Be cybersafe

Protecting your accounts and personal information is a top priority for Edward Jones. The firm uses multiple layers of tools and services to protect our systems from cyber threats. There are also steps you can take to protect yourself at home. Here are some tips to safeguard you and your family.

Passwords

- **Give accounts unique passwords.** Use a different password for work, financial services sites, social media and email.
- **Make password phrases long and strong.** If possible, use a phrase that is memorable to you, such as TheCatIn-TheHat8!. Strong passwords contain a combination of upper- and lowercase letters, numbers and special characters, such as !@#$.
- **Don't use common words.** If your password must be short, use a misspelled version of the word, such as kArtoon7 instead of Cartoon7. And change your passwords regularly. Passwords to sensitive information, social media and email should be changed at regular intervals.

Email

- **Look for malicious signs.** Scammers can make harmful emails appear to come from a friend or well-known business. Before clicking on links or opening an attachment, look for signs of a malicious email, such as odd word choices, misspelled words, urgent requests or offers that seem too good to be true.

  If there is a suspicious link inside the email, use your mouse to hover over the link and see if the pop-up wording matches the link description.
- **Guard your personal information.** Don't respond to requests for account numbers, passwords or other personal information in an email or a text message, unless you initiated the conversation. If you're unsure, confirm the request by calling the person directly (use a known phone number) who sent it or contact the business through an email listed on their official website.

Computers

- **Keep your antivirus software updated.** Install antivirus software on your computer, and ensure it's up to date. Consider setting up automatic updates and an automatic service renewal.
- **Back up your data.** Regularly save your

 OPR-11085C-A EXP 31 JUL 2023

critical data onto a backup device or service. Keep a copy of your backup data disconnected from your device and the internet when not in use.

- **Be careful of what you install.** Don't install bootleg or unlicensed software, which could infect your computer with a virus. Also, don't download peer-to-peer file-sharing programs, which could unknowingly give anonymous computer users access to your personal files.

Online accounts/e-commerce sites

- **Consider creating unique user IDs for all your accounts.** When possible, don't use your email address as a user ID for online accounts.
- **Enable multifactor authentication.** This safeguard verifies your identity in multiple ways each time you log in. Edward Jones uses this confirmation method each time you log in to Online Access.
- **Opt for safety over convenience.** Don't select "remember my password" in your browser for the websites you visit or allow e-commerce sites to store your credit card information. Officially log out of sites instead of simply closing the window.
- **Use only secure sites for purchases.** Look for https:// in the web address. The "s" stands for secure.

Mobile devices

- **Keep your devices up-to-date.** Install updates to your operating systems and applications as soon as they are available to ensure you have the latest security patches.
- **Use password protection.** Choose a strong password for your screen lock. For example, don't use "1234" or "0000," which are easy to guess.

Public Wi-Fi

- **Limit your use if possible.** Hackers can set up their own Wi-Fi networks with fake names designed to lure you in and access your personal and login information. For example, is "Hotel-Guest" or "Hotel Wireless Guest" the hotel's official Wi-Fi network? If you don't know, ask an employee.
- **Make a clean break.** Remember to log off a public Wi-Fi network when you are finished.
- **Turn off certain features.** Turn off file sharing and auto-connect to nonpreferred networks.
- **Use your own hot spot instead.** A best practice is to use your own private mobile hot spot or cellular phone data service instead of public Wi-Fi. Remember to turn off your phone's hot spot when you are not using it and protect it with a password.

Home networks

- **Change your default names and passwords.** Create your own user names and passwords for your router and wireless network. Hackers can easily search online to find the default information that came with your devices.
- **Set up a separate guest network.** If you give guests your Wi-Fi password, you're opening up access to all the devices you have connected to your Wi-Fi network. To protect your information, set up two wireless networks: one with a password for your family's use and one for guests.
- **Encrypt what you send over your wireless network.** Encryption scrambles the information you send so others can't read it. Wireless routers often come with the encryption feature turned off. To turn it on, check the directions that came with your router.

Social media

- **Use strict privacy settings.** Review your privacy settings regularly, and consider setting them so only people you know or approve can view your information.
- **Limit what you share online.** Watch what you list in your social media profiles and share in your posts. Keep your full name, address, birthday and even vacation plans private.

For assistance with your personal devices, contact your internet service provider or the device manufacturer.

