T.RowePrice

Understanding cybersecurity threats and how to protect yourself from them

Make Your Plan
August 2024

Key Insights

- With the rapid advancement of technology and artificial intelligence, cybercriminals have developed more sophisticated methods to gain access to our personal data and financial resources.
- Protecting yourself and your family requires thoughtful actions, vigilance, awareness, and attention to detail when interacting online and over the phone.
- T. Rowe Price uses strict safeguards to minimize security risks and help ensure that your online communications and transactions are safe and reliable.

Lindsay Theodore, CFP®
Thought Leadership Senior Manager

Thomas Byrd
Cyber Security Senior Manager

Cyberfraud refers to illegal activities carried out using digital technologies—particularly the internet—to deceive, manipulate, and steal from individuals and organizations. Cybercriminals can perpetrate scams via email (phishing), text messages (smishing), telephone (vishing), and social media platforms. Under the guise of legitimate communications from trusted sources, they aim to trick targets into revealing sensitive information so that they can ultimately gain unauthorized access to data or funds. When it comes to protecting yourself, knowledge is the key to prevention.

A growing but avoidable threat

The threat of cyberfraud has become increasingly difficult to ignore in today's interconnected world. Complaints to the FBI's Internet Crime Complaint Center (IC3) nearly doubled between January 2019 and December 2023. Perhaps even more concerning, the reported financial losses resulting from suspected scams over this five-year period grew by over 350% from USD 3.5 billion to USD 12.5 billion (See Fig 1). Experts believe these numbers to be underestimated since many scams go unreported.

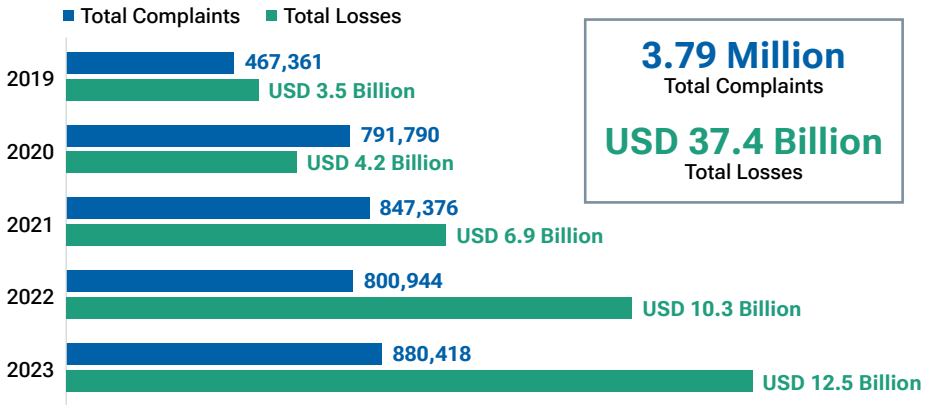
Start with the basics: Secure your accounts

While cybercrimes have grown in number and sophistication, there are steps you can take to reduce your risk of becoming a victim. Here are several basic but powerful security measures T. Rowe Price recommends for protecting yourself and your financial accounts.

- **Develop and maintain strong passwords.** Unique, complex usernames and passwords (which include a mix of letters, numbers, and special characters) are crucial to maintaining account security. T. Rowe Price recommends having unique usernames and passwords for all of your online account providers. This can help to ensure that a breach in one account does not compromise others.

Complaints and losses reported to the FBI's Internet Crime Complaint Center over the last five years

(Fig. 1) For complaints and losses over the years 2019 to 2023, the IC3 received a total of 3.79 million complaints, reporting a loss of USD 37.4 billion.



See Additional Disclosure.
Source: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

- **Sign up for Multi-Factor Authentication.** Multi-Factor Authentication adds an extra layer of security by requiring two forms of verification before granting access to an account. Once set up, in addition to your password, you will enter a one-time security code that is sent to your multi-factor method (via text, email, etc.). At T. Rowe Price, we recommend that investors choose to use Multi-Factor Authentication every time they log in (versus only when logging in on a new device).

