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

Utility shut-off scammers threaten to turn off the lights on consumers during pandemic. Don't fall for scammers tricking you out of hundreds or thousands of dollars through utility scams. (*by fraud.org 7/01/2020*)

As the world reels from the COVID-19 pandemic, in addition to the threat to public health, the virus is also wreaking unprecedented economic havoc. Tens of millions of Americans are out of work, and many are wondering how we are going to keep the lights on. Unfortunately, scammers are aware of this, too. NCL has recently seen a spike in consumer complaints about scammers posing as local power company representatives threatening to shut off fearful consumers.

The anatomy of the scam is highly consistent: a consumer receives a call from someone claiming to be with the electric utility company. The caller warns the consumer that their power is about to be shut off over an unpaid bill. The only way to avoid this is to pay up immediately, typically via wire transfer, gift card, or some other difficult-to-stop payment method.

Such a call can be very scary—particularly for those who may need electricity to power medical devices or run their small business. Unfortunately, due to the COVID-19 pandemic, many consumers are having trouble keeping up with their bills, which may make them even more vulnerable to this scam. And even for consumers who are confident they've paid their bill, the impending threat of a shut-off at the height of summer heat can cause a panic.

The story we received recently from a consumer in Detroit, Michigan is typical of these scams. She writes: *"I was called by [someone] claiming to be a manager for DTE stating that my bill had not been paid and my services were going to be shut off and would not be turned back on for another week if I didn't pay him in 40 minutes. I was told to drive to a Speedway where I loaded $400 on to one card and $387.63 on the second card. I immediately gave the man the 14-digit code on the back and he advised me that services would not be shut off."*

<u>To spot the red flags of these scams, and avoid becoming a victim, here are some tips that you can use:</u>

- **Don't panic**. According to the National Association of Regulatory Utility Commissioners, electric utilities in all 50 states have placed moratoriums on disconnections during the COVID-19 crisis, either voluntarily or in response to government orders. If someone contacts you claiming that they're about to shut-off your electricity, it's a scam.

- **Worried? Contact the power company.** A utility will never initiate a disconnection without contacting you via the mail first. If you received a call from someone claiming they're about to turn off your power, hang up and contact your electric company. Their toll-free phone number and website address is typically listed on your electric bill.

- **Beware of unusual payment methods.** Anyone who asks you to pay an overdue electric or other utility bill via wire transfer, gift card, bank-to-bank transfer, bitcoin, or any other unusual payment method is almost certainly trying to scam you.

- **Do not give out personal information.** Utility imposters may offer to connect their victims to federal assistance programs or payment plans to help pay their overdue bills. They just need to "verify" the victim's information. In reality, these scammers are trying to gather the information they need to steal your identity. If you suspect something is amiss, hang up and call your utility company directly.

Lost your job? Be careful ID thieves don't take your unemployment benefits, too! For the tens of millions of newly jobless, unemploy ment benefits are a lifeline. Unfortunately, scammers are after that lifeline too. (*by fraud.org 6/01/2020*)

The latest reports are historically grim: nearly 40 million Americans have been thrown out of work due to the COVID-19 pandemic. For the tens of millions of newly jobless, state unemployment insurance benefits are a lifeline that helps them keep the lights on and provide food for their families.

Unfortunately, to add salt to the wounds of the newly unemployed, circumstances are ripe for identity thieves. The combination of billions of dollars in federal stimulus money flowing in to state unemployment funds and tens of millions of new claimants has created a once-in-a-lifetime opportunity for identity thieves seeking to steal those benefits.

According to the Secret Service and multiple media reports, organized rings of criminals are working to siphon off unemployment insurance payments, potentially worth hundreds of millions of dollars, intended for workers laid off due to the COVID-19 pandemic. In the state of Washington, for example, scammers reportedly made off with unemployment benefits worth nearly $1.6 million in a single month. This scam is reportedly even affecting consumers who have not yet lost their jobs.

How the scam works:
Identity thieves use databases of personal information *(likely obtained via data breaches)* to create phony accounts on state unemployment insurance office websites. Once they successfully create an account, they have the benefits direct-deposited into a bank account controlled by the scammer or an accomplice. The scammer then uses the deposited funds to purchase untraceable bitcoins, gift cards, or money orders. Those purchases are often performed by so-called "money mules" who may themselves be ensnared in a romance fraud or work-from-home scheme run by the scammers.

<u>If you've recently become unemployed, the following steps can help you reduce your risk of becoming a victim of this scam:</u>

1. Log on and create a profile on your state unemployment office's website as soon as you are laid off. This will reduce the window of opportunity for scammers to create fake profiles in your name and steal your unemployment benefits.

2. If you have already created a profile with your state unemployment office, log in and verify that no one has filed a claim in your name. If you've used a password on your profile that you've used on other accounts, change your password to something unique that you haven't already used elsewhere.

