

Protect yourself from these scam techniques

Phishing emails

Recently several members have replied to phishing emails appearing as emails from PayPal. The email asks people for their ATM card number and PIN. Please do not ever give this information over the internet. PIN numbers are never asked for from anyone.

NCUA alert E-mail Scams

Another email scam is going around informing members that their home banking access needs to be updated in order to provide better security. This is a scam please do not click on any links within this email.

A member received an e-mail notifying them that they can collect \$20 by completing a survey. This is a scam. Do not provide any account information.

Members are receiving e-mails from service@cuna.com the above address notifying them that their account access has limited for security reasons and please enter personal information to remove the limitations. Please do not respond to this e-mail. Town & Country will never ask for personal information via e-mail. If you receive this e-mail and respond to it in error please contact the credit union immediately.

Telephone Scam

A credit card phone scam has been reported by a few Maine credit unions. This scam has been targeted to VISA and MasterCard holders where the callers do not ask for a card number, they already have it. The caller introduces themselves as so and so from the Security and Fraud Department at VISA/MasterCard. They proceed to give a badge number and the phone number that is on the back of all VISA/MasterCards implying that the consumer can call back to make sure that the caller is legitimate. The caller continues to explain that the consumers card has been flagged for an unusual purchase pattern and that they are calling to verify a charge. After the consumer says they did not authorize those charges, the caller explains that the credit card company will issue a credit to their account. The caller also explains that this is a company they have been watching and the charges range from \$297 to \$497, just under the \$500 purchase pattern that flags most cards. The caller continues to provide the consumer with their address, telephone number, and reiterates calling VISA/MasterCard with any questions. The caller then asks the consumer for the three digits code on the back of the credit card, to verify that the card is in their possession. This number is the security code for the credit card and is the only way a scammer can complete a charge. Once the caller hangs up the scammer can complete any transaction. Never give out PIN information to anyone.

Phony credit union employee calls

Please be aware that individuals are contacting members by phone telling them that their account number is changing and ask them to give them their existing account number to confirm. Town & Country will never contact members by phone and ask for account information that the credit union would already have on record. If someone calls you about this similar situation or you have other suspicious calls please contact Town & Country immediately.

Counterfeit money orders

Counterfeit Walmart money orders are being sent to individuals contacted online asking them to cash the money order at their financial institution. However, the amount of the money order is larger than the amount agreed to online. The individual asks that they send the "extra" back via wire transfer. Many people have lost large amounts of money to this scam. If you receive a money order online please contact the credit union for help in determining whether it is valid or not.