A publication of the Finance Department, The Salvation Army Canada & Bermuda Territory.

Money & Mission

Editorial

We are quickly becoming a cashless society. For many people, debit and credit cards and other forms of electronic payment are replacing the use of cash. The finance department is actively promoting the use of electronic transaction processing to eliminate paper cheques. Electronic transaction processing is not only less costly and more efficient, but also reduces the possibility of fraud.

Of course, clever fraudsters will always find a weakness in any system that they can exploit. This issue contains a special feature article by our senior editor, Patricia

The Salvation Army
Giving Hope Today

Volume IV, Issue 16
May 21, 2014

Comments, Suggestions?

Do you have comments on any of the topics raised in this issue, or suggestions for a future issue? Write to us at: Money&Mission@can.salvationarmy.org.

Subscription:

To subscribe, send us an e-mail with the subject line "Subscribe".

To unsubscribe, send us an e-mail with the subject line "Unsubscribe". We'll be sorry to see you go, but we'll promptly take you off our mailing list.
Send your request to: Money&Mission@can.salvationarmy.org.

Editorial Team

Managing Editor:
R. Paul Goodyear
Senior Editor:
Patricia Dunbar
Design Editor & Production Manager:
Angela Robertson
French Translator:
The Salvation Army Translation Department

Finance Department Offices:

2 Overlea Blvd
Toronto, ON M4H 1P4
(416) 425.2111 ext. 2237

Dunbar, which highlights the ways in which fraudsters can access your credit card and what you can do to protect yourself.

Special Feature

Credit Card Theft

We are hearing of an increasing number of cases of fraud on the Army's corporate credit cards. Often, cardholders ask us how their cards could be stolen when they are still sitting in their wallets.

As long as they can steal the card number at some point in the payments process, fraudsters do not need to be in physical possession of your card to use it. When you use your credit card to make a purchase, the card number is sent through a payment network. If a hacker can gain access to any part of this payment network they can steal your card information. The payment network begins at the point where you enter your credit card information. This can be a terminal in a store or restaurant, an online shopping site, or on a paper form like a magazine subscription or a utility bill.

Credit card theft is a growing industry with

116 - 276 Midpark Way SE
Calgary AB T2X 1J6
(403) 201.9223

884 - 167 Lombard Ave
Winnipeg MB R3B 0T6
(204) 975.0735

101 - 85 Thorburn Rd
St. John's NL A1B 3M2
(709) 579.3919

Please click here for back issues of *Money & Mission* or to see our index by topic.

For more information about the Finance Department please see visit http://salvationist.ca/departments/finance/ .

Salvationist.ca
The voice of The Salvation Army
THE SALVATION ARMY Giving Hope Today

fraudsters developing ever more creative ways of stealing card information. In this article, we will describe some of the most common types of fraud and what you can do to protect yourself.

How are credit card numbers stolen?

Shopping online Using your credit card online can be dangerous if you are using a website that isn’t secure. Unsecured sites make it easy for thieves to break into the server and access customers’ credit card numbers.

Data breaches According to the Privacy Rights Clearinghouse, over 600 million records have been stolen since 2005. If a company or website that has your credit card information has a data breach, then it is likely that your credit card number can fall into the wrong hands.

Neal O'Farrell, founder of the Identity Theft Council said that data breaches are the most common way for a hacker to steal your credit card number. While some data breaches make national news, others are actually never discovered by the company or the consumers. "In data breaches, it has nothing to do with what the credit card user did, but that another organization or business with access to his/her credit card number did not protect it properly," O'Farrell says.

Phishing This is an attack that uses cleverly designed emails to convince you to give your credit card information directly to the hacker. The email is a fraud, but it looks like it is from someone you actually do business with, such as your bank, a store or an auction site.

Framing/Poisoning This is another common form of on-line attack. Hackers replace the real pages on a web site with pages that send you to their site where they steal your credit card information as you enter it. A poisoned web site can download and install a program to capture what you type on your keyboard: passwords, credit card numbers and bank accounts. This is known as keystroke logging.

Card skimmers your card number can also be stolen by an illegal device that copies your credit card number, which thieves then either use for their own purposes or sell to others. Card skimmers can be implanted in readers, such as at gas stations and ATMs, or an employee can run your card through a skimmer when you hand it over for payment.

Credit card machines at retail stores Similar to having your card information stolen by skimmers, it is possible for thieves to pull a fast one on employees at stores and switch out store-owned credit card terminals for a card reader of their own. They can then collect credit card data from store customers.

How can you prevent credit card theft?

Unfortunately, there is no fail-safe way to prevent your card number from being stolen, particularly if it involves skimming or a data breach. However, there are things you can do to reduce your chances of being a victim.

***Check your credit card usage online between billing cycles*.** Make a habit of logging onto your account once a week to verify that you have made all of your charges. Thieves will often charge very small items to test the card. Contact US Bank immediately if you notice any suspicious activity. If you are not already set up for access to AOL, US Bank's online system, contact thq_treasury@can.salvationarmy.org.

***Check for card skimmers*.** While it can be hard to spot a compromised card reader, get in the habit of checking for anything that looks unusual before inserting you card. Familiarize yourself with photos of compromised card readers to help you be on the alert.

Install anti-virus on your computer and keep it up-to-date with the latest virus signatures. Do a full virus scan of your computer at least once a week. If your computer has firewall software, turn it on too.

Never follow links or open attachments in emails unless you are absolutely sure who sent this email to you.

Never follow links or take any actions on things that happen on your system randomly such as pop-ups that say you have 30 viruses on your system and need to clean them right away! Just close the message window by clicking the red X in the upper right corner. If you cannot exit the program, the best thing to do is restart your computer.

Never respond to phishing emails, no matter how genuine they look. Financial institutions will NEVER ask you for account and other proprietary information by email. *When shopping on-line, make sure you use secure websites to make payments*. Look for sites with verified secured connections and updated SSL certificates (i.e. the lock icon on the payment page). Also, do not send credit card information or personal data via email if you can avoid it.

***Consider installing** keystroke encryption **technology**,* to protect yourself from keystroke logging.

Go paperless. Avoid sending your full credit card information through the mail where it can easily be intercepted by thieves

Do not allow unsolicited service to your credit card terminal, if you have one at your location. Unless you have requested a service call, refuse service if someone claiming to be a technician wants to "update" or "inspect" your terminal. It is very likely to be a fraudster trying to install a card reader on your terminal. If in doubt, contact Moneris (the provider of the Army's terminals) at 1-866-319-7450. Similarly, do not leave your terminals unattended. Fraudsters may attempt to distract sales staff so that they can attach a reader to your terminal. Inspect your terminals regularly for signs of tampering (e.g. cracks, missing or loose screws) and contact Moneris immediately with any suspicions.

If you've already been a victim of credit card fraud, you may have a virus or other harmful program running on your computer that is stealing your credit card, bank and other personal information. Be safe. Have your system checked out by a PC professional as soon as possible.