CREDIT UNIONS

Fraud Prevention Guide

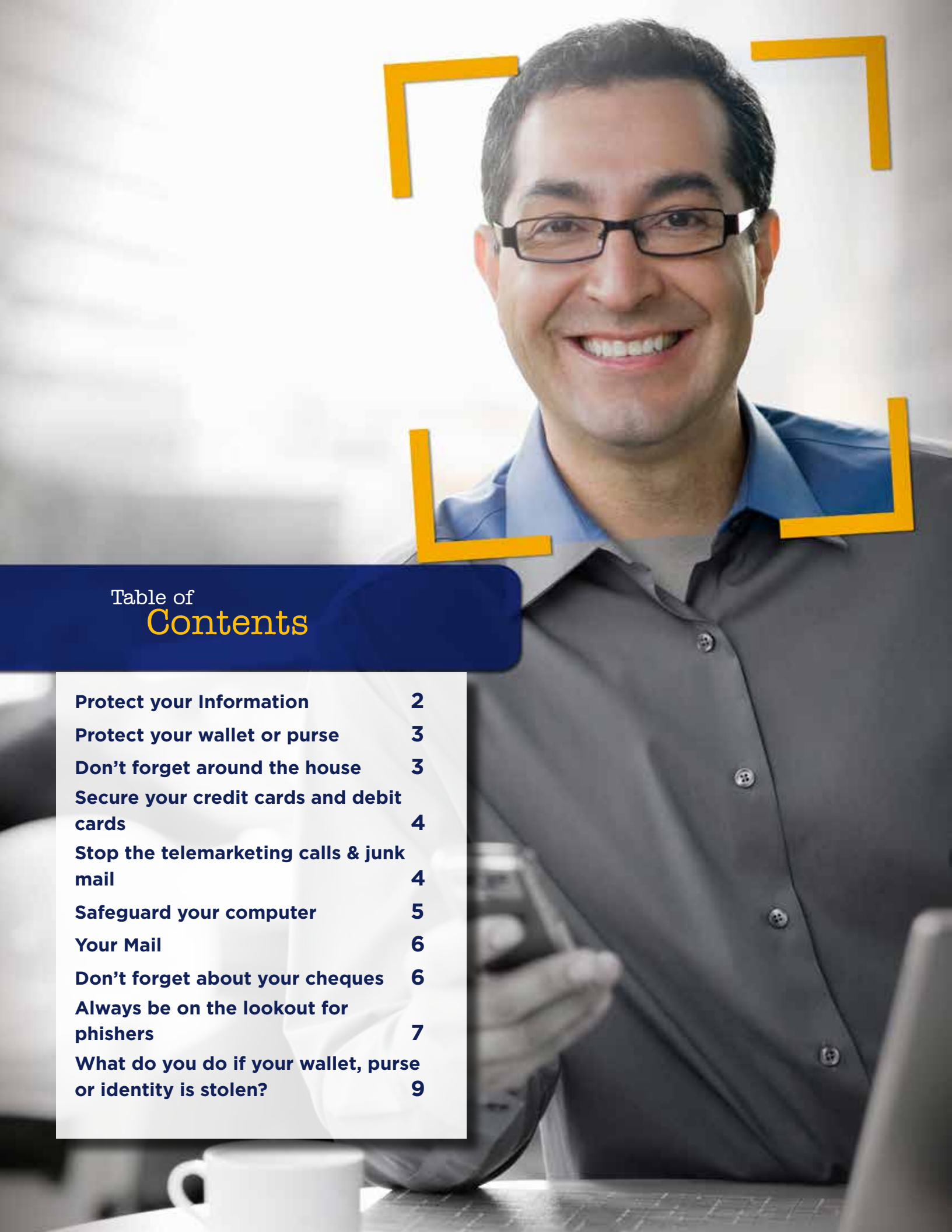


Table of Contents

Protect your Information

Our world has become smaller and more connected than ever before. While on one hand this has many advantages, on the other hand there are adverse side effects of this connectivity; information about us has become more important and more plentiful than ever. Treat your information like it was gold.

How safe are you from identity fraud?

