INTERNET FRAUD

Online scams and viruses are constantly evolving and they threaten the security of computers worldwide. As criminals evolve their tactics, you need to keep your PC's security software (virus detection, security patches, etc.) up-to-date. The more you know about how to protect your computer and yourself, the less likely you are to be negatively impacted.

- Be suspicious of any email with urgent requests for personal financial information.
- If you don't know the sender, do not use the links in the email.
- Avoid completing forms in email messages that ask for personal financial information.
- Be sure to use a secure web site when submitting credit card or other sensitive information via the web browser.
- If you are not sure of the website's legitimacy, or if the offer sounds too good to be true, don't provide your personal or financial information. Verify the website by checking with a consumer information site such as the Better Business Bureau.
- Regularly check bank, credit and debit card statements to ensure all transactions are legitimate.
- Use security software (virus detection, firewalls, etc.) that update automatically.
- Keep your passwords for online activity in a secure place; do not leave them in plain sight or share them.
- Make sure your browser is up-to-date and security patches have been installed.
- If your home PC is utilized by multiple family members, consider purchasing a second PC (ex: laptop or netbook) that will only be utilized for your online banking and storing of your financial information (ex: Quicken or TurboTax). A PC utilized by multiple users presents the opportunity for malware unknowingly downloaded on to it.
- If you think that your PC has been compromised, stop using it immediately, disconnect the internet access and have it checked for malware. If you believe that your online banking has been compromised due to malware, notify your financial institutions immediately.

Email Phishing

Phishing (pronounced "fishing") is a scam to steal valuable information such as credit card and Social Security numbers, user IDs, and passwords. In phishing, also known as "brand spoofing," an official-looking email is sent to potential victims pretending to be from their ISP, credit union, bank, or retail establishment. Emails can be sent to people on selected lists or on any list, and the scammers expect some percentage of recipients will actually have an account with the real organization.

Protect Yourself

Canandaigua Federal Credit Union will never send an email to verify your account information. If you receive an email claiming to be from the Credit Union that requests that you provide personal information in an unsecure email or via a link to a website, please contact the Credit Union immediately.

IDENTITY THEFT

Identity theft occurs when someone uses your personal information without your knowledge to commit fraud or other crimes. In many cases, the victim is unaware of the activity until months after the incident. The effect of identity theft can be costly to you in terms of time and money.

Identity Theft can happen in various ways:

- After someone steals your wallet, purse or mail.
- By stealing personnel records from employers.
- By pretending to be financial institutions or businesses and sending spam email (called phishing) or pop-up messages in an attempt to get you to reveal your personal information.
- Identity thieves will also rummage through the trash at your home or workplace looking for bills or other documents with your personal information on it.

To protect your identity, you should:

- Review your credit reports. You can do this for free annually! Visit Annualcreditreport.com or call 1-877-322-8228, which were established to handle consumer requests by the consumer reporting companies Equifax, Experian and TransUnion.
- Place a fraud alert on your credit bureau files if you feel information has been exposed.
- Adopt daily practices like shredding your personal & financial documents, staying aware of the latest scams, protecting your home computer with anti-spyware, virus detection software and firewalls. Keep these programs up to date.
- Secure your mail by utilizing a Postal Service Mail Box or by placing your outgoing mail into locked mailbox.
- Sign up for estatement services – not only does it protect your monthly statement, it also cuts down on paper and postage expense!
- Safeguard your Social Security Number – don't leave your Social Security Card in your wallet and ask why when a person requests your SSN for business purposes.
- Don't leave a paper trail. Never leave ATM, credit card or gas station receipts behind.
- Know with whom you are speaking with before providing any confidential information. If you are not sure about the legitimacy of the caller, hang up and call back by utilizing a telephone number familiar to you.
- Never click on links sent to you by an unsolicited email.
- Be alert for warning signs of possible Identity Theft, such as:
- Regular bills that do not arrive as expected.
- Denials of credit for no apparent reason.
- Account Statements or credit cards in the mail that you were not expecting.
- Calls or letters concerning purchases you did not make.

If you think your identity has been compromised:

- If your bank accounts have been compromised, immediately notify those Financial Institution(s). Make a note for your file of what Institution was contacted, who you talked to and the date/time your call was made.
- Place a verbal password on your accounts to prevent thieves from calling in and finding out more about your financial transactions.
- Close or transfer those accounts that have been compromised or tampered with to a new account number.
- Request that any account that was fraudulently opened in your name be closed immediately.
- Place a Fraud Alert on your Credit Report. You can do this by contacting the Credit Bureaus:
- **Experian**: 1-888-397-3742
- **Equifax**: 1-800-685-1111
- **Trans Union**: 1-800-888-4213
- Request a copy of your Credit Reports and review them carefully. Question any unknown activity and report disputes in writing.
- File a police report and maintain a copy in your file for future reference.
- File a report with the Federal Trade Commission. You can do this online via ftc.gov.
- Keep an eye out for future attempts. Identity Thieves often will lay low for months and then strike again, hoping to catch you off guard.

