Identity THEFT NEWSLETTER

Keeping You Informed!

MERCK SHARP & DOHME
FEDERAL CREDIT UNION
(215) 996-3700
msdfcu.org

NCUA
Your savings federally insured to at least $250,000 and backed by the full faith and credit of the United States Government.
National Credit Union Administration, a U.S. Government Agency.

EQUAL HOUSING LENDER

Vol. 25, No. 1 | *Don't become the next victim...* | Fall 2023

Signs of Child Identity Theft

- **Turned down for government benefits**
- **Calls about bills in your child's name**
- **Letter from the IRS about taxes your child owes**
- **Child's student loan application is denied**

When your child turns 16, you may want to check if there's a credit report in his or her name. This could help you spot identity theft, since children under 18 usually don't have a credit report. If there's inaccurate information in your child's credit report, you'll have time to correct it before he or she applies for a job, a college loan, a car loan, or a credit card, or tries to rent a place to live. ■

Got An Urgent Message About A Virus On Your Computer?

Computer **technical support scams** involve unsolicited offers to fix a "problem" with your computer or software. Fraudsters behind these scams are out to get access to your computer—and your credit card or bank account number. Legitimate companies **will never** contact you by phone, email or text message to say there's a problem with your computer. **Do not click on any links or call a phone number.**

Tech support scammers all use scary language and other high-pressure tactics to get you to act right away.

Here are three ways tech support scam criminals target (most commonly) older adults:

❶ WEBSITES

An unexpected pop-up window may tell you that your computer is infected with a virus. This "ad" may prompt you to call tech support immediately using the number displayed. When you call the number, the "tech support" representative may request remote access to your system—or ask you to pay a fee for computer repairs. You may be asked to provide personal information, which could be used later to steal your money or identity.

❷ EMAILS OR TEXT MESSAGES

Just like a website pop-up, tech support scam emails are made to look like they come from credible, recognizable companies. These messages can contain malicious links or attachments that send you tech support "alerts" when you click on them or open them. These fake alerts can actually freeze up your screen or keyboard to make you believe something is wrong with your machine.

❸ PHONE CALLS

Scammers carefully choose vulnerable targets—like older adults or people with disabilities. Posing as a tech expert, they may claim your computer has malware or other dangerous issues that must be addressed right away. They may request remote access to your system, which can allow them to install malware or steal your information. The scammer may even pretend to repair the supposed issues on your computer—and then demand payment via difficult-to-trace methods such as money transfer or gift card.

According to the FBI's IC3 Report, in 2022 Tech and Customer Support fraudsters made 32,538 victims with total reported damages amassing $806,551,993 in the U.S. alone. ■

SCAM ALERT: "Grandmom, Help!"

Emergency Scams Take Advantage of Loved Ones

Emergency scams, sometimes called "grandparent scams," prey on the willingness of an unsuspecting, worried individual to help friends and family in need. Often, they will impersonate their targets' loved ones, make up an urgent situation, and plead for help… and money. Social media sites allow scammers to look up information and offer plausible stories. They may even incorporate nicknames and real travel plans into the con to convince their targets.

How The Scam Works

Emergency scams are about a family member or friend in a dire situation. You get a call, email, or social media message from someone claiming to be a distressed family member. They may say they've been arrested while traveling overseas, or there was an accident, medical emergency, or other crisis. They provide convincing details, such as family names and school details.

A common version is the "grandparent scam," where the con artist contacts a grandparent claiming to be their grandchild and asking for money. The plea is so persuasive that the grandparent wires money to the scammer, only to find out their family member was safe and sound later. This scam can also work in reverse, where the "grandparent" calls their grandchild pleading for help.

Recently, the FTC has warned that scammers are using voice cloning techniques to imitate the voices of loved ones. The technology enables con artists to copy the voices of persons close to you from videos they may find on social media or other sources. This adds to this scam's confusing and frightening aspect.

TIPS:

- **No matter how dramatic the story is, resist the urge to act immediately.** Check out the story with other family and friends (call them directly). Don't call the phone number provided by the caller or caller ID. Ask questions that would be hard for an impostor to answer correctly.
- **Familiarize yourself with what family members share online.** Social media sites allow scammers to look up information and offer plausible stories.
- **Never wire any money if there is any doubt about a call.** ■

7 Tips For Protecting Yourself Online

Identity theft is becoming increasingly sophisticated as swindlers deploy an ever-evolving array of techniques and tools to hijack your personal information. If successful, a scammer can use your identifying information to open credit accounts, file a tax return or assume your identity in other ways. We recommend the following tips to keep you safe online:

1 Keep your computers and mobile devices up-to-date.

Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.