- Order your credit report at least twice a year.
- Memorize your SIN number and passwords.
- Do not use personal information for passwords.
- Consider making your phone number unlisted.
- Monitor all your bank statements and bills monthly for any unknown charges. If you fail to get a statement, notify the company immediately.
- Do not give your information out over the phone. If the caller is not someone you normally do business with, get their name and call them back on a number that you know to be legitimate.
- Attempt to limit the number of people who have your SIN number. Canada Revenue Agency, other government agencies, your financial institutions and your employer have legitimate reasons for needing your SIN number; retail stores do not. Do not give out your SIN number as ID.

Protect your wallet or purse

It used to be that thieves stole our wallets or purses to get the cash inside. Now the real value is in all the information we carry. With your SIN number and driver's license, an identity thief has everything they need to virtually become you.

- Copy the front and back of all cards and identification in your wallet or purse and store in a safe place in your home. This ensures that in the event the contents go missing, you will have all the information you need to report the cards.
- Don't carry your SIN number, birth certificate, or passport in your wallet or purse unless you need them.
- Only carry cards and identification that you need or use on a regular basis. Is carrying fifteen credit cards truly necessary?
- Don't leave your purse unattended in a shopping cart to wander down the aisle to pick something up.
- Keep your wallet or purse in a safe place while at work. You just never know.

Don't forget around the house

Canadians produce a lot of garbage. Generally, we sort our recyclables, bag it up, and set it outside for pick up. Once it's out the door, we don't have to worry about it right? Well... all that trash lying around is a prime target for an identity thief because they know we often throw out credit card offers, bills, and receipts. Make sure you shred anything with any personal information on it with a cross-cut shredder before you throw it away.

- Don't leave personal information lying around at home, in your vehicle or at the office. Keep your birth certificate, passport and SIN# in a safe place, such as a safe deposit box at your credit union, when you're not actually using them.
- When you receive a renewal or replacement for a document or certificate that contains identity information (such as your driver's license or vehicle registration) make certain you destroy the old one.

Secure your Credit Cards and Debit Cards

Identity thieves love to shop — when they don't have to pay! With your credit card number or other access to your accounts, the identity thief can shop originally all on your coin.

- Cancel all credit cards that you do not use or have not used in the last six months.
- If you order a new card or one has expired, ensure you receive the new card in a timely manner.
- If not, call the company to see if they were sent or if there has been a change of address on your account. Some card companies routinely send out a mailer a few days after your card was mailed to you, however you will only receive it as long as they have your correct address.
- Do not throw credit/debit card receipts away in public trashcans or leave them at ABMs or Merchants. Shred them at home.
- When using your ABM or debit card, watch for "shoulder surfers" who may be trying to see your PIN number.
- Cut up expired and unused credit and debit cards. The card may have expired but the number may still be valid.
- MasterCard SecureCode™ is a free online service which makes shopping online more secure by enabling you to choose a private code to protect you against unauthorized card use when you shop online at participating merchants. Similar to entering a PIN at an ATM, you will enter your password for validation before your online purchase is completed. This ensures your card is only being used by you.
- Visit www.securecode.com/cumastercard to enroll.
- Your Credit Union MasterCard account is monitored 24 hours per day, 7 days per week, and if unusual or suspicious activity is detected, you will receive a call to make sure you are the one using the card.

Stop the telemarketing calls & junk mail

Besides calling and bothering you at suppertime, telemarketers keep a wealth of information about you, and they sometimes sell it. Reduce the number of people marketing to you... the better off you'll be.

