• Don’t use public computers at kiosks, cafes, hotels or public wireless networks to conduct financial transactions of any nature.

• Do not respond to e-mail or phone prompts that request online banking credentials.

• Be aware of advertising scams for virus scanners showing what looks like a real virus scan of your computer. Never click OK for a popup that states software needs to be installed / purchased to solve the problem.

• Be aware that banner ads are being used by hackers to hide malware that can be installed on a PC without the user even clicking on them.

• Immediately report any suspicious e-mails, application popups, unexpected error messages, or an unfamiliar login screen to Regions Client Services at 1-800-787-3905.

• Create strong passwords and protect them. Avoid using passwords such as birthdays and pet names.

• Choose passwords that cannot be easily guessed.

• Use alphanumeric passwords along both upper and lowercase letters.

• Change your password at least every 60 days for online banking systems.

• Do not store a list of passwords on the computer or keep them near your computer.

• Never share your logon ID or passwords.