2 Set strong passwords.

A strong password is at least eight characters in length and includes a mix of upper and lowercase letters, numbers, and special characters.

3 Watch out for phishing scams.

Phishing scams use fraudulent emails and websites to trick users into disclosing private account or login information. Do not click on links or open any attachments or pop-up screens from sources you are not familiar with. Forward phishing emails to the Federal Trade Commission (FTC) at **spam@uce.gov** — and the company, bank, or organization impersonated in the email.

4 Keep personal information personal.

Hackers can use social media profiles to figure out your passwords and answer those security questions in the password reset tools. Lockdown your privacy settings and avoid posting things like birthdays, addresses, mother's maiden name, etc. Be wary of requests to connect with people you do not know.

5 Secure your internet connection.

Always protect your home wireless network with a password. When connecting to public Wi-Fi networks, be cautious about what information you are sending over it.

6 Shop safely.

Before shopping online, make sure the website uses secure technology. When you are at the checkout screen, verify that the web address begins with **https**. Also, check to see if a tiny locked padlock symbol appears on the page.

7 Read the site's privacy policies.

Though long and complex, privacy policies tell you how the site protects the personal information it collects. If you don't see or understand a site's privacy policy, consider doing business elsewhere. ■

No, That's Not The IRS Texting About A Tax Refund Or Rebate. It's A Scam!

IRS impersonators have been around for quite a while. But as more people get to know their tricks, they change their approach. So instead of contacting you about a tax debt and making threats to get you to pay up, scammers may send you a text about a "tax rebate" or some other tax refund or benefit.

The text messages may look legit, and mention a "tax rebate" or "refund payment." But no matter what the text says, it's a scammer phishing for your information. And if you click on the link to claim "your refund," you're exposing yourself to identity theft or malware that the scammer could install on your phone.

If someone contacts you about a tax rebate or refund:

- **Never click on links in unexpected texts.** Don't share personal information with anyone who contacts you out of the blue. Always use a website or phone number you know is real.
- **Know that the IRS won't call, email or text to contact you for the first time.** They'll always start by sending you a letter. If you want to confirm, call the IRS directly at **800-829-1040**.
- **Find the status of any pending refund** on the IRS official website. Visit **Where's My Refund** at **www.IRS.gov/refund**
- **Report unsolicited texts or emails claiming to be the IRS.** Forward a screenshot or the email as an attachment to **phishing@irs.gov**

If you clicked a link in one of these scam texts or emails and shared personal information, file a report at **IdentityTheft.gov** to get a customized recovery plan based on what information you shared. ■

Don't Pay For Help With Your Federal Student Loans

Pay Your Student Loans—Not A Scammer!

Federal student loan repayments are starting again in October. But scammers might try and tell you they can help you avoid repayment, lower your payments, or get your loans forgiven—for a price. Here's how to spot and avoid these scams.

The best source of information on your federal student loans is **Federal Student Aid** (**https://studentaid.gov**). Also, you don't need to pay to sign up for any programs to lower your payments or get forgiveness—it's all free at **StudentAid.gov/repay**. And you can do it yourself.

The calls and texts that offer "help" might be tempting. But before you act, know how to spot the scams:

- ✓ Don't give away your FSA ID login information. Anyone who says they need it to help you is a scammer. If you share it, the scammer can cut off contact between you and your servicer—and even steal your identity.
- ✓ Don't trust anyone who contacts you promising debt relief or loan forgiveness, even if they say they're affiliated with the Department of Education. Scammers try to look real, with official-looking names, seals, and logos. They promise special access to repayment plans or forgiveness options—which don't exist. If you're tempted, slow down, hang up, and log into your student loan account to review your options.

As you get ready for repayment, here are some steps to take:

- ✓ Update your contact information with FSA and your loan servicers. This way, you'll get timely updates about your repayment plans.
- ✓ Enroll in a repayment plan. Use FSA's Loan Simulator to estimate your monthly payments and compare your repayment options. If you've defaulted on your loans, look into the **Fresh Start** program.

If you spot a scam, the FTC wants to hear about it: **ReportFraud.ftc.gov** ■

Federal law allows you to get a **FREE COPY** of your credit report, at your request, from each credit reporting company – Equifax, Experian, and TransUnion.

AnnualCreditReport.com
1-877-322-8228