IT'S NOT JUST AN INTERNET PROBLEM

JULY 2, 2015

My name is Debbie Wood. Airstreamer 11 years. Full-timer for 8 years. I had a 33 year career as an IT professional. My husband and I have tremendous internet exposure through our website and online blog. I've been banking on-line for 23 years so this is a subject that has always interested me.

After reading an article in AARP Magazine about identity theft, I decided to do some research about how to better protect myself and my parents.

I was surprised to find that, contrary to popular belief, most problems do not seem to be due to internet usage and presence.

Thieves get our information from the most ordinary places: our trash and mailboxes.

Once identity thieves have a few key pieces of personal information, they have wonderful tools available to them on the internet to utilize the information and wreak havoc with our lives.

What is Identity Theft? It is a crime where a thief steals your personal information, such as your full name or social security number, to commit fraud. The identity thief can use your information to fraudulently apply for credit, file taxes for refunds, or get medical services.

These acts can damage your credit status, and cost you time and money to restore your good name.

You may not know that you are the victim of ID theft until you experience a financial consequence such as receiving mystery bills, call from collection agencies or being denied loans.

What, Me Worry?

The article I read in AARP Magazine entitled “She Stole My Life” told about a woman who had her identity stolen to the point that she had trouble proving that she was herself. It got me thinking about what I could do to be better protected. More importantly, it got me to thinking about how to improve my parents’ security.

Like the woman in the article, my parents are prime targets. They have no Internet access or presence. They use paper statements for everything. Their statements arrive to an unlocked mailbox. They pay all bills with paper checks. Although they shred financial statements, they throw credit card solicitations and the like in the recycle bin.

U S Dept of Justice Stats for 2014

Identity Theft / Fraud Statistics	Data
Average number of U.S. identity fraud victims annually	**12,157,400**
Percent of U.S. households that reported some type of identity fraud	**7.5 %**
Average financial loss per identity theft incident	**$5,130**
Total financial loss attributed to identity theft in 2014	**$26.35 B**

How big of a problem is Identity Theft?

Here are the US DOJ statistics from 2014.

And these are the known cases!

Identity theft is the fastest growing crime in America.

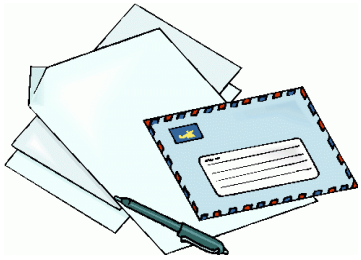
According to a survey conducted by the US Dept of Justice, it was concluded that more than 1 in 14 of all households in the United States had one member who had been a victim of identity theft in some manner or the other.

This means that the odds are highly against you.

Households aside, identity theft has an impact on governments and businesses as well. More than 64% of these frauds have occurred as a result of stolen or misplaced credit cards which were then used for purchases.

Recovering from ID Theft

- Estimated by the FTC at about 6 **months and 200 hours** of work
- Doing What?
  - phone calls
  - written correspondence and responses
  - keeping track of creditors
  - working with credit bureaus and law enforcement agencies
- Making certain you are not held responsible for the debt incurred by the theft



Until it happens to you, you might not fully understand the impact of having your identity stolen.

On the two occasions that I've had credit card numbers stolen, I spent many hours on the phone resolving the issues and then more time changing automatic payments to the new cards. Fortunately, the incidents didn't cost me any money.

When we had our cell phone number hijacked, we lost use of our cell phone for a week and spent hours getting the $900 of calls removed from our account. We first had to pay the bill and wait for the fraud investigation to resolve the issue and refund us the money. Significantly, we were out of the country when we learned of the fraud and resulting loss of service.

For other people the impact can be much greater. While the banks, credit card companies and businesses bear most of the cost, you have the job of convincing them that you are the real owner of the accounts and getting your damaged credit repaired. In many cases, your losses may include not only out-of-pocket financial losses, but additional costs associated with trying to restore your reputation and correcting erroneous information.

The emotional toil, sense of violation and investment of time required can be tremendous. I don't think that my parents would be up to the task.

