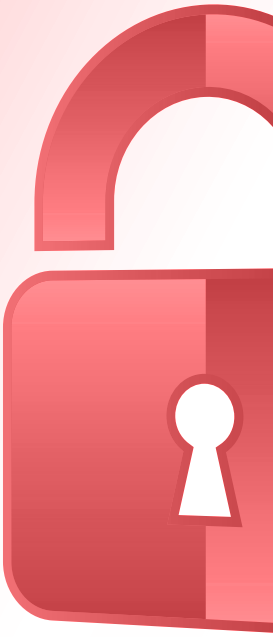
Effective Online Security Tips

Simple steps to help protect your information and transactions

- Avoid using public computers or unsecured Wi-Fi networks (such as kiosks, cafés, hotels, or public hotspots) for any financial transactions.
- Never respond to emails, calls, or messages requesting online banking usernames, passwords, or login credentials.
- Be cautious of fake virus or security alerts that appear as pop-ups. Do not click "OK" or install software claiming your computer is infected.
- Understand that banner ads may contain hidden malware that can install without any user interaction.
- Create strong, secure passwords and keep them private. Avoid using easily guessed information such as birthdays, pet names, or common words.
- Use complex passwords that include upper- and lowercase letters, numbers, and symbols. Change online banking passwords at least every 60 days.
- Do not store password lists on your computer or keep them written near your workstation.
- Never share your login ID or passwords with anyone.