SCAM ALERT

TCU Check Scam Alert

Please be aware of fraudulent Teachers Credit Union checks circulating nationwide due to several scams: secret shopper, car wrapping, amazon gift cards, purchase eBay items, etc. If you receive a postage paid envelope with instructions and a bank or credit union check, it is most likely a scam – please don't fall victim to these scams. Please call 608-362-8983 to verify all Teachers Credit Union checks before cashing or depositing them. Thank You!

#1
IRS WARNS OF EMAIL SCAM ABOUT TAX REFUNDS

The Internal Revenue Service (IRS) issued a consumer alert about a Internet scam in which consumers receive an email informing them of a tax refund. The email, which claims to be from the IRS, directs the consumer to a link that requests personal information, such as Social Security number and credit card information.

This scheme is an attempt to trick the email recipients into disclosing their personal and financial data. The practice is called "phishing" for information.

The information fraudulently obtained is then used to steal the taxpayer's identity and financial assets. Generally, identity thieves use someone's personal data to steal his or her financial accounts, run up charges on the victim's existing credit cards, apply for new loans, credit cards, services or benefits in the victim's name and even file fraudulent tax returns.

The bogus email, which claims to come from "tax-refunds@irs.gov" tells the recipient that he or she is eligible to receive a tax refund for a given amount. It then says that, to access a form for the tax refund, the recipient must use a link contained in the email. The link then asks for the personal and financial information.

The IRS does not ask for personal identifying or financial information via unsolicited email. Additionally, taxpayers do not have to complete a special form to obtain a refund.

If you receive an unsolicited email purporting to be from the IRS, take the following steps:

*Do not open any attachments to the email, in case they contain malicious code that will infect your computer.

*Contact the IRS at 1 (800) 829-1040 to determine whether the IRS is trying to contact you about a tax refund.

The IRS has seen numerous attempts over the years to defraud the public and the federal government through a variety of schemes. You can find more information on these schemes on the criminal enforcement page at www.IRS.gov.

IMPORTANT INFORMATION FROM YOUR CREDIT UNION

RECENTLY, AREA CREDIT UNIONS HAVE INDICATED THAT SEVERAL OF THEIR MEMBERS HAVE BEEN SCAMMED INTO DIVULGING THEIR PERSONAL AND ACCOUNT INFORMATION OVER THE INTERNET.

PLEASE BE AWARE THAT TEACHERS CREDIT UNION WILL NEVER SOLICIT EITHER PERSONAL AND/OR ACCOUNT INFORMATION FROM YOU EITHER VIA EMAIL OR VIA OUR WEBSITE. WE WOULD HAVE NO REASON TO DO SO AS ALL OF THIS INFORMATION WAS PROVIDED TO US AT THE TIME YOUR ACCOUNT WAS OPENED. THERE WOULD NEVER BE REASON FOR US TO "CONFIRM" OR "VERIFY" THIS INFORMATION IN THIS MANNER.

IF YOU SHOULD RECEIVE AN EMAIL THAT LOOKS LIKE IT IS FROM TEACHERS CREDIT UNION, IT IS IMPORTANT THAT YOU ***DO NOT OPEN*** THE EMAIL, BUT DELETE THE MESSAGE IMMEDIATELY. IF YOU DO OPEN THE MESSAGE AND SEE A LINK TO A WEB PAGE, ***DO NOT CLICK ON THE LINK.*** THE LINK WILL TAKE YOU TO A "PHONY" WEB SITE TAT IS SET TO LOOK LIKE OURS, BUT IT IS NOT.

SHOULD YOU BE SCAMMED IN SUCH A MANNER, PLEASE REPORT THE INCIDENT TO US AS WELL AS THE INTERNET FRAUD COMPLAINT CENTER AT http://www.ifccfbi.gov/index.php

#3

Email scam targets credit union members.

At least two Wisconsin credit unions have reported that their members recently received fraudulent emails trying to trick them into disclosing personal information. The phony emails appear to be from the National Credit Union Administrations (NCUA), but they are not.

The email asks recipients to click on a link to verify credit union account registration. If the recipients do so, the link directs them to a false website--which appears to be the NCUA site but is not--and asks for their credit union account numbers and PIN's, along with other personal information.

NCUA does not ask credit union members for such personal information. Any one who receives an email that purports to be from the NCUA and asks for account information should consider it to be a fraudulent attempt to obtain their personal account data for an illegal purpose and should not follow the instructions in the email.

If you responded to such an e-mail and provided any confidential account information, please notify your credit union immediately of the scheme. You should also change your account's PIN, and take any additional action recommended by your credit union to protect your account.

Please forward the email scam/phishing message you have received to federal investigators at JWilson@IC3.gov with a copy to DavidE@NCUA.gov

were to be

#4

Teachers Credit Union has seen a new scam hit the local area. We wish to make you aware of this situation and ask that you use caution in any situation with similar characteristics. If it sounds too good to be true, it is!

A Teachers Credit Union member received a letter from Spain indicating he had won an international lottery. A check was not included with the letter, but he was told that his prize could be picked up in person or wired to his account. Of course, in order for this to be done, he had to provide personal account information, including mother's maiden name. Remember, never give this information to anyone unless you are the one to initiate the contact. Once fraudsters have this information, your identity and your credit history may be hijacked. Our member was correct to be suspicious. We provided him the address and phone number Consumer Protection in Madison, which is 1-800-422-7128.

We have also heard of similar "lottery scams" from other credit unions over the years. However, asking for account information is a new "twist" on the old scam. Even if a check were to be forwarded to you as your "international lottery prize," Teachers Credit Union would place a hold on the check for the time period it takes to clear (or not to clears, as the case might be) strictly for your protection.

#5

It has come to our attention that members are receiving emails supposedly from Teachers Credit Union. The email indicates that their Visa and/or MasterCard account information may have been compromised and that they must verify their information in order to avoid a permanent account suspension. The member is then directed to click on a website to verify their credit &/or debit card information. They are then directed to a “Spoofed” website; i.e. a website with a counterfeit Teachers Credit Union logo that LOOKS like Teachers Credit Union’s website BUT IS NOT.

Please be advised that Teachers Credit Union would NEVER contact you via email for verification of account information as we already have all your account information on file. This email is being generated by currently unknown persons who are sending out a mass mailing to hundreds of thousands of people with the hopes of finding one TCU member who will provide their confidential account information. Please do NOT respond to such an email. Please delete the email and do NOT open it. A sample of the fraudulent email is shown below.

Dear member,

Credit Union was notified by Visa and Mastercard that some members card information may have been compromised as a result of a security breach that recently occurred involving unauthorized access into a third party processor`s data system.

This breach is not associated with C.U computer systems. C.U requires the customer to provide up-to-date and accurate information. For your protection, we have limited access to your account. A temporary block has been placed on your account until we receive your account information.

If your card number has been compromised you will be notified by phone and/or e-mail. Please note that failure to reply within 5 days will result in permanent cancelation of your account with Credit Union

Click on the following link to remove this temporary block placed on your account

Counterfeit link is provided here

Please be aware that our Teachers Credit Union website www.tcubeloit.org is a SECURED website and your account information is secure. These services have NOT been impacted by this “Spoof” email. However, we feel we MUST notify you that someone is attempting to use our credit union’s logo to gather your personal account information. However, you can rest assured that your account information and our website information are safe, secured and protected!

Sincerely,

Suzanne Kralick, President