1. **Secure Access Credentials**:
    - Safeguard your login credentials and personal identification numbers (PINs).
    - Avoid storing this information on your computer.

2. **Password Security**:
    - Change passwords or PINs regularly.
    - Utilize complex combinations of characters, including uppercase and lowercase letters, numbers, and special symbols. Passwords should be at least 8 characters long.
    - Avoid easily guessable passwords such as names or birthdays.

3. **Protect Personal Information**:
    - Refrain from disclosing sensitive personal details unless dealing with trusted entities.
    - Keep information like addresses, phone numbers, social security numbers, and bank account details private.

4. **Transaction Monitoring**:
    - Regularly review transaction history and statements to identify unauthorized activity.
    - Promptly report any discrepancies or unauthorized transactions to your bank.

5. **Website Verification**:
    - Verify the authenticity and security of websites before conducting transactions.
    - Check for "https" in the URL and a closed padlock icon indicating a secure connection.
    - Avoid accessing sites through unsecured links or redirects.

6. **Computer Security**:
    - Install and maintain reputable antivirus software and personal firewalls.
    - Keep operating systems and web browsers updated with the latest security patches.
    - Exercise caution when downloading files or opening attachments to prevent malware infections.

7. **Privacy Policy Awareness**:
    - Familiarize yourself with website privacy policies, especially regarding data usage and security measures.
    - Ensure comfort with the policies before sharing any personal financial information.

8. **Online Behavior**:
    - Avoid sending sensitive information via regular email.
    - Refrain from multitasking with other browser windows while banking online.
    - Use personal devices with adequate security measures for online banking activities.

9. **Mobile Banking Security**:
    - Enable passcode locks and encryption on mobile devices.
    - Install antivirus and anti-malware software if available.
    - Utilize secure communication protocols and setup remote wipe capabilities for lost devices.

10. **Continuous Vigilance**:
    - Log off from banking sites when not in use.

- Clear browser cache and history to prevent unauthorized access.
- Stay informed about security measures and contact your bank for any concerns or assistance needed.