

# PROTECT YOUR FINANCIAL TRANSACTIONS



Caisses populaires  
acadiennes

*higher, further, together*



[www.acadie.com/en](http://www.acadie.com/en)

It's a wealth of ways to strengthen the security of your financial transactions.



By implementing simple measures to mitigate fraud. Thwarting fraud by limiting the victims. Taking further precautions. And fewer risks. Strengthening your online security means working together toward a single purpose: protecting your assets and your data. That's why we have a few indications and security measures to recommend. That's why you should apply them. Because at your Caisse populaire acadienne, we do everything in our power to protect you. Because you too have the power and the responsibility to protect yourself.

# TABLE OF CONTENTS

<b>The Caisses populaires acadiennes take broad steps</b> .....	4
<b>La Populaire Card</b> .....	5
Basic security rules when you use your La Populaire Card .....	5
<b>At the ATM and merchants</b> .....	6
Criminals want your PIN... and your money.....	6
How can you protect yourself? .....	6
Measures to ensure increased protection .....	7
<b>AccèsD Internet: for optimum security</b> .....	8
How do they do it?.....	8
Protect yourself.....	8
The Caisses populaires acadiennes strike back .....	9
<b>Fraudulent e-mail</b> .....	11
Scammers are learning new tricks too... ..	11
Don't fall into the trap.....	12
<b>Telephone solicitation</b> .....	13
Typical case .....	13
Your best weapons .....	13
<b>Here are some important resources</b> .....	14

## THE CAISSES POPULAIRES ACADIENNES TAKE BROAD STEPS

We spare no effort to ensure your security and confidentiality when you carry out transactions, whether it's at your caisse, at the ATM, on the Internet or at merchants when you use direct payment.

Our online transactional services meet the highest security standards in the financial industry and comply with the *Personal Information Protection and Electronic Documents Act*. Reliable, proven technologies are used to protect your information should an alteration, loss or unauthorized access occur.

No matter how effective, all protection systems require a minimum of secure behaviour from the user so that the measures in place provide their full advantage. The indications to be followed are generally simple and undemanding. You need only be well-informed, which can be accomplished by reading the following few pages. Among other things, you will learn how to prevent criminals from posing as you to carry out transactions with merchants, with your Caisse populaire and other financial institutions.

As a member of the Interac Association, the Caisses populaires acadiennes participate in awareness activities regarding the protection of debit card PINs. That's why we post the new "Protect your PIN" icon.

# LA POPULAIRE CARD

## Basic security rules when you use your La Populaire Card

The basic rules to follow to protect your money are very simple:

- 1)** Don't lend your La Populaire Card to anyone.
- 2)** If your card is lost, stolen or withheld by an ATM, immediately notify your caisse or call the Help Centre at 1 800 361-5121.
- 3)** Regularly verify your statements and balances to be sure that all the transactions were actually made by you. If you see any fraudulent entries, quickly contact your caisse or the Help Centre at 1 800 361-5121.
- 4)** Never give your PIN (personal identification number for use at ATMs and direct payment terminals) or your passwords (codes to enter AccèsD Internet) to anyone. **No financial institution, police officer, your Caisse populaire acadienne representative or merchant is authorized to ask for your PIN or AccèsD passwords. They are yours and yours alone.**
- 5)** Do not select a PIN or a password that is easy to guess, like your address, telephone number or date of birth.
- 6)** Memorize your PIN and passwords; do not write them down anywhere, especially not on your card.
- 7)** Be discreet: hide the keypad with your hand or body when you enter your PIN.

- 8)** Do not enter your PIN a second time without first making sure the transaction was cancelled and getting your statement.
- 9)** Never lose sight of your card during a transaction.
- 10)** Take your card and the statement at the end of the transaction.
- 11)** Change your PIN and passwords right away, if you suspect that someone watched you enter any of them on the keypad.

## AT THE ATM AND MERCHANTS

### **Criminals want your PIN... and your money.**

The most successful defrauders are big on guts and imagination. How do they do it?

Cards can be copied and cloned at ATMs or at merchants during transactions. Then the thief tries to obtain your PIN when you enter it on the keypad.

