leadership series

Personal Security from All Angles

Fidelity INVESTMENTS

Get educated on personal security and risk

> **Fidelity Security** employs the most sophisticated technologies and best practices available in an effort to make certain that your sensitive information and accounts are well protected, both online and in person. See Fidelity.com for the security features we provide.

GARY ROSSI
VICE PRESIDENT
FIDELITY SECURITY SERVICES

Cyber Fraud

While most people recognize that online fraud, or cybercrime, is a potential threat, few know how or why they may be at risk. Not understanding who the adversary might be or how they commit their crimes can put individuals at risk.

"The Bad Guy"

Economic cybercriminals pose the greatest online risk to your and your family's financial data and assets. Make no mistake; many of these thieves are highly skilled and sophisticated, and use technology to steal.

How cybercriminals operate

Indiscriminant targeting—these criminals cast a wide net, hoping the sheer quantity of potential victims will yield sufficient economic benefits (see Scam Dictionary, page 4).

Specific victim targeting—a growing and more-concerning trend. In these cases, criminals spend a great deal of time and effort identifying a worthwhile target. They develop a victim profile based on public and private information with the goal of stealing from financial accounts.

Although the actual criminal act can take several forms, the basic steps are often similar. Below is a relatively common scenario.

SEND PHISHING EMAIL	GAIN ACCESS	MANIPULATE ACCOUNTS
An individual opens an email that appears to be from a trusted source and then clicks on a link or opens an attachment that installs malware on the computer.	Malware allows a criminal to obtain login information and thereby gain access to an individual's financial accounts.	The bad guy can then log in to and manipulate accounts to steal money.

SCAM DICTIONARY

KEYLOGGER

A technology that records consecutive keystrokes on a keyboard to capture username and password information.

PHISHING

An attempt to obtain financial or other confidential information from a user, typically by sending an email that mimics a legitimate organization, but contains malware (e.g., keylogger) that operates in the background to collect sensitive information.

SPEAR PHISHING

A highly personalized form of phishing where an email appears to be from a friend or financial institution, with an attachment or link to a site that downloads malware—usually spyware or a keylogger that operates in the background to collect sensitive information.

MALWARE

A software program designed to damage or cause unwanted actions on a computer system, including viruses, worms, and Trojan horses.

RANSOMWARE

A type of malware that restricts access to computer systems until the target pays a ransom to the malware operator to remove the restriction.

WHALING

A spear-phishing technique that targets high-net-worth individuals, family offices, and corporate executives.

Make yourself a difficult target

Taking some of these simple steps may discourage a potential adversary.

Limit your exposure

Treat your computing devices as you would your front door—restrict access and use strong security measures.

ACCESSING ACCOUNTS

- Use two-factor authentication whenever possible.
- A password's length and complexity determine its strength.
- Do not use the same password for multiple financial relationships.
- Change passwords frequently—even strong passwords.
- Always access accounts via a secure network. The convenience of public Wi-Fi is more than offset by the exposure of your login credentials to potential thieves that "hijack" the network's traffic, capturing sensitive documents and passwords.
- Ensure that your financial services firms offer fraud guarantees and strong authentication options.

EMAILS

Emails can be the easiest way for a criminal to transmit malware to your device.

- Use a dedicated email account for financial transactions.
- Be wary of unsolicited emails—especially if there is a link to a website or a request for personal information—even if they appear to come from a recognized entity.
- Ask yourself if the email attachment seems necessary and if it makes sense. For example, does your favorite charity typically email you? Does your alma mater often ask you to open an attachment within its emails?

ADDITIONAL STEPS

- Consider using a dedicated device for financial transactions.
- Install industry-standard systems and software, keep them up to date, and perform regular backups—including on mobile devices.
- Regularly back up sensitive data to an external drive and the cloud to protect yourself from ransomware.
- Consider adding a "security freeze" at the credit bureaus to avoid additional accounts being opened in your name.
- Leverage voice biometrics, such as Fidelity MyVoice℠.

Managing Your Digital Footprint

Online personal information can increase your "surface area" for attack. Protect yourself from unwanted attention, and know what is online about you and your family.

How much of your private information is actually public?

