Check It Before You Click It - Phishing, Malicious Links & Spoofed Headers

Table of Contents:

Related Links:

LSU Security Awareness

LSU Email Overview

What is Phishing?

The word "Phishing" is a variant of the word "fishing." It generally comes

from an analogy of spammers sending many emails (casting a wide fishing net) in hopes of catching a user (the fish). Though many users don't fall victim to the scams, it only takes a few to make it successful.

What is the point of phishing?

"*Phishers" typically attempt to steal information from you. This information includes (but isn't limited to) MyLSU ID and password, email login information, banking information, and more. Attackers can use this information for different reasons including gaining privileged access to LSU's network, sending malicious spam from your email account, stealing sensitive personal information, etc. Your financial/banking information could be used steal your identity, pilfer funds from your account, send money out of the country, and more.*

Check It Before You Click It

Most **phishing scams** can be avoided by sticking to these basic principles:

1. Log in with your **myLSU account ID** at official lsu.edu sites *ONLY* & pages such as my.lsu.edu and tigerware.lsu.edu.

2. *Never* provide your password or other sensitive information in an email message.

- **You** are responsible for your MyLSU ID. *DO NOT* share your MyLSU password with *ANYONE for ANY REASON*.
- Email is *NOT* a secure way to send out personal information. ALL email messages can be intercepted when they is sent, and email messages are *NOT* encrypted or protected by default.
- If an attacker gains access to your email account, *ALL* of the sensitive information stored there will be accessible to the attacker.

3. Be suspicious of messages such as these:

- You are urged to take "*Immediate Action*", there is a *sense of urgency*, or you are threatened that your account will be shut down.
- Claim that your email inbox is *Full* or *near its quota* and needs to be upgraded.
- Claim that you must login to enable security features or other services.

Phishing Messages often mask a malicious site to look like an official LSU page. This can trick users into believing they are visiting a legitimate site. For this reason you shouldn't automatically trust what you see in email messages. Text links that appear as one link but lead to another should be treated as highly suspicious.

LSU ITS has recently instituted Safe Links to circumvent malicious URLs in emails.

More information for Office 365, OWA, OS X Mac Mail, and iOS users can be found at the following link:

Safe Links

Spoofed Headers - Faking the From: Field

There is a belief that if an email says it is from an account, like *webmaster@lsu.edu*, then it must actually be from webmaster@lsu.edu. The unfortunate reality is that the "**From**:" field can be easily faked to appear as any account or person. This is commonly referred to as "**spoofing**".

In the phishing examples above, the message says it is from LSU, however it also provides an email address of *help@it.net*. While that email address could be an instant indicator that LSU *DID NOT* send the message, keep in mind

that even the email address can be spoofed to show *servicedesk@lsu.edu* or *webmaster@lsu.edu*.

If you are not sure about an email message's legitimacy:

Send an email to the *servicedesk@lsu.edu*. Include the following information:

- The **Original Message**.
- The email message's **Full Header Information** which ***is** necessary **for ITS to determine if the email message was spoofed or not***.
- How to obtain the Full Header Information?

Reporting Phishing Attempts & Additional Security Information

The LSU IT Security and Policy (ITSP) Team has deployed Cofense Reporter, an application that provides users the ability to report suspicious e-mails to the ITSP team quickly and efficiently. The application is available for all @lsu.edu mailboxes automatically. For more information on how to use this utility, click here.

There are numerous kinds of phishing attempts and other scams targeting users, many of which LSU cannot take any action on. However here are a few cases where we recommend you contact *security@lsu.edu*:

- You have a phishing message that contains malicious links.
- You clicked on a link or responded with personal information to a potential email scam and need help determining what to do.
- You have a scam message you believe came from another LSU user.

As long as you do not click on any malicious links or respond to the email with personal information, you as well as your computer should not be at risk.

Junk, spam, or suspicious emails in LSUMail can be reported directly from your mailbox in OWA or Outlook.

- To learn how to mark an email as junk, please visit GROK article 17521.
- To learn how to report suspicious emails or phishing, please visit GROK article 19636.

As always, if you have any concerns or comments please feel free to email the **LSU IT Security & Policy Office** with any of your questions via *security@lsu.edu*.