Week 3: Think Before You Click!

**Phishing** is when cyber criminals send an email to try to get you to share personal or financial details, or entice you to click a link, which can then install malware onto your desktop or mobile device.

**Email Safety Tips:**

1.) **Avoid responding to emails that don’t look legit.** Follow up directly via phone or in person with the sender instead of clicking the link. Do not reply to the email.

2.) **Stop and think before you click!** Cyber attackers try to use a sense of urgency to get you to act. Take a step back and think about what the sender is asking. Listen to your instincts if something doesn’t seem right!

3.) **Hover over those links!** Hover your mouse over any links embedded in the body of the email. If the website address in the link looks strange, don’t click on it.
Report suspicious emails sent to your TC Gmail to the Service Desk!

Next week, our security topic is how to stay safe online when you’re away from work. For more information, stop by one of our **30-minute workshops** being held at the CIS Service Desk (70 Grace Dodge). Workshops are offered at 10am and again at 2pm on the dates listed below:

**Monday, 10/22: How to keep your family safe online**

**Tuesday, 10/23: Open Wifi: Everyone is watching**

**Thursday, 10/25: How to do a “health check” on your home computer and mobile device**

You will be entered into our drawing for prizes—including Amazon gift cards and an Apple iPad—each time you attend one of our workshops in October. The drawing for the prizes will be held during our CIS Cyber Showcase, November 1 from 1-3pm, at Everett Lounge. Faculty, staff and students are all welcome!