UGEFCU
UTICA GAS & ELECTRIC FEDERAL CREDIT UNION
215 Old Campion Road
New Hartford, NY 13413
(315) 733-1596
www.ugefcu.com

For more identity theft prevention tips, call or stop in to UGEFCU today. And if you ever become a victim of identity theft, remember that we're here to help.
(315) 733-1596
Toll-free 800-990-7499
www.ugefcu.com

NCUA Adv. #120 - Nov. 2021

Prevention tips

Take these tips with you to become a smarter consumer and avoid fraud:

• Know who you're dealing with. Make sure to check with your state or local consumer protection agency and the Better Business Bureau (BBB) to see if the seller, charity, company, or organization is credible. Be especially wary if the entity is unfamiliar to you. Always call the number found on a website's contact information to make sure the number legitimately belongs to the entity you are dealing with.

• Pay the safest way. Credit cards are the safest way to pay for online purchases because you can dispute the charges if you never get the goods or services or if the offer was misrepresented. Federal law limits your liability to $50 if someone makes unauthorized charges to your account, and most credit card issuers will remove them completely if you report the problem promptly.

• Guard your personal information. Crooks pretending to be from companies you do business with may call or send an email, claiming they need to verify your personal information. Don't provide your credit card or bank account number unless you are actually paying for something and know who you are sending payment to. Your social security number should not be necessary unless you are applying for credit. Be especially suspicious if someone claiming to be from a company with whom you have an account asks for information that the business already has.

• Stay safe online. Don't send sensitive information such as credit card numbers by email because it's not secure. Look for clues about security on Web sites. At the point where you are asked to provide your financial or other sensitive information, the letters at the beginning of the address bar at the top of the screen should change from "http" to "https" or "shttp." Your browser may also show that the information is being encrypted, or scrambled, so no one who might intercept it can read it. But while your information may be safe in transmission, that's no guarantee that the company will store it securely. See what Web sites say about how your information is safeguarded in storage.

• Be cautious about unsolicited emails. They are often fraudulent. If you are familiar with the company or charity that sent you the email and you don't want to receive further messages, send a reply asking to be removed from the email list. However, responding to unknown senders may simply verify that yours is a working email address and result in even more unwanted messages from strangers. The best approach may simply be to delete the email.

• Resist pressure. Legitimate companies and charities will be happy to give you time to make a decision. It's probably a scam if they demand that you act immediately or won't take "No" for an answer. Some scammers may also demand you pay off a loan immediately or damaging consequences may occur, always take time to look into who is requesting the money before you pay up.

• Don't believe promises of easy money. If someone claims that you can earn money with little or no work, get a loan or credit card even if you have bad credit, or make money on an investment with little or no risk, it's probably a scam.

• Fully understand the offer. A legitimate seller will give you all the details about the products or services, the total price, the delivery time, the refund and cancellation policies, and the terms of any warranty. Contact the seller if any of these details are missing, if they are unable to provide the details, it may be a sign that it's a scam.

• Get off credit marketing lists. Credit bureaus compile marketing lists for pre-approved offers of credit. These mailings are a goldmine for identity thieves, who may steal them and apply for credit in your name. Get off these mailing lists by calling 888-567-8688 (your social security number will be required to verify your identity). Removing yourself from these lists does not hurt your chances of applying for or getting credit.

• Check your credit reports regularly. If you find accounts that don't belong to you or other incorrect information, follow the instructions for disputing those items. You can ask for free copies of your credit reports in certain situations. If you were denied credit because of information in a credit report, you can ask the credit bureau that the report came from for a free copy of your file. And if you are the victim of identity theft, you can ask all three of the major credit bureaus for free copies of your reports. Contact the credit bureaus at: Equifax, 800-685-111; Experian, 800-311-4769; TransUnion, 800-888-4213.

• Everyone can request free copies of their credit reports once a year. A new federal law entitles all consumers to ask each of the three major credit bureaus for free copies of their reports once in every 12-month period. Go to www.ftc.gov/credit or call 877-382-4357 for more details and to see when you can make your requests. You don't have to ask all three credit bureaus for your reports at the same time; you can stagger your requests if you prefer. Do not contact the credit bureaus directly for these free annual reports. They are only available by calling 877-322-8228 or going to www.annualcreditreport.com. You can make your requests by phone or online, or download a form to mail your requests.

• Be cautious about offers for credit monitoring services. Why pay extra for them when you can get your credit reports for free or very cheap? Read the description of the services carefully. Unless you're a victim of serious and ongoing identity theft, buying a service that alerts you to certain activities in your credit files probably isn't worthwhile, especially if it costs hundreds of dollars a year. You can purchase copies of your credit reports anytime for about $9 through the bureaus' Web sites or by phone: Equifax, 800-685-111; Experian, 800-311-4769; TransUnion, 800-888-4213.

