

# Identity Theft: Avoidance Is Key

by Judy Hart, Informative & Protective Committee Chairman

## Who and Why?

Experts learn avoidance tactics with every new crime committed. Identity theft is one of the most loathsome crimes that occurs both in cyber space and with each new device that criminals can contrive to steal a person's identity. Criminals' prime motivations in stealing identities has to do with financial gain for themselves. And they work hard to drain your accounts. They want your tax returns. They want your credit card numbers and bank account numbers. They want to use those credit cards to purchase goods that you cannot fathom paying for. They want your inheritance and your hard-earned money.

Who are they? Criminal sounds too kind. They are pond scum and bottom dwellers. They are hackers for hire. They will sell your information to the highest bidder online. They are trans-national thieves. Hillary isn't the only person being hacked. Retirees and children are some of the easiest targets. Unfortunately, the children's stolen identities often take longer to detect because no one suspects their identities could be useful, but these scum buckets open new accounts in their names. They have excellent credit. When they register for a college loan, their credit is already ruined. No government loans are forthcoming. Retirees, on the other hand, have nice pockets of savings that can be drained before they are even aware.

## What Avoidance Tactics Can You Take?

Unfortunately, you may not be able to prevent every theft, but you can take steps to educate yourselves and be wary. We retirees need to be the watchman on the wall for each other and for our families and all innocents. Here are a few steps to help you begin claiming and securing your identity:

- Create longer, stronger passwords mixed with both capital and lower case letters, numbers, and symbols, none of which should connect with your name.
  - Never use anything that can be found in a dictionary.
  - A mnemonic method to help you remember your frequently used passwords includes using the first letter of a sentence such as "My Number 1 Aunt Thelma bakes delicious chocolate pies every four days." It becomes <mN1@TbDcpeFd!>.
  - Strengthen passwords for inboxes, banks, brokerages, and other financial institutions.
- Regularly change your passwords every few months. It's a nuisance, I know, but so is having your identify stolen!
- Do not use the same password for multiple accounts.
- For goodness sakes, do not save your passwords on your mobile devices.
  - Do not carry them with you in your purse or wallet.
  - Store them in a safe place.
- Regularly update your software devices. Those updates usually include security patches.
- If your device uses thumbprint identification, by all means use it. Also use a passcode for extra protection.
- Closely monitor your financial accounts, always looking for unfamiliar transactions.

- Credit cards are preferable to debit cards. When a thief uses your debit card numbers, your money is poof! gone! vanquished!
  - If you get your money back in a few weeks, you are blessed; the snotbag has probably already drained your entire account and any accounts linked to the debit card account.
  - If you notify your credit card company, your account is often credited with the absconded funds, your card is cancelled, and you have to wait for the new card a minimal number of days. Sometimes, you may have to pay a \$50 fee.
  - In reality, both cards have zero-liability protection.
  - Stick to one card so that you can easily spot felonious purchases. Of course, you have to regularly check your statements.
    - Be reminded that the pond scum have electronic devices to scan your card numbers right through your wallet or purse.
    - Why not purchase a secure RIFD blocking wallet to protect your credit cards, bank cards, cash and coins? They prevent electronic pick pocketing.
- There is a whole set of rules for using credit cards in foreign countries. My friend's company card was stolen twice. She learned that you can use credit cards at hotels in London, but pay with cash only in taxi cabs.
- Be wary of odd-looking ATMs. The bottom dwellers use "card skimmer" devices to grab your information as you're grabbing cash.
  - If the card insert slot looks larger or deeper than normal, walk away.
  - The scoundrels also use cameras, so never use an ATM without covering your hand as you type in your PIN. The scoundrel may get the number from the back of the card, but he or she will not have the PIN needed to access your account.
  - Use the hotel safe for your passport, bank cards, and IDs if you do not need to be carrying them.
- Never shop on public Wi-Fi; never check your bank balance on public Wi-Fi; never do anything on public Wi-Fi that requires you to give personal financial information.
  - Save your shopping for your safe home, where the thieving mongrels may not break in and steal. There you possess a password-protected network.
- Never click on links in e-mails or texts. These links are often phishing schemes from the tricksters, hoping that you will trust and release your personal information.
  - Savvy identity thieves send e-mails that look like your bank or some other easily recognizable business organization. The link may take you to an innocent looking site, but "he-who-should-not-be-named" is simply seeking your login credentials.
  - Watch for red flags like typos, pitiful grammar and spelling, threatening language, and demands for money.
  - Call the company or organization directly and confirm the inquiry.
- Photocopy all your cards and IDs and keep them in a secure place.

These "avoidance tactics" skim the surface of what you need to do to keep your identity secure. If you want to know more, attend the Informative and Protective Services session at the 64<sup>th</sup> annual TRTA Convention in Austin, Texas, March 27-29, 2017. Our Informative and Protective Services Committee will meet you and provide a whole array of information at the Hilton at 500 E. 4<sup>th</sup> Street.

## Sources Consulted

Chatzky, Jean. LifeLock Educational Advisor. <[www.lifelock.org](http://www.lifelock.org)>. 1 Jan. 2017.

Kelly Hultgren, LifeLock Educational Advisor. <[www.lifelock.org](http://www.lifelock.org)>. 1 Jan. 2017.

Schronk, Lisa. Personal Text Message. Jan. 2, 2017.

Warren, Cory, editor of *LifeLock Bloghome*. <[www.lifelock.org](http://www.lifelock.org)>. 1 Jan. 2017.

PS: In technical report writing, writers always use the same word to designate clearly the idea being convey. Obviously, I broke this rule 100 times. If you are confused and not entertained, the words **thief** or **thieves** is equivalent to the following synonyms:

Criminals

Pond Scum

Bottom Dwellers

Hackers

Snot Bag

Scoundrels

Thieving Mongrels

Tricksters

He-Who-Should-Not-Be-Named