EMPLOYEE SPOTLIGHT

READ TIME: 8 MINUTES

Cybersecurity Safety Tips

By Seth Yoder

Seth Yoder from the System Wellness Committee recently sat down with Cindy McKendall from Technology Services to discuss cybersecurity and what steps we all can be taking at work and home to protect ourselves.

Q. How does working at the University of Illinois make us targets for cybersecurity attacks?

A. As employees, each of us has access to information that cyber-criminals want. Whether you have access to financial records, research data, or student information, that access and that information is valuable to cyber-criminals. And that makes each University of Illinois employee a target. But there are things each of us can do to protect ourselves and the University of Illinois System.

Q. Are there cybersecurity best practices we should be following when we use our personal computers for work?

A. Yes! These are good tips to follow, no matter what kind of device you're using.

• Don't click on any attachments or links that seem suspicious or unusual. If you get a suspicious email to your work account, report it to Tech Services at this link: https://answers.uillinois.edu/illinois/page.php?id=50007

• Back up personal files now. You can copy your files to a cloud service, an external hard drive, or a USB drive to back them up. That way, if your computer gets compromised or infected, you won't lose all your important files. You should also follow your department's procedure for storing work files in an appropriate place that gets automatically backed up.

• Install and run antivirus software on your personal computer. If you do not already own antivirus software, you can get the following free downloads.

UIUC/UIS: https://webstore.illinois.edu/Shop/product.aspx?zpid=2508

UIC: https://accc.uic.edu/services/security/antivirus/

All University of Illinois computers should already have antivirus software installed and running.

• Make sure to install software updates that are pushed to your computer. These updates often fix newly discovered security vulnerabilities, and installing them will help protect your computer against threats.

Q. Phishing is a common threat we often hear about. Do you have any tips and tricks on how to recognize a phishing attempt?

A. Phishing attacks are getting more sophisticated, which requires us to be more diligent in identifying them. The following information will help you identify a phishing attempt.

• A phishing email often has a sense of urgency and will ask for some type of immediate action.

• Many phishing attempts resemble trusted companies with logos and branding that look legitimate.

• The grammar or spelling in many phishing attempts can seem "off," once you read it carefully.

Q. Are there training and resources available on cybersecurity at the University of Illinois?

A. Yes, the University of Illinois currently offers the following training modules on cybersecurity:

- Creating strong passwords
- Phishing
- Ransomware
- Safer web browsing
- Two-factor authentication

To access this training please visit go.illinois.edu/securitytraining and login with your NetID and password. Trainings will continue to be added so please be sure to visit the site even after you completed all the currently available trainings.

In addition, there is also a biweekly cybersecurity newsletter called Work Secure at Illinois. Here are the links to the first three:

Updating Software

Running Antivirus

Avoiding Phishing