Latest scams experienced by other credit unions

1. The first one was an IRA check from Fidelity for about $130,000.
This was a member that had an old IRA previously and had recently opened up a new IRA a few months prior. She was given instructions from the fraudsters to put about $50,000 into her savings and $40,000 into her checking and the rest into her IRA. Everyone was concerned about the tax implications and warned her about those. She was also asked about fraud but was sure it wasn't. The fraudsters had told her she was going to be an agent for UNICEF and she would get paid like a part time job. They needed the money in green dot cards and she got to keep some of it.

2. The second one that just happened was a man got the phone call about his Amazon account being hacked and that someone had bought an iphone 12 from California. The caller said they were going to reimburse them $300. The member let them remote into his computer while he was logged into home banking. The fraudster made a transfer of $30,000 from the member savings to their checking *(the money was the members already and was 'seasoned').* The fraudster then pretended to be upset because he 'made a mistake' and put in $30,000 instead of $300 and that he was going to get fired etc. He begged the member to wire him the difference back to wire info that he had given him. The wire was a wire to Thailand. The member came in and every person didn't feel right about it. I pulled the member aside and explained that there has been a lot of fraud and that he could talk to us if he suspected anything or had any questions and that we were trying to protect him. He said he had gotten a personal loan from a friend a few years prior and was just paying it back now. About a day after the wire went through he came back in and told me that he had lied to me and he thinks he was scammed. He then told me the story about the amazon phone call.

Scholarship Scams

(by Fraud.org staff)

Prospective college students often look to scholarships as a way to lessen the financial burden on parents and to avoid taking out student loans. Unfortunately, scam artists know how stressful paying for college can be and they've tailored scholarship scams to separate eager students and their families from their money.

Stay safe. Be Informed.

• **Know who you're dealing with.** It may be a search company that is offering to help locate scholarships for which you may be eligible, rather than a foundation that actually awards scholarships. Most foundations don't charge a fee to apply for a scholarship; if they do, it is very small. Scholarship search companies always charge for their services.

• **Beware of search services that guarantee you'll receive scholarship money.** No search service can control the decisions of scholarship sponsors.

• **Get the details in writing.** A search service should be willing to give you a written explanation of exactly how it works.

• **Make sure you understand the refund policy.** The company should explain upfront whether you can get your money back if you don't receive a scholarship and what you have to do to qualify for a refund. Some fraudulent search services set difficult requirements, such as obtaining letters of rejection from each scholarship listing, to make it virtually impossible to get a refund.

• **Do your own scholarship search.** A search service may provide information that is outdated or doesn't apply to you. You may be better off finding scholarships yourself. Ask your high school guidance counselor and college financial aid offices for help. Another good source of information is College Parents of America.

Scammers… Holiday Shoppers Beware! *(by Fraud.org staff)*

Record-breaking backlogs at the nation's ports this fall are a significant contributor to the inflation that is hitting Americans right in the pocketbook recently. And with the disruptions likely to last into 2022, it could be harder than ever for consumers to get sought-after toys and must-have gifts this holiday season.

Unfortunately, consumers' eagerness to get their hands on PlayStation 5's, L.O.L. Surprise! Dolls, and Baby Yodas — combined with global supply chain disruptions — are likely to play right into scammers' hands. Each year, fraudsters set up fake websites, run bogus online auctions, or post ads on Craigslist and social media claiming to be able to obtain and resell sought-after gifts. Internet merchandise scams regularly top Fraud.org's annual Top Ten Scams list. This year, with the supply chain disruptions making toys scarcer than ever, parents are likely to be even more vulnerable to these scams.

A 2018 survey by Experian found that 8 percent of consumers reported being a victim of identity theft during the holiday season, with 43 percent of those victims saying that the theft happened while shopping online. As millions more Americans continue to shop online due to the COVID-19 pandemic, the threat of identity fraud during the holiday shopping season has only grown.

To stay safe this holiday season, Fraud.org recommends shoppers take the following steps:

• Steep discounts = Too good to be true. If your child is desperate for an XBOX Series X (retail price: $499 and up) and you see one online at a steep discount, chances are that it's a scam. Whether you're searching for an impossible-to-find toy or just a pair of slippers for your spouse, the safest places to buy are with retailers you've purchased from in the past.

• Watch out for emails or text messages promising must-have gifts or discounts. Email and text message phishing scams are a tried-and-true method for scammers to find victims. Don't click on links or attachments (such as those pointing you to "discount codes"), as these can infect your computer or cell phone with malware or even encrypt your files with ransomware.

• Beware of counterfeit toys. According to the Toy Association, nearly 1 in 5 (19 percent) of parents report that their child has received a counterfeit or knock-off toy purchased online. Counterfeit toys are not made in adherence with strict federal toy safety standards, increasing the potential for dangerous products to enter your home. You can reduce your risk of buying a dangerous toy by shopping with brick-and-mortar retailers and trusted online marketplaces.

• Credit cards are the safest way to pay. Regardless of where you buy toys, paying with a credit card gives you dispute resolution rights in case the transaction goes bad. If a seller asks you to pay with a gift card, via a peer-to-peer payment app, wire transfer, or even cash, you are likely to be out of luck if the gift never arrives or is not in the condition you expected.

