Privacy and security measures

How we protect you

3rd Floor The Workplace - 461 La Promenade - Telfair 80829 - Moka – Mauritius - Tel: (230) 207 8600 - Fax: (230) 210 2300 - Email: serviceclient@bcpbank.mu - BRN : C06046679

At BCP Bank (Mauritius), we believe that the confidentiality and security of your information is of utmost importance. Our systems and security procedures are designed to keep your personal and financial data confidential at all times.

However, you also have a significant role to play and should adopt the following practices in order to keep your personal and financial information protected from unauthorised use.

Security regarding use of Digital Services

- Your login credentials are your access to your accounts through our Digital Channels and should always be kept confidential.
- You must take all necessary precautions to protect access to your mobile phone, as OTPs (One-Time Passwords) for verifying online transactions will be sent to it and must be kept secure.
- To ensure you receive the OTPs, you must ensure that your mobile phone number is updated with the Bank, and immediately inform us of any change.
- Your attention is drawn to the fact that no one at BCP Bank (Mauritius) will ever ask you for your login ID or personal Code.
- You are strongly advised not to give out any personal information to anyone over the phone or any other means. Neither the Bank, nor any reputable company will ask you for your password or Personal Identification Number(s) (PIN) via email or over the telephone.
- You are recommended to inform the bank if you receive unusual telephone inquiries regarding your accounts or unusual online requests for account information.

Your personal code or password is the key to your online account information, and you are advised to:

- ✓ Protect your personal code/password and ensure it cannot be easily accessed or shared.
- ✓ Change your personal code/password on a regular basis.
- ✓ Change your personal code/password immediately if you believe that your password has been exposed.
- ✓ Create a personal code/password which is unique to you and which cannot easily be guessed by someone else.

3rd Floor The Workplace - 461 La Promenade - Telfair 80829 - Moka – Mauritius - Tel: (230) 207 8600 - Fax: (230) 210 2300 - Email: serviceclient@bcpbank.mu - BRN : C06046679

- ✓ Avoid associating the personal code/password with anything personal such as birth dates, telephone numbers, or other familiar numbers.

- ✓ Memorise the personal code/password and never to write it down or reveal it to anyone.

Your Online Protection

- ✓ Install firewall software on your Personal Computer ('PC') to help prevent unauthorised individuals or information from entering your computer system. This is important for computers that use a broadband connection to access the Internet;

- ✓ Ensure that your computer has the latest version of an antivirus software installed and that updates are done regularly;

- ✓ Anti-virus scans should be run regularly on computer systems using an up- to-date antivirus software, in order to detect malwares. Anti-virus software can scan the incoming and outgoing email and attachments for computer infections like worms, viruses, Trojan Horses and other malicious code that can affect the computer files and operation;

- ✓ Keep the software of your PC updated and apply all security patches, where applicable;

- ✓ Consider acquiring anti-spam software to filter unwanted email or spam from incoming email list until it is deleted;

- ✓ Do not input or share personal information on a website form or application that does not display the "https://" before a website address or does not display a padlock symbol in the lower right-hand corner of the webpage. This commonly ensures that the online session is in a secured environment and that the personal information entered is protected;

- ✓ Password-protect your PC to prevent unauthorised individuals from accessing your information and change it every 30 - 60 days;

- ✓ Disable the 'AutoComplete' function to prevent others from seeing your logon information each time the Internet Banking is used;

- ✓ Always log off and close your browser after every online banking session and shut down your PC when not in use;

- ✓ Avoid using Internet Banking at Internet cafés, libraries, and other public sites to avoid your information from being copied, traced or re-entered after you have left

3rd Floor The Workplace - 461 La Promenade - Telfair 80829 - Moka – Mauritius - Tel: (230) 207 8600 - Fax: (230) 210 2300 - Email: serviceclient@bcpbank.mu - BRN : C06046679

- ✓ Use internet banking only on secure WiFi Networks. Avoid using free-wifi in public places where security measures are not enforced.

- ✓ Read the privacy policy of the websites you access, to learn about information privacy and how it is used in email offers, advertisements or sweepstakes. Learn how to remove your name from their promotional database to eliminate future unwanted email or spam;

- ✓ Verify the source of your emails before opening them and always run anti-virus software before opening email;

- ✓ Do not send any sensitive, personal or financial information unless it is encrypted on a secure website from a trusted source;

- ✓ Be aware that there are phishing emails and websites designed to trick consumers and collect personal information. If you receive an email or a page link requesting confirmation of personal details, do not input information - even if the page appears legitimate;

- ✓ Do not click on suspicious licks requesting for confidential or personal data

- ✓ Do not respond to a chain letter email in the event that an attachment contains acomputer virus. The best response is to delete it;

- ✓ Do not open an email or email attachments from unknown sources. Scan emails through your anti-virus software first;

- ✓ Do not double-click on an email attachment that contains an executable file or files with extensions "exe", "com", or "vbs" unless you can verify and trust the source.

- ✓ Do not share personal or confidential information on the net or social media.

Your Offline Protection

- ✓ Do not give out your login credentials or any personal information to anyone on the telephone, from a website or otherwise. No one at the Bank's level will request such kind of information;

- ✓ Do not share access to your PC or personal mobile devices with strangers;

- ✓ Disable the 'File and Printer Sharing' capabilities on your computer to prevent anyone on the Internet from browsing or deleting your computer files;

- ✓ To review your bank and credit card statements for unauthorised transactions or withdrawals and notify the bank immediately if any discrepancies are suspected on the statement;

3rd Floor The Workplace - 461 La Promenade - Telfair 80829 - Moka – Mauritius - Tel: (230) 207 8600 - Fax: (230) 210 2300 - Email: serviceclient@bcpbank.mu - BRN : C06046679

To be up to date dated on email news and the steps you may take to help keep your online experience secure.

Should you be the victim of an illegal activity on your account:

- You are recommended to notify the bank immediately on (+230) 2071000 if you suspect that you may be a victim of fraud or if you suspect that there may be illegal activity on your accounts.
- Moreover, you are also advised to file a police report and obtain copies of the report so that you may share and reference it for any claims.

IMPORTANT!

The use of our Digital Banking Services is subject to the terms and conditions set out in your agreement with the Bank including, but not limited to, those set out in the "Personal Banking General Terms & Conditions" or "SME & Corporate General Terms & Conditions" as may be applicable.

3rd Floor The Workplace - 461 La Promenade - Telfair 80829 - Moka – Mauritius - Tel: (230) 207 8600 - Fax: (230) 210 2300 - Email: serviceclient@bcpbank.mu - BRN : C06046679