3. If you receive communication that someone else has applied for unemployment benefits in your name or your unemployment benefits claim was denied because someone else already applied, file a fraud complaint with your state's unemployment office promptly. The U.S. Department of Labor maintains a list of state unemployment fraud hotlines.

4. Put a credit freeze on your credit report with the three major credit reporting bureaus (Experian, Equifax, and TransUnion). If identity thieves have the personal information necessary to steal your unemployment benefits, they likely also have the information they need to take out credit or engage in other criminal activity. A credit freeze will prevent anyone from accessing your credit file until you unfreeze it with a PIN.

5. If you're looking for work, beware of online ads or unsolicited email and text offers to participate in work-from-home job opportunities. Common schemes involve offers to be a mystery shopper, payment processing agent, money transfer agent, or other similar jobs where you are asked to allow deposits to be made to your personal bank account. These jobs don't exist and participating in one (even unwittingly) could land you in legal trouble.

Federal Trade Commission: Consumer Information Scammers don't really give refunds (*by consumer.ftc.gov*)

<u>The FTC has been cracking down on deceptive tech support operations that call or send pop-ups to make people think their computers are infected with viruses.</u> Scammers ask for access to computers, then charge people hundreds of dollars for unnecessary repairs. In Operation Tech Trap, the FTC and its partners announced 16 actions against deceptive operations, and the FTC temporarily halted the operations of several defendants.

Recently, a woman who lost money to one of the defendants in the FTC cases got a call from someone who claimed to be with a company the FTC sued. *(It was a lie. In reality, the company has closed.)* He said the company wanted to give her a refund. He asked her to give him access to her computer, fill out paperwork and buy a prepaid card. She knew that didn't sound right, so she didn't cooperate. And she contacted the FTC right away.

We're grateful for her call, and want to share this warning: If you lost money to a tech support scam or other fraud, you might get a call from someone claiming to give you a refund, or help you recover your money – but only if you give them personal information or some money. Those calls are scams. Don't give out personal or financial information to anyone who calls you, and never give them access to your computer. And then report the call to the FTC.

Spot the top ten scams plaguing Americans. The most common frauds reported by consumers in 2019.

(*by fraud.org 2/26/2020)*

Each year, we monitor and analyze the complaints to track trends in scams and how con artists are tweaking their pitch to succeed at finding new victims. Our data helps us identify emerging scams we'd never heard of, what scams are fading into the sunset, and new twists on old classics. So without further ado, here are the most reported scams from 2019 and, just as important, tips on how to spot and avoid them so that you don't become a statistic on next year's report …

1. Internet merchandise scams
The set-up: Scammers offer cut-rate merchandise on the Internet in the hopes that consumers looking for a deal will buy.

How to avoid it: Buy from reputable sellers. If the price for an item is well below the price offered on e-commerce sites like Amazon, there's a good chance it's a scam, particularly if the merchandise is electronics, luxury apparel, or medications.

2. Phishing/spoofing
The set-up: Scammers use legitimate-looking emails or spoofed Caller ID to get consumers to think they're getting an email or phone call from the government, their bank or another entity. Once the scammer has the victim convinced they're someone they're not, they threaten them to get money or sensitive personal information.

How to avoid it: If someone you don't know calls you on the phone or sends a threatening email demanding quick payment, it's likely a scam. Delete the email or hang up the phone.

3. Fake prizes, sweepstakes, or free gifts
The set-up: The scammer contacts you to let you know you've won a big prize. All you must do to collect is pay them a fee for "insurance," "taxes," "processing" or some other reason.

How to avoid it: The prize doesn't exist. They're just after your money. If someone asks you to pay money to win money, it's a scam.

4. Fake check scams
The set-up: Someone you've never met in person sends you a check and asks you to deposit it into your personal bank account. Then they ask you to send them some or all the proceeds from the check via wire transfer, by buying a gift card, or some other method.

How to avoid it: Don't deposit the check and definitely don't send money based on funds that may appear available if you deposit it. The bank will catch on, and you'll potentially be left owing the bank for the negative balance.

5. Advance fee loans, credit arrangers
The set-up: Scammers offer a "guaranteed" credit card or bank loan to consumers looking for cash. All the victim needs to do is pay an up-front fee to obtain the loan.

How to avoid it: Only look for loans or credit cards from reputable lenders. If a lender offers you a "guaranteed" credit card or loan without a credit check, it's probably a scam.

6. Romance scams/sweetheart swindles
The set-up: Someone you've met online on a dating website, online forum or via social media quickly develops a friendship or romantic relationship with you. Eventually, they ask for money for a visit, to cover an unexpected emergency, or some other reason.

How to avoid it: Don't leave protected dating website messaging platforms for unprotected text or instant messaging chats. Never send money to someone you've only met online or talked to over the phone.

