Secure NOC

In recent years, phishing and social engineering attacks have continued to rise as cyber criminals refine strategies and execute successful phishing campaigns. Attackers are taking advantage of end users in order to steal credentials or take over their computer. The majority of data breach cyber-attacks are a result of a successful phishing email scam.

Phishing

Phishing is a form of social engineering that uses legitimate-looking email or fraudulent websites to encourage users to give up personal data or information, such as social security number, credit card numbers, passwords, etc. It is an attempt to acquire sensitive information about you and could lead to identity theft.

Phishing emails are typically sent to a large group of individuals that appear to come from trusted Web sites, like a bank, credit card company, social networking site, or an online store. Phishing messages often tell a story and attempt to trick you into clicking on a link or opening an attachment.

Types of Phishing

Spear Phishing: Targeted, sophisticated phishing messages personalized to victims. Spear phishers learn about the victim by spying on their personal email, social media and other online habits. The perpetrators use the information they have gathered to portray themselves as a legitimate entity and will create tailored messages to your interests in order to steal personal information such as your NOC username and password.

Vishing: Phishing conducted over the phone by scammers portraying as a trustworthy entity in an attempt to convince the target to take action.

Smishing: Phishing conducted via SMS text messages. Smishing is a security attack in which the user is tricked into downloading malware onto their smart phone or device.

Business Email Compromise: Form of phishing attack where a criminal impersonates a person of authority such as an executive, president, supervisor, dean, etc. The scammer attempts to get an employee or vendor to transfer funds or sensitive information.

Learn to Spot Phish

Although identifying phishing emails can be difficult, there are indicators that if spotted, can help to prevent an account compromise or identity theft. It can be helpful to focus on one part of an email at a time. Each part offers its own set of clues and questions to ask.

Analyze the Sender Details: Who sent the email and when was it sent? Was this message expected? Would this person typically send an email like this?

- *Confirm the Sender's Identity*: The display name of the sender can be spoofed to look like a legitimate person or organization. Hover over the name or double click the email name to view the actual email address.
- *View the date and time of the message*: Is it ordinary for this person to be sending this type of message at this time?

Analyze the Context: What is the purpose of the email? Is it personalized?

- *Beware of Urgent Subject Lines*: Invoking a sense of urgency or fear is a common phishing tactic used by scammers. Be cautious of subject lines and message content that invoke a sense of urgency or fear.
- *Look Out for Generic Salutations*: If the message is from a supposed familiar source, but contains a generic greeting and signature, it could be a sign of a phish.

Analyze the Content: What is the tone of the email? Does the message contain a call to action?

- *Think Before you Click*: Don't click on links or download attachments from unknown sources, especially when they're unexpected. While a website address might look perfectly valid, hover your cursor above the link and a different URL address may display altogether.
- *Trust Your Instincts*: If you receive an unexpected email from a seemingly trustworthy source that seems out of character, don't respond to the email. Instead, reach out directly to the individual through a trusted channel to confirm the message. Never respond directly to a suspicious email.