

CYBER THIEVES AND IDENTITY THEFT

Introduction

Focus

This *News in Review* story explores the growing problem of identity theft. You will learn how cyber thieves operate, why it is so difficult to catch them, and what you can do to protect yourself.

Further Research

The Web site of the Office of the Privacy Commissioner of Canada at www.privcom.gc.ca/id/phishing_e.asp contains a great deal of information about identity theft, including updates about some of the recent scams that have occurred in Canada.

Just imagine. One day you receive a phone call asking you why you haven't made the scheduled payment on your new truck. You reply, "What new truck?" because you have not bought a truck. The caller describes the truck that you purchased the previous month, although you did no such thing. This is exactly what happened to 29-year-old Michelle Brown.

Brown immediately cancelled all her credit cards, issued fraud alerts, and notified her bank. But it was already too late. Brown's identity had been stolen, and authorities couldn't catch up to the thief. Over the next year and a half, Brown's identity was used to rent property, engage in drug trafficking, and purchase more than \$50 000 worth of merchandise. Eventually, the thief was arrested and jailed, but Brown estimates she has spent over 500 hours trying to clear her name and credit reputation.

Brown's case is not unusual. Identity theft—the criminal use of personal information to make fraudulent purchases, open accounts, or take out loans—is the fastest growing economic crime in Canada and throughout the

world. Although exact numbers are hard to determine, the RCMP estimates that \$2-billion was stolen through some form of identity theft in Canada in 2007. And that is just the tip of the iceberg, since only one in 10 thefts in Canada is reported.

In this *News in Review* story you will learn how criminals steal personal information. Often these thefts occur after a criminal has gathered someone's personal information online. This can occur when people disclose too much information on social networking sites like MySpace or Facebook, or when people click on a malicious Web link, or visit a questionable Web site. In other cases, criminals simply collect papers with important banking or personal information out of people's garbage or recycling bins.

In any event, once your identity is stolen, you stand to lose money and time and may have trouble restoring a clean credit history. However, there are a number of steps you can take to reduce the chances of becoming a victim yourself.

To Consider

You have likely grown up with the Internet. Do you consider yourself to be Internet savvy? Record the steps you take to protect your identity and personal information while online. Also record the steps you take to protect your computer from viruses and spyware. When you are finished, share and discuss your list with a partner. Add any new points to your own list. You may choose to take the Spam Q and A on the following page to assess your computer smarts.

Did you know . . .

On May 11, 2004, Canada's Task Force on Spam was established to oversee and co-ordinate the implementation of the Anti-Spam Action Plan for Canada. The final report was released in May 2005. One of the results of the task force was the development of an anti-spam icon that could be hosted on partners' Web sites and would contain a link to user tips. Check out the anti-spam logo at the Stop Spam Here Web site, www.stopspamhere.ca/spyware-e.html#stats. How effective do you think this logo is? Explain.

Spam Q and A

One of the ways your personal information can be stolen is after your computer is infiltrated by a cyber thief. Cyber thieves can attach spyware to your computer, get you to click on malicious Web links, or direct you to malicious Web sites. The following spam quiz includes a selection of questions from the Canadian organization "Stop Spam Here." Answers are below. Visit the Web site at www.stopspamhere.ca for a complete explanation of each of the answers.