- **Regularly monitor and review your account activity.** Make sure you review your account activity on a regular basis and at least every 30 days for financial accounts. This will enable you to spot unusual transactions and report them in a timely manner. Consolidating your accounts can help make this easier. The fewer accounts you have (and the fewer notifications and statements you need to monitor), the likelier you'll be to catch suspicious transactions.

- **Set up alerts and notifications.** Many companies (including T. Rowe Price) enable you to customize alerts for specific actions, such as deposits, withdrawals, transfers, login attempts from new devices, or password changes. These alerts can inform you instantly about critical account activity. In the event that the action was not initiated by you, you can call the provider to inform them of the incident and work with them to correct it and secure your accounts.

Take reasonable measures to interact safely online and over the phone

In addition to securing your accounts, there are several actions you can take to further reduce your exposure.

Best practices for proactively engaging securely online

Often, engaging online is a choice. The following tactics can help to protect you.

- **Exercise caution when using public Wi-Fi networks.** Especially when checking financial accounts or executing transactions, stick to trusted private Wi-Fi networks.

- **Use secure websites starting with https://.** This signifies that you are in a secure, encrypted online session.

A quick note on cryptocurrency:

Due to a variety of factors including minimal regulation, block chain technology, anonymity, irreversibility, and volatility, trading cryptocurrency carries a great deal of risk and is highly susceptible to fraud. Unless the investor is very tech savvy and has a high tolerance for risk, they may want to stick to more heavily regulated securities such as mutual funds, stocks, bonds, ETFs, and bank savings. For investors who want to diversify into cryptocurrency, an ETF may be an option for a relatively small portion of their portfolio.

- **Log out of websites.** Also, regularly clear cookies and browsing history from your internet browser.

- **Keep all computer and device operating systems, antivirus software, and internet browsers up to date with the latest version.** This can help to ensure that you have the most recent security patches in place.

Best practices for avoiding inadvertent exposure to social engineering

Social engineering is a technique utilized by cybercriminals to manipulate, influence, or deceive people into making security mistakes, performing an action, and disclosing sensitive information. The following steps can help to minimize your risk:

- **Be cautious and take your time, especially when you receive unsolicited communications.**
  - Review with a critical eye any unexpected email, text message, or other communication purporting to be from a legitimate source.
  - Look for red flags, such as poor grammar, requests for immediate action, or offers that seem too good to be true.
  - Always err on the side of caution, particularly when the requested action is unusual or bypasses normal business processes.
- **Do not click on links or respond to emails or text messages from unknown senders.**
  - Instead, if the sender purports to be representing a trusted company, type that company's official URL directly into your browser.
  - Log in via their secure website or call the company using the phone number on your statement to further investigate the matter.
  - If the sender is completely unknown to you, disregard.
- **Avoid providing personal or financial information requested via phone, email, text message, or social media.**
  - Government agencies (such as the IRS or Social Security) and companies like T. Rowe Price will not request personal information by email, text, or social media.
  - It is generally a best practice to disregard calls or texts from completely unknown numbers. If follow-up is needed, use a known phone number or alternate email address to verify any request before acting. Do not use the contact information provided by the potential scammer.
  - Typically, if the reason you are being contacted is legitimate, the company or individual will follow up using more formal communication channels, such as via first-class U.S. mail or express mail.

Develop awareness about common targets and scams

Unfortunately, adults over age 60 are the most common targets of cyberattacks, likely because they are viewed as having the largest savings balances. (See "Seniors and cyberfraud.") Luckily, there are resources available to keep the public informed. The U.S. Department of Justice's Transnational Elder Fraud Strike Force keeps an ongoing list of common elder fraud scams: https://www.justice.gov/elderjustice/senior-scam-alert. To further educate our customers, we have compiled a list of these and other scams—and actions you should take if you suspect you're being targeted.