Visit **edwardjones.com/privacy** for information on what Edward Jones does to protect your accounts from cyberthreats.

Brad Smith, AAMS™, CRPC™
Financial Advisor

2111 Eaton Ferry Road
Littleton, NC 27850
252-629-2555

Protect yourself:

What is computer intrusion?

Passwords and antivirus software can help protect your computer—and the information that's stored there. But what if someone accesses your computer without your knowledge?

Who is a target?

Anyone who owns a computer or other electronic device connected to the internet could be a target for computer intrusion.

Four common scenarios

1. Someone calls from a software company or internet provider claiming they have detected errors coming from your computer or device. You may even get a "pop-up" on your screen with a link or number to call. The caller might suggest your computer has some sort of virus or spyware.

   The caller will offer to fix the issue for you remotely if you follow a few simple steps. The caller will walk you through a few clicks on your keyboard and obtain your Internet Protocol (IP) address. With this information, the caller can take control of your computer.

2. Another scenario is someone may call claiming the company you purchased your virus protection plan through went out of business. The caller may offer a refund and ask to gain access to your system to deposit the funds directly into your account.

Brad Smith, AAMS™, CRPC™
Financial Advisor
2111 Eaton Ferry Road
Littleton, NC 27850
252-629-2555

3. You may receive notice that your computer and financial accounts have been compromised by a foreign entity. You'll be encouraged to move the contents of your accounts into the scammer's account for safekeeping while your computer is being serviced.

4. Once a scammer has gained access to your computer, any information stored there is at risk. The thief could also install spyware or other malicious software, which could allow them to steal your user IDs and passwords, and access your accounts. Some scammers have even coerced people into paying large dollar amounts (via credit card or gift cards) for the alleged computer repair.

Red flags

There are certain warning signs that can help you detect potential scams.

- You receive a call from someone saying they have detected something wrong with your computer.
- You receive a notification from your financial institution that your account information has been changed.
- You receive a "pop-up" on your computer to call Microsoft or another software provider with a number that does not belong to that company
- Your account statement reflects activity you did not authorize.

Tips to protect yourself

- Never provide your IP address or give control of your computer to someone you don't know.
- Remember that companies will never call the general public. They have absolutely no way of telling from a remote area whether a computer has software issues.
- Never click on a link in an email you receive unless you are positive you know the sender.
- Never call a number provided to you on a pop-up. Look up the legitimate company and call the publicly known number.
- Be sure you're running current virus detection software on your computer.
- Always use two-factor authentication on your financial accounts. This is a great fraud deterrent.

Reporting a computer intrusion scam

If you feel you've been victimized, contact your financial institutions immediately to make sure your information has not been compromised and your accounts have not been accessed.

If you paid a scammer with a credit card, follow your card issuer's procedures to dispute any unauthorized charges.

Disconnect your computer from the internet and contact a reputable company to have your computer serviced and your hard drive professionally cleaned. Then change all your passwords. If you change your passwords before having your computer cleaned, you may be unintentionally giving the scammer your new passwords.

If you have questions or need further assistance, please contact your Edward Jones financial advisor.

Protect yourself: Be alert to financial fraud

At Edward Jones, we want to empower our clients and their families to help protect themselves. We understand that confidentiality is key in any financial relationship. We also recognize that your personal and financial data contain your private information, and we are committed to keeping this information secure and confidential.

Fighting financial fraud starts with education as well as communication between family members and their financial professionals. The following information can help you recognize possible issues, prevent fraudulent activity and protect yourself or a loved one if fraud does occur.

Older adults can be a target

- According to the FBI, scam artists often seek out older Americans because:
  - They have concentrated wealth
  - They are less likely to report fraud
  - They were raised to be polite and trusting, and con men prey on these qualities
  - Mental impairment may make it difficult for them to recognize financial schemes
- Older adults, especially those who are new to the role of household decision maker, may be more prone to scam artists who demand quick decisions.
- Seniors may feel indebted to someone who has provided unsolicited advice or other assistance.
- Older victims may not report crimes because they are concerned their relatives may think they no longer have the mental capacity to take care of their own financial affairs.

Facing the facts

The number of elderly victims has risen at an alarming rate, while the loss amounts are even more staggering. In 2021, over 92,000 victims over the age of 60 reported losses of $1.7 billion to the IC3. The average loss per victim was $18,246. This represents a 74 percent increase in losses over losses reported in 2020.[2]

Although elder abuse comes in many forms, elder financial abuse has been identified as the third most commonly substantiated type of crime against seniors, following neglect and emotional/psychological abuse.

