



Fraud and cybercrime are serious threats, so constant vigilance is key. Our firm plays an important role in helping safeguard your assets, but you can also take action yourself to protect and help secure your information. This checklist summarizes common cyber fraud tactics, as well as security tips and best practices. Some suggestions may be things you're doing already, whereas others may be new to you. We also cover actions to take if you suspect that your personal information has been compromised. If you have questions, we're here to help.

Cyber criminals exploit our increasing reliance on technology. Methods used to compromise a victim's identity or login credentials—such as malware, phishing, and social engineering—are increasingly sophisticated and difficult to spot. A fraudster's goal is to obtain information to access your account and assets or to sell your information for this purpose. Fortunately, criminals often take the path of least resistance. Following best practices and applying caution when sharing information and executing transactions makes a big difference.

How we can work together to protect your information and assets

Safe practices for communicating with TCI

- **Keep us informed** regarding changes to your personal information.
- **Expect us to call you to confirm email requests** to trade, move money, or change account information.
- **Establish a verbal password** with our firm to confirm your identity—or request a video chat.
- **Please send all documents** containing personal information to TCI via our secure client portal.

Follow general best practices

- **Be suspicious** of unexpected or unsolicited phone calls, emails, and texts asking you to send money or disclose personal information. If you receive a suspicious call, hang up, then call back using a trusted contact number.
- **Be cautious when sharing sensitive information** and conducting personal or confidential business via email because it can be compromised and used to facilitate identity theft.
- **Do not disclose on social media sites personal or sensitive information**, such as your birth date, contact information and mother's maiden name.
- **Be cautious when receiving money movement instructions via email.** Call the sender at their known number (not a number provided in the email) to verbally validate all instruction details before following instructions or providing your approval.
- **Protect yourself** from phishing attempts and malicious links.
- **Check your email and account statements** regularly for suspicious activity.
- **Do not verbally disclose or enter confidential information** on a laptop or mobile device in public areas where someone could potentially see, hear, or access your information.
- **Verify payment requests you receive by phone or email.** Requests for payment using gift cards, prepaid debit cards or digital currency are frequently associated with fraud or scams.

Keep your technology up-to-date

- **Keep your web browser and operating system up-to-date** and be sure you're using appropriate security settings. Old software, operating systems and browsers are more susceptible to attack.
- **Install anti-virus/anti-malware/anti-spyware software** on all computers and mobile devices.
- **Enable the security settings** on your applications and web browser.
- **Do not use free or found USB thumb drives**—they could be infected with viruses or malware.
- **Turn off Bluetooth** when it's not needed.
- **Safely and securely dispose of old hardware.**

Be cautious with public networks

- **Avoid using public computers.** If you must use one, go to the browser settings and clear the browser history (cache) and cookies when you're finished.
- **Use only wireless networks you trust** or that are protected with a secure password.
- **Use your personal Wi-Fi hotspot** instead of public Wi-Fi.
- **Do not accept software updates** if you are connected to public Wi-Fi.

Be strategic with your login credentials and passwords

- **Do not use personal information** such as your Social Security number or birthday as part of your login ID.
- **Create a unique password** for each financial institution with which you do business; use passwords that are long and contain a combination of characters, numbers and symbols. Consider using a password manager to create, manage and store passwords that are unique and secure.
- **Do not share your passwords.**
- **Use two-step verification whenever possible.**

Be sure you're on a secure website

- **Check the URL to see whether it's a secure connection.** Secure sites begin with *https* rather than *http* and are generally considered safer.
- **Download apps only from Google Play or Apple's App Store.**
- **Do not visit websites you don't know**—such as those advertised in pop-up ads and banners.
- **Log out completely** to terminate access when you've completed a secure session, such as for online banking or a credit card payment.

Beware of phishing

- **Do not click on links or attachments** in emails and text messages if you question the validity of the sender.
- **Hover over questionable links** to reveal the site's full URL and see where the link really goes. Do not click on links that don't match the sender or don't match what you expect to see.
- **Be suspicious** of emails that have grayed-out Cc: and To: lines—they may have been sent to a mass distribution list.
- **Check the sender's domain name in the email address.**
- **Activate the spam filters** in your email settings to help prevent unsolicited emails from going to your inbox.

What to do if you suspect a breach or fraud

- Call our office at 1-877-733-1859 so that we can watch for suspicious activity and collaborate with you on other steps to take.

Visit these sites for more information and best practices:

- National Cybersecurity Alliance > [StaySafeOnline.org](https://www.staysafeonline.org)
- Federal Trade Commission > [How to Protect Your Personal Information](https://www.ftc.gov/identitytheft)
- Federal Deposit Insurance Corporation > [Consumer Assistance Topics](https://www.fdic.gov/consumers/consumerassistance/)
- Federal Bureau of Investigation > [Scams and Safety](https://www.fbi.gov/scams-safety)