1. You receive an e-mail from an organization asking that you "Verify your account information within 24 hours or your account will be frozen." This e-mail may request your password, login name, Social Insurance Number (SIN), credit card details, or other personal information. You know the organization and think you may have subscribed to one of their services. What do you do?
 - a) You reply to the e-mail asking them why they want this information.
 - b) You reply to the e-mail with the information asked for.
 - c) You delete the e-mail.
2. To reduce spam, you can:
 - a) Use one e-mail address for friends and family and instruct them not to supply that address to others. Create a second address for trusted businesses.
 - b) Create temporary "throw-away" e-mail addresses that you use for specific purposes such as newsgroup and newsletter subscriptions, message board postings, and other online services that require an e-mail address.
 - c) Do both a and b.
3. You have an easy-to-remember password and you use the same password everywhere, even for your bank account. You have heard that you should use different passwords for your accounts and change them regularly. What should you really do?
 - a) Continue using the same password.
 - b) Create passwords made up of mixed characters and numbers (such as 5gtha6bp), and change your account passwords once a month.
 - c) Create three passwords based on your favourite names and rotate those between your accounts every three months.
 - d) Keep a list of 20 short, easy-to-remember word passwords in a file on your computer. Then you can look them up and change your account passwords every six months.
4. To help minimize the amount of spam you receive, turn off the preview pane—a window that allows you to preview the contents of an e-mail message—in your e-mail software.
 - a) True
 - b) False
 - c) Good e-mail software protection allows you to use the preview pane without potentially harming your computer system.
5. After checking your e-mail, your computer starts behaving unusually. You:
 - a) Install or update anti-virus and firewall software and run a full-system scan.
 - b) Configure your firewall so that it prompts you every time a program on your computer attempts to connect to the Internet.
 - c) Check for any unauthorized use of your personal accounts, including banking, credit card, e-commerce, e-mail, and any other password-protected account.
 - d) a, b and c

Answers 1. c, 2. c, 3. b, 4. a, 5. d

CYBER THIEVES AND IDENTITY THEFT

Video Review

Further Research

PhoneBusters is a national anti-fraud call centre jointly operated by the Ontario Provincial Police and the Royal Canadian Mounted Police. PhoneBusters collects information on telemarketing fraud, advanced fee fraud letters, and identity theft complaints. You can learn more about fraud and identity theft by checking out their Web site at www.phonebusters.com.

Further Research

The Web site of the popular television show *America's Most Wanted* has information related to cyber-bullying, identity theft, and Internet predators. Check it out at www.amw.com/safety/?cat=11.

Respond to the following questions as you view the video.

1. What is the general profile of an identity thief?

2. How do identity thieves use chat rooms?

3. How do police and other people trying to stop cyber crime use the same chat rooms?

4. How large is the problem of identity theft?

5. How much does it cost thieves to buy the following?

a) A credit card _____

b) Your full profile _____

6. Why don't the authorities shut down the chat rooms where stolen personal information is bought and sold?

7. Describe what happened to the following two people.

a) James Perks

b) Cory

CYBER THIEVES AND IDENTITY THEFT

Identity Theft

Further Research

The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and e-mail spoofing. The organization provides a forum to discuss phishing issues, trials and evaluations of potential technology solutions, and access to a centralized repository of phishing attacks. See their Web site (www.antiphishing.org) for statistics and examples of phishing e-mails.

What Is It?

Identity theft involves stealing or misrepresenting the identity of another person or business. Once an identity has been stolen it can be used to withdraw money, open new bank accounts, apply for loans or credit cards, and purchase vehicles or property. In some cases, the thief may even use the stolen identity to engage in criminal activity such as drug dealing.

How Does It Happen?

There are a lot of ways that thieves can steal an identity. One way is to get possession of a person's debit card (ATM card) and their personal identification number (PIN). The information on debit cards is much easier to steal than the information on credit cards. So experts advise using cash or credit cards whenever possible.

Another way thieves steal information is by "phishing." Phishing involves sending an e-mail to a user falsely claiming to be a legitimate business or organization in an attempt to scam the user into disclosing private information. Usually, there is an HTML link within

the e-mail that you are asked to click on. Once you click on the link you are taken to a fraudulent Web site and asked to provide personal information.

One of the more recent scams to steal personal information is called "vishing" or voice phishing. Vishing involves the criminal use of technology called Voice over Internet Protocol (VoIP). The way it works is that a person receives a recorded telephone message claiming to be from an established organization. The message asks the person to call the company back at a fraudulent phone number and then requests that the person punch in their personal information on their telephone pad. The thieves convert the key tones back into numerical format and steal the information.

You might be surprised to learn that one of the most common ways for thieves to steal the information they need for identity theft is simply to search through garbage. Many people recycle bank statements, credit information, or pre-printed forms that contain personal information. When those documents are disposed of without being shredded they can fall into the hands of identity thieves.

For Discussion

Have you or any of your friends or family members had any experience with "phishing" or "vishing?" If so, explain the situation and how you handled it.

