MERIDIAN PRIVACY & SECURITY

Our Privacy Policy

Meridian is dedicated to protecting your privacy and your personal, business and financial information. We carefully follow privacy policies and security practices in everything we do, to support our commitment to you.

Our Privacy Principles describe how we collect and use Member information, how it may be shared and with whom, our security practices and your choices. We will not collect, use or disclose your personal information without your consent, except where required by law, or sell your personal information to third parties.

Have a question about privacy?

Please speak to a representative at your Branch or Commercial Business Centre

Meridian Contact Centre, Toll Free:
1-866-592-2226 (request your Branch Manager)

Fax 905-988-1521

Or

Email Us: PrivacyOfficer@meridiancu.ca

Mail
Meridian, Attention: Privacy Officer
3280 Bloor Street West
Centre Tower, 7th Floor
Toronto, ON, M8X 2X3

Online Comment Card:
www.meridiancu.ca/giveusyourfeedback

Our Canadian Privacy Principles

We are committed to protecting your privacy and your right to control the collection, use and disclosure of your personal information. whether it is under Meridian's control, or information that has been transferred to a third party for processing, in accordance with *Canada's Personal Information Protection and Electronic Documents Act (2000)*.

- **Accountability:** We have designated a Privacy Officer who is responsible for overall privacy governance and all employees are accountable for compliance to these principles.
- **Identifying Purposes:** Before or at the time we ask you for personal information, we will identify the purposes for which it will be used or disclosed. We may ask for information about your identity, transactions, your application, financial behaviour, or other details particular to the product or service.
- **Consent:** You are always in control of your personal information. We require your knowledge and consent for the collection, use, or disclosure of personal information (except when specific legislative or circumstances apply) and we will explain how your information will be used and with whom it will be shared, in a clear, comprehensive and easy to find manner. We will make it easy to withdraw your consent at any time; however this may affect our ability to provide products and services, or fulfill our commitments to you.
- **Limiting Collection:** We only collect information needed for the purposes we have identified, or the products and services you have requested, and we only collect information by fair and lawful means. This may include (but is not limited to) obtaining personal information about you to establish and verify your identity; better understand your needs; assess your suitability and eligibility for products and services; recommend other products and services; to provide on-going service; detect fraud to both you and the Credit Union; for collection purposes; or, compliance with legal requirements. We keep this information only for as long as it is needed for the purposes described above, even if you cease to be a Member.

Examples

- When you open an account we need your name and address in order to provide you with regular account statements.
- When you apply for credit-related products, we need information about your financial situation in order to make sound credit-granting decisions, both for you and for us. We require your written consent to obtain credit reports about you. Once we have granted you credit, we are required by the terms of contractual agreements with the credit bureaus to supply regular, current information on the status of loans or credit in order to maintain accuracy, completeness and integrity of information. We do not disclose more than is required, nor for periods longer than required.
- If you open an interest-bearing account or an RRSP or other registered product, by law and for income tax reporting purposes we are required to ask for your Social Insurance Number (SIN).

We will ensure our employees are appropriately trained to be able to explain the purposes for which they are collecting your information.

- **Limiting Use, Disclosure and Retention:** Unless you consent otherwise or it is required by law, your personal information will only be used or disclosed for the purposes it was collected. We retain your documentation for the longer of: (a) the duration required to provide products, services or commitments to you; and (b) our legal and regulatory requirements. At the end of this period, we will securely dispose of your personal information.
- **Accuracy:** To ensure we are able to satisfy the purposes for which you have provided your personal information, we will list specific items of personal information.
- **Safeguards:** We will protect your personal information with appropriate physical, technological and organizational safeguards relative to the sensitivity to the information, regardless of the format in which we hold it (physical or electronic) and even when it is being disposed. We regularly train our employees on the importance of maintaining the confidentiality of your information.
- **Openness:** We will make clear, easy to read and consistent information about our policies and practices relating to the management of personal information readily available in writing, by telephone, in publications and on Meridian's website. We will include details of who is accountable for these policies and practices; to whom access requests may be sent; and to whom concerns may be addressed. We will also describe what personal information (if any) is made available to other (including subsidiaries or parents) and why. We will not sell your personal information.
- **Individual Access:** Upon request, we will inform you as to the existence, use, and disclosure of your personal information and be given access to that information. You are entitled to question the accuracy and completeness of the information and have it amended as appropriate. We will endeavour to provide this information to you within 30 calendar days, however occasionally we may need additional time and we will communicate these reasons to you.
- **Challenging Compliance:** You are able to challenge our compliance with the above Privacy Principles. We have simple and easily accessible complaint procedures and we will take appropriate measures to correct information handling practices and policies, where deficiencies are identified. We will notify you of the outcome of investigations.
- **Marketing Preferences:** To manage your marketing preferences, please contact us at 1-866-592-2226, visit your local branch or email the Privacy Officer below.

