

City & County Employees Credit Union Member Security Awareness

City & County Employee's Credit Union's (CCECU's) commitment to Security;

As your credit union we are committed to your financial safety, we feel the first step to keeping you safe is to educate you.

Remember CCECU will never ask for your personal information, account number, password, or any sensitive account information via email or text message. If you receive an e-mail/text message that looks to be from CCECU, but asks for account information, consider it to be an attempt to obtain your personal account data for an illegal purpose. You should **NEVER** follow the instruction in any suspicious email/text message.

Please report any suspicious e-mails, text messages or websites to CCECU by forwarding the message to citycountcrun@qwestoffice.net. If you suspect identity theft or have any question regarding this notice, please contact us at 701-237-4493.

Online Banking Security Tips

Never give out any personal information including User Names, Passwords, SSN, Date of Birth.

Create difficult passwords which include letters, numbers, & symbols when possible.

Don't use personal information for your user names or passwords.

Avoid using public computers to access your Online Banking.

Don't give any of your personal information to any websites that do not use encryption or other secure methods to protect it.

ATM Security Tips

Treat your card like cash, keep it in a secure place to prevent it from being lost or stolen.

Memorize your PIN. Never write it on the card, or store it with your card.

Always pay close attention to the ATM and your surroundings, especially after dark. Use another location or return at a later time if anything suspicious is noticed. If you are at an ATM when you see something suspicious, cancel the transaction, put your card in your pocket and leave immediately.

Minimize the amount of time you spend at the ATM. Prepare your transactions before your arrival at the ATM.

Don't select an ATM at the corner of a building. Corners create a blind spot. Use an ATM located near the center of a building.

Be alert for the presence of a Card Skimmer on the ATM. A skimmer is a device that read the magnetic data on your card as you insert or swipe your card into the ATM. Look for glue or tape residue, something that wasn't there the last time you used the ATM.

Report a lost or stolen card at once. Even though your card cannot be used without your PIN at an ATM, remember that a debit or credit card could be used to make purchases with merchants. It is important that you notify the credit union as soon as you notice the card missing; this can prevent or reduce any loss on your account and a new card can be issued to you promptly.

If you notice fraudulent charges on your monthly statement or online banking account history, notify the credit union immediately.