- LinkedIn and other business networking sites
- Facebook, Twitter, Instagram, and other social media sites
- Online ancestry/genealogy sites
- Corporate websites containing executive biographies
- Profiles related to outside affiliations (boards, charities, etc.)
- Real property records (home listings, local assessor information, etc.)

Reduce online access to your information

- ☐ Professional consultants can determine what is online about you and your family.
- ☐ Limit disclosure of unnecessary details on social/business networking sites.
- ☐ Enable security features available on social media sites, and stay abreast of current privacy policies.
- ☐ Ensure family consistency in limiting online information.
- ☐ Review online biographies and limit the level of personal detail.

Best practices

WHEN TRAVELING

- Don't broadcast travel plans.
- Ensure family does not publicly share information as it happens, such as "We are boarding our flight for Europe!"
- Be aware of posting photos tagged with locations.
- Limit personal information on automatic "out-of-office" replies.

WHEN DONATING MONEY

- Charities and political organizations are often required to periodically disclose donor information.
- Consider using business addresses or a personal P.O. Box for these purposes.

OTHER CONSIDERATIONS

- Ensure photos and personal documents are stored in a secure online repository or offline.
- Remove detailed photos and information from old real estate listings to provide only basic information to those who look up your address online.

Home Safety and Security

A comprehensive residential safety and security plan can provide you with peace of mind while you enjoy the comforts of your home. An effective plan involves taking reasonable, practical precautions to mitigate common issues. Consider the following:

While many homeowners have installed (or inherited) home alarm systems, they do not fully understand their features or monitoring strategy.

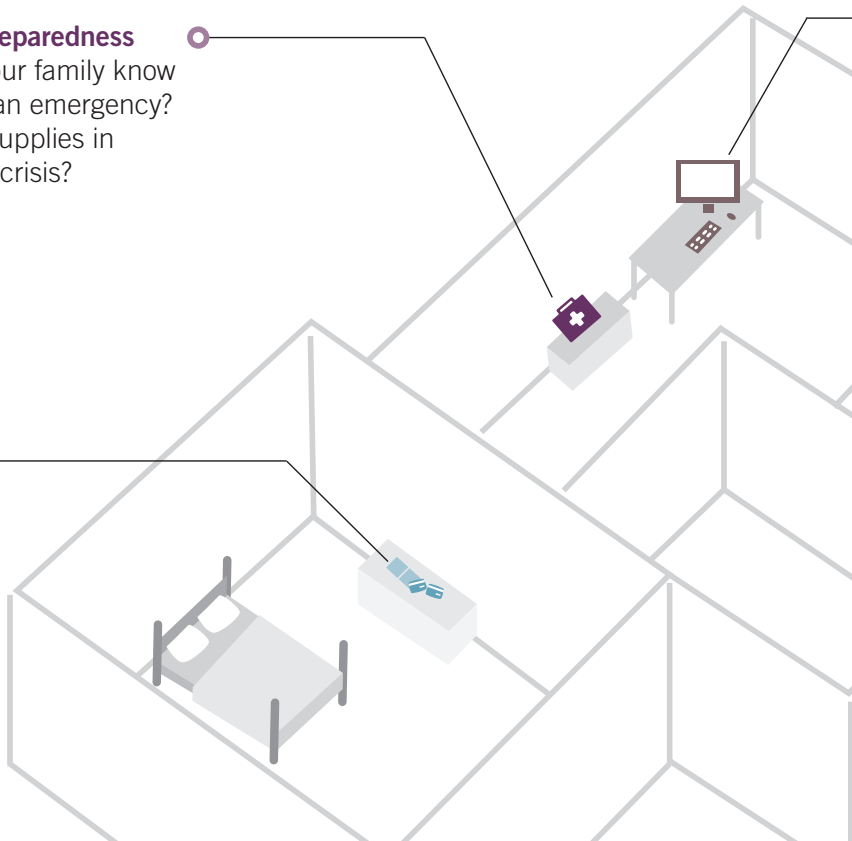
Who has access to your home, family, and personal information?

Do you have an emergency plan for such events as a medical situation or severe weather?