### **How can you protect yourself?**

The three best ways to protect yourself from card cloning are simple:

- Protect your PIN by following the above basic rules
- Never lose sight of your card during a transaction
- Take your card and the statement after each transaction

## Measures to ensure increased protection

To reduce the amounts that can be fraudulently withdrawn from your account, the Caisses populaires acadiennes have put the following solutions in place:

- The default total amount for ATM withdrawals from **other Canadian financial institutions** is set at **\$300 Canadian\* per day**. For additional withdrawals, you can go to a Caisse populaire acadienne ATM.\*\*
- The default total amount for ATM withdrawals from **other financial institutions outside Canada** is **\$500 Canadian\* per day**.
- The default direct payment purchase limit (including withdrawals) at merchants is set at **\$1,000 Canadian\* per day**.
- For certain types of transactions—withdrawals, deposits, transfers – at the Caisses populaires acadiennes ATMs, you must confirm your identity by entering your day and month of birth.

For further information on these limits, contact your caisse directly.

**NEVER DISCLOSE YOUR PIN,  
EVEN TO A CAISSE POPULAIRE  
ACADIENNE EMPLOYEE.**

\* May change without prior notice.

\*\* Unless you have reached an agreement to the contrary with your caisse.

## ACCÈSD INTERNET: FOR OPTIMUM SECURITY

When you use Accèsd Internet, you navigate in complete security. Our transactional services and online applications meet the highest security standards. But you must be vigilant. Despite these precautions, you can create flaws in the security system by omitting to carry out the necessary actions to secure your computer. Here is some advice to better arm you against the key attackers interested in your confidential information so they can get a hold of your assets.

### How do they do it?

Defrauders use different methods to get your confidential information:

- fraudulent e-mail or site posting a false logo or image of a company you know or already do business with
- exchanges in a discussion forum
- computer viruses and spyware
- computer piracy attacks

Data collected about the victim can include passwords, credit or debit card numbers, social insurance numbers, dates of birth and personal information. This data is then sold to criminals or used to access credit, chequing or savings accounts, for example.

### Protect yourself

Here are steps to take to reduce your risk of becoming a victim of Internet fraud:

- Never use the automatic entry and password memorization tools available in your browser.
- Change your password regularly – every month and IMMEDIATELY if you suspect that someone might know it.
- Equip yourself with known antivirus and anti-spyware programs and a firewall, and keep them up-to-date.

- Make sure you see the security symbol on the screen (closed padlock) and **manually type** the address of the AccèsD site (<https://accesd.acadie.com/en/accesd>).
- Terminate your session properly by clicking on **Log off** at the top of the screen and close your browser; that way you destroy all copies of Web pages stored on your hard disk and therefore prevent any dishonest or accidental intrusion into your accounts.
- Empty your memory cache (see [www.acadie.com](http://www.acadie.com) for further explanation) and avoid using a public or shared computer.
- When you need to delete documents containing personal and confidential information, like your account or credit card statements, make sure they are completely deleted.

## The Caisses populaires acadiennes strike back

The Caisses populaires acadiennes use the most advanced technologies to ensure your security on AccèsD Internet:

- Transaction encryption

All operations carried out with our online transactional services are encrypted using the best market practices to ensure confidentiality when information circulates between our secure site and your PC or mobile browser. That's why AccèsD users can only access the service with the most recent versions of browsers that accept the 128-bit SSL.2.0 security protocol (Netscape – 4.6 and up, except Netscape 6.0; Microsoft Explorer – 5.0 and up; and Safari).

SSL means Secure Sockets Layer. This protocol enables the encryption of the data being exchanged and guarantees the identity of our servers. It ensures that the data exchanged can only be viewed by authorized people.

- Security of online transactions

The electronic transactions you carry out with the Caisses populaires acadiennes are stored on our servers. That means that they are secure, and none of the related information can be intercepted by a third party.

- Security seal

Make sure you always navigate in a secure environment when you transmit confidential information. If you don't see the security seal on the screen (closed padlock), or if you see a broken seal (open padlock), the Internet transmission security of your transaction is not guaranteed; a third party could intercept it.

The security seal can appear in different places depending on the browser used. Visit [www.acadie.com](http://www.acadie.com) to find out more.