Prevention, the Best Cure

- As consumers, you have little ability to stop or prevent identity theft.
- However, there are some positive steps to take which will decrease your risk.

This is why I began my research and decided to share with you what I've found. I know you read articles about this topic often but it's worth hearing one more time. Preventing identity theft starts with managing your personal information carefully, comprehensively and sensibly.

Unfortunately, we can't prevent data breaches or theft from financial institutions or retail companies. All we can do in these cases is to be vigilant about monitoring our accounts and checking our credit reports.

How do they do that?

- Easy for criminals to obtain personal info without breaking into your home:
  - Mailboxing
  - Dumpster diving
  - Shoulder surfing
  - Skimming
  - Carding

Mailboxing – talk about later

Dumpster Diving – trash & recycle

Shoulder surfing - in public places, for example, criminals may engage in "shoulder surfing" , i.e., watching you from a nearby location as you punch in your credit card number or a PIN.

Skimming is another way that payment card information is stolen while the card is being used in an otherwise legitimate transaction. The thief can get your card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victims' card numbers.

Carding is a term used for a process to verify the validity of stolen card data. The thief presents the card information on a website that has real-time transaction processing. If the card is processed successfully, the thief knows that the card is still good. The purchase is usually for a small monetary amount, both to avoid using the card's credit limit, and also to avoid attracting the card issuer's attention.

MAILBOXING

- Prime targets: bank statements, credit card offers, utility bills, credi union applications, check reorders, balance transfer checks
- In January, W-2 tax forms

- Sometimes thieves just take a photo of the mail and put it back

A locking mailbox or post office box is the best protection against mailboxing. If you have an unlocked box, then promptly remove mail from your mailbox after it has been delivered. If you're going to be away for a period of time, have your mail held at your local post office or ask someone you know and trust to collect your mail.

Deposit outgoing mail, especially something containing personal financial information or checks, in the Postal Service's collection boxes or take it to a local post office instead of leaving it in your home mailbox.

Lastly, keep new checks out of the mail. Have the bank hold new orders of checks for you to pick up to avoid the chance of the checks being stolen, altered and cashed by identity thieves.

Limit What You Carry

- Don't carry
  - Extra credit cards
  - Extra checks
  - Social Security or Social Insurance card
  - Birth certificate or passport
- Don't carry your Medicare or health insurance cards except to medical appointments

Only carry essential documents with you.

Don't carry extra credit cards or checks, your Social Security card, birth certificate or passport with you when you leave home.

If you are on Medicare, don't carry your Medicare card except to medical appointments since the Medicare number is your Social Security number.

Make a copy of your Medicare card and black out all but the last four digits on the copy. Carry the copy with you — unless you need to use your card at the doctor's office.

More on Medical Identity Theft later.

Know What's In Your Wallet

- A list of account numbers, expiration dates and telephone numbers.
- Quickly alert your creditors to prevent identity theft.
- Carry different credit cards and have backup cards.

Keep a complete and up to date list of account numbers, expiration dates and customer service numbers filed away.

If your wallet is stolen, being able to quickly alert your creditors is essential to prevent identity theft.

If you have a copier handy, take everything out of your wallet. Copy the fronts of all cards, including insurance cards. Then flip them over and copy the backs to get the phone numbers and security codes. This gives you a complete record and all the information necessary to report the stolen cards.

If you have multiple credit cards, you and your spouse or partner can carry different cards so that you still have a working card if one wallet is stolen. Or have backup cards that you can use if the one you are carrying is stolen or compromised. When traveling, it's not always possible to get replacement cards from the CC company overnight.

Be Stingy with Personal Info

- Unsolicited requests for personal information
- E-mails or calls asking you to verify information
- Give out your social security or social insurance number when absolutely necessary

Do not give out personal information over the phone, through the mail or over the Internet unless **you** initiated the contact.

Banks, credit card companies and IRS have all the information about you already and have no need to ask for it.

If you receive an e-mail that requests account or personal information there are several actions you should take:

- Don't click on any links in the e-mail. They can contain a virus that can harm your computer. Even if links in the e-mail say the name of the company, don't trust them. They may redirect to a fraudulent website.
- Don't reply to the e-mail itself. Instead forward the e-mail to the Federal Trade Commission.

