Global Information Assurance Certification Paper

Are You Secure? A Guide to Personal Security

Mitchell Choiniere

GSEC Practical Assignment
Version 1.4b
Option 1

Are You Secure? : A Guide to Personal Security

Abstract:

Within the last ten years, the advent of the "Information Age" has created a need for a sense of greater personal security. In the time it takes for someone to press "enter", access to our personal information such as credit history, medical records, and insurance information, to name a few, can be acquired with great ease. This leaves most of the population, uneducated and uninformed as to how to protect themselves, vulnerable to the real threat of identity violation.

People have always placed much importance on the security and protection of their monetary and tangible assets. We know how to acquire insurance for our belongings, how to provide physical protection for our belongings with alarm systems, and even how to defend our physical person if need be. However, the majority of the population, security professionals included, tend to overlook the most basic principles of these things we build a false sense of security around. This is because people do not understand how they are at risk. If they do not understand how they are at risk how can they possibly prevent the real threats against them.

Some forms of violation are obvious and leave the victims without a doubt that they have indeed been under attack: theft of personal belongings, physical attacks and harassment are examples of such violation. However, in many cases, people don't even know that they've been compromised. Not only do they not know they've been compromised, but they do not have the skills to respond appropriately to the situation.

I have broken down the concept of personal security into the following fields: Identity Theft, Home Computing Security, and Personal Physical Security. This paper seeks to serve as a resource to help the average person understand specifically how they are at risk. It will then explain how to prevent attacks within these three areas, and finally, to inform them how to respond in cases where violation has already occurred.

Identity Theft

What is Identity Theft?

Identity theft is the act of securing another person's vital personal information and using that information to impersonate the victim. The Identity thief can then use the stolen identity to commit various crimes such as fraud and theft.

To define what "personal information" is, it is important to know what it is *not*. Personal information does *not* include your job title, telephone number or address, or anything that might appear on your business card. Anything that can be found through publicly available information such as the telephone book is information anyone has a right to access.[1]

Personal information may be construed as factual or subjective information, recorded or not, about an identifiable individual. It can include: age, name, weight, height, medical facts, ethnic origin and religion, as well as ID numbers, income, opinions, evaluations, comments, social status, or disciplinary actions. It is also considered to be what is found in someone's employee files, credit records, loan records, existence of a dispute between a consumer and a merchant, and intentions (for example, to acquire goods or services, or change jobs).

With such a wealth of information readily available about most people, it is easy to begin to understand the devastating implications of identity theft. A victim of identify theft can experience anything from a minor misuse of their credit cards to one day discovering that their mortgage payments have been circumvented from their originally intended destinations and they are told to leave their homes. More extremely, serious criminal activity could be carried out in the name of the identity theft victim, perhaps making the victim culpable for crimes he/she did not commit.

With more education available about the reality of identity theft, people can begin to take simple but strident precautions that will reduce the threat of becoming victim to this crime whose incidence is growing exponentially. The general public presently has a very false sense of security about their personal information. Most people ask, "Why would anyone want my information?" without realizing exactly what can be done with it. With little effort, we can begin to reclaim a greater sense of security about our privacy, and continually create safer environments for our families and ourselves.

Identity Theft Statistics

In 2003 Synovate Research conducted an ID theft survey on behalf of The Federal Trade Commission (US).
http://www.ftc.gov/os/2003/09/synovatereport.pdf
I will present a few of their findings to shed some light on the staggering number of occurrences of this type of theft.

This research concludes that about 3.35 million people in America discovered that they had been victims of Identity theft in the last year alone.
It is estimated that about 10 million Americans actually fell victim to some form of identity theft in the last year. This indicates that only one third of victims even noticed.

