# AmeriFirst Bank
# Some Mobile Device Security Tips

1. Use of security software is a must. Some programs can also locate a missing or stolen phone, tablet or other similar device, while others will back up your data and can even remotely wipe all data from the phone if it is reported stolen. Definitely make sure you have anti-virus software installed, updated and running.

2. Password protect your devices so if they are lost or stolen the information is protected; and enable device tracking.

3. Do not plug USB cables into public charging stations; only connect USB powered devices using the intended AC power adapter as USB cables can be used to install malware.

4. Lock the device. Locking your device with a strong PIN or password makes unauthorized access to your information more difficult. Passwords are more secure than PINs and should be at least 8 characters long combining upper and lower case letters, numbers, and symbols. If you have an Android device and want to use a lock screen pattern, make sure the pattern includes at least 7 points and doubles back over itself (e.g. at least 2 turns). Additionally, make sure that your device automatically locks after a brief period of inactivity, preferably between 30 seconds and two minutes. This way, if you misplace your device, you minimize the opportunity for someone to access your personal information. Consider Biometrics (fingerprint or face recognitions) and when applicable 2FA – an added layer of security in the form of a second authentication factor.

5. Disable unwanted and unneeded services. Capabilities such as Bluetooth, network connections, mobile wallets, and Near Field Communications provide ease and convenience in using your smartphone. They can also provide an easy way for a nearby, unauthorized user to gain access to your data. Turn these features off when they are not needed. Also consider disabling or uninstalling other features or apps that you no longer use.

6. Be careful when downloading apps. Apps provide a lot of wonderful capabilities for your device, but they are a common way that malicious actors disseminate malware or gather information about you. Always make sure you trust the app provider and download the app from the Google Play Store, Apple's App Store, or other trusted source, as they proactively remove known malicious apps to protect users. Be proactive and make sure that you read the privacy statement, review permissions, check the app reviews, and look online to see if any security company has identified the app as malicious.

7. Maintain your device's security. Remember that setting your device to be secure is great, but you have to keep those settings, as well. It may be tempting to do away with some of the security, such as a lock screen password, or allowing the settings to change when you get an app update, but that puts your device and information at risk.

# AmeriFirst Bank
# Some Mobile Device Security Tips

8. Regularly apply updates. Manufacturers and application developers update their code to fix weaknesses and push out the updates. Enable settings to automatically apply these updates to ensure that you're fixing the identified weaknesses in the applications. At times, operating system or application updates might require a manual approach. Be sure to keep a check to ensure installed applications are up to date.

9. Install antivirus software. Install antivirus software if it is available for your device and enable automatic updating of the antivirus software to incorporate the most recently identified threats. Install a phone locator/remote erase app.

10. Misplacing your device doesn't have to be a catastrophe if it has a locater app. Many apps allow you to log on to another computer and see on a map exactly where the device is. Remote erase apps allow you to remotely wipe data from your device, helping minimize unauthorized access to your information in the event you cannot locate the device.

11. In case your mobile device is lost or stolen, you'll want a way to access your data. To make things easier for yourself, ensure you are backing up your device regularly. Also, ensure your backup process is encrypted.

12. Enabling encryption on your smartphone is one of the best ways to safeguard information stored on the device, thwarting unauthorized access.

13. Do not use public computers and open wireless networks for sensitive online transactions. Wi-Fi spots in airports, hotels, coffee shops, and other public places can be convenient but they're often not secure and can leave you at risk. If you're accessing the Internet through an unsecured network, you should be aware that malicious individuals might be able to eavesdrop on your connection. This could allow them to steal your login credentials, financial information, or other sensitive information. Any public Wi-Fi should be considered "unsecure."

14. Consider turning off features on your computer or mobile devices that allow you to automatically connect to Wi-Fi and other services such as social media websites. Also consider using a cellular 3G/4G/5G connection as a hotspot, which is generally safer than an open Wi-Fi connection. If you do connect through your hotel's Wi-Fi, verify the name of the Wi-Fi hotspot and connection instruction with hotel staff.

15. Consider disabling location services on apps when are not needed.

# AmeriFirst Bank
# Some Mobile Device Security Tips

16. Beware of Phishing Scams. Scams can come in many forms such as email or text message containing a malicious link or attachment. The malicious contents of the email or text message usually skim the data stored on the mobile device and bring them in the hands of the attackers. Approach messages with caution and think critically when receiving emails with links and attachments.