- Senior women who live alone are especially vulnerable to scams: Women are nearly twice as likely to be victims of elder financial abuse as men.[1] They may have less experience with handling financial issues and therefore may be more readily manipulated.

Common types of fraud that may affect mature investors	
Identity theft and phishing	Older adults may be less "tech-savvy" than younger generations and therefore more susceptible to phishing schemes. As thieves become more sophisticated in their online approaches, seniors may find it difficult to tell whether the business requesting their personal information is legitimate. In addition, threats of closing an account or canceling a credit card may add to the victim's insecurity and make him or her want to respond more quickly.
Caregiver fraud	A dishonest caregiver could steal valuables or cash from the person they have been paid to assist. Other schemes involve intercepting the victim's mail to obtain credit card numbers and information and then then using this information to commit identity theft.
Romance scam	Email, social networking and dating websites are commonly used to start and continue relationships. Unfortunately, these channels are sometimes used to defraud individuals by exploiting their trust and vulnerability. Once a level of trust has developed, the scammer will ask the victim to send money to help get the scammer or a family member out of a difficult financial situation. Some of these online relationships may quickly develop into what appears to be a romance. Often, promises of undying love and even marriage can result.
Lotteries/ sweepstakes	An older person may receive a call, an email or a letter stating they could win, or has already won, a "valuable" prize or a large amount of money. The recipient is then asked to send money to cover taxes, shipping or processing fees on the "winnings." The prize may never be delivered or, if so, is usually worth less than the money paid to retrieve it. In many instances, lottery scams involve foreign countries or individuals calling from long distances.
Grandparent scams	A caller may claim to be a grandchild (or another relative or a friend) who needs money. If the recipient responds with a grandchild's name, the caller can use this information to convince the recipient the call is legitimate. The thief may employ any number of scenarios to gain sympathy and money; a common tale involves an arrest or auto accident while in another country. More elaborate scams have included an "attorney" or a "public defender" to validate the story and emphasize the urgency of the situation. The thief may also plead with the recipient not to tell his or her parents.
Social Security scams	An individual will receive a call, allegedly from the Social Security Administration, notifying them there is an issue with their Social Security number (SSN), and they need to call back at a number provided or their benefits will be stopped. When the person calls back, they speak to an "officer" with the administration, who requests them to verify their name and SSN. They will then be told their SSN has been tied to or used in a serious crime, and they could face charges, along with their benefits being suspended. They will typically be instructed to purchase pre-paid money cards in order to alleviate the situation. The method of payment can escalate into other forms of payments at higher amounts, even when the person complies.

Red flags

The following red flags may indicate financial exploitation of an older adult:

- A rapid decline in the value of the victim's account
- Withdrawals from the victim's account that are inconsistent with previous spending habits
- Essential bills going unpaid, despite adequate income
- Missed appointments
- Acquaintances or family members who seem overly interested in an older adult's finances
- Concern or confusion about missing funds from an account
- Unexplained changes in beneficiary designations
- A sudden, close relationship with a new "friend"
- Statements sent to an address other than that of the victim
- Missing belongings or property
- A caregiver who isolates the older person from family, friends, community and other stable relationships
- The need to send money in order to receive a windfall (e.g., lottery winnings, estate settlements, etc.)
- The need to send additional money after an initial payment has been made

How to help combat financial fraud

Investigate before investing	• Take the time to conduct research. Asking a promoter for more information or for references is not enough because thieves have no incentive to give accurate information. • Talk to family or friends before making an important decision regarding finances. • Understand the investment, the risks and the company's history.
Know the fears con artists prey upon	Many older investors worry about the adequacy of their retirement savings, especially if they are faced with costly medical expenses. Con artists may pitch their schemes as a way to increase financial security, but only if the older adult acts immediately.
Be wary of unsolicited offers	• Thieves use email, faxes and internet postings to create a buying frenzy to boost the share price of thinly traded stocks. Once they quit promoting the company, the share price quickly falls. • If the victim sends money abroad and something goes wrong, the funds are more difficult to trace and nearly impossible to recover.
Protect personal information	• Shred financial documents and paperwork with personal information before you discard them. Many companies, including Edward Jones, offer electronic delivery, which can help reduce a paper trail. • Protect Social Security numbers. No one should carry a Social Security card in their wallet or write a Social Security number on a check. Give this number out only if absolutely necessary or ask to use another identifier. • No one should give out personal information over the phone, through the mail or over the internet unless they know the recipient is legitimate. • Thieves can use links in unsolicited emails to take advantage of older adults. Instead, type in a web address you know. Firewalls, anti-spyware and anti-virus software can help protect a home computer, especially if they are kept up to date. • Be alert if the older adult experiences any of the following, which require immediate attention: – Bills that do not arrive as expected – Unexpected credit cards or account statements – Denials of credit for no apparent reason – Calls or letters about purchases they did not make • Credit reports contain information about a person's accounts and bill-paying history. The law requires the major nationwide consumer reporting companies to give each American a free copy of their credit report on request once per year.