Greg Surber noted the following in his paper "Loosing Yourself: Identity Theft in the Digital Age"(sic)

> *…in a world where anyone with $100 and a computer can learn enough about you to steal who you are, run up huge debt and leave you to clean up the mess.*[2]

Losses to financial institutions and businesses due to identity theft in 2002, is estimated at 48 billion dollars while total personal losses were about 5 billion dollars during the same time frame. The losses can be greatly reduced if the misuse is discovered promptly. The FTC research clearly indicates this:

> *When the misuse was discovered within 5 months of its onset, the value obtained by the thief was less than $5,000 in 82 percent of cases (including all forms of ID Theft). When victims took 6 months or more to discover that their information was being misused, the thief obtained $5,000 or more in 44 percent of cases.*[3]

It is estimated that only 25% of identity theft victims actually reported the incidents to proper criminal authorities, while only an estimated 22% reported these crimes to credit bureaus.
Age also seems to be an issue, as younger victims are more apt to report these crimes than older people. Only 17% of victims between the ages of 18 and 24 didn't report these violations while a staggering 66% of people over 65 years of age failed to report these incidents

According to the FTC survey results, 52 percent of all ID theft victims discovered that they were victims of identity theft by closely monitoring their accounts. Another 26 percent reported that credit card companies or banks alerted them to suspicious account activity. Another 8 percent reported that they first learned when they applied for credit and were turned down while another 9% were certain that they had been compromised resulting from a wallet/purse being lost or stolen. Finally another 2% fell victim to waylaid mail.

The majority of victims did not identify or know who their thieves were but in the instances where they did it is broken down in the following percentages:

Family Member	9.6%
Roommate	2.1%
Workplace acquaintance	1.6%
Neighbor	1.4%
Other relation	4.8%

In 1998 he United States created an act respecting Identity theft and privacy. This act, the Identity Theft and Assumption Deterrence Act of 1998,. According to IdentityTheft.org the act:

> *…makes identity theft a Federal crime with penalties up to 15 years imprisonment and a maximum fine of $250,000. It establishes that the person whose identity was stolen is a true victim. Previously, only the credit grantors who suffered monetary losses were considered victims.*[4]

http://www.identitytheft.org/title18.htm

Risks , Threats and Prevention

The following sites offer useful information on how to protect oneself from and act upon incidences of identity theft. The quiz below offers valuable insight into ways people innocently leave themselves vulnerable.

-ID theft IQ quiz :

http://www.privacyrights.org/itrc-quiz1.htm

-Canadian Security Quiz:

http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp

Credit

It is considered good practice to check your credit rating twice a year. This way, you can see if there is any suspicious activity with your credit cards. The health of your credit rating is important to your financial security. Fraudulent use of your cards could destroy a rating you've worked hard to build. You can obtain your credit record by contacting one of the major credit bureaus. If making a credit card application or responding to inquiries from a credit company, it is good practice to send your responses via registered letter.(See pages 13/14 for addresses and phone numbers for Canadian and American Credit Bureaus)

Document Disposal

Disposal of paper documents should be done through shredding, burning, or disintegration. All documents that contain sensitive information, such as credit card statements, bank statements, income tax statements and any similar documents, should be properly disposed of by the aforementioned ways. True, this may seem a little extreme, but rifling through the trash, can and does prove to be quite lucrative for individuals who know how to use the acquired information.Small personal shredders can be purchased at most office supply stores for about $50, a small price to pay for peace of mind.

Disposal of electronic documents containing sensitive information should be done by overwriting documents before deleting. For example, if you had written a document containing your personal information to an employer and eventually sought to delete it , you would copy and paste non-sensical, random characters over the original file, save it, then delete it.

Mail

Mail can often be waylaid and you will have no idea. Be aware of when your bank statements and credit card bills are due. Missing one may indicate that something is wrong, as your mail may have been diverted or stolen.
If you have an outdoor mailbox, it should be strong and locked. Mail slots are another secure solution to protecting your personal information. Sensitive information should never be placed in a cubbyhole in a workplace. You may want to advise your employer about the dangers if need be.

In Canada you can contact Canada Post to find out if any mail that is intended for you has been diverted.
http://www.canadapost.ca

In the United States you can contact US Postal Services.
http://www.usps.com

Loss or Theft

If your wallet or purse is lost you must respond immediately. The following are a few examples of types of identification that may be lost and how to react.

