TRI-STAR TRUST BANK

November 2017

TIPS FROM YOUR

Financial Coach

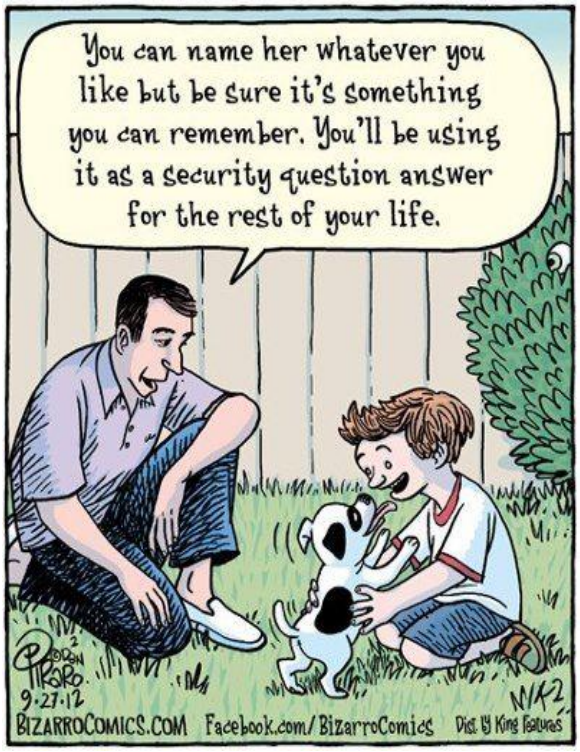
Sandy Worner, CPA, CFP®,
Vice President,
Director of Financial Planning

Bobbi Putman, CFP®
Financial Planner

Surge in Identity Theft

There were over 15 million identity theft incidence reported in 2016. This is an increase of 16%, nearly 2 million more victims than the previous year. These cyber thieves in 2016 netted approximately $16 billion dollars through unauthorized access mainly to credit cards and bank accounts. The surge is especially concerning because this was the first full year that retailers were required to use credit cards with chip technology in an effort to curb credit card cloning. Unfortunately, hackers are more resourceful than we would like, and they simply shifted actions away from card cloning onto online fraud where possession of the actual credit card is not necessary.

Regrettably, we are all guilty of certain practices and behaviors that make us soft targets to identity thieves. We carry our Social Security cards or birth certificates in our purse or wallet, we use public Wi-Fi to make a purchase or access our bank account, we save our login and password information on our devices, we make passwords predictable, and we do not shred credit card, bank account and other financial documents.



External challenges

Shielding your personal and financial information has become even more challenging when you combine the ingenuity of hackers to the serious data breaches that have recently occurred.

Within the past year, Yahoo has reported that more than **3 billion** user accounts were comprised in 2013. The information stolen includes names, email addresses and passwords.

More recently, Equifax, one of the three primary credit reporting agencies, disclosed that highly sensitive information of approximately **145 million** Americans was breached. This stolen data may include Social Security numbers, driver's license numbers, credit card information, and dates of birth.

simplify

www.tristartrust.com

Simplifying Life by Creating Wealth Solutions through Understanding.

1004 N. Michigan Ave.
Saginaw, MI 48602
(989) 921-0010

160 S. Main St., Ste 2
Frankenmuth, MI 48734
(989) 652-6600

3511 Coolidge Rd.,Ste 300
East Lansing, MI 48823
(517) 827-0045

200 E. Main St., Suite 100
Midland, MI 48640
(989) 492-7620

simplify

www.tristartrust.com

Steps to take now

For many consumers, taking proactive steps to safeguard personal information and minimize identity theft activity is an overwhelming and time-consuming endeavor. It becomes that much more difficult to prevent when industrious cyber thieves make a full-time job out of these types of criminal pursuits.

However, there are a variety of steps you can take to protect your identity from hackers. Some are fairly obvious (do not keep passwords written down in plain sight) while others a little more subtle (mail bills from the Post Office versus your home mailbox). Four key methods to protect yourself from cyber fraud are:

Monitor

Closely and regularly monitor all financial transactions. This includes credit card, bank account, and investment account activity.

Update

Make your passwords complex, update them frequently, and take advantage of 2-Factor Authentication when available.

Request

Up to 4 times per year and at least annually, request your free credit report at www.annualcreditreport.com. Review your report for mistakes and suspicious activity.

Enroll

Consider enrolling in a third-party credit monitoring service such as LifeLock, Identity Guard, ID Watchdog, or IdentityForce. These services typically cost between $10-$20 per month.

Signs that your identity has been stolen

Like in many life situations, timing is everything, and it is difficult to get out in front of a stolen identity if you do not know the theft occurred. Some signs that your personal information may have been compromised include:

1) You stop receiving bills or other expected mail.
2) You begin receiving bills for purchases you did not make.
3) You are denied when pursuing credit.
4) You notice unfamiliar bank and credit card transactions.
5) You receive tax notices from the IRS in the mail that you did not request.
6) Your E-filed tax return is rejected.
7) Your employer notifies you of an unemployment benefits request.
8) You receive a 2-Factor authentication alert you did not initiate.
9) Your credit score has changed recently, even if the change is an increase.

If you believe that your identity has been stolen, it is imperative that you act quickly. You will need to notify your creditors and banks to report unauthorized activity and close affected accounts. You will also need to file a report with the Federal Trade Commission and local law enforcement in addition to contacting all 3 credit bureaus to enact a “fraud or credit alert” and begin the process of repairing your credit.