What if I receive a call from T. Rowe Price?

Periodically, a T. Rowe Price representative may reach out to you—for instance, to discuss an account issue or offer help with your investments.

- In this case, the representative will disclose their full name, their role at T. Rowe Price, the reason for their call, and the fact that they are on a recorded line.
- Per security protocol, they will also ask to verify your identity before they can discuss your accounts openly.
- If you feel uneasy verifying yourself on a phone call you did not initiate, confirm the representative's first and last name, and let them know that you will call T. Rowe Price back on a phone number published on our official website and request to be transferred to that individual.

Awareness is key: Common scams and what you should do if you encounter them

If you suspect any of the below scams, do not send money or provide sensitive, personal, or financial information. Disconnect immediately and call IC3 to report the scam.

Common scams:	What the scammers want:	What you should do:
Social Security Administration (SSA)* Imposter Scam SSA imposters may contact you by telephone and falsely claim that your Social Security number (SSN) has been compromised and your accounts will be seized if you fail to act quickly.	Sensitive personal information (such as your SSN) or bank account number so that they can withdraw funds for "safekeeping" until the issue is resolved.	Disconnect immediately and call the SSA and IC3 to report the scam.
IRS* Imposter Scam Scammers may claim to be an IRS employee urgently informing you that you owe back taxes and will face arrest if you fail to pay.	Money transfer via wire, mobile payment app, or gift card purchase.†	Disconnect immediately and call the IRS and IC3 to report the scam.
Tech Support Scam Fraudsters may claim to be a computer technician who has detected a virus, malware, or hacking attempt on your computer. The scam may be initiated by a phone call, text message, email, or internet pop-up box.	Remote access to your computer, sensitive personal/financial information, and/or money transfer to pay for information technology help.	Disconnect the phone and/or close out the pop-up box immediately. Restart your computer and clear cookies and browsing history. Report the scam to IC3. Never click on unverified internet pop-up boxes or allow unsolicited remote access to your computer.
Lottery or Inheritance Scam Fraudulent telemarketers from outside the U.S. call claiming that you have won a sweepstakes, foreign lottery, or inheritance. They may claim to be an attorney or a public official.	Money transfers to pay fees for shipping, insurance, customs duties, or taxes associated with claiming your "winnings."	Disconnect immediately and call IC3 to report the scam. Block the phone numbers used to target you.
Romance Scam Scammers build fake profiles and contact victims through legitimate dating or social media sites.	After spending some time building trust, they eventually ask for money in the name of love.	An online love interest who asks for money is almost certainly a scammer. Generally, it's prudent to avoid accepting friend requests from strangers or carrying on relationships with people you have not verified and met in person.
Timeshare or Real Estate Sale Scam Scammers may use public records to find targets and then impersonate real estate agents, claiming to help sell the timeshare or other property for a very attractive price.	Sensitive information and money transfers to pay fees and taxes associated with facilitation of the sale.	Disconnect immediately and call IC3 to report the scam. Exercise extreme skepticism of anyone who promises to sell your timeshare or property quickly and for a great price (especially if that offer was unsolicited).
Grandparent Voice Scam (aka Emergency Scam) Callers may use voice cloning technology to sound like a loved one, usually a grandchild, in distress.	They may claim to be in an accident, injured, or in jail and that they need money sent urgently via wire transfer or mobile payment app to pay for something such as bail, a tow truck, a lawyer, or a ride share.	Disconnect immediately and call IC3 to report the scam. If you worry that it is indeed your loved one, call other close relatives to confirm the situation and/or let the caller know that you will need to speak with them in person before taking action.

