STAYING ALERT

Steps for Safeguarding your Account

Jefferson Financial FCU will never call to request personal banking information via telephone, email or text message.

Scammers and fraudsters have ways of making incoming calls, email messages and / or text messages look like it is the Credit Union, even when it is not.

With that in mind, below are best practices to protect your personal information and assets:

- Don't let anyone pressure you into sharing information such as your account number, password, PIN, User ID and / or password.
- Hang up on suspicious calls immediately. Call us if you suspect something is not right or visit a branch and speak to our staff.
- Don't respond to any email that asks you to update your personal information online by dialing a telephone number. ***We will never ask this of you.***
- If someone tells you that your account has been compromised and you need to withdraw all of your funds in cash, **this is NOT the Credit Union**. If your account has been compromised, we will instruct you to visit a branch so that we can change your account number.

See back for more...

Jefferson Financial FEDERAL CREDIT UNION

JeffersonFinancial.org

- If you receive a one-time pass code, that you didn't request, don't give the code to anyone who contacts you for it. ***We will never ask this of you.***

- If you use Online / Mobile Banking, enable Two-Factor Authentication to strengthen your login security. Steps on how to set this up can be found on our website at JeffersonFinancial.org/services/online-security

- **When in doubt, ASK QUESTIONS.** Get the advice of a trusted family member, friend or your banking representative.

A few known Scams are:

- **Mobile Deposit / Loan Scams:** A scammer gets a member to deposit a check with the promise of a finder's fee or quick money if they transfer money back to them. The check is normally fraudulent and the member loses their hard-earned money. *Get rich quick schemes DO NOT WORK.*

- **Tech Impostors:** Scammers contact you directly with "help" for a non-existent computer problem which allows them to access your personal information and credentials.

- **Family Emergency Fraudsters:** Scammers impersonate grandchildren or other family members that are in trouble / need money.

  Remind your friends and family to avoid sending gift cards, money or personal information to anyone they do not know. If this caller tells you not to contact your family member regardless of the reason, this is always a Red Flag that this is a scam.

It's important to monitor all of your accounts regularly and learn how to best protect your information. Our website has an **Online Security** section that also offers a variety of topics to keep you and your information safe.