

Your *Trust* Matters

October 2023 Newsletter



MidWestOne™
TRUST SERVICES



Dan Flynn
VP/Trust Officer
Dubuque, IA
563.585.9203

Protecting Yourself from Identity Theft and Bank Account Fraud

In today's digital age, where personal information and financial transactions are increasingly conducted online, the threat of identity theft and fraud has become more prevalent than ever. It is crucial for individuals to be proactive in safeguarding their personal information and financial assets. This article explores ten steps that can help protect individuals from falling victim to identity theft and fraud.

Strengthen Your Passwords

The first line of defense against identity theft and bank account fraud is a strong password. Avoid using easily guessable passwords, such as "123456" or "password." Instead, create complex passwords that combine letters, numbers, and special characters. It's also advisable to use different passwords for various online accounts and to change them regularly. Consider using a reputable password manager to generate and store complex passwords securely.

Enable Two-Factor Authentication (2FA)

Two-factor authentication adds an extra layer of security to your accounts. With 2FA, even if someone obtains your password, they won't be able to access your account without the second authentication factor, which is often a one-time code sent to your mobile device or email. Enable 2FA wherever possible, especially for your bank accounts and email accounts.

Protect Personal Information

Be cautious about sharing personal information online. Scammers often try to trick individuals into revealing sensitive data through phishing emails, fake websites, or social engineering. Never share personal or financial information through email or text messages, especially if you didn't initiate the communication. Verify the legitimacy of websites before entering any personal details and be wary of sharing too much personal information on social media.

Monitor Your Financial Statements

Regularly review your bank and credit card statements for any unauthorized or suspicious transactions. Timely detection of fraudulent activity can help you take immediate action to resolve the issue and prevent further damage. If you spot any unfamiliar transactions, contact your financial institution immediately.

Secure Your Devices

Ensure that all your devices (computers, smartphones, tablets) are equipped with up-to-date antivirus software and operating system security patches. Use a secure Wi-Fi network, avoid public Wi-Fi for sensitive transactions, and be cautious when connecting to unknown networks. Lock your devices with a PIN or password and enable device encryption if available.

continued on page 2

800.247.4418

MidWestOne.bank

Email: trustservices@midwestone.com

Not FDIC Insured | No Bank Guarantee | May Lose Value | Not a Deposit | Not Insured by any Federal Government Agency

Your *Trust* Matters

October 2023 Newsletter



MidWestOne™
TRUST SERVICES

Be Wary of Phishing Scams

Phishing scams are one of the most common methods used by identity thieves. These scams involve tricking individuals into revealing their personal or financial information. Be cautious when clicking on links in emails or messages, especially if they come from unknown sources. Verify the sender's identity and contact the organization directly if you receive an email requesting sensitive information.

Shred Sensitive Documents

Identity thieves may target physical documents that contain personal information. To protect yourself, shred documents like bank statements, credit card offers, and any other papers containing sensitive information before disposing of them. Consider going paperless for statements and bills to reduce the physical documents you need to manage.

Use a Secure Email Service

Choose a secure email service that offers encryption for your emails. This ensures that your communication remains confidential and less susceptible to interception. Additionally, avoid sending sensitive information via email whenever possible and use alternative methods for sharing such data, like secure file-sharing platforms.

Regularly Check Your Credit Report

Obtain a free credit report from each of the three major credit bureaus (Equifax, Experian, and TransUnion) annually and review it for any discrepancies or unfamiliar accounts. Monitoring your credit report can help you detect any fraudulent activities related to new credit applications or accounts opened in your name.

Educate Yourself and Stay Informed

Staying informed about the latest scams and fraud tactics is crucial. Scammers are constantly evolving, so it's important to educate yourself about the newest threats and how to recognize them. Government agencies, financial institutions, and reputable cybersecurity websites often provide information about current scams and prevention tips.

In conclusion, protecting yourself from identity theft and fraud requires a proactive approach to safeguarding your personal information and financial assets. By following these ten essential steps, you can significantly reduce the risk of falling victim to these malicious activities. Stay informed, be cautious, and take the necessary steps to protect your digital and financial well-being.

800.247.4418

MidWestOne.bank

Email: trustservices@midwestone.com

Not FDIC Insured | No Bank Guarantee | May Lose Value | Not a Deposit | Not Insured by any Federal Government Agency