Once you've found the padlock, click on it to view the site's security certificate. You should be able to read the name of the site's owner (for AccèsD: <https://accesd.acadie.com/en/accesd>) and the certificate's validity period.

- Confirmation number

A confirmation number is given after each transaction. It confirms that the transaction was carried out or that your request has been received.

- Automatic storing of all transactions

All transactions you carry out on AccèsD Internet are saved and appear on your account statement. That way, you can keep an eye on your account activity.

**NEVER GIVE YOUR ACCÈSD PASSWORDS TO ANYONE, EVEN A POLICE OFFICER.**

# FRAUDULENT E-MAIL

## Scammers are learning new tricks too...

Criminals quickly recognized the power of e-mail. It has even become the preferred tactic to incite Internet users to reveal personal and confidential information.

Fraudulent e-mail messages, which look like legitimate messages, suggest users click on a link or attachment for reasons such as:

- to change or update personal information
- to enter a contest
- to avoid a possible suspension of their card or account
- to apply for a product or service
- to deal with an expired account

After accepting this invitation, users are then directed to a false Web site where they are asked to provide information such as:

- ATM card number
- password
- account number
- personal identification number (PIN)
- social insurance number
- other personal or confidential information
- date of birth

## Don't fall into the trap

- Never disclose your personal identification numbers (PIN), AccèsD passwords, social insurance number, date of birth or any other personal information, whether related to your AccèsD file or not.
- To access AccèsD, manually type the address of our site (<https://accesd.acadie.com/en/accesd>) in your browser. **Never click on a link in an e-mail message.**

**REMINDER: YOUR PASSWORDS  
AND PERSONAL IDENTIFICATION  
NUMBERS BELONG TO YOU.  
DO NOT GIVE THEM TO ANYONE.**

## TELEPHONE SOLICITATION

When someone solicits you by phone, be vigilant and watch out for people who pretend to be representatives of a company that you do business with or a known organization that you support.

A Desjardins telemarketing agent may very well contact you one day to explain the benefits of one of our products. Stick to the following recommendations so you can be alert and give no chances to criminals.

### Typical case

Telephone con artists are very good at making people believe they are someone else. Some go as far as using the telephone number of a trusted company on the call display! They use excuses such as a financial emergency, a contest won by the victim or missing data in a file to obtain personal information. Once they get this information, they try, and often succeed, to pull off a scam.

### Your best weapons

- No agent will ever ask you to disclose your personal identification number (PIN) or your AccèsD passwords (Internet or Telephone) or other personal information such as your date of birth and social insurance number.

**Reminder:** No financial institution, police officer, Desjardins representative or merchant is authorized to ask you for your PIN or AccèsD passwords.

When in doubt, contact the Canadian Anti-fraud Call Centre at 1 888 495-8501 or visit [www.phonebusters.com](http://www.phonebusters.com).

## HERE ARE SOME IMPORTANT RESOURCES:

- Help Centre throughout Canada, 1 800 361-5121  
or collect outside Canada, (514) 281-9289
- Competition Bureau, 1 800 348-5358,  
[www.bc-cb.gc.ca](http://www.bc-cb.gc.ca)
- RCMP – Reporting Economic Crime On-Line,  
1 888 495-8501, [www.recol.ca](http://www.recol.ca)
- The Canadian Anti-fraud Call Centre,  
1 888 495-8501, [www.phonebusters.com](http://www.phonebusters.com)

These credit bureaus and other organizations  
will register a fraud indicator in your file:

- Equifax: 1 800 465-7166
- TransUnion:  
- outside Québec: 1 877 525-3823
- Local police authorities, companies that issue  
credit cards, banks and provincial archive



if...

You lose your La Populaire Card

You are a victim of identity  
theft or fraud

You are a victim of phishing

**Call your Caisse or Help Centre  
throughout Canada at  
1 800 361-5121  
or collect outside Canada,  
(514) 281-9289  
right away.**

**Remember: Con artists often seem  
truly nice and work quickly to create  
relationships of trust. Remain vigilant.**



**Protect your PIN**



**Caisses populaires  
acadiennes**

*higher, further, together*