

# SECURITY: ACCESS AND PAYMENT METHODS



**Desjardins**  
**Online Solutions**

Money working for people



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 Desjardins, 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>Desjardins takes broad steps</b> .....	4
<b>Desjardins Access Card</b> .....	5
Basic security rules when you use your Desjardins Access Card .....	5
<b>At the ATM and merchants</b> .....	6
Criminals want your PIN... and your money .....	6
How can you protect yourself? .....	6
Desjardins measures to ensure increased protection .....	7
<b>AccèsD Internet: for optimum security</b> .....	8
How do they do it? .....	8
Protect yourself .....	8
Desjardins strikes back .....	9
<b>Fraudulent e-mail</b> .....	11
Scammers are learning new tricks too... ..	11
Don't fall into the trap .....	12
<b>AccèsD Telephone</b> .....	13
<b>Telephone solicitation</b> .....	14
Typical case .....	14
The Desjardins way .....	14
Your best weapons .....	14
<b>Here are some important resources</b> .....	15

## DESJARDINS TAKES BROAD STEPS

At Desjardins, 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, by telephone 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 *Act Respecting the Protection of Personal Information in the Private Sector*. 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, Desjardins and other financial institutions.

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

# DESJARDINS ACCESS CARD

## Basic security rules when you use your Desjardins Access Card

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

- 1) Don't lend your Access Card to anyone.
- 2) If your card is lost, stolen or withheld by an ATM, immediately notify your caisse or call 1 800 CAISSES.
- 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 dial 1 800 CAISSES.
- 4) Never give your PIN (personal identification number for use at ATMs and direct payment terminals) or your passwords (codes to enter AccèsD Internet and Telephone) to anyone.  
**No financial institution, police officer, Desjardins 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.
- 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. You can make these changes 24 hours a day at any Automatic Teller Machine (ATM).

## AT THE ATM AND MERCHANTS

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

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

## Desjardins measures to ensure increased protection

To reduce the amounts that can be fraudulently withdrawn from your account, Desjardins has 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 Desjardins 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 Desjardins 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 DESJARDINS 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 must carry out the necessary actions to secure your computer. Here is some advice to better arm you against cybercriminals who might attempt to steal your identity and 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

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.
- Manually type [www.desjardins.com](http://www.desjardins.com) and then click on the AccèsD logo.

- Make sure you see the “s” in the address bar on the AccèsD Website before entering your password.
- Be certain the address begins with <https://accesd.desjardins.com>
- 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 viewing of your accounts.
- Empty your memory cache (see [www.desjardins.com/security](http://www.desjardins.com/security) 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.

## Desjardins strikes back

Desjardins uses the most advanced technologies to ensure your security on AccèsD Internet:

- Two-way authentication  
 After entering your Access Card number on the AccèsD home page, Desjardins systems will begin the computer recognition process – these systems recognize the computer(s) you usually use. If your computer is recognized, you will then be asked to enter your password to have access to your account information. However, if a connection attempt is made from an unrecognized computer, you will be asked one of the previously established personal questions in order for Desjardins to identify you.
- Transaction encryption  
 All operations carried out with our online transactional services are encrypted to 128 bits using the best market practices to ensure confidentiality when information circulates between our secure site and your PC browser.

- Security of online transactions

The electronic transactions you carry out with Desjardins 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.

1. You must see an "s" on <https://>
2. The field name must automatically begin by <https://accessd.desjardins.com>
3. You must see the browser's security seal (closed padlock)

The security seal can appear in different places depending on the browser used. Visit [www.desjardins.com/security](http://www.desjardins.com/security) 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://accessd.desjardins.com/en/accessd>) 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 Desjardins has received your request.

- Automatic storing of all transactions

All transactions you carry out on AccèsD Internet are saved and appear on your monthly statement of account. 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

Criminals quickly recognized the power of e-mail. It has even become a well-known 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 register as a finalist in 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
- to deal with a fraud or an error in their 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
- credit card number
- AccèsD password
- social insurance number
- date of birth
- e-mail address

## 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 [www.desjardins.com](http://www.desjardins.com) and then click on the AccèsD logo. **Never click on a link in an e-mail message.**

Have you received an e-mail you believe to be fraudulent? Forward it to us at [phishing@desjardins.com](mailto:phishing@desjardins.com). Please note that you will receive an automatic response to e-mails sent to this address. Caution: do not include any confidential information in this e-mail.

## Important

**Desjardins has implemented a 24-hour, 7-day active surveillance system to ensure quick reaction if fraudulent e-mail is detected. Furthermore, Desjardins is doing everything possible to protect its Internet service users from all types of fraud.**

**It is not Desjardins' practice to solicit Internet service users through e-mail to their personal address or by other means to obtain their confidential information. However, it is possible that your caisse or a Desjardins subsidiary contacts you via your AccèsD message box. Because they are protected by the AccèsD secure environment, these messages are highly secure.**

## ACCÈSD TELEPHONE

To avoid fraud by means of AccèsD Telephone, Desjardins set up the following procedures:

- telephone numbers exclusive to Desjardins:  
1 800 CAISSES and (514) JACCÈSD (522-2373)
- measures to authenticate members when information is exchanged:

When you call, a recorded voice asks you to choose among various options, each of which has a corresponding number. By pressing 1, you are in autonomous mode: the audio response unit indicates the steps to take for a simple transaction, such as a transfer or bill payment; the system will ask for your Access Card number and password. If you pressed 2, 3 or 4 for more complex transactions, the system directs you to the specialized agent who can best meet your needs.

- Confirmation number

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

- Automatic storing of all transactions

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

- Security of telephone transactions

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

You can talk directly to an officer at any time by dialing 0. All calls are recorded.

# 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.

## 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.

## The Desjardins way

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.

## 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. Passwords are intended to be verified by automated systems, not by people.

## HERE ARE SOME IMPORTANT RESOURCES:

- 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)

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

- Equifax: 1 800 465-7166
- TransUnion:
  - in Québec: 1 877 713-3393
  - outside Québec: 1 877 525-3823
- Local police authorities, companies that issue credit cards, banks and provincial archives



For more details,  
visit [www.desjardins.com/security](http://www.desjardins.com/security).

Or

Call 1-800-CAISSES.

If...

You are a victim of identity theft or fraud...

You are a victim of phishing...

**Call Desjardins Card Services right away.**

Montréal and surrounding area: 514-397-4415

Canada and the United States: 1-800-363-3380

Other countries: 514-397-4610 (collect) or contact VISA's world-wide customer service department



**Protect your PIN**



**Mixed Sources**

Product group from well-managed forests, controlled sources and recycled wood or fiber

[www.fsc.org](http://www.fsc.org) Cert no. SGS-COC-2319  
© 1996 Forest Stewardship Council



30%

Committed to sustainable development, Desjardins Group favours the use of paper that is manufactured in Canada in accordance with recognized environmental standards.



**Desjardins**  
**Online Solutions**

Money working for people