SHOP SAFELY!

WVU employees shouldn't use University credentials for holiday buying

To help faculty, staff and students shop online safely this holiday season, Information Technology Services offers several cybersecurity tips and an important reminder: NEVER use your University email account or Login credentials for personal online shopping.

HERE ARE SOME TIPS FOR PROTECTING YOURSELF AND YOUR FINANCES FROM CYBER-THEFT.

1 LOCK DOWN YOUR LOGIN

Enable two-factor authentication and use separate, unique passwords for all work and personal accounts. Learn more at **lockdownyourlogin.org/strong-authentication/**

2 GET SAVVY WITH WI-FI

Logging into email and banking accounts on free, public Wi-Fi puts your information at risk. Require a password or biometric scan to access your phone so no one can use it if you lose it.

3 SHOP SECURE WEBSITES

Look for the green lock icon and https:// in the URL to ensure the site is secure before using your credit card.

4 KEEP A CLEAN MACHINE

Run the most current versions of software and apps on all you web-connected devices. WVU provides free anti-virus for up to three personal devices at **freeav.wvu.edu**

5 USE SAFE PAYMENT OPTIONS

Credit cards are the safest online payment option. NEVER use debit cards.

6 WHEN IN DOUBT, THROW IT OUT

Links in emails, posts, and texts are often how cybercriminals try to steal information or infect devices. Be skeptical with suspicious-looking emails and avoid clicking on attachments.

Learn more about protecting yourself at DefendYourData.wvu.edu.

Forward suspicious-looking email as an attachment to DefendYourData@mail.wvu.edu.