Technology for Librarians 101

Computer Security - Don't Get Caught by Phishing Scams

Phishing is a high-tech scam that uses "legitimate looking" email spam (or text message) to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information. Phishing scams present a serious risk for businesses or individuals who conduct business online.

> **Therefore, if you have no dealings with the purported company sending the email, do NOT open or preview the email message — simply delete it!**

Follow these additional tips to avoid being "hooked" and becoming a victim of identity theft.

- Do NOT open emails or attachments with generic titles like "photos from a family member" even if the email address is known to you. That person's email account may have been compromised by a virus.

- Do NOT open or launch any email attachments that you are not expecting.

- Be aware that phishing scam emails are usually NOT personalized.

- If you open a message that asks for personal or financial information, DO NOT reply, fill out any form, or click on any link in the message. Legitimate companies don't ask for this information via email.

- Do NOT email personal or financial information. Email is not a secure method of transmitting personal information.

- If you are concerned about your account, contact the organization using a telephone number you know to be genuine, or open a new browser window and type in the company's correct Web address.

- If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins with "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

- Regularly log into your online accounts.

- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

For more information on phishing, including how to report it, please see the Anti-Phishing Working Group (APWG) website.

Technology for Librarians 101 is offered as part of the Nebraska Broadband Mapping and Planning Initiative, funded through a grant by the U.S. Department of Commerce's National Telecommunications and Information Administration. The Initiative aims to increase broadband adoption and use. For more information, check **http://broadband.nebraska.gov**