CYBER THIEVES AND IDENTITY THEFT

Teenagers and Identity Theft

Further Research

Internet 101 began in 2004 as a collaborative project between police forces in the National Capital Region–Ottawa. Police officers became concerned after seeing media reports of a local Web site where teenagers posted explicit photos of themselves and personal information. The result was the first Internet 101 workshop and the formation of www.internet101.ca. Check out the Web site, which contains real stories of children and teens who have had negative experiences because of contacts they made over the Internet. The site also contains tips on how to protect yourself from ending up in a similar situation.

You might be surprised to learn that teenagers are particularly vulnerable to identity theft. One of the reasons is because of the large amount of time they spend on the Internet. Another reason is that once teenagers go off to college or university they receive an excessive amount of mail containing credit-card applications and promotional materials.

MySpace and Facebook

Many teenagers spend time each day or week on MySpace or Facebook. These social networking sites have become the primary way that many teens communicate with each other. Instead of phoning one another, for example, they may log on to communicate with their friends.

Social networking sites can make users vulnerable to identity theft because they allow each user to “link” to other people’s pages by creating a list of “friends.” “Friends” can then use message boards to send and receive messages and “new friend requests.” Many MySpace and Facebook users share personal information, including photos, with each other.

Criminals who are involved in “spear phishing” act like a member of a social networking site and gain access to personal data posted on users’ pages. The phisher then uses the personal information to strike up a relationship with a particular user or users. Once a relationship is established, the thief often leaves a message in a target’s inbox, asking questions that will result in more personal information being released. Or the message may contain a link to a fraudulent site, or contain malicious code that prompts users for information. It does not take long for the thief to gather

enough information to steal the person’s identity.

Unfortunately, most teenagers who have been victims of identity theft do not find out they’ve been victimized until they try to apply for credit in their own name when they become an adult. It is at that time that they may discover that someone has been making charges in their name for years, and they could be tens of thousands of dollars in debt. According to the Federal Trade Commission, in the United States in the year 2006 nearly 11 000 reports were filed for people under the age of 18 who had discovered unpaid bills, credit cards, and loan applications in their name.

“Smileys” and Screen Savers

Another reason teenagers are vulnerable to cyber crime is because they tend to visit sites that are more likely to aggressively infiltrate a visitor’s computer. Adult sites and sites offering screen savers, “Smileys,” wallpaper bundles and cursor enhancements often attach spyware or extra software to the visitor’s computer. Many computer users are unaware that spyware has infiltrated their computer and is recording information about every site the user visits. Spyware and other malicious software can collect a host of personal information about the user.

Credit Card Offers

Very shortly after teenagers begin college or university they begin to receive offers for credit cards in the mail. In some studies, up to 50 per cent of college students in the U.S. received credit-card applications on a daily or weekly basis. Students often throw away these applications as junk mail.

However, the promotions are often pre-approved credit-card applications that contain complete personal information. Identity thieves simply have to scoop up the discarded credit-card applications from a garbage or recycling bin to steal someone's identity.

Promotional Offers

In addition to credit-card applications, teenagers and young adults receive many promotional offers, either through the mail, advertisements on campus, or online. In many cases, the promotional offers are disguised as "experiments"

where students are asked to participate in surveys in exchange for coupons, free merchandise, or the promise of a small amount of cash. Journalist Neil Weicher wrote about one scam where a company offered students free pizza in exchange for their personal information (*Business Week Online*, May 8, 2007). When he investigated, he watched students spend over 15 minutes filling in a double-sided form that included personal information about themselves and their parents in exchange for their "free" two-dollar slice of pizza.

Follow-up

In small groups, discuss your own personal experiences with the information and situations discussed in this feature. You may want to consider some of the following questions:

- How carefully do you screen your "friends" on social networking sites?
- Have you ever shared personal information on such sites?
- Do you know anyone who has ever had problems because of contacts they've made on social networking sites? How were the problems resolved?
- Have you ever received a credit-card offer or a special promotional offer containing or requesting your personal information? If so, what did you do with the offer?

CYBER THIEVES AND IDENTITY THEFT

Case Studies

Tip

If you do online banking, it is easy to check your accounts on a daily basis and catch any unusual activity almost instantly.

