Using Technology?
Positively!

A SERIES OF FACT SHEETS ON EVERYDAY TECHNOLOGIES AND OLDER CANADIANS

HOW ARE EVERYDAY TECHNOLOGIES KEPT SAFE?

Fact sheet #6 looks at safety and security issues of some everyday technologies.

Along with new technologies, new ways of committing crime have also turned up. From electronic crime to fraudulent charities, technology has provided new tools for criminals. Technology is also part of the solution, as companies, banks, organizations, police services and governments share information and take measures to combat such crime. Banks and **internet service providers** (**ISPs**) have developed pass codes and **encryption** security systems to protect their customers. Although some crimes and fraud schemes are targeted directly at older adults, there are a few simple guidelines you can follow that will greatly lessen your chances of being ‘stung’. Of course, the first and best defence is to be cautious when conducting any transaction that involves your money or your privacy.

Automated Banking Machine (ABM) Safety Tips

- Be aware of those around you, both in a line-up and at the machine.
- Be discreet when entering in your **Personal Identification Number** (**PIN**) at a banking machine, or at a store retail machine.
- Shield the keypad with your body or hand.
- Do not write your PIN down or share it. If you must write it down, keep it separate from your card.
- Be sure to remove your card and your cash from the ABM.
- If you need assistance, do not ask the person behind you. Go into the bank and speak to an employee.

Prepared by the Nova Scotia Centre on Aging, Mount Saint Vincent University for the Federal/Provincial/Territorial Ministers Responsible for Seniors. September 2001

- Keep your ABM transaction slips and debit receipts to check against your monthly bank statement or passbook.

Internet Safety Tips

- Delete any e-mail you receive from unknown companies or unknown senders (e-mails also called **spam**). Or click on 'Block sender' which will delete incoming messages from e-mail addresses on your 'Block Sender List'.
- If you are shopping online, deal with reputable companies which clearly provide contact information and security assurances.
- Ask an unknown company for references and check them out before purchasing online.
- Look for a symbol on the top or bottom of your computer screen that looks like an unbroken key or a closed padlock to show that you are in a secure environment when you enter credit card information.

- If you visit 'chat rooms' or online 'discussion groups', do not volunteer personal information such as your name, phone number or address.
- If you visit the internet regularly, look into having what is called '**firewall**' software installed to protect your computer against **hackers** or find out if your computer already has such security measures in place.
- Check for viruses e-mails sent with attachments by saving them to a disk first and then running your antivirus program.

Telemarketing Fraud

Although there are many legitimate telemarketing firms, every 48 hours another fraudulent company is identified. In 2000, more than 50 percent of Canadian victims were over 60 years of age and more than 60 percent of reported fraud victims were women. Legitimate telemarketing firms do not use pressure tactics or ask for cash only and will send out written material, giving ample time to make a decision.

PhoneBusters is a national call centre for reporting deceptive telemarketing. It is operated by the Ontario Provincial Police since 1993 and is accessible from across the country in both official languages. Besides educating the public,

PhoneBusters collects and disseminates victim evidence and statistics to law enforcement agencies. A new free video called **Stop Phone Fraud–IT'S A TRAP** is now available. Phone **1-888-495-8501** for your copy or to arrange a presentation for your organization.

SeniorBusters is a group of volunteers working with PhoneBusters to give information and telephone support to older adults who may have experienced telephone fraud. To report a fraud or get information you can reach **PhoneBusters** or **SeniorBusters** at **1-888-495-8501**. Or you can visit their web site at: **http://www.phonebusters.com**

Beware of...

- being told you've won a contest you have not entered.
- being told you have to pay a 'small fee' or shipping charge to claim a prize.
- promises of a valuable prize in return for a low-cost purchase.
- 1-900 numbers which carry automatic and substantial charges. Check out the number with the Better Business Bureau or PhoneBusters before calling.
- being asked for your credit card or SIN number for no valid reason.
- phone calls from a person claiming to be a bank inspector or police officer. Hang up and call your bank.

Consumer privacy has become a major concern for many Canadians with the increased use of debit cards, telephone and internet banking, point system award programs and other methods of information storage. Protect your personal information–social insurance numbers, health card numbers, account numbers, and marital status are all private information!

The best way to deal with fraud is to prevent it. Be aware. Be prepared. Be alert!

Sources:

Partners Against Consumer Telefraud. *Don't Fall for a Telephone Line!: Working to Reduce Telemarketing Fraud in Nova Scotia*. Brochure.

Canadian Consumer Handbook. Ottawa: Industry Canada, 1999. Cat. No. C2-422/1999E.

Lindsay, Colin. *A Portrait of Seniors in Canada*, 3rd ed. Ottawa: Statistics Canada, 1999. Cat. No. 89-519-XPE.

Statistics on Phone Fraud, Phonebusters web site, retrieved May 11, 2001 from http://www.phonebusters.com/Eng/Statistics/canada_stats7_2000.html.

Fact Sheets in the Series

1. Series Overview
2. Telecommunications: Phones and More
3. Looking After Your Money: Technology and Banking
4. Computers: Getting Online — Using the Internet
5. For the Good of Your Health: Technology and Health Care
6. *How Are Everyday Technologies Kept Safe?*
7. Older Adults Mean Business!

Techno Terms

ABM - an **Automated Banking Machine**, also known as an automated teller machine (ATM), can carry out ordinary bank transactions such as deposits, withdrawals, transfers, account updates and bill payments. An ABM allows you to conduct these transactions 24 hours a day at your convenience.

Computer Virus - a programming code that is transmitted to your computer from an infected e-mail attachment, downloaded from an infected web site or present on a diskette. Viruses can cause operating problems with your computer and are often designed to spread automatically to other computer users. You can protect your computer from a virus by purchasing virus detection software.

Encryption - conversion or scrambling of computer information. It is used to protect your information when you conduct a sensitive transmission, such as internet banking or online shopping with a credit card.

Firewall - a security feature installed on some but not all computers that protects your information by preventing access to it from other computers when you are connected to the internet. Many networks have built-in **firewalls** to ensure privacy. If you plan to use the internet regularly from your home, check into whether you already have this feature on your computer or must install firewall software.

Hacker - a term used by some to mean 'a clever programmer' and by others, to mean 'someone who tries to break into computer systems'.

Internet - a very large computer network through which individual computers are connected to internet service providers (ISP) so they can share information. The internet is open to anyone with access to a computer that is connected to an ISP.

Internet Service Provider (ISP) - a company that provides individuals and other companies access to the internet and other related services.

Online - the condition of being connected to a computer or a telecommunications system. The term is frequently used to describe someone who is currently connected to the internet.

PIN (Personal Identification Number) - a code, containing letters, numbers or both, that allows you to access your bank accounts using an ABM, the telephone or a computer.

Spam - an unsolicited e-mail flooding the internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it.