12 Ways to Protect Your Mobile Device

Your mobile device provides convenient access to your email, bank and social media accounts. Unfortunately, it can potentially provide the same convenient access for criminals. Brighton Bank recommends following these tips to keep your information – and your money – safe.

1. **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.
2. **Log out completely** when you finish a mobile banking session.
3. **Protect your phone from viruses** and malicious software, or malware, just like you do for your computer by installing mobile security software.
4. **Use caution when downloading apps.** Apps can contain malicious software, worms, and viruses. Beware of apps that ask for unnecessary "permissions."
5. **Download the updates** for your phone and mobile apps.
6. **Avoid storing sensitive information** like passwords or a Social Security number on your mobile device.
7. **Tell your financial institution immediately if you change your phone number** or lose your mobile device.
8. **Be aware of shoulder surfers.** The most basic form of information theft is observation. Be aware of your surroundings especially when you're punching in sensitive information.
9. **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.
10. **Beware of mobile phishing.** Avoid opening links and attachments in emails and texts, especially from senders you don't know. And be wary of ads (not from your security provider) claiming that your device is infected.
11. **Watch out for public Wi-Fi.** Public connections aren't very secure, so don't 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.
12. **Report any suspected fraud to your bank immediately.**