The Financial Navigator – February Newsletter

Anthem Blue Cross Blue Shield's corporate computer system was recently hacked into and approximately 8o million customers' personal information was stolen. Additional data breaches at big-name companies such as JPMorgan Chase, Home Depot, and Target raises questions about the effectiveness of corporate America's information security. Below are a couple of articles that discuss how you may protect yourself, in the articles you will find some useful tips and brief reviews of some of the identity and computer protection services currently available. There are also links to the more detailed reviews of the various services.

You may know someone who has the same questions and concerns about identity theft and protecting one's personal data. If you think it will help, feel free to forward this email and let me know if you have questions about a specific situation.

Sincerely,

Bill Simpson, CFP®, MBA
Azimuth Financial Planning, LLC
(603) 373-8793
bsimpson@azimuthplanning.com
www.azimuthplanning.com

Malware Protection

We're always being told to protect our computers from viruses, but how?

Do you really need antivirus software on your home computers?

Yes. The Internet is increasingly awash with creative malware that can severely damage your computer, destroy your files, and embed themselves quietly in your operating system; sending information that can be used by identity theft thieves, or allows hackers to turn your computer into a spam machine.

Antivirus software companies monitor the Web in real time. They are constantly identifying new strains of malware and providing updates to their software that will look for the "symptoms" of every known virus, isolate it and allow you to remove it before it has a chance to damage your files, send compromising information or invite your friends and neighbors to purchase online porn.

Top10AntiVirusSoftware.com has just released its 2015 list of the most effective programs for preventing worms, Trojan horses, viruses or malware from installing themselves on your computer. The top-rated industry leader was McAffee Software, which can be purchased for $24.99 a year. Other top-rated programs include Kaspersky

($29.99), BullGuard ($23.96), BitDefender ($19.95), Norton Antivirus ($59.99), AVG ($31.99) and ESET ($19.99). (You can buy any of the programs at a discount at www.top10antivirussoftware.com/)

Understand that like all things in the software world, the best program in 2015 may not be the top-rated the following year. And most importantly, recognize that you need to constantly respond to the free upgrades to your software, because some of the most creative programmers in the world are constantly plotting against you and your security.

Source:

http://www.top10antivirussoftware.com/.

Protecting Yourself From Identity Theft

We're hearing a lot more about identity theft these days—from hackers stealing credit card numbers from big banks and retail stores to individuals opening up credit card or bank accounts in your name, which they can use to write bad checks or make expensive purchases. Criminal identity thieves may also take out a loan in your name for a car or even a house, and some have managed to receive Social Security benefits or tax refunds that rightfully belong to others.

In some cases, when arrested for some other crime, hackers have helpfully provided a victim's name to the arresting officers, showing the police a falsified driver's license with that person's number and their picture. They post bail and skip town. When their victim doesn't show up for a court date he was never informed of, he could be arrested.

How do you protect yourself? Some of the best ways to safety are free and relatively easy.

According to the National Crime Prevention Council, the biggest threats are coming from places that might surprise you. A study by Javelin Strategy and Research found that most identity thefts were taking place offline, where someone managed to steal your credit cards, or found social security information or credit card information in a dumpster, or filed bogus change of address forms to divert a victim's mail to their address, where they can gather personal and financial data at their leisure.

Even more surprising, 43% of all identity thefts were committed by someone the victim knows.

An organization called IdentityTheft.net estimates that over 10 million people are victimized by identity theft each year, although that number may be boosted by the aforementioned mass hacking incidents. The Council and an organization called

IdentityTheft.net say that you do a reasonable job of protecting yourself by taking a few common sense steps that make it much harder for someone to make purchases in your name or withdraw funds from your accounts.

- First, never give out your Social Security number, and don't carry your social security card, birth certificate or passport around with you.
- Copy your credit cards and your driver's license, and put the data in a safe place, to ensure you have the numbers if you need to call the companies.
- When you use a credit card to buy something in a retail store, take the extra copy of the receipt with you and shred it.
- Create complicated passwords for your online bank and investment accounts, and don't write them down on hard copy paper. Try not to use the same password for every website you access. (Can't remember 50 complicated passwords? A free program called LastPass lets you save all your user names and passwords in an encrypted format, so you only have to remember a single strong pass phrase. You can also store security questions and answers.)
- Don't let anyone look over your shoulder when you're using an ATM machine.
- Be skeptical of websites that offer prizes or giveaways.
- Tell your children never to give out their address, telephone number, password, school name or any other personal information.
- Make sure you have a virus and spyware protection program on your computer, and keep it updated.
- Check your account balances regularly to make sure no unexplained transactions have occurred.

These simple precautions will keep you safe from many of the criminal efforts to hack into your life. If you feel like you need additional protection, there are a variety of protection services on the marketplace, which basically all do the same thing: they regularly monitor your credit scores, looking for changes and odd debts that might be a clue that someone has stolen your identity, and check public record databases to see if your personal information is compromised. Some will prevent preapproved credit card offers from being sent to your mailbox, patrol the black market internet where thieves buy and sell credit card numbers, and the fancier services will provide lost wallet protection, identity theft insurance and keystroke encryption software.

Which are the best? A research organization called NextAdvisor has recently evaluated and ranked eight of these services, with costs ranging from $20 a month down to $7 a month. The top rated was IdentityGuard (premium service price: $19.99 a month) which offers the most compete protection, including the aforementioned fancier services. But seven of the protection systems, including TrustedID, AARP (a white-labeled version of TrustedID), LifeLock Ultimate, PrivacyGuard, IDFreeze and

LegalShield all received good ratings; only Experian's ProtectMyID was negatively reviewed for being expensive and only monitoring one credit reporting service.

Do you really NEED these services? Possibly not. However, with the growing publicity around identity theft, these firms have become very aggressive in their marketing efforts. What they don't tell you is that you can do many of the things they do on your own. Every quarter, you can review one of your credit bureau reports for free, or—and this is easier—simply look at your statements and balances every day. The more sophisticated services are a fancy replacement for promptly notifying your bank when a credit card is lost or stolen, or when a strange charge shows up because Citibank or the Target department store was using weak security protocols.

In the near future, as more transactions take place using thumb prints or other biometric security data, we may look back on this period as the Wild West of data security, a strange unsettling time when people had to worry about their lives being hacked by strangers. Your goal is to arrive safely, unhacked, at that more secure period in our cultural evolution.

Sources:

http://www.ncpc.org/cms-upload/prevent/files/IDtheftrev.pdf.

http://www.ncpc.org/topics/fraud-and-identity-theft/tips-to-prevent-identity-theft.

http://www.identitytheft.net/.

http://www.cracked.com/article_19973_the-8-creepiest-cases-identity-theft-all-time.html.

http://www.nextadvisor.com/identity_theft_protection_services/index.php?a=2&kw=mididx2+identity%20theft%20prevention&mkwid=pK49zV76_pcri.