

Internet Security: Protecting Your Personal Information

Intact Financial Corporation abides by the highest security standards, whether they are national or international. We are fully committed to protecting the personal information you have entrusted to us. As part of this commitment we have created this simple guide detailing ways to do business online safely and securely. Please take the time to read it, as we hope these simple steps and tips will help you to protect your information.

Protect yourself online

Be aware of offers on the Internet that promise to improve your PC's Internet speed, or that ask you to download software onto your PC to participate in research. To protect your privacy and security, we recommend that you do not install or download these types of applications. Downloading this type of software may enable hackers to monitor your activities and capture personal and/or sensitive information and in some cases, to intercept all data you enter on your computer and any web site, even if that site is protected. This includes your Intact Financial Corporation Client Account and password. If you already have this installed on your system, you should remove this software in order to avoid the possibility of such monitoring.

Take care of your computer. Keep your computer up-to-date by installing and using the latest official patches, virus and spyware protection tools, and software from know and trusted suppliers.

Always use a web browser that supports at least 128-bit encryption when accessing secure websites. Most browsers now come with this level of protection, which is best for transmitting confidential data over the Internet. You can check to see if your browser supports 128-bit [encryption](#). If in doubt, we recommend that you upgrade your browser. While encryption offers a high level of security, it cannot guarantee that security breaches will not occur. Most are caused by (i) users choosing passwords that can be easily discovered by third parties; (ii) someone stealing a password that has been written down; or (iii) someone watching the user type in their password.

Your password should be changed on a regular basis to reduce the likelihood of such security breaches.

Intact's standard practices for customer contact and information gathering

Intact may communicate with clients by e-mail on occasion, so how can you tell which are from us, and which are fraudulent?

- Intact will address you by name in any e-mails.
- Intact will not include web page links in e-mails that take you to sites where you must enter your personal information.
- Intact will never ask for you to confirm your confidential information by e-mail

The collection, use and disclosure of your personal information depend on how you do business with us. We may gather information from the following sources:

- From you, on applications for our insurance and investment products, or on other forms filled out through telephone, e-mail or face-to-face interviews (ex. your name, address, telephone number, e-mail address, occupation, financial and banking information, and health information);
- From licensed agents, insurance brokers, intermediaries and financial services representatives with whom you have a relationship, as well as adjusters and inspectors;
- From your interactions with us (ex. through your payment history, underwriting and claims);
- From government and other entities, that have information on your driving record and claims history; or
- From consumer reporting agencies (ex. your credit history).

If clients have any doubt about any e-mail they have received purporting to be from Intact they should contact Intact Customer Helpdesk.

In case of suspected identity theft, loss or misuse of credentials for online finance services, please contact Intact Financial Corporation at 1 888.280.8549 or at 1 888.270.9732 for the Quebec Province, as soon as possible in order to avoid and/or minimize the impacts caused by this.

Common Attacks: Phishing, Spoofing, Advanced Fee Fraud & Identity Theft

Phishing

Phishing is an online fraud technique that involves sending official-looking e-mail messages with return addresses, links and branding that all appear to come from legitimate banks, retailers, credit card companies, etc. Such e-mails typically contain a hyperlink to a fake website that misleads account holders to enter their names and security details on the pretence that security details must be updated or changed. Once you give them your information it can be used on legitimate sites to take your money.

It is important that you be suspicious of e-mails asking for your information; see more on Intact's standard e-mail practices below.

Imitation of Intact websites (Spoofing)

Intact monitors the Internet to find imitation websites also called "spooft websites", they can be identified by the use of misspelled names, extra letters or symbols in the web address. These "spooft websites" are often the first step made by phishers in order to steal your identity. We then work with the appropriate international authority to get the websites closed down as quickly as possible – sometimes on the same day we find the website.

Advanced Fee Fraud

You may already have heard of 'advance fee fraud', where e-mails offering large sums of money are sent to thousands of e-mail addresses. Do not respond to these e-mails. Sometimes the money offered is as a result of a lottery for which you have never bought a ticket. Sometimes the money is held in an account overseas and the fraudster promises a percentage of the money in return for your help in accessing it. A modest 'fee' is often required to cover legal fees, open an account or pay customs charges. In all cases, the money promised is never received.

