Be Alert for COVID-19 Cyber Scams and Phishing Attacks

During a media-intensive crisis such as the novel coronavirus (COVID-19) outbreak, UMB's Center for Information Technology Services (CITS) wants students, faculty, and staff to be aware that cyber attackers will try to take advantage of the situation by attempting to scam you or by launching phishing attacks designed to get you to click on malicious links or open infected email attachments.

Here are some of the most common indicators that the phone call or email is most likely a scam or an attack:

- Any message that communicates a tremendous sense of urgency. Cyber attackers are trying to rush you into making a mistake.
- Any message that pressures you into bypassing or ignoring standard security policies and procedures.
- Any message that promotes miracle cures such as vaccines or a medicine that will protect you. If it sounds too good to be true, it probably is.
- Be suspicious of any phone call or message that pretends to be an official or government organization urging you to take immediate action.

Keep in mind that these types of scams and attacks can happen at work or at home and via email, text messaging, or phone call. Don't fall victim to cyber attackers playing on your emotions. **If you think you have received an attack at work, simply delete the message, or if you have concerns, report it to CITS at *help@umaryland.edu* or by calling 410-706-4357.**

SOURCE: *sans.org*

University of Maryland Baltimore