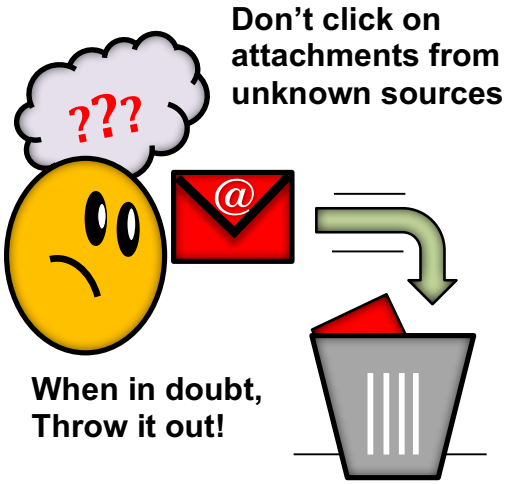
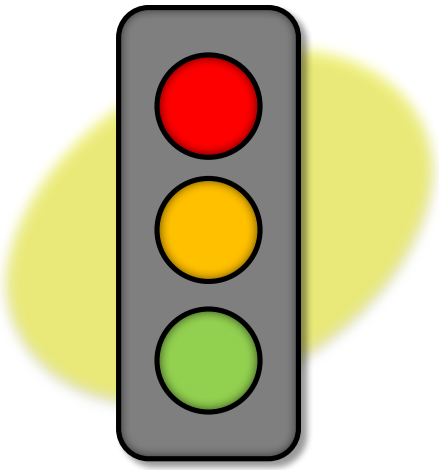
Protect yourself

Cybercriminals may send you email that looks like it is coming from legitimate institutions, businesses and individuals you may know.

If you are unsure whether an email request is legitimate, consider contacting the institution, business or individual. Use information on an account statement or search for the company online but don't use the contact information provided in the suspicious email.

Be careful of emails asking you to act immediately, especially if something sounds too good to be true. Think before taking any action.





Stop and Think before you Click!

Keep in mind that you could compromise your computer system and any personal or business information stored in it. Not all websites are safe to use.

Potential Risks

- Identity theft
- Sensitive data loss
- Financial loss

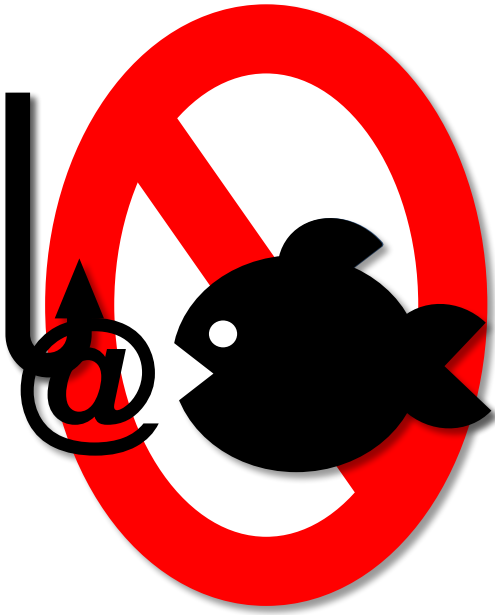
To avoid potential risks, be cautious and take your time to review the website before taking any action.

Be Aware, Be Safe!

IEEE IT Security

Cybersecurity Awareness

Protect Yourself



Avoid getting HOOKED!

IEEE IT Security

Social Engineering Attacks

These attacks manipulate human interactions and our natural tendency to trust in order to gain access to confidential information (ex. usernames, passwords or bank information, etc.) for fraudulent or malicious activities.

Common Methods

Phishing - The attacker uses email, IM or other communication channels to impersonate a reputable person or organization to gain access to login credentials or account information.

ViShing - The attacker pretends to be a legitimate business and uses telephone conversations to attempt to scam the victim in order to gain access to information that will be used for identity theft.

SMishing – The attacker uses mobile text messages to lure the victim into calling back a fraudulent number, access a malicious website or download malicious content.

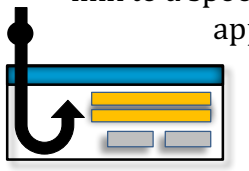
WARNING

- Don't click on links or attachments received from unknown senders
- When verifying the sender, do not use the information in the suspicious email
- Be careful of how much information you share on social media sites
- Don't assume a caller is genuine because they know about you or your company - If suspicious, terminate the call

How Phishing Works

The Bait

Email from the attacker encourages end user to follow a link to a spoofed web site that appears to be legitimate.



The Hook

A website controlled by the attacker that appears legitimate asking the victim to disclose information such as userid and password.

Use Strong Passwords

Use combinations of upper and lower case letters, numbers and Symbols

Weak: Webster
Strong: W3b$t3r
Stronger: A phras3 1s 3v3n Str0ng3r

Consider making your password a phrase: A phrase can be used to create a strong password. Consider using at least 12 characters. Use phrases that are easy to remember but hard for someone else to guess.

Use unique accounts & passwords: Using different passwords for every account helps to thwart attackers. At a minimum, separate your work and personal accounts. Make sure that your critical accounts have the strongest passwords.

If you write it down then keep it safe: Store your list in a safe, secure place away from your computer. You can consider using a password manager application to keep it safe and track your passwords.