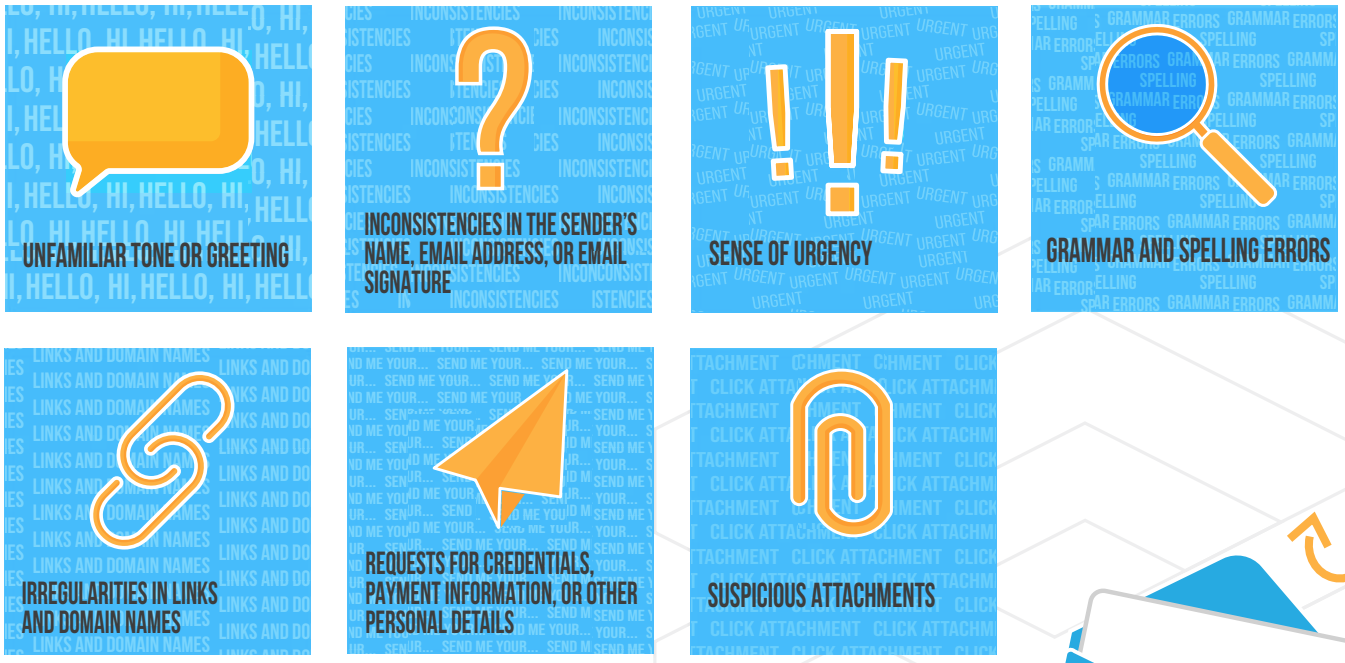
WHAT IS PHISHING?

# HOW TO SPOT A PHISHING EMAIL

Phishing is a form of cybercrime where hackers gain access to sensitive information by impersonating an account or person that already has access to data. They usually do this by sending a link that requires you to input confidential data (such as passwords, access codes, bank information, or direct computer access). This can result in a massive data breach and financial loss for the organization.

Cybercriminals use social engineering and other highly sophisticated tactics to manipulate people into giving up a wide range of personal information. In spear phishing, hackers thoroughly research and personalize communications to a targeted person or group to make it look more legitimate. They can even impersonate a close friend or coworker and send you communications that otherwise seem harmless.

## COMMON SIGNS OF PHISHING




## HOW TO HANDLE PHISHING EMAILS

- Review the display name, email address, and links for inconsistencies.
- Hover your mouse over links before clicking to examine where the link is taking you. If there's any doubt, don't click.
- Double-check any urgent requests. People are less likely to notice the small details in a situation that causes concern, worry, or time constraint.
- Do not open any suspicious or unexpected attachments, even if they appear to be from someone you know.
- Without replying to the email, check with the sender separately to confirm the validity of the request.
- Never give out personal info to unverified sources. Legitimate companies will never ask you for your login information or other sensitive data through email.
- When in doubt, report the suspicious email or incident to your IT/SOC Team immediately.