Activity: Exploring Personal Stories

Get into a small group with three or four other students. With your group members, discuss whether or not any of you know someone who has been a victim of identity theft. At the conclusion of your discussion, select one of the cases and use it to complete a "5Ws Chart." If your group does not know anyone who has been a victim of identity theft, then use one of the case studies that follow to complete the chart.

To create a "5Ws Chart" create a two-column chart in your notebook. Title your chart "The 5Ws of Identity Theft." In the left-hand column, record the words *who*, *what*, *where*, *when*, and *why*. In the right-hand column, fill in the details that answer each question. Select one member of your group to share your information with the class.

Case Study 1: Carol's story

Carol lives outside Toronto and had never given much thought to the issue of identity theft. One day she received a phone call from her bank asking her if she had recently made a series of withdrawals with her ATM card. At first, she was suspicious about whether the person calling was actually from her bank. The caller gave Carol more information about who she was and a number to phone to confirm the information. The caller was from Carol's bank.

Carol was asked to come to the bank to discuss unusual activity on her bank card. Once at the bank, Carol found out that three withdrawals for \$500 each had been made within a short period of time the night before. Another attempt to withdraw \$500 more had been made early that morning. Carol confirmed that she had not made the withdrawals, and the bank took her ATM card.

After further investigation, the bank was able to determine that Carol had been the victim of identity theft. Somehow, someone had gotten Carol's bank account number and her personal identification number (PIN). She was eventually issued a new ATM card, and the bank provided advice on how to select a PIN that is difficult for thieves to decode.

Carol has had no further problems with identity theft and feels she was very fortunate. The bank restored the money to her account and she didn't have to pay any penalties or fees related to the theft. She also says that bank employees were very helpful and never accusatory.

On a personal level, she says that she is much less trusting. She never uses independent ATMs and only uses her debit card for the most usual things like shopping at her local grocery store. She has also reduced the withdrawal and credit amounts on all of her cards. Until the theft from her account, she was unaware that her daily withdrawal allowance was \$1 500. She also tries to keep all her receipts and to double-check bank statements.

Case Study 2: Jon's Story

Like Carol, Jon hadn't given much thought to identity theft until he received a strange phone call from The Home Depot. The caller wanted to know if Jon had a Home Depot card, if he knew anyone with a Home Depot card, whether he'd ever applied for a card, or whether he'd ever purchased anything from The Home Depot in Hamilton. Jon replied "no" to all of the questions.

Jon was surprised to discover that

credit cards had been opened in his name at Staples, Office Depot, and The Home Depot and that \$20 000 had been charged to the accounts over a period of three days. Jon reiterated that he had never opened the accounts and had not charged anything at the stores in question.

The Home Depot then conducted further research. They located the specific transaction times and dates when purchases were made at The Home Depot in Hamilton. They then searched the in-store surveillance tapes from those particular times to get a visual of the person who made the purchases. Jon was asked to sign an affidavit and provide the photo on his driver's license. The Home Depot was then able to confirm that the person who made the purchases was not Jon.

While The Home Depot was conducting their investigation, Jon called the RCMP's fraud division to see what he could do about the theft. They provided him with information and recommended that he contact Equifax (www.equifax.ca) and Trans Union Canada (www.transunion.ca), Canada's national credit reporting agencies, for copies of his credit reports. Credit

reports reveal all credit activity that occurs in a person's name. Jon requested and received credit reports from both companies.

Although Jon will never know how he became a victim of identity theft, The Home Depot was able to tell him that the person who applied for the credit cards had his social insurance number and his current home address. Jon does not carry his social insurance number with him and believes he had only provided the number once in the preceding six months. And that was to his bank. Interestingly enough, Jon's name was spelled incorrectly on the credit card applications, but this did not stop the applications from being processed.

Jon did not have to pay for the debt that was acquired in his name. He has not had any further problems, but has been unable to apply for "instant" credit since the theft. Instant credit refers to credit cards you apply for in-store to receive a discount off a purchase you are making. For example, if you are purchasing something worth \$200, you may be asked if you want to apply for a store credit card to receive an instant 10 per cent off the purchase price.

