EASTERN ILLINOIS UNIVERSITY™ Business Office Operation Support Services

Don’t fall Victim to Phishing Scams (a message from ITS)

Phishing attacks are an everyday phenomenon for campus email recipients at Eastern, but becoming a victim of a phishing scam is something that never has to happen. "It's very common," said Information Technology Services’ Assistant Director of Information Security Mike Gioia. "It's a daily occurrence, and it’s growing worldwide. The most important way to combat it is for email users to identify attempts and report them to the Help Desk (581-HELP) or Information Security (581-1942)."

Avoid Phishing Scams

Phishing scams continue to target university email accounts. Everyone needs to be on the lookout for suspicious emails asking for username and password information. It only takes one or two people to fall victim to a phishing scam to negatively affect the delivery of EIU email.

How to identify phishing scams

Here are a few questions to ask to help identify phishing scams:

■ Have I given this person/company my email address before?

If not, there is a good chance this is a phishing scam!

■ Is the TO: line address to a large number of people or undisclosed-recipients?

Most business and organizations that you have dealt with in the past will address an email to your email address. If you receive an email asking for confidential or personal information, and the TO: address contains a large number of recipients, or is even undisclosed, the email is almost always a scam.

■ Is the FROM: line your own email address?

Unless you forgot your own personal information and need to ask yourself, this is a scam.

■ Is there an attachment you were not expecting?

Almost all attachments sent by people or organizations you do not know contain viruses that can steal your personal information.

Phishing is a subterfuge used to extract personal financial information from victims. Any email account holder can become a target. Phishers obtain email addresses, and then send messages to individual recipients purporting to be from a financial institution, Internet service provider or other authority requesting account passwords or personal identification or data that can give them access to the victim's bank accounts, credit cards or other personal records.

Phishing has existed almost as long as email and the Internet, and most people are aware of it, but that doesn't mean they can't be victimized. "Technology has come so far along that the easiest target of a hacker is human as opposed to a security flaw, so they use manipulation to trick people into giving up sensitive information,” Gioia said. This is known as "spearphishing" — a scam targeted at a specific user rather than broadcast toward a multitude of them.

For example, phishers targeting email users at Eastern may customize their message with the words "Help Desk" or "Panthermail" to make it seem authentic to email users at Eastern. Or they may attach a logo from a local bank or utility, all to lull the potential victim into a false sense of security.

Email account holders at Eastern should be aware: ITS will never ask them for their password or other personal information in an email. The authenticity of any email purporting to be from ITS or to be an official university email can be verified at http://its.eiu.edu/email_verification.php

Responding to a phishing email not only can cost the victim, it can also lead to the compromise of other campus accounts, too. That can occur because giving a phisher access to your account also exposes the victim's email address book, enabling the phisher to then send scam emails to all of those people, too.

"If someone's account is compromised by a phishing attack, they can spam the Eastern network," said Gioia. Further, it could allow the phisher to potentially access sensitive university account information. "It's always a tremendous risk. If someone has sensitive information and they get phished, it could cause a security breach."

The Anti-Phishing Working Group (APWG) is an international consortium that brings together businesses affected by phishing attacks, security products and services companies, law enforcement agencies, government agencies, trade association, regional international treaty organizations and communications companies. It notes:

- Be suspicious of any email with urgent requests for personal financial information.
- Phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately.
- They typically ask for information such as usernames, passwords, credit card numbers, Social Security numbers, dates of birth, etc.
- Phisher emails are typically not personalized, but they can be. Valid messages from your bank or e-commerce company generally are personalized, but always call to check if you are unsure.
- Don't use the links in an email, instant message or chat to get to any Web page if you suspect the message might not be authentic or you don't know the sender or user's handle.
- Instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser.
- Avoid filling out forms in email messages that ask for personal financial information.
- You should only communicate information such as credit card numbers or account information via a secure website or the telephone.
- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser.
- Remember not all scam sites will try to show the "https://" and/or the security lock. Get in the habit of looking at the address line, too. Were you directed to PayPal? Does the address line display something different like "http://www.gotyouscammed.com/paypal/login.htm?" Be aware of where you are going.
- Regularly log in to your online accounts.
- Don't leave for as long as a month before you check each account.
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate.
- If anything is suspicious or you don't recognize the transaction, contact your bank and all card issuers.
- Ensure that your browser is up to date and security patches applied.
- Always report "phishing" or "spoofed" emails.
- When forwarding spoofed messages to security, always include the entire original email with its original header information intact.