Phishing

Who?

Short Answer: Anyone

Long Answer: Phishing attacks can happen to literally anyone, and at CSU that means not only Students, but Faculty and Staff as well. Attackers don't care who you are, they care what they can get out of you.

What?

Short Answer: An attacker using tactics to gain information from you

Long Answer: A Method an attacker uses that attempts to trick people into giving out their personal information. Phishing attacks often look genuine and use what look to be genuine internet addresses; in fact, they often copy an institution's logo and message format. It is also common for phishing messages to contain links to websites that are convincing fakes of real companies' web pages.

Spear Phishing

Phishing attempts directed at specific individuals, companies and universities have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success. This technique is, by far, the most successful on the internet today, accounting for 91% of attacks. Attackers will mine social media sites such as LinkedIn or Facebook and personalize or impersonate users so that the spear phishing email is extremely accurate and compelling. Once a link is clicked or an attachment is opened, the door to the network is established, allowing the attacker to move forward with the advanced targeted attack.

Information attackers will "phish" for

- Usernames and passwords, including password changes
- Social Security numbers
- Bank account numbers
- PINs (Personal Identification Numbers)
- Credit card numbers
- Your mother's maiden name
- Your birthday

When?

Short Answer: Anytime

Long Answer: Phishing attacks can happen at any point in time. Depending on how clever the attacker is, it could even come from someone you normally communicate with and can come during a time that person would normally message you.

Where?

Short Answer: E-Mails, Instant Messages, Websites, etc

Long Answer: The most typical place for these types of attacks to appear is in your email, but in reality, they can come from anywhere. Be sure to check you're communicating with the intended person before sending any messages back, especially if your message is going to include sensitive information.

Why?

Short Answer: To Gain Sensitive Information

Long Answer: Attackers usually want to steal something from you for some sort of gain, usually financial. They'll steal your Social to masquerade as you and buy things on your credit, they'll steal passwords to get into your bank account and transfer money out, and they'll steal much more if you're not careful.

How?

Short Answer: If you‘re going to send information, especially if it‘s private, confirm the recipient. When receiving unexpected emails with attachments, verify the sender using an alternate mode of communication.

Long Answer: Report phishing emails that appear in your CSU inbox. If it’s truly a phishing attempt, chances are you’re not the only recipient, and you can help protect others by alerting your University IT personnel.

- Report the phish using the **Phish Alert Button (PAB)**.
- Forward the entire message to: **abuse@columbusstate.edu**

Stay Vigilant

- Report emails and text messages that ask you to confirm or provide personal information. Legitimate companies don‘t ask for this information via email or text.
- Don‘t reply, and don‘t click on links or call phone numbers provided in the message, either. These messages direct you to spoof sites.
- If you‘re concerned about your account or need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card.
- Area codes can be misleading. Some scammers ask you to call a phone number to update your account or access a "refund." But a local area code doesn‘t guarantee that the caller is local.