1st National Bank
The power of local banking

First National *Mobile*
Safety and Security

Mobile Banking Security – What You Can Do to Protect Your Information

Using your mobile device to check the balances of your accounts or to process a simple transaction is convenient and can save you time, but how do you make sure it is also secure? Here are a few things you can do to protect your information while using your mobile device:

- Treat your mobile device with the same level of care as you would a credit card. If it is lost or stolen and you have not protected it adequately, you may be at risk.
- Password-protect your mobile device.
- Store your mobile device in a safe place.
- Do not send confidential information in e-mail or text messages (e.g., account numbers). It is important to understand that text messages are not encrypted the same way your mobile device information is. If someone gains access to your phone, they will be able to view any text messages sent or received that have not yet been deleted.
- Delete messages that contain account information, including account balances, and any alerts you receive on a regular basis.
- Only download information (photos, ring tones, video clips, etc.) from trusted sources.
- Follow the same rules you use on your computer with respect to opening e-mail and attachments. Similar to phishing attacks on your computer, SMiShing attacks involve fraudsters using text messages with links in them on your mobile device. The fraudsters will use these text messages in an attempt to:
- Get you to download unsuspecting software containing viruses. Never open or respond to a text message from someone you do not know, and proceed with caution even if it comes from someone you do know.
- Take you to a "spoofed" or fake Web site that is masquerading as a First National Bank site and request your account credentials (e.g. password, user ID, etc.)
- Install antivirus software on your mobile device. Contact your carrier for specific information on available antivirus software for your device.
- If you are concerned about the sites you are accessing from your mobile device, turn on the "show URL" or "show address bar" option so that you can see the actual site addresses to ensure they start with "https." Check the information that came with your device for specific instructions.
- If you have questions about how the security features available on your mobile device work, contact your carrier. If you have questions about First National Mobile Banking, contact us at 517.546.3150.

Additional Important safety information and tips

Like any other electronic access, there is always the chance for someone to try and use it maliciously or to steal your personal information. Here are a few ways you can protect yourself:

- Never send account, social security, credit or debit card, or other sensitive banking information via text. Short Message Service (SMS) text messages are rarely encrypted and do not protect your information.

- Be aware of *"blusnarfing"*…. This is the theft of information from a wireless device through Bluetooth technology. Devices with Bluetooth enabled by default and 'always on' may present a target for exploitation and interception of data which can be done undetected. The remedy is to not use the "always on" feature if your device is Bluetooth enabled.
- Never respond to any text (or email) offer to download or use a new banking phone application. Use ONLY the applications provided by First National through our enrollment process.
- Password-protect your mobile device.
- If using an Android device, do NOT enable the "install from unknown sources" feature.
- Never store username or passwords on your mobile device.
- Keep your device with you or secure when not in use.
- Do NOT modify your mobile device as it may disable important security features.
- Install antivirus software. Just like with your PC, your phone should also be protected against viruses, malware and other malicious efforts. Your service provider can assist you with this protection, if you do not already have it.
- Do NOT respond to text messages requesting personal information such as social security, account, credit or debit card numbers. Be aware of *"smishing"*…. The practice of sending you a spoof text message with links to malicious sites or downloads of malicious software or apps used to exploit you or your personal information. The remedy is NOT to click on links in emails or text messages without first confirming that it is legitimate.
- Adopt safe practices with your mobile device just as you would with your personal computer(s) such as NOT clicking on links contained in emails, received from unfamiliar sources or that you are not familiar with.