Mesirow

3 ways to protect yourself from online theft and fraud

At Mesirow, our client focus and our values have not changed since Norman Mesirow founded the firm in 1937—we advise individuals and families to help align their financial resources with their life goals. We believe that an essential part of your financial wellbeing is the confidence that your financial identity is secure.

There are a number of ways to help protect yourself from cybercrime, including:

- Using multi-factor authentication when verifying your identity, and verifying transactions via telephone
- Creating secure passwords
- Protecting your personal information

Multi-factor authentication & transaction verification help protect you

Given the vulnerability of online data, more people are relying on multi-factor authentication to protect their accounts. Two-factor authentication adds an extra layer of security, which requires not only a password and username, but also a second factor, typically a temporary code sent to a mobile phone via an authentication app, SMS text message, or voicemail. Make sure your SMS texts are not visible on your phone while it is locked.

It is unfortunately possible for criminals to gain access to an individual’s email, allowing them to send wire transfer instructions to their victim's financial institution. This fraud is often perpetrated through an email appearing to come from an individual requesting a wire transfer from the institution. The best way to help protect against this type of criminal activity is for your financial institution(s) to always confirm the validity of each transaction, including the wire transfer amount and details, via phone. A follow-up call to a request for a wire transfer is one of the best ways to help ensure your account and assets are protected.

Help protect yourself with secure passwords and careful online chatting

- Create a secure password. Password length is more important the complexity. The longer the password is, the more difficult it is to hack.

- Avoid the use of loved ones' names (these can be easily identified by others).
- Don't use autosave for your passwords. It may be easier, but it is much less secure
- Use different passwords for different websites.
- Change your passwords regularly, even the ones you consider to be most secure.
- Consider using a secured password manager.
- Do not give out personal information over the phone, email, or internet, unless you initiated the contact. Beware of email "phishing" attempts, which are typically fake emails from your financial institution asking you to verify your personal information.
- Don't overshare on social media. This information is frequently used to confirm personal information needed to obtain passwords or travel schedules to confirm when you are out of town.

Protect your personal information

- Review your bank statements and credit card statements each month for suspicious or unrecognized transactions. If your
- financial institution provides an automatic alert system, set that up so you can be alerted to any suspicious activity.
- Consider setting up security/fraud alerts through a trusted third party service.
- Cover the PIN on your credit card so that cashiers cannot see it. With access to this PIN, criminals can use your card to order online.
- Erase the memory on phones, tablets and computers before disposing of them.
- Keep your computer's firewall, anti-virus, and anti-spyware software current.
- Confirm secure internet connection when transmitting personal data, and do not do any financial transactions while using public non-secured Wi-Fi.
- Do not carry paper copies of personal information. Only carry what you need; don't carry your full Social Security number in your wallet unless necessary.
- Shred financial and medical documents when they are no longer needed.
- Destroy labels on prescription bottles before disposing.
- Read companies' privacy policies and understand how data is collected, used and protected.

What to do when you think your information is compromised

Set up a Fraud Alert

As a precaution, fraud alerts can be placed on your credit file by contacting one of the three major credit bureaus. Once contacted, the credit bureau will notify the other two agencies.

- Experion: experian.com
- TransUnion: transunion.com
- Equifax: equifax.com

Annually, review your free credit report for unfamiliar transactions and inquiries. Reports can be requested via the FTC’s website at annualcreditreport.com or by calling 877.322.8228.

Request a Credit freeze

If you suspect you are the victim of identity theft, you may request a credit freeze from each of the three credit bureaus listed above. These freezes are designed to prevent your credit file from being released without your consent, and can be requested either online or over the phone. It is important to understand that once a freeze is placed, it may take time to “unfreeze” your credit, which may be inconvenient when getting anything that requires a credit check (such as applying for credit, insurance, utility services, and job-related activities).

Summary

Ensuring your sensitive information is secure from fraud and theft in today’s digital world is more challenging than ever. By implementing as many safeguards as possible, including those mentioned in this article, online hackers will be more likely to set their sights on an easier target.
Please reach out to your Mesirow Wealth Advisor to learn more about Mesirow's commitment to help you stay safe.

Published January 2026