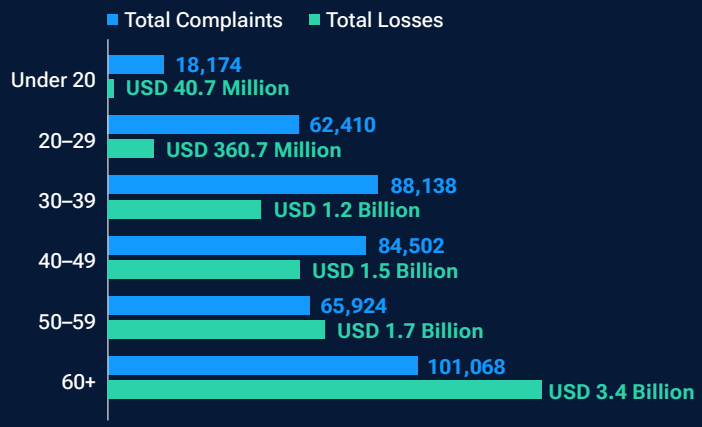
*Government agencies, such as the SSA and IRS, will never call or email you to request personal information or payment.
†Gift cards are commonly requested by scammers because they are easy to purchase and load; difficult to trace; and once the scammer has the gift card number and personal identification number, they can convert the funds to cash or purchases.

Seniors and cyberfraud

Individuals over age 60 have reported over twice as much in financial losses as compared with any other age group (see Figure 2).

2023 complaints to the FBI's Internet Crime Complaint Center by age group

(Fig. 2) Those age 60+ reported 101,068 complaints and USD 3.4 billion in losses.



Not all complaints include an associated age range—those without this information are excluded from this table. **See Additional Disclosure.**
Source: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Seniors can reduce their vulnerability by following the technology use best practices outlined in this article and recognizing red flags that clearly indicate "this is a scam."

According to the Federal Trade Commission:[1]

- If the caller says you need to buy gift cards, go to a cryptocurrency ATM, or go to the bank in person while they stay on the phone with you, **it's a scam**.
- If the caller tells you to lie to anyone who asks why you're transferring or withdrawing so much money, **it's a scam**.
- If the caller says you need to transfer or move your money to "protect it," **it's a scam**.
- If the caller tells you to cash out your savings to buy cryptocurrency or gold bars, **it's a scam**.

A good rule of thumb: Ignore unexpected requests for money. Just hang up.

If you suspect that you've been victimized, let your loved ones and impacted account providers know. Many cybercrimes go unreported (and unresolved) because seniors are too ashamed to report the incident and explore a remedy.

[1] https://consumer.ftc.gov/consumer-alerts/2024/01/did-someone-tell-you-move-or-transfer-your-money-it-could-be-scam

How T. Rowe Price helps protect your information and accounts

Although vigilance on behalf of individuals is key, companies should also have cybersecurity safeguards in place. At T. Rowe Price, helping to protect our clients' online security and privacy is a high priority. We use strict security controls to help ensure that your online communications and transactions are safe and reliable. We also maintain rigorous internal procedures for ongoing oversight and employee cybersecurity awareness training.

To help protect your information, T. Rowe Price employs a range of security measures, including:

- **Encryption and extended validation** (to ensure a secure connection with our website)
- **System activity logging** (to preserve and validate the transmissions of data)
- **Client identity verification and recorded phone calls** (for security, recordkeeping, and training purposes)
- **Automatic 10-day hold on withdrawals when crucial account information is changed** (such as the linking of a new bank account or an address change)
- **Dollar limits for withdrawal requests initiated online** (to ensure that larger withdrawals are treated with an appropriate level of scrutiny)
- **Stringent procedures for investigating and resolving suspected or reported incidents of fraud** (with the goal of recovering and reinvesting customer funds)
- **Customer-selected account security features** (such as Multi-Factor Authentication, alerts and notifications, and security questions)

T. Rowe Price also provides an account protection program

This program provides customers with assurance that their T. Rowe Price account is protected in the event that it is compromised due to fraud. Under this program, T. Rowe Price will restore eligible account losses due to unauthorized

activity if certain requirements are met. Account holders are automatically enrolled in the program but must follow these four security best practices in order to be eligible for coverage:

1. Establish a T. Rowe Price online account and Multi-Factor Authentication.

2. Maintain an up-to-date mailing address, email address, and phone number(s) on your T. Rowe Price account.

3. Review T. Rowe Price account statements, confirmations, and correspondence within 30 days after that information is posted to your online account or delivered to you by mail.