7. Recovery/refund scams
The set-up: If you've lost money in a scam, someone may claim to be able to recover those losses for you. The only catch it that you must pay a fee or hand over sensitive personal information like bank account numbers or grant access to your computer in order to recover your losses.

How to avoid it: You should never pay money or give up personal information in order to recover fraud losses. Anyone who claims to be able to help you recover your losses in exchange for a fee is just trying to scam you.

8. Computer equipment/software
The set-up: Also known as the tech support scam, a caller may claim to be with a well-known software company like Microsoft or an anti-virus company and have information that your computer is infected with malware. They request remote access to your computer in order to "diagnose" the problem. They may then urge you to buy an expensive tech support solution to "fix" the problem.

How to avoid it: If someone calls you unsolicited offering tech support, it's almost certainly a scam. Scary pop-ups on your phone or computer may also urge you to call a phone number to get the problem fixed. Don't fall for those either as they are simply a lure to get you paying for tech support you probably don't need.

9. Investment related scams
The set-up: Someone may offer you "guaranteed" returns with little or no risk in exchange for a big up-front investment. Investment in gold coins, precious metals, Bitcoin, real estate, or Internet startups are often used to entice unwary investors.

How to avoid it: Investigate anyone offering to make an investment on your behalf. Get documentation about the track record of the investment and check to make sure the "advisor" is registered with the state or federal government. If they pressure you to make a decision right away, chances are that it's a scam.

10. Family/friend imposter
The set-up: A caller claims to be a family member or friend in trouble (or someone helping them, like a lawyer, doctor, or policeman). They urge the victim to send money to help out their loved one. The scammer may have details about your friend or family member (likely gleaned from social media).

How to avoid it: Hang up the phone and call your friend or family member yourself. If they don't answer, try another relative who knows them to verify what's going on. Any urgent request to send money without verification is almost certainly a scam.

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.

Use caution when talking to 'old friends' on Facebook – *Scammers are using Facebook's Messenger service to try to defraud consumers by posing as long lost friends.*

(*by fraud.org 8/01/2020)*

We've recently heard from nearly a dozen consumers who have contacted Fraud.org about scammers using Facebook's Messenger service to try to defraud them by posing as long lost friends. Consumers who sent us complaints report that these scams begin when they receive a message on Facebook Messenger from someone impersonating a former classmate or an old friend. When the recipient responds, the scammer strikes up a conversation to build trust. Once trust is established, the impersonator urges the consumer to send a text message to a number the scammer controls to get information on a grant, prize, or even government stimulus funds. When the victim texts the number, they are urged to pay an up-front fee and/or supply personal information (Social Security number, bank account/credit card information, etc.) to collect the non-existent money. Victims who do send the money are then urged to send even more money until they catch on. Unfortunately, the money is often sent via wire transfer or gift cards, which are extremely difficult or impossible to stop or reverse.

While this scam is not new, the request to take the conversation off Facebook Messenger and on to text message is a new twist. This is likely due to the scammers trying to evade anti-fraud technology employed by Facebook.
Here are tips to reduce your risk of falling victim to this scam:

• Don't immediately assume your Facebook friend is who they claim to be. Thanks to widespread data breaches, it is not difficult for scammers to get the information they need to compromise a Facebook account. If you receive a message from someone you have not spoken to in a long time, do not assume that the message is legitimate. The safest course of action is to simply ignore the message.

• Test them. If you do engage in a conversation and become suspicious, you can try to verify the identity of the person messaging you by asking them a question only they would know *(i.e., who was our 9th grade English teacher?).*

• Beware requests to take conversations off Facebook Messenger. Complaints we have received often describe requests to move conversation from Facebook (where they can be monitored) to text message. This is a big red flag for fraud.

• Anyone who asks you to send money to get money is swindling you. If you are asked to pay money to collect a prize, grant, stimulus check, or any other type of reward, it is a scam.

• Turn on two-factor authentication and encourage your friends to do the same. One of the reasons this scam occurs is that consumers tend to re-use passwords across multiple websites *(your email and Facebook account, for example).* That means that if your username and password are compromised at one website, scammers can use that information to try and compromise your account at other websites. An effective way to reduce the risk of this is to turn on two-factor authentication. This will require anyone trying to log in to your Facebook account to supply a special code *(typically provided via text message or an authentication app)* before they can log in.

Bonus Fraud Alert: Facebook copy/paste scams
If you have perused your Facebook newsfeed for any appreciable length of time, chances are that you have come across a message from a friend urging you to "copy and paste" their message instead of using Facebook's "share" function. These "copy and paste" instructions often come at the end of a heart-warming, controversial, or political story. These messages may seem innocuous and they may make you feel good by helping to spread a message you agree with.

