Federal Credit Union

Dear Valued Member,

MC Federal Credit Union is committed to keeping you up to date on techniques used by scammers to trick you into giving up personal and confidential information, or to steal your money. Previous communications have focused on a type of Social Engineering technique called "phishing" where the scammer sends the victim an unsolicited email with links or phone numbers that all serve one purpose- to put you in contact with the scammer so they can manipulate you.

We would like to share with you another version of this type of scam called "smishing." Like phishing, this type of attack involves an unsolicited text or SMS message that appears to come from a legitimate financial institution or service. An example of this is an unsolicited message appearing to come from Zelle, a digital payments network, stating that you are due a credit to your account. The message includes a link to accept the money, however; in clicking on the link and responding to the text, the victim ***is sending money to the scammer***.

Whatever the approach may be, members of our community need to remain informed and alert to avoid becoming a victim of scams. MC Federal Credit Union would like to share some best practices to keep you and your families safe from cybercriminals as we get ready to enjoy warmer weather:

1. Beware of unsolicited communications
    - Regardless of whether it is an email or a text, always be suspicious of unsolicited communications
    - Never engage with unsolicited communications, regardless of the source
2. Never click on links embedded in an unsolicited communication
    - Links often include malware which can be used to spy on, or even take over, your device
3. Never give out personal information via text or instant messaging
    - Remember, it is not rude to ignore a text message. If it is an urgent and legitimate communication, the organization will contact you again, usually through an alternate method, such as a direct phone call
4. Beware of phony websites
    - It is not difficult for scammers to create a website that appears legitimate
    - Watch for links that direct you to share private financial information or install malware on your device
5. If the communication involves a problem with an order or transaction, log into your account with that company to verify whether there is an issue
6. Always contact the company using a publicly available and trusted phone number

Regardless of the source, **never click on a link** or call any numbers provided in an unsolicited communication. You should always use a trusted method of contacting any company, such as a known website.

If you are unsure if the communication is legitimate, never hesitate to contact a Member Services Representative. Unfortunately, we have seen scams effect members of our community and we want to help keep you safe.

You can learn more about how to protect yourself and your family by visiting us at mcfcu.org and reviewing our **Fraud and Security** page**.**

Your financial well-being is among our top priorities at MC Federal Credit Union.

Thank you for being an important part of the MC Federal community. Have a wonderful spring!

Elba L Arenas

Elba Arenas
Chief Member Experience Officer
MC Federal Credit Union