CYBER THIEVES AND IDENTITY THEFT

Protecting Your Identity

Further Research

How tough would it be to decode your password? Microsoft has a tool that tests password strength at www.microsoft.com/protect/yourself/password/checker.mspx.

Although it is true that there is probably nothing you can do to absolutely guarantee you won't be a victim of identity theft, there are a number of steps you can take to protect your identity. The following points have been compiled from experts working in the field of identity theft and from people who have been victims of identity theft.

What You Can Do

1. Buy a paper shredder.

One study, conducted in England in 2002, examined the garbage of over 400 households. More than 85 per cent of household garbage bins contained information that could be used by identity thieves. That included credit card statements, papers with a full credit card or debit card number, and intact bank-account numbers. According to Jay Foley, director of consumer and victim services with the Identity Theft Resource Center in San Diego, raiding garbage pails and recycling boxes is one of the most common ways that thieves gather information to conduct identity theft.

2. Do not share your personal information.

Do not give out any personal information over the phone or online. Keep all records containing personal information in a safe place, and shred them when you no longer need them.

3. Protect your social insurance number (SIN).

Your SIN is probably the most valuable piece of information needed for identity theft. Do not provide your social insurance number (SIN) to anyone. In some cases, doctors or dentists ask for the number, but there is no reason for them to have it. As well, don't provide

your SIN on job applications or ever write it on a cheque. If you are hired for a job, then you will be required by the company to provide the number. But do not provide it on the application before you are hired. And finally, do not carry your SIN card in your wallet.

4. Be careful with your personal identification number (PIN).

Think carefully about your PIN. The longer your PIN is the better. That is, use the maximum number of characters allowed. As well, use a mix of numbers and letters in your PIN. According to experts, a good PIN is long, is not a dictionary word, or anything that someone who knows a bit about you could guess. And although it may seem obvious, never write your PIN on your ATM card or credit cards. Surprisingly, in the majority of cases of ATM and credit card fraud, victims had written their passwords on their cards.

5. Use a firewall and virus-protection software.

Help to reduce the chances your computer will be hacked by installing virus-protection software and updating it regularly. If a hacker gets into your computer, not only can your computer be destroyed, but your personal information can be stolen and sold to criminals.

If you have a high-speed Internet hook-up, your computer is connected to the Internet at all times. A firewall program helps to stop hackers from accessing your computer.

6. Don't get caught in a phishing scam.

Phishing scams use junk e-mail, posing as legitimate e-mail, to trick people into disclosing personal information like

CYBER THIEVES AND IDENTITY THEFT

Activity: Keeping Kids Safe(r)

Most teenagers have a good sense of how to keep themselves safe while online. Many younger children, however, may not have the maturity to understand the dangers that exist online. With your experience and knowledge you can help to prevent identity theft and the exploitation of children.

Your Task

Design an educational campaign about Internet safety aimed at younger children. You will have to decide two things:

1. What information you want to include in your campaign
2. How you want to reach your audience

The Information

The following information about Internet safety and identity theft as it relates to children was taken from the article "The Complete Layman's Guide to Cyber Safety" (*Money*, December, 2006). It will provide a starting point for your product, but you will have to conduct additional research on this topic. Check out some of the Web sites referred to in the margin of the pages throughout this *News in Review* story.

- Teach kids to value privacy. Their name, phone number, address, personal and family information is not to be shared online.
- Teach kids the Internet is public. Anything they say or do online becomes part of the public domain and can be sent from person-to-person for years to come.
- Strangers are strangers. Just because you have met someone online does not mean that he or she is a friend. Don't ever arrange to meet anyone you first met online.
- Be very careful with photos. Posting photos increases the chance that someone will try to contact you. Photos can be edited and doctored and used in ways that a person never originally intended.
- Limit computer time. Parents should control computer time just the way they control time in front of the television.
- No secrets allowed. Children should expect to show parents any Web pages, blogs, or profiles on networking sites. Young children need help to make good decisions.

Your Product

Decide the best way to deliver your information. You will want your final product to be engaging and appealing to children. You may want to produce a poster series, a number of pamphlets, a video or DVD, a song, a play, or a presentation. Discuss your choice with your teacher.

Extension

If your class produces some good material, consider sharing it with younger students in your school or another school in your community.