SAFE PRACTICES

Cyber attacks originate from many sources and range from annoying to very harmful. It's up to us to consider how we use our technology in our daily work and activities and to prepare ourselves to be thoughtful and safe with the resources that support our work – email, Colleague, Blackboard, and any other L&C supported technology.

LET'S BE GOOD DIGITAL CITIZENS.

That means informing yourself about good practices and reaching out to the IT HelpDesk when you have questions or concerns. What can you do to help?

- Be cautious with emails from unknown or unexpected senders.
- Don't click on unfamiliar internet links.
- Don't download or open unfamiliar attachments.
- Be wary of using unvetted USB drives.
- Use strong passwords and don't share them.
- Make sure Sophos is running on your L&C device.
- Don't install unlicensed or unauthorized software.
- Contact the IT HelpDesk when you have questions.
- Only allow Lewis and Clark IT staff to work on your L&C device.

STAY INFORMED ABOUT THESE TOPICS

Several colleges and universities, the federal government and legitimate non-profit organizations provide resources to learn more about how to respond to phishing schemes and other activities hackers use to thwart our technology security.

KANSAS STATE UNIVERSITY

MICHIGAN STATE UNIVERSITY

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

UNIVERSITY OF CHICAGO

ILLINOIS ATTORNEY GENERAL'S OFFICE

AARP

NORTHWESTERN UNIVERSITY

FEDERAL TRADE COMMISSION

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

L&C's IT staff is updating the college's systems, policies, and procedures to help protect against future security threats. As part of the IT development plan, look for more information about training, updated resources, and new procedures.