Identity Theft

Identity and information theft is a key problem facing consumers and businesses today.

Hackers have always been interested in breaking into computer systems and causing them to crash. But now they are also interested in keeping a system up and running so they can steal information from it or use it as a launch pad for attacks against other computers. If your identity is 'stolen' you may find yourself with a reduced rating or with criminal conviction, from traffic offences in particular. This is may be because the fraudster has taken out loans, credit cards, a duplicate driver's licence, etc., in your name.

Don't think it's a serious issue? Consider this: in North America an identity is 'stolen' every 12 minutes -don't let it be yours.

Protect yourself from identity theft

1. Before you reveal any personal information, find out how it will be used and if it will be shared.
2. Don't carry your SIN card with you; leave it in a secure place.
3. Guard your mail. Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox after delivery. Ensure mail is forwarded or rerouted if you move or change your mailing address.

4. Do not give out personal information on the phone, through e-mail or over the Internet unless you have initiated the contact or know with whom you're dealing.
5. Keep items with personal information in a safe place. An identity thief will pick through your garbage or recycling bins. Be sure to tear or shred receipts, copies of credit applications, insurance forms, physician statements and credit offers you get in the mail.

We place this warning here because we are aware that the criminals carrying out these frauds do on occasion use the name of Intact or an Intact subsidiary as part of this scam.

Additional Security Tips for Online Browsing

- Don't allow your computer programs and browsers to save your password(s). For example, when you encounter a pop-up box that asks if you would like your password to be remembered, always click "NO". Saying "OK" gives anybody using your computer access to your personal information.
- Do not send personal information (such as SIN, account numbers, passwords, etc.) through e-mail.
- Keep your passwords/PINs safe. Never share, write down or disclose your Internet banking passwords to another individual, or store them in a file on your computer.
- You should always access the Intact Financial Corporation website by opening up a browser window and typing in the address directly into the address bar of the browser. Don't ever access it through a link sent to you. It may take you to a site that looks like Intact Financial Corporation, but isn't.
- When accessing any secure page, make sure the padlock icon is showing in the bottom right hand corner of your browser and that HTTPS is displayed in your browser's address bar.
- Always log off and close your browser once you have completed your banking session. While logged into any online account, do not leave your computer unattended. Although inactivity while logged into your Intact Financial Corporation account will force your session to time-out, it is advisable to log out when you're done or if you will be away for any length of time.
- We recommend avoiding the use of public or shared computers for Internet banking. Many are OK if just want to surf, but don't access sensitive information or use a log in and password. You never know what may have been installed on that "public" PC.

- Remember to always clear your cache after you have logged out of your Intact Financial Corporation account, especially when you are using a public or shared computer. This removes traces of your session from the computer's memory.

Software Removal

From the "Start" menu, select Control Panel, and then Add or Remove Programs. Locate the software you wish to remove and click 'Remove' button.

Encryption

To validate your browser's encryption level, select "Help" from the top line of your browser menu. Then select "About Internet Explorer / Netscape". A window pops up that lists "cipher strength".

How to Clear your Cache

Internet Explorer® 5.5 or later for a PC (Windows® operating system):

- <http://www.microsoft.com/windows/ie/ie6/using/howto/customizing/clearcache.mspx>

Netscape® Navigator 6.2 or later for a PC (Windows® operating system):

- <http://browser.netscape.com/faq>

Mozilla® Firefox® Navigator 2.0 or later for a PC (Windows® operating system):

- <http://www.mozilla.org/support/firefox/faq>

Internet Explorer 5.1 or later for MacOS®:

- <http://www.microsoft.com/windows/ie/ie6/using/howto/customizing/clearcache.mspx>

Are Online Financial Services Safe?

You can transact your business online with Intact Financial Corporation with confidence knowing Intact Financial Corporation uses the most up-to-date encryption technology available.

All information you share with us is held in the strictest confidence, in compliance with privacy standards followed by all major Canadian financial institutions.

Upgrade Browser

To increase your computer's security level, you need you're going to have to download either [Microsoft Internet Explorer](#) , [Netscape Communicator](#) or [Mozilla Firefox 2](#). Once you're there follow the simple prompts provided. If you're using a dial-up Internet connection, you'll want to turn off your call waiting. This is very important to ensure an uninterrupted download.

