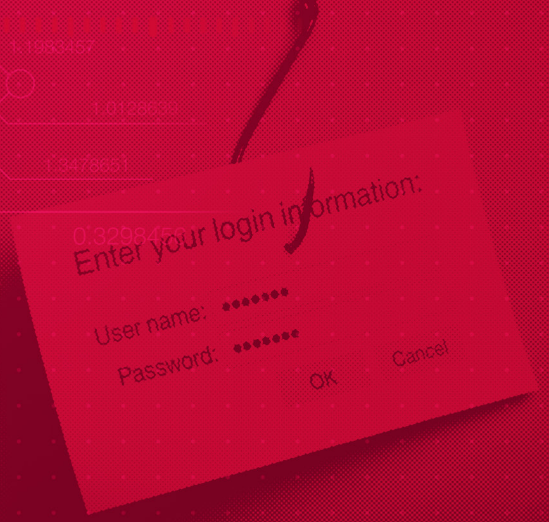
Learn what it takes to refuse the **Phishing Bait.**



CYBER SECURITY FEBRUARY 2017

Cybercriminals know the best strategies for gaining access to your institution's sensitive data. In most cases, it doesn't involve them rappelling from a ceiling's skylight and deftly avoiding a laser detection system to hack into your servers; instead, they simply manipulate a community member.

According to IBM's 2014 Cyber Security Intelligence Index, human error is a factor in 95 percent of security incidents. Following are a few ways to identify various types of social engineering attacks and their telltale signs.

- Phishing isn't relegated to just e-mail! Cybercriminals will also launch phishing attacks through phone calls, text messages, or other online messaging applications. Don't know the sender or caller? Seem too good to be true? It's probably a phishing attack.
- Know the signs. Does the e-mail contain a vague salutation, spelling or grammatical errors, an urgent request, and/or an offer that seems impossibly good? Click that delete button.
- Verify the sender. Check the sender's e-mail address to make sure it's legitimate. If it appears that your institution's help desk is asking you to click on a link to increase your mailbox quota, but the sender is "UniversityHelpDesk@yahoo.com," it's a phishing message.
- Don't be duped by aesthetics. Phishing e-mails often contain convincing logos, links to actual company websites, legitimate phone numbers, and e-mail signatures of actual employees. However, if the message is urging you to take action — especially action such as sending sensitive information, clicking on a link, or downloading an attachment — exercise caution and look for other telltale signs of phishing attacks. Don't hesitate to contact the company directly; they can verify legitimacy and may not even be aware that their name is being used for fraud.
- Never, ever share your password. Did we say never? Yup, we mean never. Your password is the key to your identity, your data, and your classmates' and colleagues' data. It is for your eyes only. Your institution's help desk or IT department will never ask you for your password.
- Avoid opening links and attachments from unknown senders. Get into the habit of typing known URLs into your browser. Don't open attachments unless you're expecting a file from someone. Give them a call if you're suspicious.
- When you're not sure, call to verify. Let's say you receive an e-mail claiming to be from someone you know — a friend, colleague, or even the president of your college or university. Cybercriminals often spoof addresses to convince you, then request that you perform an action such as transfer funds or provide sensitive information. If something seems off about the e-mail, call them at a known number listed in your institution's directory to confirm the request.
- Don't talk to strangers! Receive a call from someone you don't know? Are they asking you to provide information or making odd requests? Hang up the phone and report it to the help desk.
- Don't be tempted by abandoned flash drives. Cybercriminals may leave flash drives lying around for victims to pick up and insert, thereby unknowingly installing malware on their computers. You might be tempted to insert a flash drive only to find out the rightful owner, but be wary — it could be a trap.
- See someone suspicious? Say something. If you notice someone suspicious walking around or "tailgating" someone else, especially in an off-limits area, call campus safety.