BPR BANK

SECURITY CAPSULES

Connectivity Tips:

- Check the authenticity of the bank's website, its should show as https://www.bprbank.com which will indicate that it is secure.
- Check that the address bar is green. This tells you that it is a legitimate and safe site. If it is red, it is an unsafe site, please leave immediately and report it to:
  businesses.bpr@bprbank.com
- Click on the padlock image (🔒) located on the left side of the browser where the website address is placed, to verify that the Security Certificate is in the name of https://www.bprbank.com
- Try not to carry out transactions on the bank's website from unsafe public places such as cyber cafes, shopping malls, airports or the like.
- Connect from a safe place like your home or office.
- Do not enter our website through links located on other pages or links that you receive by email.
- Access content or links directly from the bank's website and not through emails, text messages or dubious postings.

Prevention and Monitoring Tips:

- Be sure to validate the identity of anyone communicating on behalf of the bank.
- The bank will only use approved communication channels to request or update your information.
- The bank will never send links where it asks you for information on access codes to online banking, bank accounts or details of your credit/debit card.
- Periodically review your account movements and report any suspicious information.
- Securely store or destroy documents related to your account.
- Install and keep your antivirus, firewall, and other programs that you use as a protection mechanism up to date, to minimize the possibility of installing unwanted applications.
- Verify that the antivirus is up to date and that periodic scans are carried out on all files stored on the computer.

Access Control Tips:

- Regularly update your access password.
- Define complex passwords; composed of uppercase and lowercase letters, numbers and special characters.
- Define your passwords with a minimum length of 8 to 12 characters.
- Do not share your password. Remember that this is personal and non-transferable.
- Do not allow the option to autocomplete passwords or do not store them in the browser
- Avoid using the same password for multiple accounts.
- Try not to install any pirated software on your computer, as these may contain viruses or programs to obtain your passwords.
- Be sure to log out before walking away or closing the bank's web page.
- Be sure to log out of the Bank App when not in use.

The proper use of electronic means and the follow-up of the security capsules will reduce the possibility of being victims of fraud.

Concepts:

- Identity Fraud: Identity fraud and identity theft are terms used to refer to all types of crimes in which someone improperly obtains and uses another person's personal data in a way that involves fraud or deception, usually for economic purposes. (NIST)

- Phishing: Is a cybercrime in which a target or targets are contacted by email, phone, text message, and fraudulent websites that closely resemble legitimate sources with the intent to commit financial fraud. (NIST)

- Ransomware: It is a malware that uses encryption to retain the information of the victim in exchange for a ransom. The critical data of a user or organization is encrypted so that they cannot access files, databases or applications. A ransom is then demanded to provide access. (mcafee)

- Virus: A computer program that can copy itself and infect a computer without the user's permission or knowledge. A virus can damage or delete data on a computer, use email programs to spread to other computers, or even wipe everything on a hard drive. (NIST)