From DSU: Avoid Email Scams!

Scams & Phishing
Scammers and online criminals are working overtime to exploit the COVID-19 crisis. They are after your passwords, your money, and/or control of your computer. Watch out for:

- **Gift card scams** - emails that fake your supervisor's or another DSU administrator's name and ask you to go buy gift cards or other items of online value. Typically, they promise to pay you back later, after you send off the gift card codes.
- **Fake help desk or IT scams** - vague and/or ominous messages about your account getting shut off unless you click a link or attachment to "verify" it.
- **Fake invoice or delivery notifications** - invoices you weren't expecting that demand payment or delivery notifications for things you did not order. In either case a link or attachment will be presented for you to click.

Protect yourself from these and similar attacks by developing a healthy sense of skepticism. Always verify that a message is what you think it is before acting. Don't click links or attachments for messages you can't positively identify. Actions you can take include:

- Click or tap on the name of the sender. Make sure that email address and the name match up
- Use the hover trick to find out where a link goes. Hold your mouse cursor over the link (without clicking!) or long tap the link (if you are on a mobile device) and the full address of the link will be displayed. Verify it goes where you think it should go.