CHECK SCAMS

Don't get scammed out of your hard earned money! There are many variations of the counterfeit check scam. Modern computer technology allows crooks to easily create realistic looking personal checks, business checks, Cashier's Checks or Money Orders. It could start with someone giving you an "advance" on a sweepstakes you've supposedly won, a great work from home offer or asking you to help a family in a foreign country by transferring funds to your account for safekeeping. Whatever the pitch, don't get caught with your guard down.

Here are some tips that will help you avoid becoming the victim of a counterfeit check scam:

- Shred any offer that asks you to pay for a prize or a gift. Legitimate sweepstakes offer consumers a chance to win a prize or money with no purchase or entry fee required.
- Know who you're dealing with, and never wire money or send a check to strangers. If you must send a check, consider utilizing a Cashier's Check or Money Order instead of your own personal check to keep your personal information safe.
- Watch out for any lottery, secret shopper or business offer that involves you receiving a check and requires you to forward money by MoneyGram or Western Union.

- If you’re selling something, don’t accept a check for more than the selling price, no matter how tempting the offer or how convincing the story. Ask the buyer to write the check for the exact amount. If the buyer refuses to send the exact amount, don’t send the merchandise or a refund.
- Resist pressure to act immediately. Any legitimate offer should still be good after the check clears.
- If you're concerned about the validity of a check, either contact the Financial Institution by telephone (via the number you looked up) or take the check to the local branch office of that Institution.
- Watch out for any job opportunity that asks you to be a money transfer agent. Legitimate businesses should not ask you to deposit their checks into your personal account, then instruct you to forward the funds by wire or send by MoneyGram/Western Union to other individuals or to accounts in other countries.
- It’s best not to rely on money from any type of check unless you know and trust the person you’re dealing with or, better yet until your financial institution confirms that the check has cleared. Forgeries can take weeks to be returned through the banking system, and until you have confirmation that the funds from a check have cleared your account, you are responsible for any funds you withdraw against that check, whether or not the financial institution places a hold on them.
- Resist the urge to enter foreign lotteries. It is illegal to play foreign lotteries in the United States. If you are notified that you are a winner of a lottery that you didn’t enter, chances are you’re being scammed.
- Monitor your checking account activity carefully. A counterfeiter only needs to obtain the MICR line (those funny looking numbers on the bottom of your check) to create fake checks that are presented against your account.
- Immediately report if you think you’re a victim of a check fraud scheme or if you notice something suspicious. Contact your Financial Institution as well as the local police department, or your local FBI Field Office.

PHONE SCAMS

Many people trust phone calls, especially if the person on the other side of the line knows even a small piece of information. Like email, phishing attempts can yield surprising results. Other fraud takes the form of involuntary commitment and contract approval.

Here are a few tips to recognize a phone scam:

- Never give out your credit card number on the phone unless you initiated the call to a reliable company that you know.
- Always ask for written information before you agree to anything.
- If you suspect that “something’s not right”, get off the phone right away.
- Don’t provide information that the company calling should already know.
- Avoid high-pressure sells.

Land Line Telephone Vishing & VoIP (Internet Phones) Vishing

Vishing, (Voice Phishing) also called "VoIP phishing for Internet phones," is the voice counterpart to phishing. Instead of being directed by e-mail to a Web site, an e-mail message asks the user to make a telephone call. The call triggers a voice response system that asks for the user's card number or other personal or financial information. The initial bait can also be a telephone call with a recording that instructs the user to phone an 800 number or another area code within or outside of the United States.

In either case, because people are used to entering card numbers over the phone, this technique can be effective. Voice over IP (VoIP) is used for vishing because caller IDs can be spoofed and the entire operation can be brought up and taken down in a short time, compared to a land line telephone.

Text Message Smishing

Smishing (SMS Phishing) is the mobile phone counterpart to phishing. Instead of being directed by e-mail to a Web site, a text message is sent to the user's cell phone or other mobile device with some ploy to click on a link. The link causes a Trojan to be installed in the cell phone or other mobile device.

Protect Yourself

NASA Federal Credit Union will never call you to verify your account information. Be sure to use only the phone numbers that you know to be true for the Credit Union when responding to phone messages. If you have responded to a phone scam and provided any confidential account information, please notify us immediately.

CREDIT & DEBIT CARD FRAUD

Credit and debit card fraud costs cardholders and issuers millions of dollars each year. While theft is the most obvious form of fraud, it can occur in other ways. For example, someone may use your card number without your knowledge.

Here are some tips to help protect yourself from credit and debit card fraud:

Do:

- Sign your cards as soon as they arrive.
- Keep a record of your account numbers, their expiration dates, and the phone number and address of each company in a secure place.
- Keep an eye on your card during the transaction, and get it back as quickly as possible.
- Void incorrect receipts.
- Save receipts to compare with billing statements.
- Open bills promptly and reconcile accounts monthly, just as you would your checking account.
- Report any questionable charges promptly and in writing.
- Notify card companies in advance of a change in address.

Don't:

- Lend your card(s) to anyone.
- Leave cards or receipts lying around.
- Sign a blank receipt. When you sign a receipt, draw a line through any blank spaces above the total.
- Write your account number on a postcard or the outside of an envelope.
- Give out your account number over the phone unless you're making the call to a company you know is reputable. If you have questions about a company, check it out with your local consumer protection office or the Better Business Bureau.