



ONLINE BANKING ALERT: INCREASE IN ZELLE FRAUD

Scammers are utilizing a new strategy that starts with sending you a fake Zelle transaction confirmation text. This message may appear legitimate and prompt you to share personal information.

What You Need to Know:

- **Fake Confirmation Texts:** Scammers send texts that appear to come from Zelle, confirming a transaction you did not initiate.
- **Phishing Attempts:** These texts are designed to trick you into providing sensitive information such as your account number, password, or other personal details.
- **Account Takeover:** What is happening is the fraudster is gaining access to the account and adding a fraudulent phone number to the mobile number on the member's account. That new fraudulent number is set to receive all the multifactor authentication codes/notifications. This allows them to send and confirm the Zelle transaction.
- **Immediate Action:** Do not respond to these texts or click on any links they may contain.

How to Protect Yourself:

1. **Verify Authenticity:** Always check your bank account through the official app or website to verify any transactions.
2. **Do Not Share Personal Information:** Never share your account details, passwords, or other personal information in response to unexpected texts or emails.
3. **Report Suspicious Activity: Please don't hesitate to contact our member service team immediately if you receive a suspicious text or notice any unauthorized transactions.**

Our Commitment to Your Security:

We continuously monitor for fraudulent activities and enhance our security measures to protect your personal information. Your security is our top priority.

Contact Us:

If you have any questions or need assistance, please contact our member service team at 216-535-3200 or memberservice@cenfedcu.org.

Stay vigilant, and thank you for banking with us.