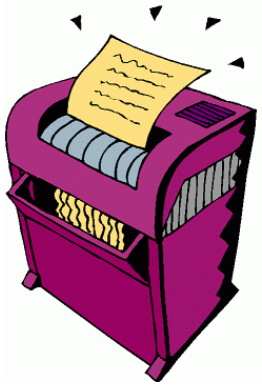
If you suspect that the e-mail is valid, contact the company using the phone numbers listed on your statements or cards.

Only give out your social when absolutely necessary. Your employer will probably need your Social to report your income to the IRS, while your bank or stockbroker may need it to report dividends or interest income. But, beyond that, when a business asks for your SSN giving it is up to you... and it's a decision you should not take lightly.

You should ask why your number is needed, how your number will be used, what law requires you to give your number and what the consequences are if you refuse.

Perhaps the worst that can happen if you say "no" to a merchant or service provider is that you'll have to take your business elsewhere.

Your Trash is Their Treasure



Shred your:

- receipts
- credit card offers
- bank statements
- returned checks
- insurance forms
- physician statements
- expired charge cards

and similar documents when you don't need them any longer.

Shred your receipts, credit card offers, bank statements, returned checks and any other sensitive information before throwing it away.

Thieves known as "dumpster divers" pick through garbage looking for this kind of information they can use to counterfeit or order new checks or credit cards. They may steal documents such as utility bills and bank statements to collect useful personal information. Alternatively, they may create fake documents. Using this information, they could open a credit card account or take out a loan in your name.

If you don't have a shredder handy, do what I do: cut out the addresses and account numbers from the document. Put the documents in recycle and the addresses and numbers in messy trash, (e.g., coffee grounds.)

Watch the Calendar!

- Follow your credit card and bank statement cycles closely.
- Contact your institution if a bank statement or credit card bill doesn't arrive on time.
- Better yet, check statements on-line and verify purchases.

Account takeover is when someone takes over another person's account, first by gathering personal information about the intended victim, and then contacting their card issuer while impersonating the genuine cardholder, and asking for mail to be redirected to a new address.

The criminal then reports the card lost and asks for a replacement card. They may then set up a new PIN and use the card until the rightful cardholder discovers the deception when he or she tries to use their own card. By this time the account has been drained.

Contact your institution if a bank statement or credit card bill doesn't arrive on time because that could be a sign someone has stolen account information and changed your mailing address in order to run up big bills in your name.

Even better, reduce what comes to your mailbox. If you use a computer, get your statements on-line and eliminate these from your mailbox. On-line accounts also allow you to monitor your activity on a weekly basis rather than waiting until your statement arrives.

I saw $5 charges for a charity I didn't recognize at the beginning of my billing cycle. I was able to cancel the credit card before the thief made any large purchases. This saved me and the company a lot of extra expense and work.

Monitor Credit Reports

- Equifax, Experian and TransUnion
- Get a free credit report every four months
- Check accuracy
- Look for anything suspicious

Establish accounts with Equifax, Experian and TransUnion and get your free credit reports once a year.

If you stagger your orders, you can get a free credit report every four months.

You should make sure the report is accurate, including monitoring it for unauthorized bank accounts, credit cards and addresses.

Also look for anything suspicious in the section of your credit report that lists who has received a copy of your credit history. Identity thieves sometimes will fraudulently obtain credit reports - and valuable details that can be used in a financial scam - by posing as a landlord, employer or someone else who has a legal right to the information.

Internet Security

- Create passwords or PIN numbers out of a random mix of letters and numbers
- My favorite vacations
  - gR@nDc&ny0N
  - p@r!5NspR1n9
- Electronic devices

Create passwords or PIN numbers out of a random mix of letters and numbers.

If random mixes are too hard to keep track of, think of favorite phrases and then alter them with similar characters to make them difficult to guess. For example, favorite vacation spots like Grand Canyon could become: gR@nDc&ny0N, or Paris in Spring becomes: p@r!5NspR1n9.

