

Privacy & Security Policy

Our Privacy and Security Policy explains how we may collect information from you online when you visit this website. Because you trust us with your financial and personal information, the Bank respects your privacy and takes strong action to safeguard that information, including your online sessions. Our Privacy & Security policy, effective as of August 1st, 2007, is for general guidance and subject to change. Please review periodically. Customer information means personally identifiable information about a customer.

Protecting information about you from Marketers Outside Belize Bank International Limited (“the Bank”)

Unlike many other financial institutions, the Bank does not sell or share any customer information with marketers outside the Bank who may want to offer you their own product and services.

Making the security of information a priority

Keeping financial information secure is one of our most important responsibilities. The Bank maintains physical, electronic and procedural safeguards to protect customer information. The Bank’s employees are authorized to access Customer Information only when they need it to provide you with products and services or to maintain your account. Our employees are bound by a code of ethics that requires confidential treatment of Customer Information and are subject to disciplinary action if they fail to follow this code.

Collection of Information

To safeguard your information online, the Bank will need to collect or remember information about you from time to time. When you visit our Website, the Bank may collect the following information in order to service your accounts, save you time and money, and better respond to your needs.

- Application information. Information that you provide to us on forms, via the Internet or otherwise.
- Transaction and experience information. Information about your online transactions and account experience, as well as information about our online communication with you.

Email

The Bank collects and keeps the contents of email you send us in addition to your contact address and the Bank’s response. This enables the Bank to respond to your request and questions. Emails sent to the Bank should be used for inquiries that are not sensitive or confidential as regular, non-encrypted Internet email. If the Bank needs information beyond your name, address, email address and telephone number, the bank will provide you with a secure email form. The Bank will not request that you confirm your Personal ID, account numbers, password or other sensitive information via email.

Cookies & Browsers

This site uses a feature of your browser called a “cookie” to assign a “username”. Cookies by themselves cannot be used to find out the identity of any user. Your Belize Bank username automatically identifies your computer – but not you – to our servers when you visit this website. Anytime a cookie is used, personal information is encrypted for our use only and protected from third party access. Unless you specifically tell us who you are (for example by completing an application), if you are just browsing our site, we will never know who you are even though we assign you a cookie.

How we may share information

The Bank does not sell or share customer information collected from our website with marketers outside the Bank who may want to offer you their own products and services. The Bank grant access to non-public personal information about you (such as your name, address, social security number and credit history) to the Bank's employees so that they can provide or offer products and services to you, process and service your accounts, and administer our business.

The Bank may share customer information within our correspondent banks and our affiliates who are contractually obligated to keep the information the Bank provide to them confidential and to use the customer information the Bank share only to provide the services the Bank ask them to perform for you and the Bank.

The Bank also may share customer information the Bank collect about you online to anyone who the bank reasonably believe is conducting a legitimate credit inquiry, including without limitation, inquires to verify existence or condition of an account for a third party such as a lender, merchant or credit bureau, in response to any subpoena, summons, court or administrative order, or other legal process issued by a regulatory, administrative or judicial authority or tribunal whether within or outside Belize, which the Bank believes requires its compliance; on a closed account, if the Bank reasonably believed you have mishandled it; in connection with collection of indebtedness or to report losses incurred by the Bank; in compliance with any agreement between the Bank and a professional, regulatory or disciplinary body; in connection with potential sales of businesses and to carefully selected service providers or third parties who help the Bank meet Customer's needs by providing or offering Bank services or their own product or services.

Our code conduct requires that your information remain confidential. Even if you are no longer our customer, the Bank will continue to treat your non-public personal information in the same way as if you were still a customer. In addition, the Bank maintains physical, electronic and procedural safeguards to guard this personal information.

Used of Shared Information

The Bank may share all the information that we collect, as described above, for the following purposes:

- To provide you with the products and services you requested
- To comply with reporting or other legal requirements
- To otherwise conduct business

Linking to other sites

The Bank may provide links to non-Belize Bank companies, such as credit bureaus or merchants. Although the Bank will only provide links to sites the Bank believe are reputable, the Bank does not make any representations concerning the linked sites' contents or availability. Please note that linked sites may have different privacy and information security policies than the Bank.

If you choose to link to websites not controlled by the Bank, we are not responsible for the privacy or security of these sites, including the accuracy, completeness, reliability or suitability of their information. If you are asked to provide information on one of these Websites, the Bank strongly urges you to carefully study their privacy policies before sharing your confidential information onto the site.

Guarding your own information

The Bank recommends that you take the following precautions to guard against disclosure and unauthorized use of your account and personal information:

- Never provide personal information (including full social security numbers or accounts and card information) over the phone unless you have initiated the call and know with whom you are speaking.
- Safeguard ATM, credit, prepaid and debit cards
- Memorize PINs (personal identification numbers) and refrain from writing PINs, social security numbers or card numbers where they can easily be found.
- Immediately change pre-assigned PINs to a personally memorized PIN.
- Store cancelled cheques, new cheques and account statements in a safe place.
- Report lost or stolen cheques, and credit, prepaid and debit cards immediately.

Personal Computer Security

One way a thief can get personal information about you is from your home computer. The following tips detail how you can add to the security of personal information on your home computer.

➤ **Install and use anti-virus programs**

Viruses can infect a home computer in many ways: through floppy disks, CD's, e-mail, Websites and downloaded files. Anti-virus programs help protect your computer against most viruses, worms, Trojans and other unwanted invaders that can make your computer "sick". Viruses, worms and the like often perform malicious acts such as deleting files, accessing personal data or using your computer to attack other computers. If a file is found to be infected with a virus, most anti-virus programs provide you with options of how to respond, such as removing the harmful item or deleting the file. Installing an anti-virus program and keeping it up-to-date is the best defense for your computer.

➤ **Firewalls, what are they and how do you use them?**

Before you connect your computer to an Internet, you should install a firewall. A firewall can be generally described as a security guard for your home computer. The guard is a piece of software or hardware that helps protect your PC against hackers and many computer viruses and worms. With a firewall you define which connections between your computer and other computers on the Internet are allowed and which are denied. There are firewall programs, both free and available for purchase, that provides the capabilities you need to help make your home computer more secure.

➤ **E-mail Attachments**

E-mail viruses and worms are fairly common. Here are steps you can use to help you decide what to do with every e-mail message attachment you receive. You should only open and read a message that passes all of these tests:

1. The know test – is the e-mail from someone you know?
2. The received test – have you received e-mail with an attachment from the sender?
3. The expect test – were you expecting e-mail with an attachment from this sender?
4. The sense test – does the e-mail subject make sense based on who is sending the e-mail?
Would you expect this type of attachment from this person?
5. The virus test – does this e-mail contain a virus?

➤ **Keep Your System Up-to-Date**

Most software vendors provide free patches to fix problems in their products. You can usually download these patches from the vendor's Website. When you purchase a program, it's a good idea to find out how the vendor provides customer support.

Changes to the Privacy & Security Policy

If the Bank makes changes to our Privacy & Security Policy or makes any material changes to our online services, the Bank will revise our Privacy & Security Policy to reflect such changes and revise the policy's effective date.