UNIVERSITY OF DALLAS
Information Systems and Technology

October 27, 2022

Greetings from your Information Systems and Technology Team!

This week's Cybersecurity Tips!

Follow these cyber security tips to protect valuable information from being disclosed to cyber criminals. Let's do our part to practice safe computing at UD.

Safe Computing Tip #1 – Save and share

It is best practice to use a shared drive or cloud service (Google Drive, Dropbox) to store important and sensitive data. Your data will be backed up and protected in the case of system failures and cyber-attacks.

Safe Computing Tip #2 – Avoid using public networks

Many UD employees have the option to work remotely. Public Wi-Fi networks are not secure and can pose a threat to your online safety. Be vigilant when using public Wi-Fi. The UD Information Systems and Technology department provides Virtual Private Network (VPN) access for faculty and staff. It should be used to access the UD network remotely. Please contact the department for questions about VPN accessibility.

Safe Computing Tip #3 – Be aware of Vishing attacks

Vishing, also known as voice scam calls, are another form of a phishing attack. Vishing calls appear to be from a trusted source, but they originate from scammers. For example, if a caller claims to be a representative of the IRS, Medicare or the Social Security Administration and requests personal information, it is a scam. Federal agencies will not reach out to you through phone, text or social media to request personal or financial information. In addition, you should be skeptical of frantic calls that have a sense of urgency, such as requests for your information to reset a password or requests for information to claim a prize before the contest is over. A hacker's primary goal is to trick you into thinking they are legitimate. If you receive any suspicious phone calls, you should simply hang up. Don't press any buttons or respond to prompts.