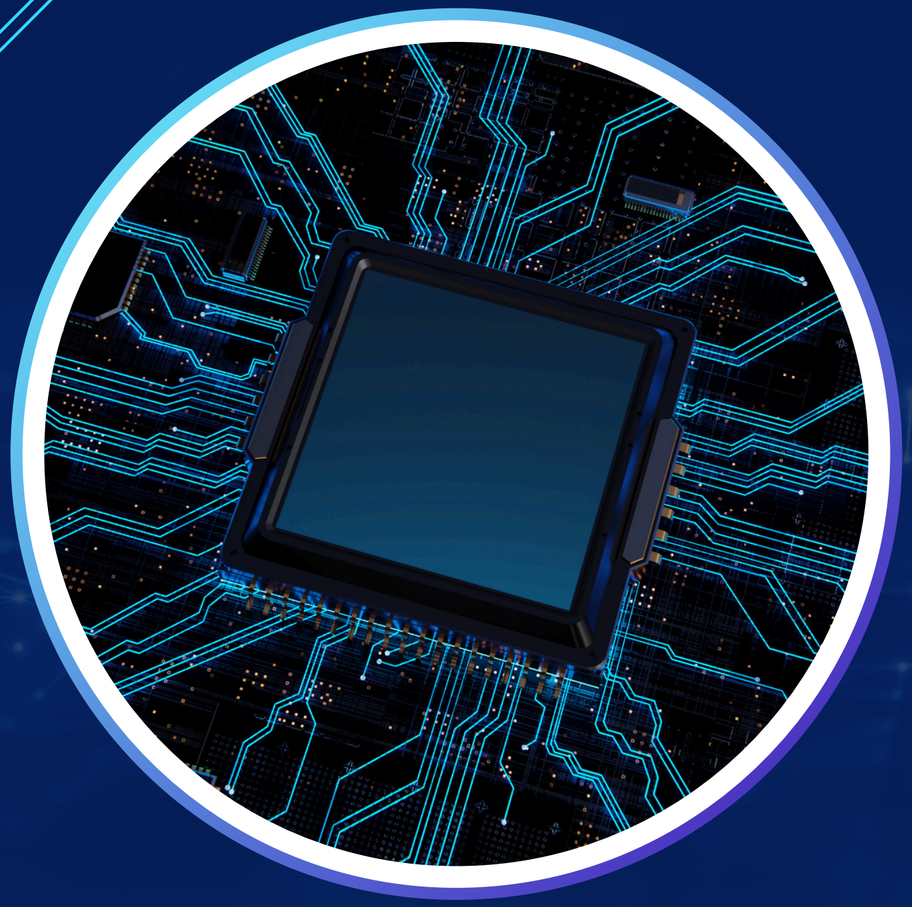
PHISHING AWARENESS

Affaf Arif



WHAT IS PHISHING?

Phishing is a type of cybercrime where malicious attackers try to scam individuals into providing sensitive data, such as usernames, passwords, and credit card numbers. They can also install malware such as viruses and worms. This is usually done by disguising themselves as legitimate institutions via electronic communications.

TYPES OF PHISHING

Email Phishing

Attackers send emails that appear to come from reliable sources, such as banks, online stores, or other genuine organizations like . These emails often contain a link to a fake website whose domain mimics the geniune one, where the victim is prompted to enter their credentials.

Spear phishing

It is an advanced and highly targeted form of phishing where the attackers aim at specific individuals, businesses, or organizations. They find the victim’s information from public sources like social media and corporate websites, or from other nefarious methods and use that information to appear more convincing and legitimate.

Smishing

It is also known as SMS phishing. Attackers can use messaging platforms to deceive individuals. They send messages that appear to come from sources such as banks or customer support of online retailers to trick people into sending money or sharing sensitive information.

Clone Phishing

The attackers create a copy of an already existing email received by the victim and change the link or website attached in it to a malicious one. They do so by sending the email to the victim and making it appear as if it was resent or updating by the original source. The malicious links can download malware into the victim’s device.

Angler Phishing

It is a very common type of phishing done through social media. It is done on platforms like Facebook, Instagram, and Twitter. The attacker pretends to be a trusted source like an old friend or family member to deceive the victim. They can also impersonate the social media of organizations and pretend to have marketing schemes to get personal details of victims.

PROTECTION AGAINST PHISHING

- Download Anti-spam softwares and browser extensions.
- Check the Hyperlink to find out the real URL before clicking on any website.
- Verify email sources such as banks by calling the comany to confirm before replying to them.
- Avoid sharing personal information such as passwords and banking details.
- Use secure and complex passwords by the help of authenticated password managers.
- Do not trust alarming messages from unknown sources.

SOCIAL ENGINEERING TACTICS