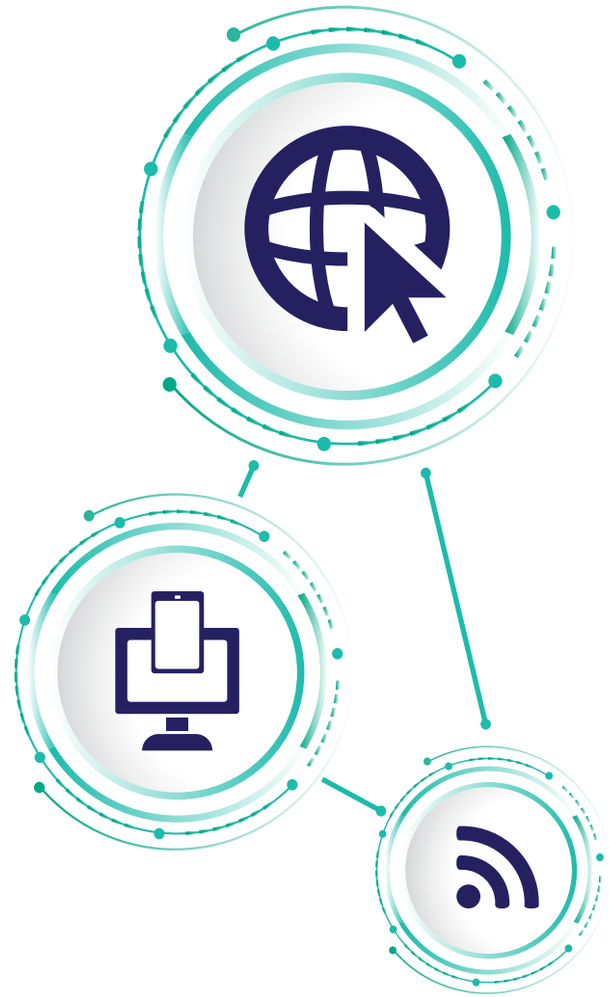
Protecting your account

****

Online Banking

- Transact only with legitimate and trustworthy online stores and vendors. Ensure secure access to your bank's official website and app. Log out after every transaction.
- Activate a 2-step verification process or multi-factor authentication wherein a unique code is sent to your smartphone before you can finalize an online transaction.
- Keep transaction records and regularly review your transaction history.
- Enable text or email alerts for any activity on your accounts.
- Report suspicious account activity to your bank immediately.
- Do not share account information or credit card details with anyone, unless you fully validate and trust their identity.
- Create and use strong passwords:
  - ✔ Mix capital and small letters with numbers and symbols. Use combinations or mnemonics that only you can remember.
  - ✔ Do not use dictionary words, names of persons and places, birthdays, telephone numbers and ID numbers (e.g., SSS, GSIS, TIN).
  - ✔ Do not use your social media passwords as online banking passwords.
  - ✔ Assign a different password for each account. Change your passwords every two months, or as frequent as possible.
  - ✔ Do not share passwords with anyone. Do not write passwords on paper.
- Stay vigilant in protecting your account from hackers, scammers and fraudsters!

