



Th[💡]ink Before
you Cl[👇]ick



PHISHING EMAIL

A technique used to obtain sensitive data such as usernames, passwords, credit card information ect.

BE-AWARE

DO NOT

- Open links or attachments from unknown senders.
- Never "unsubscribe" from spam email as this just validates your email address.
- Avoid clicking on pop-ups, even to close them. Instead, close pop-ups by pressing Alt + F4 from the keyboard.
- Avoid questionable websites
- Access website by entering the URL in the browser rather than clicking on a link itself.



Suspect You've Received a Phishing Email



Immediately report any suspicious emails to

HelpDesk@SecLexISC.com



WATCHING FOR PHISHING

Phishing Emails Usually

Have a sense of urgency prompting you to provide sensitive information such as passwords, usernames, credit card information etc.

Asking you to click on an attachment or links that will redirect you

