Don't Let a **Phishing** Scam Reel You In.

CYBER SECURITY OCTOBER 2018

Cybercriminals use phishing—a type of social engineering—to manipulate people into doing what they want. Social engineering is at the heart of all phishing attacks, especially those conducted via e-mail. Technology makes phishing easy. Setting up and operating a phishing attack is fast, inexpensive, and low risk: any cybercriminal with an e-mail address can launch one.

According to Verizon's 2017 Data Breach Investigations Report, the education sector saw a rise in social engineering–based attacks. Students, staff, and faculty all suffered losses when personal data and research were disclosed to unauthorized parties. Phishing played a part in more than 40% of these breaches. Knowing what you're up against can help you be more secure. Here are a few things you can do to guard against phishing attacks:

- Limit what you share online
  The less you share about yourself, the smaller the target you are for a phishing attack. Cybercriminals use information you post online to learn how to gain your trust.

- Protect your credentials
  No legitimate company or organization will ask for your username and password or other personal information via e-mail. Your school definitely won't. Still not sure if the e-mail is a phish? Contact your IT help desk. (Many institutions now offer a "phish bowl" so end users can quickly and easily report phishy messages or view the latest scams.)

- Beware of attachments
  E-mail attachments are the most common vector for malicious software. When you get a message with an attachment, delete it—unless you are expecting it and are absolutely certain it is legitimate.

- Confirm identities
  Phishing messages can look official. Cybercriminals steal organization and company identities, including logos and URLs that are close to the links they're trying to imitate. There's nothing to stop them from impersonating schools, financial institutions, retailers, and a wide range of other service providers.

- Trust your instincts
  If you get a suspicious message that claims to be from an agency or service provider, use your browser to manually locate the organization online and contact them via their website, e-mail, or telephone number.

- Check the sender
  Check the sender's e-mail address. Any correspondence from an organization should come from an organizational e-mail address. A notice from your college or university is unlikely to come from YourITHelpdesk@yahoo.com.

- Take your time
  If a message states that you must act immediately or lose access, do not comply. Phishing attempts frequently threaten a loss of service unless you do something. Cybercriminals want you to react without thinking; an urgent call to action makes you more likely to cooperate.

- Don't click links in suspicious messages
  If you don't trust the e-mail (or text message), don't trust the links in it either. Beware of links that are hidden by URL shorteners or text like "Click Here." They may link to a phishing site or a form designed to steal your username and password.