RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

Alert Type | **Awareness** | Watch | Warning

Phishing Scam Spoofs Zix Secure Emails

Bad actors have reportedly sent phishing emails to some credit unions spoofing Zix secure emails supposedly from CUNA Mutual Group or FIS. Although CUNA Mutual Group uses Zix to encrypt select credit union emails that contain sensitive information, these emails were not sent from CUNA Mutual Group or from our Zix account. Credit unions should remain on the lookout for suspicious emails that claim to be from our organization or other trusted entities.

Details

Some credit unions recently received phishing emails that spoofed Zix secure emails reportedly coming from CUNA Mutual Group or FIS. Unfortunately, we cannot prevent fraudsters from sending fraudulent emails, so credit unions should be on the lookout for suspicious emails that claim to be from our organization or other trusted entities.

While CUNA Mutual Group uses Zix (a brand email encryption software) to encrypt select credit union emails that contain sensitive information; these phishing emails were not sent from CUNA Mutual Group or from our Zix account.

Phishing scams often try to gather information using deceptive emails and websites. The fraudster's goal is to trick the email recipient into believing that the message is from a trusted individual or entity — in this scenario, a request from CUNA Mutual Group or FIS — and to give out confidential information, click a link, or download an attachment. Phishing emails often contain attachments or links to malicious or spoofed websites infected with malware.

These phishing scams also look to catch you off-guard, dupe you to comply with instructions from a bad actor, and get you to act quickly to urgent requests.

How to spot these phishing emails

- The Subject consistently begins with "New ZixCorp secure message from" and ends with either CUNA or FIS Global.
- The body consistently includes "Click here <xxx.softr.app> to Open Message". The beginning of the link changes but the end includes softr.app.
- The last line of the email states that the secure message expires very soon.

How to tell if a Zix email is legitimately from CUNA Mutual Group?

- CUNA Mutual Group Zix emails will come from the email address of notification@secureemail.cunamutual.com
- The email will have a banner: "New Email from the CUNA Mutual Group Secure Email Center."
- The email will never use the word "Zix." The phishing emails use it both in the subject line and in the body

Date: August 16, 2022

Risk Category: Phishing; Scams; Fraud

States: All

Share with:

- ☐ Branch Operations
- ☐ Executive Management
- ☐ IT
- ☐ People Leaders
- ☐ Risk Manager

Facing risk challenges?

Schedule a free personalized discussion with a Risk Consultant to learn more about managing risk.

Risk Mitigation

Credit unions should consider these loss controls:

- Phishing awareness and social engineering fraud training should be considered a top priority. Employees should understand the risks when opening email attachments or clicking on links from unfamiliar sources. This awareness training should also include an explanation of various phishing techniques and recent campaigns.
- Check for bad grammar, misspelled words, and suspicious domains in the content and within links.
- Never click on a link or attachment within an unverified email, text or social network site unless you have verified it is authentic.
- Verify with the sender via phone or other independent sources to determine if the email and/or request is legitimate.
- Instill the "always alert" mentality into your culture by conducting frequent social engineering training for all employees as part of your security awareness training efforts. The goal is to change employee behavior to reinforce good data security practices.
- Perform random phishing penetration tests on employees as a learning opportunity and reinforces the importance of securing your credit union's cyber network and systems.
- If an employee has received a phishing email, it should be deleted or submitted through your organization's phishing reporting system immediately. Do not open it or click on links.

Risk Prevention Resources

Access CUNA Mutual Group's Protection Resource Center for exclusive risk and compliance resources and RISK Alerts to assist with your loss control needs (User ID and Password required).

- An Employee's Guide to Phishing Emails
- Fraud & Scams eBook
- The Risk of Social Engineering Fraud eBook

Access the Protection Resource Center for exclusive resources:

- Loss Prevention Library for resources & checklists
- Webinars and Education
- RISK Alerts Library
- Report a RISK Alert

The Protection Resource Center requires a User ID and Password.