



# Personal Security Insights

Proven Strategies for Safeguarding  
Your Wealth and Family

Not FDIC Insured • May Lose Value • No Bank Guarantee

For investment professional use only.



# Key Personal Security Topics



Make Yourself a Difficult Target for Cybercriminals



Your Digital Footprint—Understand and Protect It



Protect Loved Ones from Elder Scams



Keep Your Home Secure—People, Possessions, and Information



Travel Safely

# Make Yourself a Difficult Target for Cybercriminals



## **Cybercriminals aim to steal your login information and “play you” online**

Adopt low-pain, high-impact strategies to make yourself a difficult target

### **KEY STRATEGIES**

- ✓ Use two-factor authentication
- ✓ Freeze your credit
- ✓ Consider using a dedicated device for financial transactions and accounts
- ✓ Be vigilant about cyber hygiene: use unique/strong passwords; leverage alerts; leverage voice recognition technology; keep systems and antivirus software updated; use only trusted networks

# Your Digital Footprint—Understand and Protect It

Consider hiring a professional to assess your online exposure



## What's online about you and your family?

Social media sharing (messaging and video), professional networking sites, corporate/charitable websites, government records, real estate listings/videos/tours

## KEY STRATEGIES

- ✓ Limit disclosure
- ✓ Enable security features on social media sites
- ✓ Don't share real-time information
- ✓ Get **everyone** in the house on the same page
- ✓ Periodically audit your digital footprint

# Protect Loved Ones from Elder Scams

Initiate the conversation (early and often), be empathetic, and have a strategy



## What should you look out for?

- Elder exploitation is unfortunately very common, particularly when individuals are in cognitive decline
- Perpetrators include fraudsters and con men, but also those known to and trusted by the victim
- Extra vigilance in monitoring financial accounts is highly recommended, especially after the loss of a spouse

## KEY STRATEGIES

- ✓ Prioritize the conversation—make it a core topic of financial planning
- ✓ Know the common scams
- ✓ Create oversight (ideally, with more than one person) to monitor financial accounts
- ✓ Leverage alert capabilities on accounts
- ✓ Act quickly if foul play is suspected
- ✓ Remain vigilant

# Keep Your Home Secure—People, Possessions, and Information

Consider hiring an expert to perform a risk assessment of your properties



## What should you protect?

Personal safety (top priority), valuable personal property (jewelry, cash, art, antiques, etc.), personal information and documents (birth certificates, Social Security cards, passports, passwords, financial account information, etc.), and cherished family heirlooms

## KEY STRATEGIES

- ✓ Have a plan for emergencies—for the whole family
- ✓ Vet individuals with access (house cleaners, dog walkers, nannies, etc.)
- ✓ Employ an alarm system, and understand its features and capabilities
- ✓ Weigh convenience vs. risk when using Web-enabled devices and services
- ✓ Consider an online document storage system (like FidSafe®) for vital documents
- ✓ Secure home network

FidSafe is not a Fidelity Brokerage Services LLC service. FidSafe is a service of XTRAC LLC, a Fidelity Investments company.

# Travel Safely

Take the necessary steps to embark on your next journey with confidence



## **Advance planning can make a world of difference in case of an unforeseen event**

Medical safety, financial safety, communication safety, vital document safety, home safety

### **KEY STRATEGIES**

- ✓ Register your trip with the U.S. Department of State
- ✓ Consider travel medical insurance
- ✓ Carry a working cell phone with emergency numbers and make a test call when you arrive
- ✓ Consider vaccines
- ✓ Notify your banks and credit card providers
- ✓ Carry copies of vital documents
- ✓ Protect your home while away

# Resources

The screenshot shows the Fidelity website's security resources page. At the top, there is a green navigation bar with the Fidelity logo and links for 'CUSTOMER SERVICE', 'PROFILE', 'OPEN AN ACCOUNT', 'REFER A FRIEND', and 'LOG IN'. A search bar is also present. Below the navigation bar, there are tabs for 'Accounts & Trade', 'Planning & Advice', 'News & Research', 'Investment Products', and 'Why Fidelity'. The main content area features a large image of a woman working on a laptop. Below the image, the text reads: 'We're committed to your security. We safeguard your accounts with strong encryption, firewalls, secure email, and proactive 24/7 system surveillance.' Underneath, there is a section titled 'More ways we protect you from fraud' with the subtext 'Rest assured, we offer extra security measures for the ways you like to do business.' This section contains four icons and their corresponding descriptions: 1. 2-factor authentication: 'Protect your identity: For extra protection on logins and sensitive transactions, get a security code via text or automated call to verify it's you.' 2. Money transfer lockdown: 'Lock your accounts instantly: Block electronic money movement out of your accounts, protecting your balances from unauthorized transfers.' 3. Security text alerts: 'Stay informed on account activity: Get instant security alerts on your mobile number when certain transactions or profile updates are made to your account.' 4. Fidelity MyVoice: 'Call us with added security: Use our voice recognition technology to instantly verify it's you calling, adding another security layer to your account.' A link 'See more of our security measures' is provided. Below this, there is a section for 'Fidelity Customer Protection Guarantee' with the text: 'We're proud of the trust you place in Fidelity and want to ensure that you have peace of mind when doing business with us. That's why we offer this guarantee: We will reimburse you for any financial losses that result from unauthorized activity on your accounts.' At the bottom, there is a green shield icon with a checkmark and the text: 'How strong are your passwords? If you use the same username or password at Fidelity and other online sites, your accounts could be at risk. Use strong, different passwords for each of your online accounts. Change your password now.'

## Fidelity Resources

- [fidelity.com/security/overview](https://fidelity.com/security/overview)
- 1-800-FIDELITY
- Add two-factor authentication: [fidelity.com/security/soft-tokens/overview](https://fidelity.com/security/soft-tokens/overview)
- Storing critical documents in a secure digital repository: [fidsafe.com](https://fidsafe.com)

## Other Resources

- Freeze your credit by contacting the three national credit bureaus: Equifax<sup>®</sup>, Transunion<sup>®</sup>, and Experian<sup>®</sup>
- U.S. State Department—Smart Traveler Enrollment Program: [step.state.gov](https://step.state.gov)
- Emergency preparedness for your home and family: [fema.gov](https://fema.gov)
- If you believe your identity has been stolen: [identitytheft.gov](https://identitytheft.gov)