However, by copying and pasting a message instead of using the "share" function, you may be helping marketers *(not all of who are legitimate)* build lists of people to contact later with friend requests or other messages. A tell-tale sign of such scams is misspelled or unusual words or phrases in the text of the message. Including those in a message helps the scammers search on that misspelled word or phrase and easily build lists of the people who have helped to spread the message.
The easiest way to avoid this scam is to ignore any message on Facebook that urges you to "copy and paste" instead of "sharing."

Seniors protect yourself from money scams

(*by National Council on Aging)*

1. Be aware that you are at risk from strangers — and from those closest to you. Over 90% of all reported elder abuse is committed by the older person's own family members. Common tactics include depleting a joint checking account, promising but not delivering care in exchange for money or property, outright theft, and other forms of abuse-physical abuse, threats, intimidation, and neglect of basic care needs. Everyone is at risk of financial abuse, even people without high incomes or assets.

2. Don't isolate yourself—stay involved! Isolation is a huge risk factor for elder abuse. Most family violence only occurs behind closed doors, and elder abuse is no exception. Some older people self-isolate by withdrawing from the larger community. Others are isolated because they lose the ability to drive, see, or walk about on their own. Visit the Eldercare Locator to find services nearby that can help you stay active. Or contact your local senior center to get involved.

3. Always tell solicitors: "I never buy from (or give to) anyone who calls or visits me unannounced. Send me something in writing."
Don't buy from an unfamiliar company and always ask for and wait until you receive written material about any offer or charity. A good rule of thumb is to never donate if it requires you to write your credit card information on any forms. It's also good practice to obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business license number before you transact business. And always take your time in making a decision.

4. Shred all receipts with your credit card number. Identity theft is a huge business. To protect yourself, invest in—and use—a paper shredder. Monitor your bank and credit card statements and never give out personal information over the phone to someone who initiates the contact with you.

5. Sign up for the "Do Not Call" list and take yourself off multiple mailing lists. Visit Do Not Call to stop telemarketers from contacting you.
Be careful with your mail. Do not let incoming mail sit in your mailbox for a long time. When sending out sensitive mail, consider dropping it off at a secure collection box or directly at the post office. You also can regularly monitor your credit ratings and check on any unusual or incorrect information at www.AnnualCreditReport.com.
To get more tips on protecting yourself from fraud, visit On Guard Online, which has interactive games to help you be a smarter consumer on issues related to spyware, lottery scams, and other swindles.

6. Use direct deposit for benefit checks to prevent checks from being stolen from the mailbox. Using direct deposit ensures that checks go right into your accounts and are protected. Clever scammers or even scrupulous loved ones have been known to steal benefits checks right out of mailboxes or from seniors' homes if they are laying around.

7. Never give your credit card, banking, Social Security, Medicare, or other personal information over the phone unless you initiated the call.
Misuse of Medicare dollars is one of the largest scams involving seniors. Common schemes include billing for services never delivered and selling unneeded devices or services to beneficiaries. Protect your Medicare number as you do your credit card, banking, and Social Security numbers and do not allow anyone else to use it. Be wary of salespeople trying to sell you something they claim will be paid for by Medicare. Review your Medicare statements to be sure you have in fact received the services billed, and report suspicious activities to 1-800-MEDICARE.

8. Protect your loved ones: If you know or care for an older adult, here are some warning signs that may indicate they are the victim of financial abuse:
- There are unusual recent changes in the person's accounts, including atypical withdrawals, new person(s) added, or sudden use of a senior's ATM or credit card.
- The senior suddenly appears confused, unkempt, and afraid.
- Utility, rent, mortgage, medical, or other essential bills are unpaid despite adequate income.
- A caregiver will not allow others access to the senior.
- There are piled up sweepstakes mailings, magazine subscriptions, or "free gifts," which means they may be on "sucker lists."

Every state operates an Adult Protective Services (APS) program, which is responsible for receiving and investigating reports of elder abuse, neglect, and exploitation, and in most states, the abuse of younger adults with severe disabilities. APS is the "911" for elder abuse. Anyone who suspects elder abuse, neglect, or exploitation should make a report. The reporter's identity is protected. APS services are confidential, so the reporter may not be able to learn the outcome of the case. APS respects the right of older persons to make their own decisions and to live their lives on their own terms. In cases of cognitive impairment, however, APS will take steps to protect the older person to the degree possible.
Steps to take if you're a victim of a scam:
If you think you've been scammed, don't be afraid or embarrassed to talk about it —waiting could only make it worse. Immediately:
- Call your bank and/or credit card company.
- Cancel any debit or credit cards linked to the stolen account.
- Reset your personal identification number(s).

Also, contact legal services and Adult Protective Services if warranted. To find your local offices, visit the Eldercare Locator or call them toll-free at 1-800-677-1116 weekdays 9 a.m. to 8 p.m. ET.