PROVIDENCE BANK & TRUST

Service, Stewardship and Security

Mobile Banking Security Tips

Phones and other mobile devices often contain sensitive data. Providence Bank & Trust understands this and makes protecting your information and your assets one of our top concerns. The following mobile banking security tips and precautions will help to protect the information on your phone and in the event your mobile device is lost, stolen, or otherwise compromised.

Password protect your mobile device and lock your device when it's not in use. Most devices have a security setting that makes it mandatory that you trace a pattern or insert a PIN to access the device – *we highly recommend setting this password protection*.

Install mobile security software on your mobile device when possible. Some mobile security solutions include: Norton Smartphone Security, and Lookout Security & Antivirus, avast! Mobile Security. *We highly recommend downloading mobile security software.*

Download only the official app from Providence Bank & Trust. You can download the Providence Bank & Trust Mobile Banking App from our website www.providencebank.com or from the Apple App market and Android Google Play Market. When downloading from the Apple or Android Market, verify that the app publisher is Providence Bank & Trust and/or Malazaui Software.

Be Careful of What you download. While there aren't as many examples of malware out in the mobile device market as there are on traditional PCs, the fact remains that mobile devices are just specialized computers. That means it's possible for someone to design an app that could try to access your information. You should be careful when downloading apps – not just your banking app, but all apps. Download mobile apps from reputable sources only to ensure the safety of your personal information.

Don't send personal information via SMS (text messaging). Never disclose via text message your personal or financial sensitive information including full account numbers, passwords, Social Security number, and birth date. Trust messages only from Providence Bank with the approved short codes. *We highly recommend deleting text messages from Providence Bank after you have received the information requested.*

Avoid banking while on public networks. Many mobile devices allow you to connect to different types of networks, including Wi-Fi networks. You might be tempted to check your balance or make transfers while you grab a quick drink at the coffee shop or lunch at the local bistro. But before you log into your account, make sure you are not connected to a public network.

Public connections are not very secure – most places that offer a public Wi-Fi hotspot warn users not to share sensitive information over the network. If you need to access your account information, you should switch to a secure network by utilizing your data service from your cellular

network. *We highly recommend using your data service from your cellular network or your secure Wi-Fi network at home to access your mobile banking application.*

Don't follow links. You may have heard the term "Phishing". Phishing refers to the practice of tricking someone into revealing private personal information. With a phishing scheme, that bait might be as simple as a text message or e-mail. It may be as complex as a fake website designated to mimic the legitimate website, which is called spoofing.

You should never follow a banking link sent to you in a text message or e-mail. These links could potentially lead you to a spoofed website. If you enter your information into such a site, you have just handed that data over to thieves. It's always a good idea to navigate to a website directly.

Additional Security Tips:

- If your phone is lost or stolen, notify the bank immediately. The bank can help assist you in disabling and/or changing your mobile banking profile.

- Monitor your accounts regularly. Any suspicious activity should be reported to the bank as soon as possible. The great thing about mobile banking is that you can monitor your accounts quickly and easily. If you check your account often, you'll be able to spot any potential fraud sooner rather than later.

- Use a unique password, one that is not your "usual" password, for mobile banking. The more creative the password is, the harder it will be for someone to guess.

- Turn off Bluetooth by default and use only when necessary. Theft of information from a wireless device can be made through Bluetooth connection.

- Refrain from accessing mobile banking on a phone that has been altered or opened up to allow access to any network or provider. These phones are more susceptible to maleware, viruses, and other malicious programs.