Customer Awareness

Mobile Devices

- Keep a password on your mobile devices, so if they are ever lost or stolen, a person cannot access your personal data unless they know the password.
- Some mobile devices have the ability to remote wipe the device if it is ever lost or stolen.
- Some mobile devices have the ability to erase all data on the device after the password has been entered incorrectly a certain number of times.

Internet Banking & Bill Pay Passwords

- Do not remember your passwords in your internet browser. Doing this will cause a problem when your password expires and you need us to change it. The password saved in your internet browser will have to be updated with it. It is easier to just type your credentials in each time.
- Your Internet Banking and Bill Pay passwords are used to access your personal banking information. Treat these passwords as any other sensitive personal information.
- Choose a password that is hard to guess.
- Keep your passwords safe.
- Be careful of who is around when you enter your information in, so someone does not, "Shoulder Surf," to get your information.
- Do not share your password with anyone.
- The Peoples Bank is not responsible for lost or stolen passwords.

Phishing

- Pay close attention to the Emails you receive to make sure they are legit.
- A Hacker could send an Email with a Link to a bogus site that makes it look like our online banking.
- Entering information on this site would allow a hacker to log, and access your account information.
- Do not enter your Information on a site unless you are absolutely sure it is correct.
- If you have any questions or concerns on whether the site is correct or not please contact a customer service representative at (812) 358-4000

Viruses & Malware

- Make sure to have up to date Anti-Malware software. Keeping this up to date will not lead a user to a bogus site to enter personal information.
- Make sure to have up to date Anti-Virus software. Keeping this up to date will not lead to having keystrokes logged on your computer, so that a hacker can access personal information.
- If you have any questions or concerns please contact a customer service representative at (812) 358-4000