Don't be a victim!

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

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

If you think you’re a victim of a phishing attack:

The attacks look like it's legitimate correspondence from somebody you trust, using 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

They make it seem like you're in trouble or missed something.

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

It gets your attention.

Four Reasons These Attacks Work

1. They create a sense of urgency.
   - They use words like "immediate attention" or "Respond ASAP" designed to get you to open it right away.

2. 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.

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…"

It gets your attention.

Four Quick Questions to Ask Before Opening Any Attachments or Links

1. Am I expecting this message?
   - If it’s a phone call, ask yourself, "Is this the caller I expected to hear?"
   - If it’s an email, ask yourself, "Is this the email I was expecting?"

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?
   - Is this from somebody I know?

3. 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?
   - Does the message sound like it's coming from the sender?

4. If it's an email, does the email address match the name of the sender and organization?
   - Email addresses 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@tsc.edu is likely authentic. A message from registrur@memchang.stream is a phishing scam.

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

1. Do not wait! The damage from phishing attacks only gets worse with time.

2. Don’t reply! Do not reply to the email. Do not click the link or open the attachment. Do not give out any account information, logins, passwords under any circumstances.

3. Don’t do it! Contact the TSC IT Help Desk. (956)295-3800 or helpdesk@tsc.edu.

4. Do it! Contact the TSC IT Help Desk. (956)295-3800 or helpdesk@tsc.edu.

The attacks last long. Ask yourself: What is going to motivate someone to want to trick me? Do not open that attachment! ATTACHMENTS ARE DISGUISED AS: