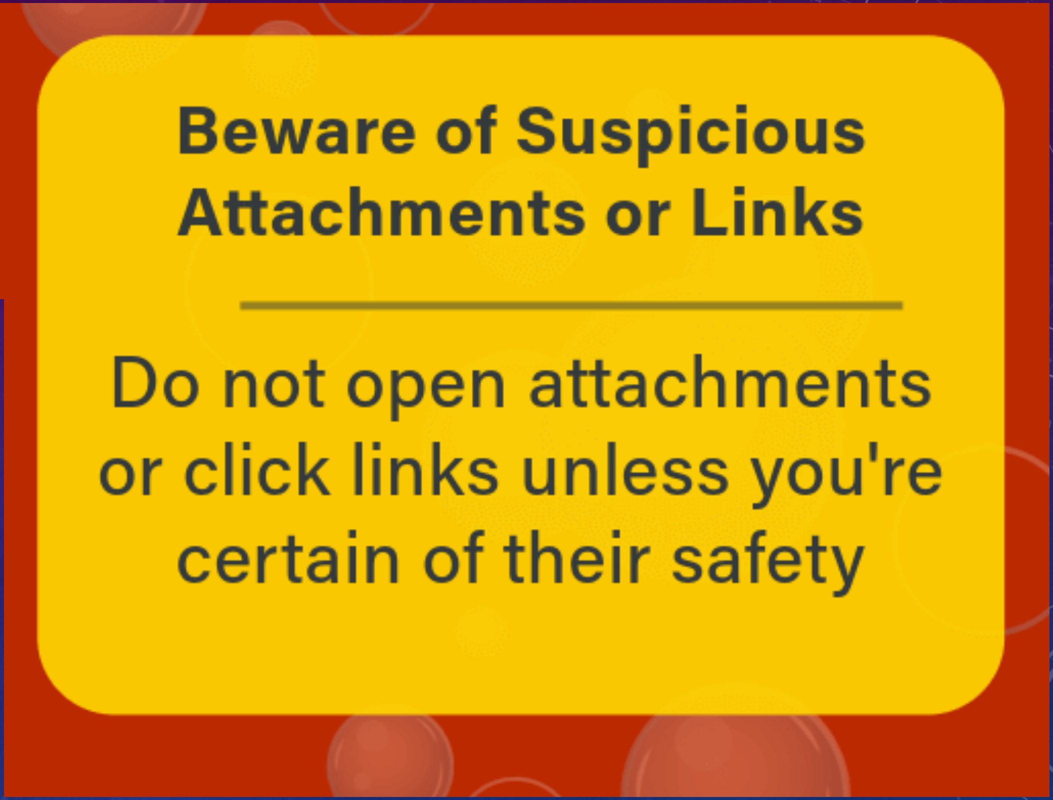
Learn How to Spot the Phish!



Scrutinize the Email's Greeting

Impersonal or generic greetings might signal a phishing attempt.

Learn How to Spot the Phish!



Beware of Suspicious Attachments or Links

Do not open attachments or click links unless you're certain of their safety

THESE SLIDES

Always Use Multi-Factor Authentication

Enable MFA for stronger, layered protection against unauthorized access to your accounts.

AI Doesn't Keep Secrets

Large language models (like ChatGPT) are powerful tools, but remember, they're not secret keepers. Avoid sharing sensitive, personal or company information.

Always verify caller identity and never share sensitive information over unsolicited calls. If in doubt, end the call.

CISA.GOV/
SECURE-OUR-WORLD

RECOGNIZE & REPORT PHISHING

Phishing often tries to get us to open a harmful attachment or share personal information. Learn what to look for to avoid the "phish hook."

USE STRONG PASSWORDS

Using strong passwords and a password manager are some easy ways to protect ourselves from someone logging into an account and stealing data or money.

TURN ON MFA

Multifactor authentication means using more than a password to access an app or account. With MFA, we might be asked to enter a text code or use a fingerprint. It makes us much safer from someone accessing our accounts.

UPDATE SOFTWARE

Don't delay software updates. Flaws in software can give criminals access to files or accounts. Programmers fix these flaws as soon as they can, but we must install updates for the latest protection!