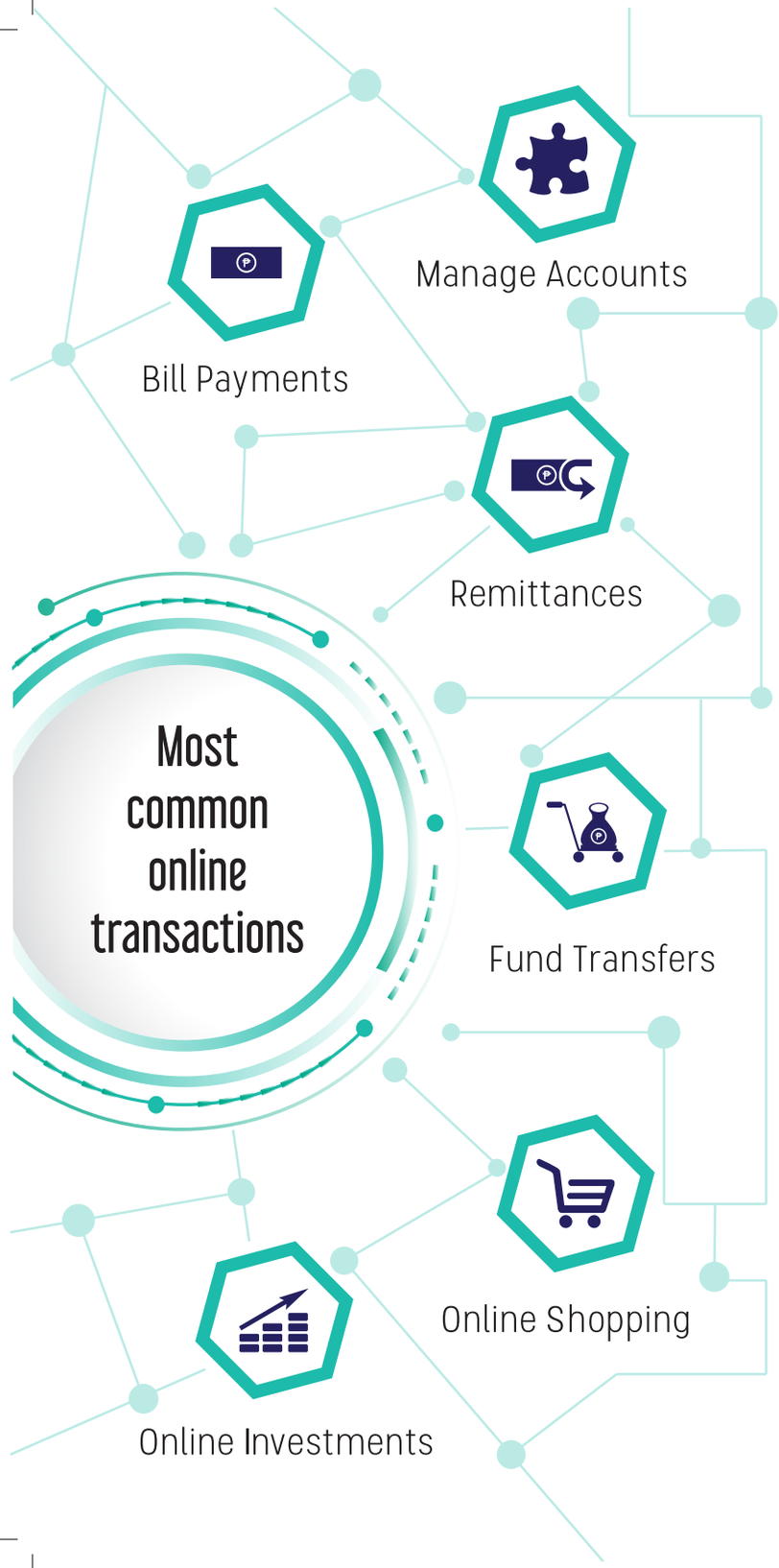


consumeraffairs@bsp.gov.ph

(02) 306-2975 | (02) 306-2974

(02) 708-7088

Consumer Empowerment Group
Center for Learning and Inclusion Advocacy
Bangko Sentral ng Pilipinas
Ground Floor Multi-Storey Building
BSP Complex, A. Mabini St., Malate
1004 Manila, Philippines



Online Banking

is a convenient way of conducting banking transactions, but may expose the bank and its clients to cyber risks. Below are some safety tips to keep in mind when banking online.

Gadgets

- Update security and anti-virus features of your computer, tablets, and smartphones.
- Upgrade operating systems and apps as soon as new versions are available.
- Download legitimate banking apps only.
- Do not download and install suspicious software, files and email attachments.
- Do not use jailbroken or rooted mobile phones or gadgets.
- Do not let other people use your gadgets while logged-in to your bank account.

Connections

- Make sure you have a reliable internet connection to avoid disruption and delays on transactions.
- Avoid using public computers and free wifi connections.
- Always use a virtual private network (VPN) when transacting online.
- Set your WiFi router to the highest security settings. Enable router firewall and encryption. Reduce the WiFi signal range.

Websites

- Type the address or url directly on the address bar instead of clicking links.
- Make sure the website is secure. It should start with https:// and the closed padlock icon is visible.
- Be wary of phishing emails that ask for your personal information or give you links to spoofed or fake websites.
- Clear your browsing history and cache regularly. Delete cookies. Disable plug-ins. Disable the “Save pass-words” feature.
- Always log out from websites, social media accounts, email accounts and apps after every use.