PREVENTING HIGH-TECH IDENTITY THEFT

Presented by The Monument Group Companies

Featured speaker: David Floyd

November 19, 2014

Introduction

- Preventing Identity Theft (this session)
- Monitoring for Theft (future session)
- Responding to Theft (future session)

Overview

- What is identity theft?
- High-tech methods
  - Phishing emails
  - Spyware
  - Data retrieval from discarded devices
- Minimizing Risk
  - Device Safety
  - Safe device disposal
  - Internet Safety
  - Create strong, private passwords

What Is Identity Theft?

- Someone steals your personal information
- Someone uses your personal information without your permission
- Can damage your finances, credit history and reputation

High Tech Methods: Phishing Emails

- Scammers use addresses that appear legitimate to collect your information and use it to commit fraud
- Logos and links can appear to be authentic
- Legitimate companies never ask for personal information via email or text

High Tech Methods: Spyware

- Malware and Spyware are installed on your device without your consent. They can be used to steal personal information, send spam, or commit fraud.

- Scam artists try to trick people into clicking on links that will download malware and spyware to their computers.

- Your computer may be infected with malware if it slows, crashes or displays repeated error messages. Other signs are many pop-ups, new toolbars or icons, or laptop battery that drains more quickly than it should.

High Tech Methods: Data Retrieval

- Something as simple as posting a resume online can be valuable to identity thieves.
- Identity thieves can assemble pieces of the overall picture from different sources: your Social Security number from one source, your date of birth from another, your home address from a third.
- Posting or emailing any such personally identifying information puts you at risk.

Minimizing Risk: Device Safety

- Use anti-virus software, anti-spyware software, and a firewall and keep them updated
- Create strong passwords
- Keep your computer's operating system, browser, and security up to date
- Lock your laptop when you step away
- Encrypt data while browsing online
- Don't use public wireless networks to send sensitive information

Minimizing Risk: Device Disposal

- Even if files appear to be deleted, the underlying data remains on hard drive.
- To remove data permanently, use a utility wipe program – these programs are inexpensive or can be found online for free.
- Use manufacturer or service provider's information to determine how to remove memory in a mobile device.
- Hard drives and mobile devices can also be professionally destroyed.

Minimizing Risk: Internet Safety

- Only provide personal or financial information if you typed in the web address yourself and see a URL that begins with https or see the lock icon.
- Be cautious about opening attachments or downloading files from emails, regardless of who sent them.
- Don’t email personal or financial information unless it is encrypted.
- Don’t overshare on social networking sites.

Minimizing Risk: Strong Passwords

- Always use strong passwords
- Password strength is determined by two things:
  - The length of the password, how large a set of characters and symbols it is drawn from, and whether it was created randomly or in a more predictable way
  - How the password is stored and used

Minimizing Risk: Strong Passwords

- The longer the password the better
- Use upper and lower case letters, along with numbers and symbols
- Avoid using the same password twice
- Don’t use information that may be associated with your name
- Try using the initial letter of words in a sentence

Minimizing Risk: Strong Passwords

- If you must write passwords down, keep them locked in a safe place.
- Use an online password storage site such as Dashlane, SecureSafe, or PasswordBox.
- Change passwords often.

Summary

- Identity protection is treating your personal information like your other valuables.
  - You lock up your house, you may have home security and monitoring in order to keep thieves out.
- Treat your personal information online in the same manner.
  - Lock your information with strong passwords.
  - Don’t share too much personal information online
  - Shred both sensitive documents and old computer hard drives, memory sticks, removable disks, etc.
- In the next presentation, we will cover how to monitor for identity theft and how to respond if your identity has been stolen.

Additional Resources

- www.monumentgroupwealth.com
- Visit our website for additional identity theft resources
- New resources will be added over time

Contact

We welcome your questions. Please contact us at:

The Monument Group Companies
801 Main Street, Concord MA 01742

Byron E. Woodman, Jr.
bwoodman@woodmaneaton.com

Lee C. McGowan, CFP®
lmcgowan@monumentgroupwealth.com

978-369-0960