If fraud occurs:

- Placing a "fraud alert" on a credit report entitles the person to a free copy of their credit report and tells creditors to follow certain procedures when opening accounts in that person's name or making changes to existing accounts. For an initial 90-day fraud alert, call one of the following:
  - Equifax: 866-349-5191
  - Experian: 888-EXPERIAN (397-3742)
  - TransUnion: 800-680-7289
- Keep copies of documents and records of conversations about any theft.
- File a complaint with the Federal Trade Commission at **877-ID-THEFT (438-4338)**. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. **You can also file a complaint online at ftc.gov/complaint.**
- If theft of mail has occurred, contact the U.S. Postal Inspection Service at **877-876-2455.**
- Contact the Social Security Administration's Fraud Hotline at **800-269-0271** if a Social Security number has been used fraudulently.

Additional resources

- Federal Bureau of Investigation – Be Crime Smart (fbi.gov/scams-and-safety)
- Federal Bureau of Investigation Internet Crime Complaint Center (IC3) (ic3.gov/default.aspx)
- FINRA Scam Meter (tools.finra.org/scam_meter/)
- identitytheft.gov
- Securities and Exchange Commission – Investor Alerts and Bulletins (sec.gov/investor/alerts.shtml)
- The U.S. Department of Justice Elder Justice Initiative (justice.gov/elderjustice)
- U.S. Postal Service (usps.com)
- AnnualCreditReport.com (annualcreditreport.com) 877-322-8228
- edwardjones.com/privacy
- Identity Theft Resource Center (idtheftcenter.org)
- National Consumers League (nclnet.org)

[1] The MetLife Study of Elder Financial Abuse, Mature Market Institute, 2011

[2] IC3 Elder Fraud Report, 2021

Brad Smith, AAMS™, CRPC™
Financial Advisor
2111 Eaton Ferry Road
Littleton, NC 27850
252-629-2555

Protect yourself: What is a grandparent scam?

Grandparents often have an emotional bond with their grandchildren. When a grandchild calls with a problem, the grandparent most likely feels compelled to help. But what if the voice on the other end of the line is really a scam artist?

Who is a target?

This scam preys on the emotions of older adults who want to help their grandchildren and other family members.

Common scenarios

Someone claiming to be a grandchild or another relative calls an older adult, tricking him or her into providing information that can convince the victim it's really a relative. The caller may describe an emergency (such as an arrest or auto accident in a foreign country) and ask for money to be wired urgently. More elaborate scams may have someone posing as an attorney or a public defender in order to validate the story and emphasize the urgent need for money.

The caller may plead with the grandparent not to tell his or her parents or other family members. This can reinforce the emotional bond and make the grandparent feel compelled to help since the grandchild came to him or her first for help.

Red flags

- You receive a call from someone who doesn't readily identify himself or makes you guess who he is.
- A grandchild contacts you instead of his or her parents to ask for money.
- The caller wants you to act immediately because of some urgent, impending deadline and begs you not to tell anyone, especially his or her parents.
- The caller asks you to wire money to a person or place that you don't recognize, or to a country other than where the caller says he is located. (For example, the caller might claim to be in a Canadian jail but ask you to wire money to Jamaica.)

How a grandparent scam works

In this example, the grandmother might later claim the caller knew her grandchild's name and school, when in fact she supplied this information.

Scammer: Hi, Grandma. This is your favorite grandson. Can you guess which one?

Grandmother: Bobby?

Scammer: Yes, this is Bobby! Do you remember where I go to school?

Grandmother: State College.

