10 Tips for Protecting Your Mobile Devices

As consumer use of mobile devices continues to climb, cyber criminals are targeting those gadgets more frequently. According to a report by the Federal Reserve, 52 percent of smartphone users say they have used mobile banking in the past 12 months.

"We continually review and revise our security protocols to keep up with evolving online threats, but it's also important for users to take appropriate steps to prevent sensitive data from being compromised," says Erica Fowler, Information Security Officer for United. "Mobile devices, by their very nature, are exposed to both physical threats – like being lost or stolen – as well as technical threats from malicious websites, infected downloads, and unprotected Wi-Fi connections."

United Bank suggests following these 10 steps to protect your mobile devices:

- **Use the passcode lock on your smartphone and other devices.** This will make it more difficult for thieves to access your information if your device is lost or stolen.
- **Log out completely** when you finish a mobile banking session.
- **Improve the security of your phone** by enabling useful features like geolocation, remote disablement, cloud data-backups, enhanced access controls, and malicious software detection or by adding a mobile security app with these features.
- **Use caution when downloading apps.** Apps can contain malicious software, worms, and viruses. Beware of apps that ask for unnecessary "permissions", and only download apps from trusted sources like Google Play and Apple App Store.
- **Download the updates** for your phone and mobile apps.
- **Tell your financial institution immediately if you change your phone number** or lose your mobile device.
- **Be aware of shoulder surfers.** The most basic form of information theft is observation. Be aware of your surroundings especially when you are punching in sensitive information.
- **Wipe your mobile device before you donate**, sell or trade it using specialized software or using the manufacturer's recommended technique. Some software allows you to wipe your device remotely if it is lost or stolen.

- **Beware of mobile phishing.** Avoid opening links and attachments in emails and texts, especially from senders you do not know. And be wary of ads (not from your security provider) claiming that your device is infected.
- **Watch out for public Wi-Fi.** Public connections are not very secure, so do not perform banking transactions on a public network. If you need to access your account, try disabling the Wi-Fi and switching to your mobile network.

If, despite these controls, your mobile device is lost or compromised, please contact your nearest United Bank branch or call 800.327.9862 immediately to report any suspected fraud. We may be able to help you by increasing surveillance on your debit and/or credit card account(s), reissuing credit and/or debit cards with new numbers, and other measures to help protect your financial assets and records.

United Bank's mobile app can be downloaded free from the Apple App Store or Google Play and is a convenient option for checking balances, transferring funds and depositing checks. Our app has been designed with your security in mind, and we work with our software development partners to remain up-to-date on the latest security features.