Set up passcodes on your smartphones, laptops and tablets to prevent unauthorized use if they are lost or stolen. Forty-four percent of us with smartphones have not set up a passcode on them!!!

Security Questions

- Thieves can find your mother's maiden name on the ancestry/census records websites, also your siblings' names.
- Use creative or silly names like nicknames that only a family member would know
- Keep track of what you use but not in a file on your computer unless in a secure password vault.

And what about those security questions that you are required to answer

Thieves can find your mother's maiden name on the ancestry/census records websites, also your siblings' names.

When you provide answers, use creative names like nicknames that only a family member would know.

Make up silly answers to the questions, favorite ice cream flavor: nilly vanilly, first automobile: heavy Chevy.

Just remember to keep track of what you use but not in a file on your computer unless in a secure password vault.

Be wary of strangers who strike up a conversation asking where you are from, where you went to school, or similar questions. They may say they are from the same town and ask if you know so-and-so. They will steer you to reveal information about your family in the spirit of making conversation. The FBI calls this "elicitation", a technique used to discreetly gather information. It is a conversation with a specific purpose: collect information that is not readily available and do so without raising suspicion that specific facts are being sought. The conversation can be in person, over the phone, or in writing.

Medical ID Theft

- Theft of your health insurance information
- Stolen by employees at medical facilities, or thieves who hack into medical databases or break into medical facilities
- Can cost you thousands of dollars and even threaten your life and health

Medical identity theft is the fastest growing segment of identity theft.

According to the World Privacy Forum, a stolen medical identity is worth 50 times a stolen social number. Given the value, there is clear motivation for thieves to go after patient data.

Medical thieves can heist your health-insurance number, Social number and other personal information. Often the information is stolen by employees at medical facilities, and resold on the black market. Thieves also may hack into medical databases or break into medical facilities.

The stolen identities are used to run up large hospital bills in your name, then the thieves disappear without paying. This can ruin your credit.

Fraudulent insurance claims can max out your health-policy limits. This can leave you with no coverage when you have a medical emergency, or need an expensive operation or other treatment.

Medical ID theft can threaten your health or even life. A thief's treatment history can end up on your medical records. This could include the wrong blood type, or medicine to which you're allergic. Your life thus could be on the line if you receive the wrong treatment based on the thief's medical history.

False claims against a health insurance policy can raise your health premiums — costing you yet more money.

Fight Back

Avoid medical ID theft:

- Examine your EOBs
- Monitor your insurance benefits
- Check your medical records
- Protect your health insurance information

Here are ways you avoid medical ID theft.

Review the explanation of benefits (EOB) form sent by your health insurer. Most people ignore the EOBs because it says “This is not a bill” in big bold type. If you see treatments you never received or providers that you don’t recognize, immediately notify your insurer and medical providers.

Ask your insurer for a listing of benefits paid out under your policy. Do this at least once a year.

If you suspect you’re a victim of medical ID fraud, get a copy of your records from your doctor, hospital, pharmacy or laboratory and make a written request for corrections.

It is very important to safeguard your insurance cards, explanation of benefits, and any health plan correspondence in the same way you would protect your credit cards.

Unless you check your medical records closely, you may discover you were defrauded only after the damage has been done.

What are the chances?

- 2014 was a bad year for the over 12M victims of identity theft
- No one expects or plans to be a victim
- Manage your personal information carefully
- Be vigilant about monitoring your accounts

No one expects or plans to be a victim. You may be merely inconvenienced by having to replace cards or change bank accounts

It could be more time consuming than expensive.

However, like the unfortunate woman in the AARP article that started me on this investigation, you could lose your identity, have your credit rating ruined and spend years trying to restore your accounts, credit, and peace of mind.

Unfortunately, it's not possible to entirely prevent identity theft and credit fraud.

It starts with managing your personal information carefully, comprehensively and sensibly.

We cannot prevent data breaches or theft from financial institutions or retail companies. All we can do is be vigilant about monitoring our accounts and checking our credit reports.

Following these precautions, and those from other sources you have, may help you manage your personal information more carefully and reduce the chances that you will become a victim of identity theft.