RESIDENTIAL SAFETY AND SECURITY TAKES MANY FORMS

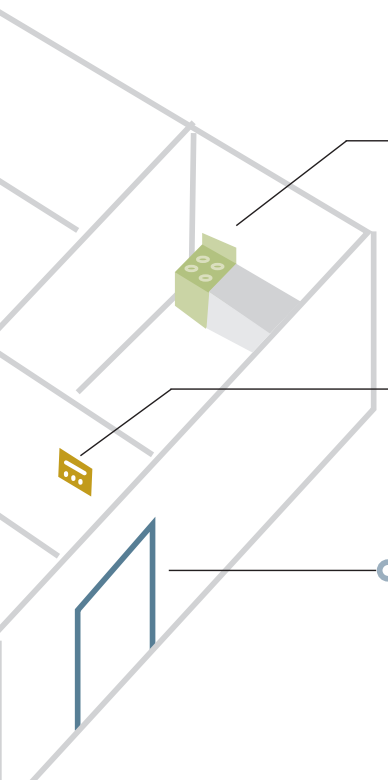
Emergency Preparedness
Do you and your family know what to do in an emergency? Do you have supplies in the event of a crisis?

Protecting Personal Information
Is your personal information organized and secure? Are you disposing of sensitive information properly?



Secure Your Home

- ☐ Consider a professional "all hazards" risk assessment that will assess your home in a wide range of areas.
  - Ensure consultants are independent fact finders not tied to a specific product or service.
  - Similar to a comprehensive home inspection, a finished product should provide a roadmap with action steps to reduce risk.
- ☐ Meet with your alarm service provider and review monitoring protocols.
- ☐ Enable included security features on your home network/ router (firewalls, change default passwords, etc.).
- ☐ Consult a licensed locksmith to ensure that keys cannot be easily duplicated, or consider alternate locking devices.
- ☐ Review physical security features of your home and property. Are pathways well lit with motion-activated lighting? Is landscaping cut back to eliminate potential hiding spots?
- ☐ Organize personal files and properly store or shred them when they're no longer needed.
- ☐ Review public websites for emergency preparedness information.



Home Network
Do you regularly back up data?
Do you have a strong password protecting your router from being hacked?

The "Internet of Things"
Besides your home computer, many common devices can provide a window into your personal network (thermostats, appliances, etc.).

Alarm System Monitoring
Do you know how your home is monitored and what will occur in the event of alarm activation?

Controlling Physical Access
Who has keys or alarm codes to your home? Do you use the alarm you have? Is the lighting around your home sufficient?

Vetting Individuals with Access

While it's uncomfortable to think anyone with access to your home would abuse that trust, it is worth investing the effort to properly screen individuals with access.

It's not just about full-time or live-in help. Part-time employees, such as tutors, nannies, dog walkers, and cleaners, may have as much access as a housekeeper.

Online search engines (Google, Yahoo, etc.) can help you conduct basic research and may highlight obvious issues or areas for concern.

With individual consent, online providers can perform local or national criminal checks, if provided with basic personal information.

Be aware that individual state laws vary widely on what type of information may be publicly available, for how long, and how it can be used when making employment decisions.

Comprehensive vetting by professional providers can examine multiple aspects of an individual's background, including credit history, employment, and education verification.

Travel Safety

Accidents happen everywhere. Taking a few reasonable steps to assess your personal risk when traveling will go a long way toward ensuring that you and your travel companions are well prepared.

RESEARCH YOUR DESTINATION

Make sure you are aware of common risks and security issues. For international travel, the U.S. State Department website https://step.state.gov/ provides up-to-date country information and travel advice.

BASIC MEDICAL SUPPORT

Know where to go in the event of a medical problem (local referrals, medication replacement, etc.).

SHORT-TERM TRAVEL/ MEDICAL INSURANCE

It can assist in a catastrophic event requiring emergency medical treatment, evacuation, etc. Your medical insurance provider or corporate travel desk may be a good place to start looking for these services.

REDUCE TIME IN CROWDED AIRPORTS

To help you move quickly through crowded areas, reduce time in queues by preprinting boarding passes, enrolling in trusted-traveler programs, and minimizing checked luggage.