Encryption: The key to Intact Financial Corporation Internet security

Encryption involves converting information into a scrambled code while being transmitted. Encrypted data cannot be read by anybody who intercepts it. When it is received from you, it is decrypted back to plain text. The same is true when we information is transmitted to you.

How does encryption work?

Everything that travels through cyberspace during your online session, from your password to your instructions and commands, becomes a string of unrecognizable numbers before it is transmitted via the Internet. Both Intact Financial Corporation's computers and the browser you use to surf the Web understand the mathematical formulas, called algorithms, that turn your online session into numeric code, and back again to meaningful information.

These algorithms serve as locks on the vaults of your account information. And while Intact Financial Corporation and your computer can easily translate this code back to a meaningful language, this process would be a daunting, almost impossible task for unauthorized intruders. That's because there are billions of possible keys that could potentially solve each formula -- but only one that will work. Each time you begin an online session, your computer and Intact Financial Corporation's systems agree on a random number that serves as the key for the rest of the conversation. What that random number could be depends largely on the strength of encryption your browser utilizes.

What's the difference between domestic-grade encryption and international-grade encryption?

The difference between these two types of encryption is one of capability. Domestic-grade encryption is exponentially more powerful than international-grade encryption. Think of it this way: 40-bit encryption, also called international-grade encryption, means there are 240 possible keys that could fit

into the lock that holds your account information. That means there are many billions (a 1 followed by 9 zeroes) of possible keys. 128-bit encryption, also called domestic-grade encryption, means there are 288 (a three followed by 26 zeroes) times as many key combinations than there are for 40-bit encryption. That means a computer would require exponentially more processing power than for 40-bit encryption to find the correct key.

How do I know if my online session is encrypted?

You know that your data has been encrypted on a given Web page by looking for the following icons in the lower portion of your browser:

Browser

Netscape Communicator 4.0 Microsoft



Mozilla's Firefox 2.0



Internet Explorer (any version)



NOTE: Netscape displays the icon on the lower left corner of the browser. Microsoft and Firefox displays the icon on the lower right corner of the browser. In addition, Netscape Communicator 4.0 displays the icon in the navigation toolbar.

Netscape Navigator 1.1X identifies its browser using 128-bit encryption with an icon with 2 keys. Netscape Communicator 4.0 and Microsoft Explorer do not display an icon that distinguishes between 40-bit and 128-bit encryption. However, with Netscape Communicator 4.0, you can click on the icon to determine what level of encryption is being used for a particular Web page.

We ensure that all online sessions with Intact Financial Corporation are encrypted.

Please note that the installation, downloading, or use of certain software may result in the ability of third parties being able to analyze or collect your information by redirecting secure transmissions through their servers. While we will endeavor to protect all information as much as possible by notifying you of such redirection and by blocking access when such software is detected by Intact Financial Corporation, we cannot guarantee the security and privacy of any information should you decide to use such software, and Intact Financial Corporation shall not be liable due to its inability or failure to provide notice of redirection of your information, or for its inability or failure to block access when such software is detected. You acknowledge that Intact Financial Corporation will not be liable for any damages arising from the use of such software irrespective of whether we are aware of such risks.

What type of encryption do I need?

Intact Financial Corporation recommends that you use 128-bit encryption (also called "domestic" or "U.S." grade encryption).

We can help you determine whether your browser is secure enough for [online browsing](#), and we can help you download a browser with the encryption you need.

There are currently two levels of encryption available in today's popular web browsers: 40-bit encryption and 128-bit encryption. We recommend that you use a 128-bit browser, because it provides a much higher level of security. We've provided download locations for Microsoft's Internet Explorer, Mozilla's Firefox and Netscape 128-bit browsers.

"Netscape" is a registered trademark of Netscape Communications Corporation. "Mozilla"

and "FireFox" are registered trademarks of the Mozilla Foundation. "Windows", "Internet

Explorer" and "Microsoft" are either registered trademarks of Microsoft

Corporation in the United States and/or other countries. Mac OS is a trademark

of Apple Inc., registered in the U.S. and other countries.