Phishing: Fraudulent Emails, Text Messages, Phone Calls & Social Media

As any type of fraud, phishing can be extremely damaging and has already claimed victims on campus. Use these pages to find out more about phishing - what it is and what risks it poses. Don't get hooked!

What is Phishing?

Phishing refers to different types of online scams that 'phish' for your personal and financial information (e.g., your passwords, Social Security Number, bank account information, credit card numbers, or other personal information).

Phishing messages can come from a growing number of sources, including:

- **Email**
- **Phone calls**
- **Fraudulent software (e.g, anti-virus)**
- **Social Media messages (e.g., Facebook, Twitter)**
- **Advertisements**
- **Text messages**

What is spear phishing?

- More sophisticated attacks, known as *spear phishing*, are personalized messages from scammers posing as people or institutions that you trust. They often collect identifiable information about you from social media or the compromised account of someone you know to make their messages more convincing. Never transmit sensitive information over email or social media, even if the message requesting information appears to be legitimate.

Signs of phishing include:

- **Ultimatum:** An urgent warning attempts to intimidate you into responding without thinking. *'Warning! You will lose your email permanently unless you respond within 7 days'*.
- **Incorrect URLs:** Scammers may obscure URLs by using hyperlinks that appear to go to a reputable site. Hover your mouse over any suspicious links to view the address of the link. Illegitimate links often contain a series of numbers or unfamiliar web addresses.
- **No signature or contact information:** Additional contact information is not provided.
- **Too good to be true offer:** Messages about contests you did not enter or offers for goods or services at an unbelievable price are likely fraudulent.
- **Style inconsistencies:** Pop up windows that claim to be from your operating system or other software may have a different style or colors than authentic notifications. Messages that claim to be from a reputable organization may be missing branding aspects such as a logo.
- **Spelling, punctuation, or grammar errors:** Some messages will include mistakes. *'Email owner that refuses to update his or her Email, within Seven days'*
- **Attention-grabbing titles:** "Clickbait" titles (e.g., "You won't believe this video!") on social media, advertisements or articles are sensationalist or attention-grabbing and sometimes lead to scams.