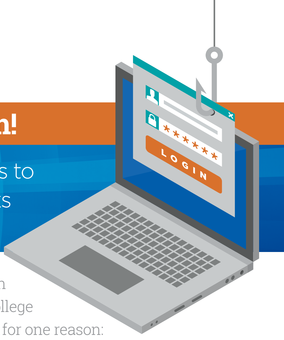
Dynamic Campus

Don't be a victim!

Quick and easy ways to spot phishing attacks before it's too late



There has been a sharp rise in phishing attacks targeting college students and faculty like you for one reason:

THE ATTACKS WORK.

Here are some quick and easy ways to avoid becoming the next victim.

ATTACKS CAN COME FROM ANYWHERE

Email is the most common method of phishing attack, but hackers don't stop there. They have also been known to attack using:

- **Text, SMS or iMessage (also called "SMishing")**
- **Social media**
- **Phone call (also called "Vishing")**
- **Regular mail**

DON'T OPEN THAT ATTACHMENT!

The goal of most email or social phishing attacks is to get you to **open an attached file**.

THE ATTACHMENTS ARE DISGUISED AS:

- **Word, Excel or PDF documents**
- **Links to Google Docs**
- **Links to Office 365**
- **Website links**
- **Zipped files**
- **Photos**

Those attachments actually contain a virus that installs malicious code (malware) on your computer. The malware is usually difficult to remove and can replicate to other devices once it infects your PC, phone or tablet.

Four Reasons These Attacks Work

How do they trick us into opening a file full of viruses? Four proven ways get us to overlook potential warning signs:

1 The attack looks like it's **LEGITIMATE CORRESPONDENCE FROM SOMEBODY YOU TRUST**, using a information they've already gathered about you online. This is called "spearphishing." These sophisticated messages may appear to come from:

- **Your college or university's registrar, bursar or financial aid office**
- **Your institution's IT support team or help desk**
- **Your employer, bank, or credit card companies**
- **The IRS**
- **Your favorite brands**
- **Your social media sites**

2 **THEY CREATE A SENSE OF URGENCY.** They use words like "immediate attention" or "Respond ASAP" designed to get you to open it right away.

3 **THEY MAKE IT SEEM LIKE YOU'RE IN TROUBLE OR MISSED SOMETHING.** For instance:

- **"Key documents missing..."**
- **"Our records indicate..."**
- **"Unable to process your account correctly..."**

4 **THEY USE ANGER, THREATS OR EVEN PROFANITY IN THE SUBJECT LINE AND MESSAGE.** This is effective because:

- **It gets your attention.**
- **It triggers an emotional response from you.**
- **It reinforces that sense of urgency.**

Four Quick Questions to Ask Before Opening Any Attachments or Links

1 Am I expecting this message?

Did you get an email asking for your W2 from your employer... even though you're not current employed? Did you get a text asking you to verify your account... with a bank you don't do business with?

- NO → DELETE IT!
- YES

2 Is this from somebody I know?

You may recognize the company the email is from, but do you recognize the sender's name? Is it somebody you do business with?

- NO → DELETE IT!
- YES

3 If it's an email, does the email address match the name of the sender and organization?

Emails can be easily made to look like they are coming from any sender, but the email address itself is much harder to fake. A message from **registrar@yourcollege.edu** is likely authentic. A message from **registrur@memchang.stream** is a phishing scam.

- NO → DELETE IT!
- YES

4 Does the message sound like it's coming from the sender?

Does the message reference specific details from your relationship? Is the overall length and tone of the email consistent with other messages you've received from the sender?

- NO → DELETE IT!
- YES → BUT YOU'RE STILL NOT SURE

DO NOT reply to the email.

DO NOT click the link or open the attachment.

DO NOT give our any account information, logins, passwords under any circumstances.

DO contact them to confirm! Call them or send a new message asking them to verify they sent you the attachment.

If You Think You're a Victim of a Phishing Attack:

DON'T WAIT!

The damage from phishing attacks only gets worse with time.

CONTACT THE IT HELP DESK.

They can help you determine the best course of action based on the type of attack and information provided.