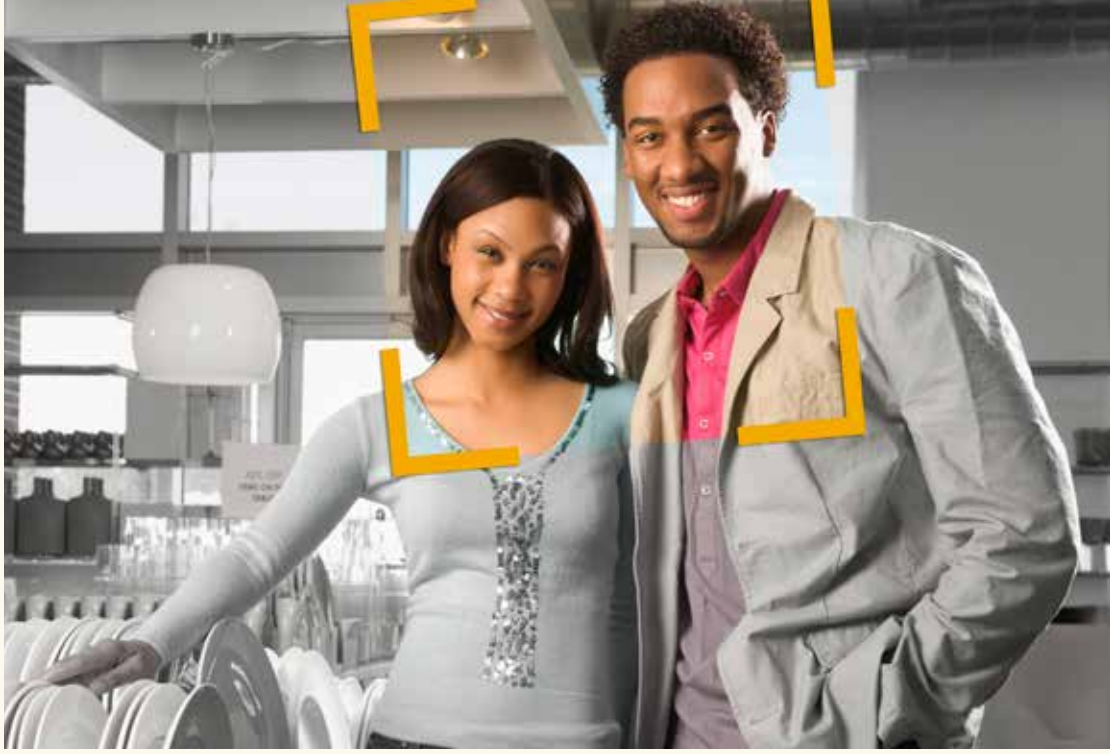
- When an unwelcome telemarketer calls, ask to be placed on their "Do Not Call" list. They must oblige you.
- Write companies that send you junk mail and ask that your name and address be removed from their mailing list.
- If there is a postage paid envelope in the junk mail, send it back with a note asking that your name be deleted from their list.
- Some of your junk mail will have an 800 number on it. Call it to have your name deleted.

Safeguard your computer

What does your computer know about you? Probably lots, and it will divulge your life to a hacker. Hackers can slip a virus into our computer that tells them everything we do on our computer, including purchasing online. Take precautions to lessen the chance of this happening to you.

- Never leave your computer unattended.
- Update your virus protection regularly or set-up for automatic updates. It is recommended that you install new security patches and an anti-spyware program.
- Use a firewall.
- Do not download files sent to you by strangers or click hyperlinks from people you do not know.
- Do not open emails from unknown sources or respond to spam.
- Do not click hyperlinks that come in an email message. Instead type in the known URL of the particular company.
- Look for the https at the start of the address or the locked padlock at the bottom of the page to know you are on a secure server when shopping on the internet or inputting personal information.
- When banking or shopping online, ensure you sign out of the website and clear your internet file/caches.
- Don't send personal or confidential information over email. Email messages are not secure.
- Use strong passwords. These are combinations of numbers and letters that are not personal in nature or sequential. It is suggested you consider the following:
    - o Change your personal access code (PAC) regularly
    - o Ensure no one observes you typing in your PAC
    - o Do not select a part of your PIN (your ATM "key") or another password
    - o Keep your PAC confidential and don't share it with anyone
    - o Disable automatic password-save features in the browsers and software you use to access the internet.
- Do not store passwords on your computer or within MS Outlook's notes.
- Prior to submitting ANY personal information to an internet website, review the privacy policy for an understanding of how your information may be used.
- Do not disclose your true birth date to online surveys. If it is a required field on the survey, choose a birthday you would much rather have, also do not disclose your SIN# or other personal banking information.
- Before you dispose of a computer, delete all personal information. Use a "wipe" program to overwrite the entire hard drive.
- We would discourage using public or a friend's computer to access your personal or banking information. Extra caution should be used if you choose to do so.

