Identifying Fraudulent Email (a.k.a. 'Phishing')

Phishing is the practice of sending falsified emails with the aim of stealing personal information such as passwords, credit cards, or other sensitive data. Since the basic format of email is highly malleable and copyable, it's relatively easy to make a message look and sound official, and since email is used for many formal and official communications, it's possible to be duped into sharing information with the wrong people, or opening your computer to attack. It's also possible though, and often fairly easy, to spot a number of things that give away the fraud.

Signs of a Spoof

Most often, scammers will first:

- Attempt to make the message appear to come from a trusted source, like Lehigh, your bank, Google Docs, Ebay, Paypal, etc.
- State or imply some amount of urgency, indicating that an account will be closed, a 'prize' will be forfeit, a legal action will be taken against you, etc.

Next, they will require some action on your part, such as:

- Reply to the email with your password, social security number, address, account number, etc.
- Click on a link to go to a web page (to 'log in' or enter other information, verify your address, etc).

Certainly, a legitimate message could do similar things. So how do you know if it's real? There are a number of things to check that can be quick giveaways:

- Fluent English? -- while the instance of poor English in scams is decreasing, it's a good indication that the person sending the message isn't an employee of a legitimate company doing business in the United States.
- Mail Domain -- while it's not hard to spoof, a lot of scams don't even bother to change their mail domain -- that bit after the '@' in their email address. All messages from legitimate Lehigh departments read '@lehigh.edu' on the end of the email address. Not '@lu.com' or '@lehigh.org' or anything else.
- Personalized -- most professional communication will be addressed to a single person, and the sender will know your name. While it's true that blanket messages are occasionally sent out by legitimate departments, they will usually specify a the name of responsible person or contact with a name and position for you to contact that can be independently verified, and communicated with via other means than offered in the email.

What Should You Do?

If you are suspicious, the most important technique is to find another route (besides information or links in the email) to verify any claims. Avoid clicking links in the email. Open a web browser yourself, and go to Lehigh's website, the bank's website, or whatever organization yourself, using your regular route to the site. Use a telephone, and call that person or organization, and ask about the email.

The second most important thing to do, if you're at all uncertain, is to report it. One thing about phishing is that you're likely not alone in receiving the message. 'Phishing' is like real fishing in that the message has been sent to many people, and the scammer is hoping that one person (or a few) out of perhaps hundreds or thousands will "take the bait." If you have strong suspicions, forward the email to the LTS Information Security Office at security@lehigh.edu or the LTS HelpDesk at helpdesk@lehigh.edu. They'll be able to examine it more closely, and notify others to be aware.

Report Phishing in Gmail

Lehigh's Gmail system makes it easy as well: With the questionable message open, select the small 'down arrow' next to the 'reply' button. In the menu, choose 'Report Phishing'.

Examples

To hone your spoof-spotting skills, and to see if your spoof has already been reported, LTS maintains a 'Rogues Gallery' of examples of phishing emails that have targeted Lehigh. How might you have spotted these as fake?

Helpful Tutorials

- How to be skeptical about email (What to look for)
- How to understand web addresses (How to tell if a link is a Lehigh link)
- Reading Email