Passports:

In Canada contact the Passport office http://www.ppt.gc.ca/menu_e.asp

Passport Office
Department of Foreign Affairs and International Trade
Ottawa, ON K1A 0G3
Canada

In the US: http://travel.state.gov/report_ppt.html

US Department of State
Passport Services
Consular Lost/Stolen Passport Section
1111 19th Street, NW, Suite 500
Washington, DC 20036 or call (202) 955-0430

Credit Cards:

If you have lost a credit card report it immediately! All major credit card companies have 24 hour 800 numbers to report lost or stolen cards. Once a card is reported lost you are no longer liable for unauthorized purchases beyond %50 per card. Be sure to shred any unused pre-authorized card offers along with statements and receipts.[4]

Visa Card - 1-800-847-2911
MasterCard - 1-800-MC-ASSIST

Social Security/Insurance Card:

You should NEVER carry your Social Security or Social Insurance (Canada) card on your person at any time. Memorize your number and leave your card at home. If this card gets into the wrong hands it is an easy pass for someone to steal your identity. If you do happen to lose your card contact one of the following departments:

Canada: http://www.hrdc-drhc.gc.ca/sin-nas/010_e.shtml

United States: http://www.ssa.gov/

Driver's License:

Contact your local DMV.

Basic Home Computer Security

Passwords

Passwords should NOT be simple or predictable. Refrain from using passwords like abc123 or "qwerty". Passwords should be at least eight characters in length and should be composed of upper and lower case letters, numbers and other characters such as ampersand or dollar sign.

Family member names or birthdates should not be used, especially your mother's maiden name, because it is one of the details to acquire birth certificates. It is also requested by financial institutions. Avoid forward or reverse dictionary names as hackers often use password decoding software that reference many kinds of dictionaries.

Anti-virus

All home computers must have anti-virus software installed to protect from viruses and backdoor Trojans. These can compromise your data as well as take control of your computer and again your identity. Be sure to update your virus definitions as often as possible as your anti-virus software is only as good as the most recent set of virus definitions, Many anti-virus programs include "live-update" features which automatically download the most recent virus definitions from the vendor's website.

Some examples of popular anti-virus software are:
Norton/Symantec
Mcafee
Sophos
PC Cillin
F-Secure

Firewalls

Firewall software is also recommended for any home computer that is connecting to the internet. This type of software will help protect you against hackers trying to exploit vulnerabilities and gain control of your computer.

Education

The best way to stay secure is to be aware of how your home PC can be compromised and take appropriate measures to ensure that it stays secure. You should make simple policy when it comes to computer use and all those in your household that use the PC must be made aware and follow acceptable use policies that you have set.

Web Browsers
Assure that web browsers are tuned for children and that anti pop-up software is used or a web browser that prohibits pop ups such as Mozilla FireBird.
Most web browsers have access control settings that can filter material based on content, such as language and nudity. These can be set to levels appropriate to the intended age group. Most common is Microsoft's Internet Explorer. In this program you can find these settings by going to Tools: Internet Options: Content: Content Advisor Settings.

Access Control
User profiles should be set up for all users. There should be one administrator account and the others set up as users without permissions to install software or make system changes. The administrator account should never be connected to the internet, it should only be used to make system changes when needed.

E-Commerce
Credit cards should only be used when website is secure. An easy way to tell is by checking the URL if it begins with https:// as opposed to just http:// . The s in https indicates that it is a secure server. This of course does not mean that you are totally safe. You should exercise extreme caution when using your credit card online and when unsure of the legitimacy of the online vendor don't use your card online.

Operating System Updates
Care should be taken that operating systems are updated by downloading and installing the latest security patches available. These patches will ensure that the most recent vulnerabilities in your operating system are no longer a threat. In Windows you can do this by going to the "Tools" menu of Internet Explorer and clicking "Windows Update".

Personal Physical/Home Security
In this section we will talk about personal security in the home. We will discuss access, fire prevention, and basic home security. Most people understand basic precautionary measures, yet are these enough in the face of a potential emergency?

Fire Prevention
Fire prevention is not necessarily seen as a security issue, but proper fire safety procedures will help safeguard against the loss of your most important assets, your life, your family, your home and all documents and assets inside. Most homes have a simple smoke detector and maybe one fire extinguisher. Yet it is important to determine that these devises are adequate, as well as practice regular maintenance. There are two types of smoke detectors: ionization and

photoelectric. They're both effective smoke sensors and must pass the same tests to become certified. Photoelectric detectors respond more quickly to smoldering fires, while ionization detectors respond more quickly to flaming fires. A smoke alarm uses one or both methods and sometimes a heat a detector to warn of fire. These devices may be powered by batteries or 120 volt house wiring. These devices should be cleaned and the battery changed at least once a year.

