rev. 092613

Online Banking Best Practices

Planters Bank is dedicated to protecting our customer's financial information, accounts, and keeping their identities safe and secure. It is important to educate customers so they are able to understand how to protect themselves against fraud. Customer Awareness is the key to protecting you and your personal information from scams, password compromises, computer security and unauthorized account activity.

Protect Your Computer

- Invest in anti-virus, anti-spam and anti-spyware software and keep it up-to-date. Viruses are harmful computer programs that can be transmitted in a number of ways. Although they differ in many ways, all are designed to spread from one computer to another through the Internet and cause havoc. Most commonly, they are designed to give the criminals who create them access to those infected computers.
- Make sure the latest Windows and security updates are installed.
- Enable a personal firewall.
- Watch for signs of spyware-frequent pop up ads, unexpected icons on your desktop, random error messages or sluggish computer performance which are all signs of infection.
- If you download anything from the Internet such as music, movies, or pictures, make sure you do so only from trusted websites. Downloads can be infected with spyware attached to the file.
- Avoid using public, insecure wireless networks and public computers. If necessary to use a public Internet or unsecured wireless connection, always run an anti-virus software afterward.
- Log off when you are finished with a site and close your browser when you are not using the Internet.
- Never access the bank's web site from a link provided by a third party. Instead, type the bank's URL address into the web browser or use a "book mark" that directs the web browser to the bank's web site.

Password Protection

- Create strong passwords using eight or more characters that contain a combination of upper and lower case letters, numbers and symbols.
- Never share your account numbers, log in ID's or passwords.
- Change your password often, preferably every 30-60 days.
- Do not select the "Remember Me" password option.

Monitor Your Account Activity

- Use online and mobile banking to monitor account activity. Keep good records so you know what transactions you have completed and the amounts.
- Contact the bank immediately if you see any transaction that you are not familiar with or do not remember.
- Balance your checkbook, and verify all account and credit card statements as soon as they arrive.
- Set up message alerts for balance and transaction activity.

Planters Bank
MEMBER FDIC

How to Spot Phishing and Other Email Scams

- Planters Bank will never send email messages that request confidential information such as account numbers, passwords or PINs. It is possible that you may receive emails or phone calls purporting to be from Planters Bank. This is called "phishing" or "spoofing." The goal of spoofing is to get information, such as your Social Security Number, bank account numbers, debit/credit card numbers with or without validation number, passwords and PINs. These emails or phone calls typically imply a sense of urgency to get you to provide your information without considering the consequences. NEVER respond to emails or phone calls. If you suspect that an email or phone call is fraudulent, you should immediately contact Planters Bank.
- Phishing attacks are not the only threat to be aware of – other online threats include spyware. "Spyware" loads malicious software programs onto your computer without your knowledge via email attachments, Internet downloads, messenger chats, or file sharing. These programs, also known as "Trojans," or "keyloggers," are designed to capture your logins, passwords, or other personal data as you log into authorized websites. They may present a fake web page when you type in an authentic website address to trick you into providing confidential information.
- An email may instruct you to click on a link or call a phone number to update your account or even claim a prize. The message will often threaten a dire consequence, such as closing your account. if you don't respond immediately. These are clear signs that someone is "Phishing" for your information.
- Email is not a secure form of communication, do not use it to send or receive confidential information.
- If you suspect that any of your personal information has been compromised, contact Planters Bank immediately.

Additional Security Measures

- Check your credit report periodically. The Fair Credit Reporting Act (FCRA) requires each of the nationwide consumer reporting companies–Equifax, Experian, and TransUnion–to provide you with a free copy of your credit report, at your request, once every 12 months. The three nationwide consumer reporting companies have set up a central website and a toll-free telephone number through which you can order your free annual report. To order, go to www.annualcreditreport.com or call 1-877-322-8228.
- Reducing your risk of identity theft starts with protecting your personal information. Always be diligent about protecting your identity.
- Invest in a paper shredder to securely dispose of any documents containing personal information.
- Consider paying all your bills electronically with online bill pay. This method is considered more secure than mailing paper checks.

For more information regarding Online Fraud, Security and red flags of identity theft visit:

- http://www.ftc.gov
- http://www.staysafeonline.org
- http://www.onguardonline.gov

Planters Bank
MEMBER FDIC