Email Safety: Best Practices

Reading Safely

Most people are already aware, but something like 90% of the email moving on the internet is unwanted junk mail. A growing and dangerous fraction of that is actually much more dangerous, and comprises fraudulent attempts to gain illegal access to the computers we all use. This is generally called 'phishing' and can take numerous forms, but most commonly comprises an email with an urgent subject line demanding immediate action on the part of the reader. The body of the message includes a link to allow the reader to 'log in' to a server to take that action. Lehigh has a burgeoning 'rogues gallery' of examples, but all of them are essentially 'social engineering': attempts to play on one or another of users' common issues to fool them into either handing over key information like account names, passwords, credit card numbers, etc., or downloading malicious software that does that automatically, or worse.

The best defense against these threats is to be well acquainted with the organizations that you expect to send you email, and maintain a good understanding of how you would be expected to respond. The following items are helpful to keep in mind:

- No Lehigh LTS personnel will EVER ask you for your password via email.
- Real system administrators don't have to ask for passwords. They set them, and send them to you.
- Any website that asks for a Lehigh password will have a 'lehigh.edu' domain name.
- The 'From' field on an email message can be made to show whatever the sender wants it to. Digital signatures are the only practically reliable method for validating the source of an email.
- Logo graphics, and even entire website designs are easy to copy and paste from the internet. Don't let them fool you!

Writing Credibly

It may seem like another thing that anyone should 'just know', but it's far too easy to quickly send a poorly constructed note. More importantly, with the potential danger presented by the constant onslaught of scams and phishing, the people to whom you're sending that email will be doing a great deal of filtering, and may just miss it or dismiss it as fake. Either way, it's worth taking some time to review a few features that make up a good email:

- If you're sending a message to a large group (more than 10-20 people) consider using a mass-mailing program that sends your message to each user individually, and may be capable of automatically merging data about each user with the body of the message. Messages having multiple recipients or 'unspecified recipients' are more likely to be regarded as spam.
- Create a concise subject line that captures the subject of the email without being 'over the top'. Excessive use of capitalization, exclamation points, dollar signs, question marks, or inflammatory keywords increase spam ratings of messages, since creating urgency is a primary spam / scam tactic.
- Address your recipient by name. Junk mailers often do not know the actual name of the recipient, only an email address, and are unable to do this.
- Separate web links as paragraphs unto themselves, and display the entire text of the link, so that the user can easily see and evaluate the domain of the URL.
- Properly identify yourself: aAt the end of the message, Include information (possibly in a signature file) that identifies you, the organization you're with, and other means by which to contact you and verify that you are who you say you are, and or why you have business with them.
- Consider a digital signature or certificate that can be verified automatically by secure email clients.