Scams can strike anyone at any time of the year. If you suspect that you or someone you know has become a victim of this scam or any other fraud, report it at once. You can file a complaint at Fraud.org via our online complaint form. We'll share your complaint with our network of law enforcement and consumer protection agency partners who can investigate and help put fraudsters behind bars.

Credit Repair Fraud
(by Fraud.org staff)

Good credit is important—a bad credit history can prevent you from getting a loan, housing, or a job. Promises to "fix" your credit report may be tempting, but they're not true.

Stay safe. Be Informed.

• No one can erase negative information if it's accurate. Only incorrect information can be removed. Accurate information stays on your record for 7 years from the time it's reported (10 years for bankruptcy). Even information about bills you fell behind on but now are paid will remain on your report for these time periods.

• Credit repair services can't ask for payment until they've kept their promises. Federal law also requires credit repair services to give you an explanation of your legal rights, a detailed written contract, and three days to cancel (this applies to for-profit services, not to nonprofit organizations, banks and credit unions, or the creditors themselves).

• You can correct mistakes on your credit report yourself. If you were recently denied credit because of information in your credit report, you have the right to request a free copy from the major credit bureaus, regardless if your state law provides one for free as well, otherwise there is a small fee. It doesn't cost anything to question or dispute items in your report. Follow the instructions provided by the credit bureau. The major credit bureaus are:Equifax, 800-685-1111; Experian, 800-682-7654; and TransUnion, 800-916-8800. Contact all three, as the information each has may vary.

• You can add an explanation to your report. If there is a good reason why you weren't able to pay bills on time (job loss, sudden illness, etc.) or you refused to pay for something because of a legitimate dispute, give the credit bureau a short statement to include in your file.

• Know that you can't create a second credit file. Fraudulent companies sometimes offer to provide consumers with different tax identification or social security numbers in order to create a new credit file. This practice, called "file segregation," is illegal, and it doesn't work.

• If you have credit problems, get counseling. Your local Consumer Credit Counseling Service (CCCS) can provide advice about how to build a good credit record. The CCCS may also be able to make payment plans with your creditors if you've fallen behind. These services are offered for free or at a very low cost. To find the nearest CCCS office, call toll-free, 800-388-2227, or go to www.nfcc.org.

UGEFCU members can be assured of confidential financial counseling with our certified credit union staff, call us: (315)733-1596

FRAUD!ORG
a project of the National Consumers League

Report scams to the National Fraud Information Center/ Internet Fraud Watch at fraud.org.
Sign up for email scam alerts and read more scam articles.

Government Grants
(by Fraud.org staff)

Claims of "free government grants" from the US government asking for personal information such as your Social Security and bank account numbers or pay a "processing fee." But instead of giving you a grant, the plan is to steal your identity, your money, or both.

Stay safe. Be Informed.

• **The government doesn't telephone people or send unsolicited letters or emails to offer grants.** If someone contacts you unexpectedly and offers you a grant, it's a scam. Don't provide your financial account numbers, Social Security numbers, or other personal information in response to such an offer. Crooks "phish" for that information to steal victims' money and impersonate them for other illegal purposes.

• **Government grants never require fees of any kind.** You might have to provide financial information to prove that you qualify for a government grant, but you won't have to pay to get one.

• **Government grants require an application process.** They aren't simply given over the phone and are never guaranteed. Applications for government grants are reviewed to determine if they meet certain criteria and are awarded based on merit. If you didn't apply for a government grant and someone says you're receiving one, it's a scam.

• **Government grants are made for specific purposes, not just because someone is a good taxpayer.** Most government grants are awarded to states, cities, schools, and nonprofit organizations to help provide services or fund research projects. Grants to individuals are typically for things like college expenses or disaster relief.

• **Don't be fooled by official or impressive sounding names.** Swindlers claiming to provide or help get government grants often invent impressive-sounding names and titles for themselves and the companies they represent. They operate under many different names and phone numbers, take your money, then leave town to start all over again.

• **Beware of services offering government grant information for a fee or requesting your personal information to provide it.** Information about government grants and other benefits is free (though there may be a fee for some print publications) and you don't have to give personal information to get it.

Resources for Information about Government Grants and Benefits

Center for Digital Business
Online catalogue of federal domestic assistance programs. Hard-copy available for a fee through the Government Printing Office, (202) 512-1800 or toll-free outside of the DC metro area, (866) 512-1800.

Federal Student Aid
Information and applications from the U.S. Department of Education for student financial aid programs. Telephone hotline, (800) 433-3243, operates Monday-Friday 8 a.m. to midnight Eastern Standard Time, Saturday 9 a.m. to 6 p.m.

Benefits.gov
Information about a wide variety of state and federal government benefits and programs. Telephone hotline, (800) 333-4636, operates Monday-Friday, 8 a.m. to 8 p.m. Eastern Standard Time. www.grants.gov Information about grants available from government agencies. Telephone hotline, (800) 518-4726, operates Monday-Friday, 7 a.m. to 9 p.m. Eastern Standard Time.