There are several types of home fire extinguishers. Knowing how to properly select and use a fire extinguisher is an important skill. Since different materials require different extinguishing agents, there are three types of fire extinguishers: Class A, B, and C. Class A is used for wood, paper, cloth, etc. Class B extinguishers are used for flammable liquid fires, such as grease fires. Class C extinguishers are used for electrical fires as their agents to not conduct electricity. Some extinguishers are a "BC" class, as they can be used on both flammable liquid and electrical fires. A Class A extinguisher should NEVER be used in the case of an electrical fire.[5] By being aware of the classes of extinguishers, you can determine that a Class B or C or combination of both would appropriate for your kitchen and furnace room near the electrical panel. A Class A would serve as a general extinguisher. Of course just having these is not enough. Everyone in the household old enough to understand how to operate them should be trained in their use. Follow manufacturer's instructions for maintenance and must be carried out by qualified persons.

Smoke detection and fire extinguishers are one way to protect your family, however a vital yet often overlooked step is the home fire escape plan. Create one and practice it with your family.

Security Alarms

It is a good idea to have a home security alarm system. There are many different services available at varying prices. Many providers should be consulted in order to ascertain your needs.

Miscellaneous Tips on Home Security

A small fireproof safe should be acquired for all important documents such deeds, passports, birth certificates, etc. All other important documents should be in a locked filing cabinet.

All windows should have a latch and all exterior doors should have a keyed deadbolts. A sliding door security bar should be installed on all sliding glass doors. It's also good practice to change your locks if you lose a key. The codes on digital door locks should be changed every six months. Motion activated lights are a good idea for outside your home.

All hazardous materials should be stored in a locked metal cabinet.

Child Safety and Security

Our children are the most vulnerable members of our society and the victims of many crimes. It is of utmost importance to teach children basic precautions in protecting themselves. There are now self defense courses designed specifically for children. Some establishments such as MacDonald's restaurants have days on which children can have identification cards made their finger prints taken. This can make the tracking of missing children easier for the police.
The website http://www.klaaskids.org/ is a valuable resource on the protection of children and also has very detailed information on the subject of child fingerprinting. http://www.klaaskids.org/printathon.htm

The following child safety tips come from http://nsi.org/Tips/child.htm

- Never go into your house or apartment if the door is ajar or if a window is broken.
- To lock the door when he or she comes home and to keep all doors and the windows locked.
- To check in with you by telephone or report to a neighbor at a regularly scheduled time.
- To avoid walking or playing alone on the way home from school.
- His or her full name, address and telephone number—including area code.
- Your full name, the exact name of the place where you work and its telephone number.
- How to use both push-button and dial phones to reach the operator or report an emergency.
- How to carry a key so it's secure but out of sight.
- How to answer the telephone without letting callers know that he or she is home alone.
- How to get out of the home safely and quickly in case of fire.[6]

In Conclusion

This paper has covered very basic principles of protection against assaults on personal security. The information is by no means exhaustive. The links are provided in hope that the reader will be motivated to learn further ways to prevent attacks upon their personal security and information.

To the lay reader, some of this information may seem overwhelming and even frightening. The thought of potential devastation is certainly not a pleasant one. However, with increasing awareness of the problems of personal security threats, the public will gradually become more vigilant in their efforts to practice basic security measures. Most of the suggestions are not difficult or particularly time consuming to execute, and go a long way in protecting the individual.

QUICK PERSONAL SECURITY CHECKLIST

1) Shred credit card statements or receipts.
2) Shred utility bills and cancelled cheques.
3) Shred these all sensitive documents before disposal.
4) Never carry SSN/SIN card in wallet.
5) Request a copy of personal credit report at least once yearly.
6) Passwords are secure and changed several times yearly.
7) Overwrite electronic documents before deleting.
8) Anti-virus software installed.
9) Firewall software installed.
10) Ad-aware and anti-spyware software installed.
11) Home network behind router.
12) Locked mailbox at home.
13) Locked mailbox and desk at work
14) Locked workstation when unattended at work.
15) Online credit card transactions on secure channels only.
16) Never share passwords with anyone, ever.
17) Establish and enforce home computer usage policy.
18) Have list of Credit Card company phone numbers.
19) Proper fire extinguishers are installed, functional and maintained.

