SPECIAL EDITION ***4/20/2018***

pcm FRAUD NEWS

PCMCU wants to keep you in the know about what's trending in fraud.

We would like to bring immediate attention to a couple of fraud trends we are seeing.

Phishing / Computer Takeover Fraud

We are experiencing calls from members who are allowing remote access to clean and speed up their computers. You may see a pop-up or alert stating that you have a virus or that there is a problem with your computer and ask that you call the number listed so they can help diagnose and fix the problem. They lead you to believe they are from Microsoft, Apple or another such company. We have found these cases to be fraudsters who want you to believe that they are legitimate. Once they gain access to your computer they may install tracking malware or will search for personal or financial information.

Please do not allow anyone to access your computer. If you have already allowed access, power down your computer and disconnect it from the internet/wi-fi connection. We recommend reaching out to someone you know or a local company to look at your computer if you feel you have been a victim of this scam. We also recommend changing passwords to any sites you visit on that computer, **but from another device**. To protect yourself from computer fraud, keep your anti-virus software up to date, never allow access from outside parties and do not save passwords to frequently visited sites. If you have provided debit or credit card information, contact your financial institution or credit card company to immediately cancel your card.

Friendship / Romance Fraud

Another trend on the rise is when a fraudster, most of the time a person you've met online and now consider a friend, is allowed access to your online banking account. After they log in, they have the ability to make a mobile deposit into your account and may ask you to return a portion or all of the money to them by sending a wire transfer, Western Union or purchasing gift cards. The check deposited is then returned as fraudulent or NSF and it is your responsibility to repay the credit union for those funds.

Another version of this scam occurs when you log into your online banking while the fraudster has remote access to your computer. They convince you that they will give you money or provide a refund of some kind. ***They are able to create a fictitious image of your account to show a deposit, when in fact there has been no deposit made.*** Typically, they explain that they have accidentally given you too much and ask that you just send the rest back in gift cards or a wire. Gift cards are on the rise for fraudsters to receive some sort of financial gain from their scam. Online banking systems are very secure but when you allow someone to access your computer, you are taking the risk. Please be cautious of this particular scam as they can create what seems to be a trustworthy relationship/friendship with you first.

We ask you to please never share your login access or credentials to anyone!

We Can Help!

PCM Credit Union cares about you as our member and does not want anyone to fall victim to these scams. We are here to help and to answer questions you may have. Please know that we have fraud rules in place on our debit and credit card programs. Although you may be inconvenienced with a denied charge on your card at some point, your legitimate transaction may have hit one of our fraud rules. Our fraud rules are based mainly upon current fraud trends and are in place to protect our members as best we can. Please contact us if you have any questions or concerns or have fallen victim to any of these current fraud trends. ***PCM is here to help!***