BEWARE OF SCAMS AND SKIMMERS

September 26, 2018 - Beware of the many tactics fraudsters and criminals use to obtain personal information and try to access your accounts … and, ultimately, try to take your money.

“The two types of scams we are seeing most frequently are those in which people are tricked into giving out their online banking credentials and also computer scams,” reports Brittany Leeper, senior fraud analyst at Interra Credit Union, Goshen.

Fraudsters obtain online banking credentials by requesting usernames and passwords, promising to deposit money back into the account as a way of “testing” to see if the account is legitimate. Then, the unsuspecting victim is instructed to send either the full or partial amount via Western Union, MoneyGram or with gift cards. After the person has completed the transfer, the fraudster promises to deposit the money back into the account.

With computer scams, victims are often prompted to call a phone number listed in a pop-up screen promising to provide virus protection. “The fraudsters may then hack into the computer and online banking, making transfers between accounts,” Leeper said. They manipulate the person into believing he or she over-deposited new money into an account and is then instructed to purchase gift cards to pay them back. “The victim is none-the-wiser, follows the instructions and loses money in the process,” she noted.

Consumers in several states, including Indiana, are also receiving calls from spoofed telephone numbers that even appear to be from the credit union or other financial institution. The caller claims to be a credit union or bank employee in the fraud or security department. The victim is tricked into providing the security code on the back the debit card, along with the card’s expiration date. These criminals already possess the counterfeit mag stripe cards and use the information to change the PINs, using the counterfeit cards to make ATM withdrawals and purchases.

Another way the criminals gain card information is by using skimmers, and law enforcement reports indicate increased activity in northern Indiana with an increase in area card skimming. Be on the lookout at ATMs and at the gas pump, too, Leeper advises. “Before you insert your card at the pump or at an ATM, stop and take a look,” she said. “Does anything seem different?”

What is skimming? Criminals place a card reader over an existing one and use it to obtain the owner’s card information, affecting both debit and credit cards.

How can you tell if a skimmer has been placed on an ATM?

- At the ATM, the bad guys may use a 3-D printer to create a new keyboard to put on top of the real one. The keyboard may look different from the rest of the ATM, or the keys could seem bigger.
- Wiggle the card reader to see if it's loose. The criminals may place a card reader on top of the existing one.
- Be wary if it's hard to insert your debit or credit card.
- Avoid ATMs that don't have much traffic.
- Always cover the keyboard when you enter your PIN, as some bad guys may conceal a pinhole camera near an ATM and record your PIN entry. On others, however, the camera may actually be placed inside the skimmer.

At the gas pump fraudsters must open the fuel dispenser door to insert the skimmer.

- Is there a broken seal or is there a strip of tape that has been broken? If so, then this is likely a sign that the pump has been tampered with.
- Avoid gas pumps that are out of sight of the clerk.
- While "pay at the pump" is convenient, there is less chance of fraud if you pay the clerk inside the station.

Be proactive!

- Most financial institutions, including Interra, offer transaction alert options that you can sign up for on debit cards and credit cards. That way, you will know when suspicious activity takes place.
- When you use online banking, you have the ability to monitor your account activity frequently.
- Make sure to check all your account statements for the accuracy of transactions.

Leeper offers these suggestions to you help protect yourself:

- NEVER give out your online banking credentials, account numbers, passwords, etc.
- NEVER purchase gift cards as payment.
- ALWAYS be wary of anyone who calls and claims that urgent action is needed or appears to be threatening in any way.
- ALWAYS change your PIN numbers frequently.
- Legitimate financial services providers, like Interra will NEVER contact you to ask you what your account number is.

"If you believe you have been victimized, it's important to contact your financial institution immediately," Leeper added.