Scammer: Yes, that's right. Well, I was at State College, and I decided to drive to Mexico with some friends, and we got into a little trouble...

Tips to protect yourself

- Ask the caller a question he should be able to answer, such as his mother's or father's first name.
- Remain calm despite the "emergency" nature of the call. Take the time to do your research so that you make a decision based on facts rather than emotion.
- Be careful with what you say—do not provide information the caller can use.
- Ask family members whether the grandchild actually is traveling outside the country.
- Call the grandchild back at a phone number you already have rather than one supplied by the caller.

Reporting a grandparent scam

If you believe you have become the victim of a grandparent scam, please contact your local law enforcement agency and immediately notify the financial institution(s) the funds were sent from. Contact your Edward Jones financial advisor if you need further information or guidance.

Brad Smith, AAMS™, CRPC™
Financial Advisor
2111 Eaton Ferry Road
Littleton, NC 27850
252-629-2555

Protect yourself:
Identity theft

The typical identity thief uses someone else's reputation to obtain money, conceal the thief's own identity, receive services or secure employment.

With synthetic identity theft, which is a more sophisticated form of identity theft, an imposter creates a new identity by using your personal information but altering it so that credit bureaus create subfiles for the new accounts. These accounts don't appear on your credit report, making synthetic identity theft difficult to detect.

Who is a target?

Anyone can be a target of identity theft. And anyone with a valid Social Security number is a potential target of synthetic identity thief.

Common scenarios

Skilled identity thieves obtain personal information by:

- **Dumpster diving –** They look for bills or other papers containing your personal information.
- **Skimming –** They steal credit and debit card numbers by using a special storage device when processing your card.
- **Phishing –** They send spam or pop-up messages asking you to reveal personal information.
- **Changing your address –** They divert your billing statements to another location.
- **Traditional theft –** They steal wallets and purses. They take mail that identifies you, including bank and credit card statements. They steal personnel records from their employers or bribe employees who have access.
- **Data breach –** They access, copy, transmit, view or steal information from electronic information storage platforms.

Red flags

Be alert to the following:

- Mail that doesn't arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Significant, unexplained changes in your credit score
- Collection calls or letters about purchases you did not make

Tips to protect yourself

- Shred financial and other personal documents before disposing of them. Consider electronic delivery, which can reduce your paper trail.
- Do not carry your Social Security card or write your number on a check. Provide it only if absolutely necessary, or ask to use another identifier. Typically, you are required to provide your Social Security number only when dealing with a law enforcement government agency; when opening an account with a bank, brokerage or other financial services firm, or an insurance company; when a background investigation or credit check is required while seeking employment; and when obtaining health care. Some states require Social Security number disclosure in other cases, so always ask why your number is required.
- Never provide personal information on the phone, through the U.S. mail or email, or over the internet unless you know the request is legitimate.
- Do not click on pop-up ads or links in unsolicited emails.
- Keep your computer security and antivirus software up to date.
- Do not use an obvious password, such as your birth date, your mother's maiden name or the last four digits of your Social Security number.
- Maintain confidential documents in a secure location in your home.

Brad Smith, AAMS™, CRPC™
Financial Advisor
2111 Eaton Ferry Road
Littleton, NC 27850
252-629-2555

- Periodically inspect your credit report. The law requires the major nationwide consumer reporting companies – Equifax, Experian and TransUnion – to give you a free copy of your credit report each year if you request it. Visit AnnualCreditReport.com or call 877-322-8228 to order your free credit report each year. You also can write to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Reporting identity theft

Contact the Federal Trade Commission:

- **Online:** identitytheft.gov
- **Phone:** 877-ID-THEFT (877-438-4338)

Additional steps include the following:

- Place a fraud alert on your credit reports. This tells creditors to follow certain procedures when opening accounts in your name or making changes to your existing accounts. For an initial one-year fraud alert, call one of the following:
  - Equifax: 888-836-6351
  - Experian: 888-EXPERIAN (888-397-3742)
  - TransUnion: 833-395-6938
- Close any accounts that have been tampered with or established fraudulently.
- Call the security or fraud department of each company where an account was opened or changed without your OK. Follow up in writing, with copies of supporting documents.
- Use the ID theft affidavit at identitytheft.gov
- Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
- Keep copies of documents and records of your conversations about the theft.
- File a report with law enforcement officials to help you with creditors who may want proof of the crime.

