Don’t Get Hooked by Phishing!

Published on Oct. 26, 2020

Have you ever received an email from out of the blue that asks you to click a link and take immediate action? The email may ask you to upgrade your mailbox storage limit, complete a survey or sign in to view a document. If you’ve ever acted on or responded to one of these emails, you’ve been a victim of phishing.

Common signs of a phishing email

If you didn’t already know, phishing is a form of fraud where a cybercriminal attempts to steal your personal and confidential information. Phishing emails typically ask you to sign into a fake website within a short amount of time. You may also be asked to provide personally identifiable information (PII), such as your password or bank account number.

While email is a popular form of phishing, there are several other types that a cybercriminal can use. Spear phishing attacks target specific individuals in an organization with more personalized messages to increase the likelihood that a recipient takes action.

Cybercriminals can also target you through your mobile device using vishing or smishing. With vishing, you’ll receive a phone call where the caller asks for your personal or financial information. Smishing uses SMS or text messages to target you with links designed to steal your PII.

No matter what form of phishing you encounter, there are always common signs you can look for. These include:

- Misspellings in the subject line or body of the email
- A sense of urgency to take action or respond to the email
- A link or attachment that you are directed to open
- An email signature that does not look legitimate
- A reply-to email address that is different from the sender's address.

In addition to these signs, be on the lookout for emails that offer you a "part-time job opportunity" or ask you to purchases a gift card as a "favor." Students and employees are often prime targets for these types of phishing attacks.

What to do if you receive a phishing email

If you've received an email that features some of the common signs described above, do not click on any links, open any attachments or reply to the sender. Instead, forward it to the Computing and Technology Services (CTS) Help Desk at help@duq.edu. Afterward, delete the message.

When the CTS Help Desk receives reports of a phishing email, they can block the sender and any links in the email, keeping students, faculty and staff safe from cybercrime. According to KnowBe4, a security awareness training platform, 1 out of 3 people will likely click on a suspicious link in an email or obey a fraudulent request. By reporting phishing emails to the CTS Help Desk, you not only protect yourself from being phished but also other members of the Duquesne community.

Interested in learning more about phishing at Duquesne? Head over to duq.edu/phishing for more phishing tips and to view recent phishing emails delivered to Duquesne email inboxes.