Partnership banking means....
your security is our priority.

Security Awareness Checklist

FIRST PARTNERS

You Succeed. We Succeed.®

First Partners Bank is committed to ensuring the security of your confidential information. We invest in the technology and resources needed to protect your financial information and identity during your loan and banking process.

However, there are also things you can do to further reduce your risk of financial or identity theft. The following is a checklist of steps you can take to add to your overall security.

Computer System Security

□ Equip all computers and networks with updated and reliable antivirus, malware and spyware detection software.

□ Keep your antivirus software current. An automatic update option is usually found in the software's configuration settings.

□ Use your antivirus, malware and spyware software to scan emails.

□ Beware of unusual system performance such as program failures, multiple browser window pop-ups or random computer restarts. This could be an indicator that an attempt is being made to take control of your computer or mobile device.

□ Keep your computer Operating System (OS) updated to the most current version available.

Identity Theft

□ Keep all your banking information, such as statements, checks and even debit or credit cards, in a secure place. Make it a practice to shred statements, checks, credit card offers, charge receipts and credit applications before discarding them.

□ Never provide any personal or financial information over the phone or by email unless you know for certain the person or company with which you are dealing.

□ Always deposit outgoing mail into an official U.S. Postal Service collection box. Promptly collect incoming mail.

□ Regularly review your bank statements, credit card statements and your credit report to ensure that all activity is accurate.

□ Order a free credit report annually so you can review it for completeness and accuracy. If it contains a mistake, file a dispute with the credit bureau.

Corporate Account Takeover

Even small to medium businesses need to protect themselves from identity theft. Hackers will look for opportunities to obtain access to web banking credentials or remote control of computers in order to drain deposit accounts and credit lines. As a business owner, it's important to be proactive in minimizing and avoiding threats to your financial security.

□ Use a dedicated computer for financial transactional activity. DO NOT use this same computer for general web browsing or email.

Corporate Account Takeover (continued)

□ Apply Operating System (OS) and application updates regularly.

□ Ensure that anti-virus, malware and spyware software is installed and automatically updated to the most current version.

□ Include host-based firewall software on all computers.

□ Use the latest version of internet browsers such as Explorer, Firefox or Google Chrome and include pop-up blockers. Keep patches up to date.

□ Turn off your computer when not in use.

□ Do not batch approve transactions. Instead, review and approve each one individually.

□ Review your banking transactions and your credit report regularly.

□ Contact your IT provider to discuss the best way to safeguard the security of your computers and networks.

User ID and Password Security

□ Keep login credentials confidential and in a secure place.

□ Do not store credential information on your computer or mobile device.

□ Do not keep written login and password information in a location where others can view or access.

□ Do not use “easy” passwords. Use a unique combination of upper case, lower case, numbers and special characters.

□ Change your passwords periodically.

□ Please note that First Partners Bank will never ask for your login credentials.

Personally Identifiable Information

□ Apply Operating System (OS) and application updates regularly.

□ Ensure that anti-virus, malware and spyware software is installed and automatically updated to the most current version.

□ Include host-based firewall software on all computers.

□ Use the latest version of internet browsers such as Explorer, Firefox or Google Chrome and include pop-up blockers. Keep patches up to date.

□ Turn off your computer when not in use.

□ Do not batch approve transactions instead review and approve each one individually.

□ Review your banking transactions and your credit report regularly.

□ Contact your IT provider to discuss the best way to safeguard the security of your computers and networks.

Credit, Debit & ATM Cards

□ Keep your cards and PINs in a secure location.

□ Choose a PIN different from your personal information such as street address, telephone or date of birth.

□ Limit the number of cards that you carry with you.

□ Cancel any cards that you do not use.

□ Retain receipts from all card transactions.

□ Sign new cards as soon as you receive them.

□ Report lost or stolen cards immediately.

ATM and Merchant Skimmer Scams

□ Beware of “card skimmers” when using your ATM, debit and credit cards at gas stations or retailers. A skimmer is a device that is placed over the card reader or terminal which collects the card information and security codes.

□ Take a close look at the ATM before using it. One sign of a skimming device is traces of adhesive material attaching it to the ATM.

□ Wiggle the keypad. If it’s loose or appears to be detaching from the ATM, don’t use it.

□ Look at the bank’s ATM cameras and confirm they are not positioned to capture your PIN as you enter it.

ATM and Merchant Skimmer Scams (continued)

□ Pull on the card slot. This can sometimes dislodge a skimming device on top of the card reader. Do this at the ATM or gas pump.

□ If you experience something suspicious, such as being asked to enter your PIN twice or unusual messages on screen, use a different ATM and report it to the bank.

Internet and Email Fraud

□ Beware of suspicious emails from unknown addresses or those unlikely to send an email, such as the IRS.

□ If you accidentally open a suspicious email, do not click on any of the links or open attachments.

□ Never click on links in emails asking for account information, such as account or routing numbers, PIN, passwords or Social Security number. A warning that your account will be closed if you do not update or verify information, or an email with grammar and spelling errors are all good indications that the email is a scam.

□ If you need to update information, go directly to the institution's website and login.

□ Be sure your Internet connection is secure by double checking the website URL address and look for the "lock" icon in the browser status window at the bottom right. The website should begin with https://. If the "s" is missing, the connection is not secure.

□ Be sure to install and run updated anti-virus, malware and spyware software and keep them automatically updated.

□ Install a software or hardware firewall to help filter malicious connections.

844.840.0924

www.FirstPartnersBank.com

Birmingham | Destin | Huntsville

Rev. 5/16

EQUAL HOUSING LENDER

Member FDIC.