LCCC IT Director Discusses Safety Precautions To Phishing E-mails

by Dan Brannan, Content Director
October 13 2021 3:12 PM

GODFREY - Student Trustee Sam Copeland brought up an issue with phishing e-mails at the Lewis and Clark Community College Board meeting on Tuesday. LCCC Executive Director of College Effectiveness and Grant Development, Brett Reinert, who is over IT at the college, said they have seen an uptick in phishing e-mails to the student and team member accounts. However, Reinert said he and his staff are making sure they have the appropriate security measures in place as safeguards.

Reinert also said they are educating our users so they have the skills to recognize and avoid these types of fraudulent activity.

“We do take student concerns seriously, so we’re making sure that we have the right security components in place to respond when these e-mails are received, and the college is working on giving the IT Help Desk a more visible, physical presence on campus to increase consumer awareness about these scams,” Reinert said.

“Anyone who suspects that they have received a phishing or scam e-mail should be encouraged to share these incidents with the HelpDesk at:

helpdesk@lc.edu

How To Recognize and Avoid Phishing Scams

Scammers use email or text messages to trick you into giving them your personal information. But there are several things you can do to protect yourself.

How To Recognize Phishing

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they're often successful. The FBI's Internet Crime Complaint Center reported that people lost $57 million to phishing schemes in one year.

Scammers often update their tactics, but there are some signs that will help you recognize a phishing email or text message.

Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you're eligible to register for a government refund

- offer a coupon for free stuff