4. Contact T. Rowe Price immediately at **1-800-225-5132** if you suspect any unauthorized account activity, if you notice errors or discrepancies in your account, or if you are not receiving your T. Rowe Price account statements.

Conclusion

While cybercrimes have grown in number and sophistication, the red flags and similarities across scams have largely remained the same. Cybercriminals often aim to create a sense of urgency through fear or the promise of something that sounds too good to be true. They often pressure their targets into acting fast and they almost always ask for money—but via odd methods such as through gift card or gold bar purchases, cryptocurrency transfers, or mobile payment apps. To protect yourself, take your time, ask questions, and trust that if something feels suspicious, it probably is. Take proactive measures to secure your accounts, and remember that if there is an urgent matter that must be resolved, trusted institutions will contact you through appropriate, formal business channels.

Learn more about how T. Rowe Price helps protect your security.

To become a more educated and aware online consumer, visit OnGuard Online, a service of the U.S. Federal Trade Commission and other federal agencies. OnGuard Online provides information about avoiding scams, understanding mobile apps and Wi-Fi networks, securing your home computer, and protecting family members. For additional information about actions you can take to protect yourself, speak with your trusted financial professional.

If you become a victim of cybercrime, do not feel ashamed. Let your loved ones and impacted financial institutions know, then report it to IC3 (a service of the U.S. Federal Bureau of Investigation). For additional guidance on steps to take if you suspect you've been scammed, visit the Federal Trade Commission's website.

We recommend that investors of all ages add a **trusted contact** to their T. Rowe Price and other financial accounts. A trusted contact is a person we might reach out to in the case that we suspect you might be the target of a scam.

INVEST WITH CONFIDENCE®

T. Rowe Price identifies and actively invests in opportunities to help people thrive in an evolving world, bringing our dynamic perspective and meaningful partnership to clients so they can feel more confident.

Additional Disclosure

As appropriate, complaints are reviewed by IC3 analysts, who apply a crime type and adjust the total loss. Crime Types and losses can be variable and can evolve based upon investigative or analytical proceedings. Complainant/Entity is identified as the individual filing a complaint. Some complainants may have filed more than once, creating a possible duplicate complaint. Complaint counts represent the number of individual complaints received from each state and do not represent the number of individuals filing a complaint.

Important Information

This material is provided for informational purposes only and is not intended to be investment advice or a recommendation to take any particular investment action.

The views contained herein are those of the authors as of August 2024 and are subject to change without notice; these views may differ from those of other T. Rowe Price associates.

This information is not intended to reflect a current or past recommendation concerning investments, investment strategies, or account types, advice of any kind, or a solicitation of an offer to buy or sell any securities or investment services. The opinions and commentary provided do not take into account the investment objectives or financial situation of any particular investor or class of investor. Please consider your own circumstances before making an investment decision.

Information contained herein is based upon sources we consider to be reliable; we do not, however, guarantee its accuracy. **Actual future outcomes may differ materially from any estimates or forward-looking statements provided.**

Past performance is not a reliable indicator of future performance. All investments are subject to market risk, including the possible loss of principal. All charts and tables are shown for illustrative purposes only.

T. Rowe Price Investment Services, Inc., distributor. T. Rowe Price Associates, Inc., investment adviser. T. Rowe Price Investment Services, Inc., and T. Rowe Price Associates, Inc., are affiliated companies.

ID0007389
202408-3812354