For further information on PIPEDA, please visit:
https://www.priv.gc.ca/en/privacy-topics/

Meridian Contact Centre, Toll Free:
1-866-592-2226 (request your Branch Manager)
Fax 905-988-1521

You may also contact us by mail or online:

Meridian,
Attention: Privacy Officer
3280 Bloor Street West
Centre Tower, 7th Floor
Toronto, ON, M8X 2X3

Email us: privacyofficer@meridiancu.ca

Online Comment Card:
www.meridiancu.ca/giveusyourfeedback

Our European Privacy Principles

While Meridian Credit Union does not have operations in Europe, we are committed to ensuring to full transparency to our Members residing in the European Union under the European Union's General Data Protection Regulation (2017) ('GDPR'), to ensure they are aware of all of the personal data we handle; specify how we protect their personal data; and provide greater control over how we use their personal information.

For further information on GDPR, please visit: http://www.knowyourprivacyrights.org

Meridian Contact Centre, Toll Free:
1-866-592-2226 (request your Branch Manager)
Fax: 905-988-1521

You may also contact us by mail or online:

Meridian,
Attention: Privacy Officer
3280 Bloor Street West
Centre Tower, 7th Floor
Toronto, ON, M8X 2X3

Email us: privacyofficer@meridiancu.ca

Online Comment Card:
www.meridiancu.ca/giveusyourfeedback

Your Online Privacy

Meridian offers you a variety of ways to bank and interact with us online. Our digital channels offer you control and convenience as well as access to our digital services.

Digital banking provides convenient access to information and the ability to perform transactions from home, work or other locations. It is important to be aware that when you communicate via the Internet, other people and software can also communicate with your computer. An inadequately protected computer can be accessed by an unknown party or a virus in a very short period of time.

What we are doing to protect your security

Meridian Online Banking offers you the best security currently available in a commercial environment so that your personal and financial information is protected while in transit between your computer and our server. This is done through the use of industry standard security techniques:

- In addition to encrypted passwords, Meridian's Online Banking services offer enhanced security features, including the use of challenge questions, to help you identify that you are accessing Meridian's Online Banking site (and not a fraudulent site masked to appear as the legitimate online banking site). You will be asked to answer one of your personal challenge questions if you sign in to Meridian's Online Banking or Mobile Banking App from a computer or mobile device that you have not previously registered as 'trusted'.
- Encryption ensures that information cannot be read in transit or changed by scrambling the data using a complex mathematical formula. Some browsers can create a more secure channel than others, owing to the 'strength' of their encryption. Meridian uses the strongest channel available - referred to as 128-bit SSL (Secure Socket Layer). If you have a browser that only supports 'weaker' encryption such as 40-bit or 56-bit SSL, you will need to upgrade your browser before using our site. The longer and more complex the 'key' is, the stronger the encryption. The 40 and 128 refer to the length of the key. Since 128 is longer, than 40, it is more secure.
- Use of robust and multi-layered security of servers and applications, multiple layers of internal and external firewalls which protect Meridian's online environments.
- Regular reviews of our security practices and technology updates as well as regular reviews to ensure our security and privacy policies and standards reflect our industry leading position.
- Access to our databases is strictly managed and systems are in place to ensure security is not breached, including the physical security of our computer hardware and communications.
- Automatic session terminations - To help you protect your information, if there has been no activity for 15 minutes, you will be prompted that your session will be terminated and have the option to continue with your session, if not replied to within 5 minutes; your online banking session will end automatically.

What you need to do to protect your computer and password

Protecting your password and answers to your secondary challenge questions.

Just as you play a vital role in ensuring the security of your home and your possessions, you too share in the responsibility for ensuring that your personal information is adequately protected. In order for us to ensure that only you are accessing your accounts, we need a unique way of

knowing that it's you. Just as the key to your home protects unwanted entry, the online banking 'key' - your password and your secondary challenge questions - ensures that only you can access your accounts.

It is your responsibility to ensure that your 'key' to Meridian Online Banking is protected. Please observe the following security practices:

- Select a password that is easy for you to reMember but difficult for others to guess.
- Select your security questions that only you know the answer to.
- Select your security image and phrase that is easy to reMember and meaningful.
- Do not select a part of your PIN (your ABM 'key') or another password.
- Keep your password and secondary challenge answers confidential - do not share.
- Do not write your password down or store it in a file on your computer.
- Never disclose your password to anyone for any reason. Ensure no one watches you type in your password.
- Change your password regularly. We suggest every 90-120 days.
- Members are reminded that any password that has been in use prior to March 2012 will be required to follow new requirements the next time their password is reset.

