POPULAR BANK

Information Security Guide
Security Slopes

PREVENTIVE RULES

PRIVATE KEYS OR TOKENS

- Your username, secret key or password, personal identification number (PIN), Token are your personal, private, and non-transferable data. Protect them because they are valuable.
- They are identification and access keys to the Popular Bank systems (they are yourself) and therefore constitute confidential information that you must not share, much less provide to anyone through any e-mail message, SMS, Internet social network, phone call or page on the Internet, as this information can be used, without your consent, to carry out unauthorized banking operations.
- Protect the answers to the security questions that you have established, as an alternative authentication measure.
- Popular Bank Ltd. Inc. will never contact you by phone, email or SMS asking you to disclose all or any of your financial data or for access to applications.
- Make sure you are not being watched while entering your financial information on our website. Know that there are people who dedicate themselves to looking behind your back (shoulder surfing) with the intention of capturing your private or confidential data.
- When composing your password or your PIN, do not choose options that are easy to deduce (your names, surnames, identity card, date of birth or digits like your telephone number). Preferably combine the chosen letters or words (alternating upper and lower case) with numbers and special characters.
- Change your password regularly, at least four times a year.
- Do not repeat the same password for the different systems with which you interact.
- Do not write your password or PIN on any document, device, or system that others could access, including the back of your debit card.
- Tear up or shred any notes or documents that you are going to throw away that contain some or all your personal financial information. Please know that there are people dedicated to searching through garbage (dumpster diving) in search of data or images and acting on your behalf, usurping your identity, to carry out transactions in bank accounts.
- Enter your financial data in secure environments.
- Keep your Token in a safe place.

EQUIPMENTS

- Keep your computer's operating system up to date and install security patches regularly.
- Have an antivirus on your computer and update it periodically according to the update period established by the brand used by you.
- Use a firewall to protect yourself from possible attacks while surfing the Internet.
- Turn off completely when you finish using your computer and don't put it into hibernation mode. Remember that SAVING is good for us (“Saving energy helps reduce greenhouse gases”).
- Bank only on trusted computers. Public computers (in cafes, universities, internet centers, libraries, etc.) should be used with caution because they are shared equipment and the files that are downloaded (account statements, etc.) could be used later by anyone and removed from the computer without your permission.
- Install an anti-spyware program to prevent spyware from running on your computer.
- Be careful when opening files with 2 or 3 extensions in its name (for example: worldofwarcraft.jpg.exe) because this is most likely the disguise of malicious software.
- Periodically, back up your information by making backup copies on external devices (external hard drive, CD, DVD, or USB sticks).
- Do not protect the backup on the same computer since you could lose all the stored information in case of an accident.

NAVIGATION

- Navigate through familiar Internet sites. Be careful when visiting them, especially if you are asked to download programs or other types of files for their operation.
- When you browse the Internet, find out about the privacy policy of each Internet page you visit if you decide to interact through it; it should explain what information it collects from you, how it is used, and whether it is shared with third parties.
- Do not leave the computer unattended while connected to an Internet page that requires your username and password for access. And, if you're done making your transactions, sign out and then close your browser completely.
- If you're going to be away from your computer for a while, and you don't want to turn it off, lock the screen.
- Do not accept the execution of programs whose download is activated without your request.
- Know about the existence of deceptive viruses (hoaxes).
- Do not provide your personal data on web pages whose electronic address (URL) does not include the ese (https://) and verify that the security certificate corresponds to the page you are visiting.
- When browsing from a public computer remember to clear your browsing history. If you do it on your personal computer, also periodically delete the temporary files and cookies that are installed in each browsing session.

- Look for and disable the Settings feature for Privacy Control or Automatic Password Storage. Typically, you should remove the check next to the option that each browser sets:
    - INTERNET EXPLORER
        - Tools>Internet Options >Contents>Personal Information>Autocomplete> Disable usernames and passwords
    - MOZILLA FIREFOX
        - Tools>Options>Security>Remember passwords for sites
    - GOOGLE CHROME
        - Tools>Personal stuff>never save passwords.
- Update your computer's browser, since in addition to maintaining the encryption level recommended for secure connections, this action will correct different vulnerabilities that have been detected and resolved by its supplier.
- Update your email management program.
- Never access the Popular Bank Ltd. Inc. page from links contained in an email.
- When making virtual banking transactions or purchases, verify that you are in a secure environment by verifying that the Internet page you visit contains the elements of an encrypted communication session.
    - The protocol with which the electronic address begins contains an "s" indicative of safe (https://) and
    - An icon of a closed padlock or key appears in the bottom corner of the browser.

GENERAL

- Popular Bank will never ask you to reveal your personal financial data via email.
- Always pay attention to the details of these type of messages. Be aware that there are pages on the Internet designed to trick you into providing your personal and financial information.
- The fraudulent nature of the messages is reflected in the wording of its content, in the composition of its electronic address, which is not the official one of Popular Bank, and in the fact that the environment of the page to which it links does not have the elements of a secure site.
- Do not open emails or files, or click on links, that come from unknown, unexpected, or meaningless titles.
- If you receive emails asking for your financial information, do not provide what is requested. Immediately report what happened by forwarding that message to the email: phishing@bpd.com.do and delete it from your computer immediately afterwards.
- Don't rely on easy-to-obtain gifts or promotions or respond to messages that urgently request your personal financial information.
- Never leave your email account exposed to others. Someone malicious could steal your contacts, send inappropriate messages on your behalf, or even intercept an email in which some or all your personal financial information appears.

- Periodically check your email management program, specifically the Outbox and Sent Emails, to detect messages that you have not sent. If you discover any unknown correspondence, it is a sign that your computer is infected with a malicious program or that your credentials were stolen, and you should proceed to change your password. Additionally, update your antivirus and antispyware program and check your computer with these softwares.
- Immediately report the loss of your checkbooks or checks. Take the necessary precautions to detect and remove the invasion by disconnecting from the Internet and running anti-virus and anti-spyware programs.