Protecting Elders

Unfortunately, one of the fastest growing areas of fraud is the financial exploitation of our senior population. Although cognitive decline associated with age, mental disabilities, injuries, dementia, or other medical conditions can present significant risk factors, victims of financial exploitation may not be suffering from any diminished capacity issues. Their funds may be misappropriated at the hands of a trusted individual, as the result of undue influence, or by falling victim to a variety of scams targeting vulnerable populations.

Although every situation is different, to the right are three practical steps to reduce the risk of an elderly person being victimized. Also, a link to Fidelity's publication, "Aging Well: A planning, conversation, and resource guide," can be found on page 13.

> "One in five elderly people will be financially exploited. Only 1 in 44 cases are reported."[1]

1

Create oversight

Ideally, more than one trusted person should have insight into their financial activity. Work with family and friends to create clear accounting for a senior citizen's financial accounts.

2

Set alerts

Set up automatic alerts with financial institutions that trigger when significant transactions are requested, or when profile changes are made.

3

Act quickly

If you are concerned about potential fraud, seek assistance early—problems will only get worse over time. Your Fidelity representative can assist you.

[1] *National Adult Protective Services Association, as of June 2016.*

Resources

Fidelity Security Overview
https://www.fidelity.com/learning-center/personal-finance/family-financial-safety/security-360

Fidelity Customer Protection Guarantee
https://www.fidelity.com/security/customer-protection-guarantee

How to add two-factor authentication on your Fidelity account
https://www.fidelity.com/security/soft-tokens/overview
1-800-FIDELITY

How to add voice biometrics on your Fidelity account
https://www.fidelity.com/security/fidelity-myvoice/overview
1-800-FIDELITY

How to add alerts on your account
http://www.fidelity.com/security/monitor-your-accounts

If you believe your identity has been stolen
www.identitytheft.gov

Emergency preparedness for home and family
www.fema.gov

Selecting a vendor for background checks or internet analysis
http://www.napbs.com/

Additional information on protecting seniors from exploitation
www.napsa-now.org
"Aging Well," a guide by Fidelity Investments
https://www.fidelity.com/bin-public/060_www_fidelity_com/documents/Aging_Well_Guide.pdf
AARP Fraud Watch
https://www.aarp.org/money/scams-fraud/fraud-watch-network/

How to add a "security freeze" at the credit bureaus
https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

U.S. State Department—Smart Traveler Enrollment Program
https://step.state.gov/

Storing critical documents in a secure digital repository
www.fidsafe.com

AUTHORS

Gary F. Rossi | Vice President, Fidelity Security Services

Gary Rossi has more than 30 years of experience as a private sector and law enforcement security professional with deep expertise in investigations, cyber fraud, risk mitigation, and strategic planning. Gary joined Fidelity Investments in 2003 and served as Fidelity's Head of Corporate Investigations for nearly a decade, which included leading all customer fraud/identity theft matters, anti–money laundering cases, and cyber-related investigations. Gary and his team created a comprehensive anti-fraud program to protect Fidelity's customers from sophisticated cyber criminals. Gary now leads the Fidelity Security Services group, working directly with many clients to assist them in better understanding current security threats and with building appropriate mitigation strategies.

Prior to Fidelity, Gary served for 14 years as a special agent for the Federal Bureau of Investigation (FBI). He specialized in a wide variety of white collar crime investigations, which included sophisticated financial frauds, cybercrimes and public corruption matters. Gary functioned as the Chief of the FBI's Undercover and Sensitive Operations unit at FBI Headquarters in Washington, DC. This unit was responsible for overseeing many of the FBI's most sensitive and complex cases. Prior to the FBI, Gary worked as a CPA for Arthur Andersen & Co., and as a consultant for the cyber security consulting firm @Stake (now Symantec). Gary holds a degree in accountancy and management from Bentley University.

Jon Dougherty | Program Manager, Personal Security Education Program

A 23-year veteran of Fidelity Investments, Jon most recently served as the Vice President of Risk Technology, where he was responsible for the delivery of technology services in support of Global Security Operations across the enterprise. His responsibilities included planning/forecasting and oversight of solution delivery and support teams as well as the Global Security Operations Center—Fidelity's 24x7x365 emergency management, alarm monitoring, and event and crisis management function. Jon received his bachelor's degree from Westfield University and is a member of ASIS International.

762158.3.0 1.9878766.102