

UNIVERSITY OF DALLAS

Information Systems and Technology

October 12, 2022

Greetings from your Information Systems and Technology Team!



This week's Cybersecurity Tips!

As an employee you are a high-end target for cyber attackers. 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 - Look out for Phishing Emails and Social Engineering

If you receive any suspicious emails that are requesting personal information, files or unexpected requests, please report it by clicking the Phish Alert button in your email . Do not click on any suspicious links or respond to the emails

Safe Computing Tip #2 - Lock your Devices

Never leave your computer or smart devices unattended without locking them or logging off. Walking away from your computer poses a security risk to you and UD. You can simply lock your computer by holding down the **Windows Logo Icon** key and the **L** key on your keyboard. If you are using a Mac device, you can use the keyboard buttons **Control-Shift-Power**.

Safe Computing Tip #3 – Practice Good Password Hygiene

Poor password practices can put UD at risk of a cyber-attack. Your password should be strong, unique and easy to remember. The word "password" and the numbers "12345" should never be used for your password. They are commonly used and make it easy for cybercriminals to hack into the network. Practice using strong passwords that contain at least 12 characters; uppercase and lowercase letters; numbers; and special symbols like **&**, **!** or **#**. In addition, do not share your passwords or leave your written passwords out for display. Following these suggestions will help to prevent any social engineering attacks such as tailgating and physical breaches.