Protecting your computer

- Never leave your computer unattended while using banking services.
- Always exit the Meridian Online Banking using the logout button and close your browser if you step away from your computer. Your browser may retain information you entered in the login screen and elsewhere until you exit the browser.
- Prevention of Browser Caching (storing of pages) is enabled by default when using Meridian Online Banking. This prevents secure pages and page information from being stored on your personal computer. It is also a beneficial security feature if you are accessing the site from a shared computer, such as at a friend's house or through a publicly-accessible computer, such as at a library or airport.
- Secure or erase files stored on your computer by your browser so others cannot read them. Most browsers store information in non-protected (unencrypted) files in the browser's cache to improve performance. These files remain there until erased. They can be erased using standard computer utilities or by using your browser feature to "empty" the cache.
- Disable automatic password-save features in the browsers and software you use to access the Internet.
- Install and use a quality anti-virus program. As new viruses are created each and every day, be sure to update your anti-virus program often. It is recommended you update anti-virus definitions automatically. Scan all download files, programs, disks and attachments and only accept files and programs from a trusted source.
- Install and configure a personal firewall on your computer to ensure others cannot access your computer through the Internet.
- Install new security patches as soon as your operating system and Internet browser manufacturers make them available.

Protecting your information when using a public computer

You should be extra vigilant when using publicly available computers. Even if you adopt the tips above to protect your information, you need to bear in mind that even benign programs, like popular desktop search programs, can pose a security risk. Certain programs, such as Google Desktop, cache items that you have viewed so an unwelcome third party can easily search and find those pages again later.

To ensure a safe and secure Internet session, only visit reputable sites. If you visit any questionable web site before Meridian Online Banking, we recommend you close your browser and restart it before proceeding to Meridian Online Banking.

Fraud: Recognize it. Report it. Stop it.

Electronic identity theft can occur when you respond to a fraudulent email that asks for your personal banking information (This is called Phishing). Armed with this information, a person may be able to access your accounts or establish credit, pay for items or borrow money using your name. For this reason, Meridian uses different methods to help you confirm the Meridian Online Banking site is legitimate and secure. These include the selection of a unique personal image, challenge questions and answers and a unique personal code.

Safety precautions for online banking

We will never ask you for your personal passwords, personal information numbers or login information in an email.

If you receive such an email:

- Do not click on any links contained in the email or reply to it;
- Immediately forward the e-mail to onlinebankingsecurity@meridiancu.ca.
- Delete the email once reported.
- Check the address of any webpages that ask you to

enter personal account information. In the toolbar at the top of the page any legitimate banking web site will begin with 'https' to indicate that the page is secure.

- Look for the padlock found in the lower right corner of your screen. If the is legitimate, by clicking on the padlock, you can view the security certificate details for the site. A fraudulent site will not have these details.
- Type in our web address yourself to ensure you are transacting with our server.
- Check your bank and credit card statements regularly to ensure that all transactions are legitimate.

By working together, we can defend potential online information security threats.

Contact Meridian at 1-866-592-2226 immediately if you suspect someone has gained knowledge of your password or if you suspect any loss, theft or unauthorized use of your account.

Our Cookie Policy

We use "cookies" as a fundamental part of our interaction with your web browser

A "cookie" is a small text file that's stored on your computer, smartphone, tablet, or other device when you visit a website or use an app. Some cookies are deleted when you close down your browser. These are known as **session cookies**. Others remain on your device until they expire or you delete them from your cache. These are known as **persistent cookies** and enable us to reMember things about you as a returning visitor.

Our website **www.meridiancu.ca** ("our site") uses session and persistent cookies to distinguish you from other users of our site. This helps us to give you the best possible experience when you browse our site, and also allows us to improve our site. By continuing to browse our site, you're agreeing to our use of cookies.

All of this helps us to make our site better for you. For example, it means we can ensure you find what you're looking for easily and speed up your searches.

Please note that third parties (including, for example, advertising networks and providers of external services like web traffic analysis services) may also use cookies. We have no control over these. Third party cookies are likely to be analytical/performance cookies or targeting cookies.

You can block cookies within your browser, by activating its setting that allows you to refuse all or some cookies. Please keep in mind that if you use your browser settings to block all cookies (including essential cookies), you may not be able to access all or parts of our site.

To find out more about cookies, including how to see what cookies have been set and how to manage and delete them, visit **www.allaboutcookies.org**. Alternatively, you can search the internet for other independent information on cookies.

100%. Guaranteed.

We use world-class encryption security

Security that's the equal of any financial institution in Canada. But the true test is this. We're so confident in our online security that any unauthorized transactions will be reimbursed completely. **100%. Guaranteed.**

Of course, in order to take advantage of a guarantee like that, you need to do your part as well. Mostly common-sense things, like the following:

- Keep your password and security questions confidential
- Don't store your password and Member Number together
- Contact Meridian immediately if you've noticed suspicious activity, and make sure that you comply with terms set forth in your account agreements
- Always log out of your Online Banking session and make sure you're using up-to-date anti-virus software

If you take care of those things, we've got your back the rest of the way.