SCAMS

Tips on Fraud, Online Safety, and More

The Commercial & Savings Bank

330.674.9015 www.csb1.com csb_bank

Prepared for informational purposes only by The Commercial & Savings Bank.

Member FDIC

The Commercial & Savings Bank

Four Tips for Keeping Your Money Safe

In today's digital age, safeguarding your money and personal information is crucial. This guide empowers you to confidently navigate potential issues by staying informed about the latest scams and fraud tactics.

THINK BEFORE YOU CLICK

Don't click on anything in an unsolicited email or text message. Look up the company's phone number on your own; don't use the contact information provided in the message. Call the company to ask if the request is legitimate.

KNOW WHO YOU'RE TALKING TO

Do not answer phone calls, texts, social media messages, or emails from people you do not know. Don't provide information unless you're certain of who you are speaking to.

RESIST PRESSURE TO ACT QUICKLY

Urgency is often a red flag. Scammers often do this to cloud your judgment. If you are in a situation where cash or information is requested immediately, it's likely a scam.

DON'T FREELY SHARE PERSONAL INFORMATION

Most organizations won't contact you and ask for your username and password or other personal information like your address, birthdate, or social security number.

PHISHING ATTACKS

A phishing attack can take the form of an email, text message, social media direct message, and more. In a phishing scam, you might receive a message that appears to be from a legitimate business or from someone you know. The sender requests that you update or verify your personal information by replying to the message or clicking a link to visit their website. While the web address may look familiar, the scam sends you to a spoofed website that is used solely for stealing your information.

Spoofing: when someone disguises an email address, sender name, phone number, or website URL (often just by changing one letter, symbol, or number) to convince you that you are interacting with a trusted source.

Quishing: when a hacker embeds a malicious URL into a QR code that directs to a phishing site where users unknowingly share personal and/or financial information. Always check the URL shown when scanning the QR code before continuing to the site!

SCAN ME!

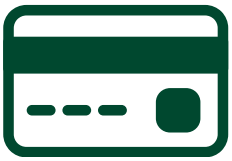
Scammers might impersonate...

- **Websites or stores you frequently visit**
- **Your financial institution**
- **An employee at your workplace**
- **Charities or non-profits**
- **A federal agent from the IRS**

Do not share any personal information through email or text, including bank account and credit card numbers.

The Commercial & Savings Bank

Common Types of Fraud



Gift Card Scams

Only scammers will tell you to buy a gift card and give them the information on the card. No real business or government agency will ever ask you to buy a gift card and use it to pay them.

Romance Scams

Scammers often create deceptive profiles on dating sites or social media and quickly profess their love. They consistently cancel plans for in-person meetings and eventually request money for emergencies, fabricated travel plans, or financial setbacks, all while using a sense of urgency to deceive individuals.

Bitcoin and Cryptocurrency Scams

Never trust demands for payment solely through digital currency. This is a trick used by scammers to exploit the anonymous format of cryptocurrencies to protect themselves.

Pet Scams

Many scammers will create ads, social media posts, or entire websites to sell fake pets, most commonly puppies. Always insist on visiting the animal and the breeder before purchasing, or only pick up and pay for the pet in person.

Family Emergency Scams

Stay vigilant if someone claiming to be a family member or police officer on behalf of a family member reaches out urgently, especially if they ask for money due to a crisis. Verify their identity by hanging up and calling them back before providing financial assistance to avoid being tricked by emotional manipulation.

Common Types of Fraud

Investment Scams

Be cautious of investments that guarantee high returns or promise little to no risk. If an offer sounds too good to be true, it probably is. Avoid investments based on how many people you recruit or how much of a product or service that you buy yourself.

Online Seller Scams

Be cautious when buying things online, especially if you're unfamiliar with the seller or the platform. Some scammers create fake websites or listings to trick people into paying for items that don't exist. Always double-check the legitimacy of sellers and avoid making purchases on unfamiliar websites. Be wary if a price appears too good to be true - this is a common tactic to collect your data and financial information.

Pop-Up Advertisement Scams

If you encounter unexpected pop-up ads online, be careful not to click on them. Some ads can lead to fake websites or ask for personal information. Install a reliable ad blocker on your device to minimize the risk of falling victim to these scams.

Charity Scams

When donating to charities, be sure to verify their legitimacy. Some fraudsters pretend to represent charities/nonprofits that don't exist or aren't genuine. Contact known organizations directly and only share personal or financial information if you are confident in the charity's authenticity. Sometimes, scammers even use national or local tragedies to take advantage of people who want to help.

The Commercial & Savings Bank

ADVICE FOR HOW TO PROTECT YOURSELF ONLINE

Trustworthy & Reliable Website Criteria

A trustworthy and reliable website will have a website certificate and use encryption to protect information submitted on the website. **To ensure the sites you visit are safe, look for a closed padlock icon and "https://" (NOT "http:"), in the URL to ensure the site has a certificate and encrypts your information, protecting it from scammers.** Also, be sure to check spelling and brand/organization names before providing sensitive information.

Check for:	https://
Use Caution: Not Secure –	http:// ⓘ Website Not Secure –

**could vary depending on browser/device*

Staying Safe on Social Media Platforms

Since 2021, people have reported losing $2.7 billion to scams started on social media; that is more than any other contact method. Scammers use social media to impersonate individuals, hack profiles, and manipulate personal information to deceive you, your friends, and family. Common social media scams involve fake ads, deceptive investment opportunities, or fraudulent romance schemes. Ensure you have proper privacy settings and be cautious of oversharing information through posts and especially direct messages.

How to Report Identity Theft

If you believe that your identity has been stolen, there are a few ways you can report it:

Report your identity theft to the Federal Trade Commission (FTC), either online at IdentityTheft.gov or phone at 1.877.438.4338 or TTY 1.866.653.4261. If you report online with the FTC, you will be provided with an identity theft report and recovery plan. If you create an account, you will be able to manage your recovery plan and will have access to prefilled form letters to send to creditors. Report the theft to any financial institutions you have accounts with.

You may also report identity theft to your local police. This may be necessary if you know who the thief is, if the thief used your identity in an interaction with the police, or if a police report is required by any of your creditors affected by the theft.

After reporting your identity theft to the federal government agencies, one of the three major credit reporting agencies (Equifax, Experian, or TransUnion) should be contacted so a freeze alert can be added to your accounts. This prevents others from opening any new accounts or cards with your name.

FOR MORE INFORMATION ON SCAMS AND FRAUD

The Commercial & Savings Bank

Checking Your Credit Report

The Fair Credit Reporting Act (FCRA) allows everyone to check their credit report once every 12 months for free from each of the three national credit reporting agencies: Equifax, Experian, and TransUnion. Take advantage of your free credit reports, as this will not harm your credit score and regularly checking can help protect you from possible identity theft.

EQUIFAX® experian™ TransUnion®

Be careful of imposter sites promising free credit reports. There is only one website, annualcreditreport.com, with the authority to fill orders for free credit reports under law. The three nationwide credit reporting companies and annualcreditreport.com will never ask you to submit any personal information through email or on the phone.

If you are ever asked to provide personal information, be suspicious of a possible scam. The only information you need to provide to receive your annual free credit report is your name, address, Social Security number, and date of birth.

Sources

- https://www.cisa.gov
- https://www.consumer.ftc.gov
- https://www.usa.gov
- https://www.fbi.gov
- https://www.consumerfinance.gov
- https://www.ipata.org