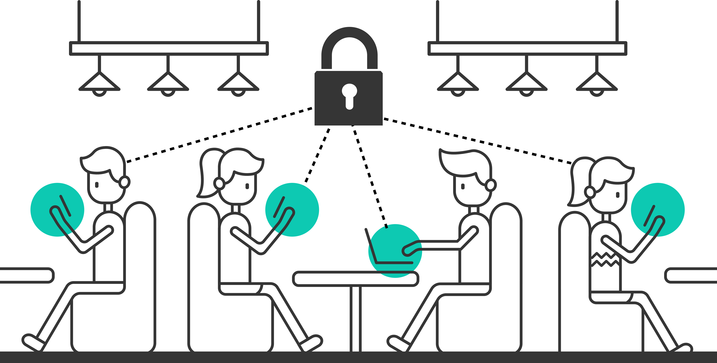

Don't Get Caught in the Net

Phishing threats are real and everyone is a target!

With the increase in phishing attempts, it is crucial to take proactive measures to help protect yourself and LSUA's security.

Below are quick tips for how to spot and handle phishing emails.

Everyone is Responsible

- LSUA students, faculty, and staff should take security precautions and understand the potential consequences of online actions and behaviors as they enjoy the benefits of the internet.
- Every user of the LSUA system is responsible for the security of their data and helping to protect the integrity of the system.
- Every user has an impact on the security of every other user of the LSUA network.
- IET is responsible for implementing and maintaining network security infrastructure.

What is Phishing?

- Phishing is an attempt by malicious actors pretending to be a legitimate enterprise for the purpose of stealing private information, such as usernames and passwords, social security numbers, date of birth, and banking information.

Why should you care about Phishing?

Any organization with personally identifiable information is a target for a phishing campaign.

Phishing attacks can turn into identify theft if a user fall for the trap.

$1.6M is the average amount lost in a successful spear phishing attempt.

Email Security

- Email is the top method for phishing attacks. Below are the best email security practices.

Create a strong password.

- Creating a strong password is key to protecting your personal information at LSUA. Be sure to use different passwords for your accounts.
- Use a variety of characters including numbers, upper case letters, lower case letters, and special characters.
- Use passphrases.

  For example:

  "I saw George the Bear at LSUA in 2014" translates to the passpharase:

  iSgtB@LSUAi2014

Keep your security and computer software up to date.

- Software updates frequently include patches for newly discovered security vulnerabilities that could be exploited by cyber-attackers.
- LSUA IET Services manages the software updates for Windows, Symantec, Office, and etc. from the server-side.

Use caution with email attachments.

- Never open or download an attachment from an unknown source. Attachments may contain viruses that can compromise your computer and personal information.
- If an attachment requests you to enable macros, please do not enable them until you are sure that the attachment is legitimate.

Never send personal information such as passwords, social security numbers, or credit card numbers via email. Email should not be treated as a secure communication channel for sensitive data.

Never reply to any email from an unknown source.

How to Spot Fake Emails

- The "from user" and email address does not match.
- Sense of urgency.
- Incorrect capitalization.
- Strange requests.
- Bad spelling and grammar.
- Odd time to receive an email from the spoofed user.
- Vague naming (Client, Employee, Admin, User)
- Link and URL does not match.

REFERENCES

https://iatraining.disa.mil/eta/disa_sn_v21_fy17/launchPage.htm
https://www.risk3sixty.com/2015/01/26/designing_an_effective_information_security_training
https://www.businessnewsdaily.com/10763-free-infosec-resources.html
https://us.norton.com/internetsecurity-malware.html
https://www.lsu.edu/it_services/its_security/announcements.php
https://www.lsu.edu/it_services/its_security/phishatLSU.php

LSUA