Don't Get Hooked by "Phishing" Scams

Most people have online accounts with various Web sites, and this makes them vulnerable to a variety of cybersecurity threats. Students and teachers alike are vulnerable because identity thieves use deceptive tactics to solicit personal information from anyone with an e-mail account. Becoming familiar with the ways that criminals try to solicit personal information through online social engineering can help deter identity theft or protect electronic privacy.

Often, online scammers or identity thieves will distribute e-mails hoping that a vulnerable or dismissive recipient will provide them with personal information. This criminal activity is called "phishing."

The most common forms of phishing schemes are fraudulent e-mails that imitate trustworthy Web sites – banks, payment sites, companies, employers, or even an employer's Information Technology (IT) department. Commonly, an e-mail will claim that the entity needs to verify account information.

Be wary of e-mails which include a request for "log-in" information for various Web sites. Recipients of phishing e-mails are usually directed to a different Web site via a hyperlink (although sometimes they are asked to call a phone number). Recipients are then asked to enter information such as user names, passwords, identification numbers, or credit card numbers. Finally, recognize that phishing scams often claim an artificial sense of urgency (i.e., "Log in within two days or your account will expire").

Sometimes a rogue Web site will visually imitate another entity's log-on site. By "logging in" with a user name and password, an unknowing victim has already provided his or her personal information to the scammer. Once a scammer knows the victim's information, they can access the Web site. An immediate remedy available to all users who suspect their password has been compromised is to sign on and change it.

Clicking on a suspicious hyperlink is deceptive. Phishing e-mails may include Web site addresses that seem authentic, yet relay users to a different site. Whenever a new Web page is visited, it is a good idea to check that the Web site address (URL) did not change.

One way to avoid phishing scams is to type any URL into a new Internet browser instead of clicking a hyperlink or copying the URL provided in a suspicious e-mail. Because phishers can make links appear as if they go to one site while directing users to another, this can help ensure that the Web site is authentic and not an imitation of another site.

In addition, when logging into a personal account on any Web site, ensure that the URL starts with "https" instead of "http." The extra "s" ensures that the Web site enables "secure" transmission of data with a computer's Internet browser.

The Federal Trade Commission maintains OnGuardOnline, a Web site that provides practical tips to protect personal information, secure computers, and guard against Internet fraud. For tips on how to avoid phishing scams, visit www.onguardonline.gov/topics/phishing.aspx.