20) Fire escape plan drawn up and practiced by whole family.

CREDIT BUREAU INFORMATION

Canadian Credit Bureau Contacts

Equifax

http://www.equifax.com/EFX_Canada/

Phone number:
1-800-465-7166
8:00 AM until 5:00 PM EST, Monday to Friday

Address
Equifax Canada Inc.
Consumer Relations Department
Box 190 Jean Talon Station
Montreal, Quebec
H1S 2Z2

Trans Union of Canada

http://www.tuc.ca/

(For all provinces except Quebec)
Telephone
1-800-663-9980 or (905) 525-0262
7:00 AM until 8:00 PM EST

(For Quebec residents)
Telephone number
1-877-713-3393 or
(415)335-0374

Address
Trans Union of Canada Inc.
Consumer Relations Center
PO Box 338, LCD 1

Mailing Address
Trans Union (Echo Group)
1600 Henry Bourassa Boul
Ouest Suite 200

Hamilton, Ontario
L8L 7W2

Montreal,PQ
H3M 3E2

US Credit Bureau Contacts

Equifax

http://www.equifax.com

Credit reports, call: 800-685-1111
P.O. Box 740241, Atlanta, GA 30374-0241

To report fraud, call: 800-525-6285 and write:
P.O. Box 740241, Atlanta, GA 30374-0241
.

Experian

http://www.experian.com

Credit reports call: 888-EXPERIAN (397-3742)
P.O. Box 2002, Allen TX 75013

To report fraud, call: 888-EXPERIAN (397-3742)
P.O. Box 9530, Allen TX 75013
1-800-972-0322

Trans Union

http://www.transunion.com

To order your report, call: 800-888-4213
P.O. Box 1000, Chester, PA 19022

To report fraud, call: 800-680-7289
Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634
1-877-553-7803

REFERENCES

1) Privacy Commissioner of Canada. “Frequently Asked Questions - Privacy Commissioner of Canada” (2003)
URL:http://www.privcom.gc.ca/faq/faq_01_e.asp#004 (Oct.8 2003)

2) Surber,Greg. “Loosing Yourself:Identity Theft in the Digital Age” 2002
URL:http://www.sans.org/rr/papers/14/686.pdf (Oct.1, 2003)

3) Synovate. “FTC-Identity Theft Survey Report” September 2003.
URL:http://www.ftc.gov/os/2003/09/synovatereport.pdf (Oct.8 2003)

4) Credit Creep. “Lost Credit Cards - Credit Card Fraud - Where to report lost credit cards”2001 URL:http://www.creditcreep.com/fraud.html (Oct.4 2003

5) Yonkers Fire Department. “Home FireExtinguishers”
URL:http://www.yfd.org/Exting.htm (Oct. 21 2003)

6) National Parent-Teacher Association. Child safety Checklist
URL:http://nsi.org/Tips/child.htm (Oct 22, 2003)

Other References

7) http://www.consumer.gov/idtheft/

8) http://www.privacyrights.org

9) http://www.secretservice.gov/faq.shtml#credit_card_fraud

10) http://www.idtheftcenter.org/

11) http://www.privcom.gc.ca/legislation/02_07_01_e.asp

12) http://www.privacyrights.org/itrc-quiz1.htm

13) http://www.hrdc-drhc.gc.ca/sin-nas/010_e.shtml

14) http://www.klaaskids.org/

15) http://www.ssa.gov/

16) http://travel.state.gov/report_ppt.html

17) http://www.usps.com

18) http://www.ppt.gc.ca/menu_e.asp

19) http://www.usps.com

20) http://www.usdoj.gov/criminal/fraud/text/idtheft.html

21) http://usps.com/postalinspectors/idtheft.htm

22) http://www.klaaskids.org/printathon.htm

Last Updated: May 22nd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event