Your mail



Mailboxes are a treasure trove of fabulous information. In rural areas we even put up a bright red flag telling everybody who drives by that there are important articles inside. Thieves aren't looking to pick up your holiday greeting from Auntie Jocelyn; they are however looking for your bills with your name, account numbers and Cheques inside.

- Get a PO Box or locked mailbox, if possible.
- Do not use your mailbox for outgoing mail. Drop mail off at a post office.
- Never put the flag up on your mailbox to alert others that there is mail inside.
- Pay attention to your mail; reduce incoming mail by using direct deposit, email bill payment, e-statements, etc. Where possible, turn off the option to receive the paper copy.
- Have Canada Post hold your mail when on vacation or arrange for a neighbor to pick it up.
- Advise Canada Post, service suppliers, etc. of address changes.

Don't forget about your cheques

Be careful of the information you provide on your Cheques. You never know who is going to see your cheque once it is written and they may record information from it.

- Consider putting only your first initial and full last name on your Cheques.
- Have Cheques delivered to your credit union, not your home.
- Destroy all Cheques immediately after you close a Chequing account.
- Do not use deposit slips as scrap paper.

Always be on the lookout for phishers

Scam artists are always on the lookout for a new and better way to get your money! Emails may "appear" to come from reliable and trusted sources such as government agencies, financial institutions, online auctions etc... directing recipients to web sites that ask them to verify personal information such as name, SIN#, account and credit card numbers, passwords and other information. This scheme is called phishing and many of the emails claim to be updating their computer files and need your response right away. Or there is a scam going around and they just need to "validate" your information. Remember, legitimate agencies do not use email as a means to request or verify your personal information.

Delete it! Don't hit "reply" –

- Should you receive an email with little warning that an account will be closed if you do not confirm your billing information, do not hit reply, or click on any links in the email. DELETE the email. If you are concerned it may be genuine, contact the company or agency cited in the email by using the phone number or web address that you know to be legitimate. If you hit reply it may take you to a webpage that looks exactly like the "real" website, however the URL address will be slightly different and you may be typing in your information directly into the thieves' database.

Be careful about what you email –

- Before submitting financial information through a website, look for either the padlock icon in the lower right hand side or the "https" in the website address. Both of these indicate that the information is secure during transmission. Remember your credit union will not request your
- personal information by way of email.

Look at your statements –

- Always review all statements for any odd or unfamiliar transactions immediately. If your statement does not show up at all, call the company to confirm mailing address and balances.

Please be aware that identity thieves have phones too. A new twist on phishing fraud is Vishing. Rather than request that you click on an internet link, the phone call requests you to call a specific phone number.

The phone message advises that your account may be compromised and requests that you call a specific phone number and enter your account details. Vishing often will use "Call Spoofing" to give you the appearance that the fraudster is calling from your financial institution.

If you have received such a message and returned the call to that telephone number and provided account/personal details, contact your credit union immediately.

- Remember your credit union will never email or contact you requesting your PIN, password, etc.

What do you do if your wallet, purse or identity is stolen?

If the worst has happened, you want to get it resolved as quickly as possible. This reduces the amount of damage that can be done. Here are the steps to take to help resolve the issue.

- Cancel your credit cards. The faster you cancel them, the fewer transactions can be debited. Remember that photocopy that you have stored in a safe place? Pull it out so that you have all the information you need.
- Notify your financial institutions.
- Contact issuers of identification cards or documents (such as drivers license, passport, etc.) and request replacements.
- File a police report. It's easier for you to prove your case to creditors with a filed report. Get a copy of the report or report number for your own records.
- Ask the two national credit reporting agencies to place a fraud alert on your name and SIN#. A fraud alert tells creditors to contact you before they extend credit, open a new account or change your existing accounts.
- With appropriate identification, you can also request a copy of your credit report be mailed from the credit reporting agencies to you free of charge. Visit their websites at www.equifax.com or www.tuc.com for details on what is considered acceptable identification. If you receive a copy of your report and do not find any unauthorized activity, it is recommended that you continue to check your credit reports periodically.
- Contact the Canadian Anti-Fraud Center online at http://www.antifraudcentre-centreantifraude.ca.


CREDIT
UNIONS

CREDIT UNIONS

@PEICreditUnions