craft bank

## Mobile Banking – Best Practices

As the use of mobile devices increases for banking, Craft Bank wants our customers to know that we take security very seriously.
The widespread use of mobile phones and mobile and text banking means much more convenience for customers and better ways to monitor account activity. Unfortunately, it also means there are more opportunities for fraud. Craft Bank provides a secure environment for Mobile Banking by keeping our Online Banking services up to date to protect our customers from fraudulent activity.

As a Craft Bank customer, there are several things that you can do to significantly reduce the risk of fraud and identity theft while using our Mobile Banking services.

- Password protect your mobile device, change the password frequently and lock the device when you are not using it. Never use passwords that include birthdays, names, pet names, Social Security numbers or that repeat numbers or letters. Do not configure your mobile applications for auto-login capability. Keep your device in a safe location and do not leave your mobile device unattended in public places.
- Frequently delete text messages received from us on your mobile device, even though they do not contain sensitive information. Never disclose personal information about your accounts via a text or Email message. For example: account numbers, passwords, or any combination of personal information.
- When you log into Mobile Banking, be aware of the people around you. Even if you are speaking on your phone, be careful not to give account numbers or other personal information within earshot of others.
- If you change your mobile number or lose your mobile device, immediately log into online banking to disable mobile and text banking, change your Sign On information to Online Banking, and call us to report a lost or stolen device.
- Do not modify your device. This could leave it susceptible to infection from a virus. This includes modifying your mobile device to give yourself more control, enable features that void warranties, change the root file systems, or allow modifications to install third-party software or hardware components.
- If possible, install reputable mobile security software on your device such as an anti-virus and anti-malware. Consider using tools that allow you to remotely wipe your mobile device if it is lost or stolen.
- Only download applications from reputable sites/stores after reviewing feedback from other users and closely review application permission requests. Always start by contacting Craft Bank to verify what the apps or mobile products are called and where to sign up.
- Monitor your accounts. Check balances and items that are presented on a regular basis. This will help to spot any suspicious activity.
- Set up transaction Email or Text alerts so that you can be notified if your balance drops below a certain level and other transaction information so you will be better aware of your transactions and balances.

- Do not access banking or shopping applications using your private Sign On credentials while connected through public Wi-Fi connections. Ensure your home wireless network is configured to use Wi-Fi Protected Access II (WPA2) Wireless Security Technology. Disable discoverable mode after enabling Bluetooth® devices if your Smartphone does not automatically default to "off" after adding a device.
- Ensure your Username and Password are hidden when interacting with Craft Bank's Online Banking and Mobile Banking App.
- Delete any confidential information from the device prior to any third-party servicing.
- Do not store financial information in your mobile device.
- Keep your mobile device operating system and applications up to date with the latest patches.
- Be cautious of opening unsolicited files, text messages, or applications, especially if they are received from unknown sources.
- Never respond to a "phishing" text or email that requests your PIN, account number, or any debit or credit card number. Remember that Craft Bank will never request your information in this manner.

Craft Bank has provided these Best Practices to assist you in protecting your confidential and financial information. Please implement these practices to help reduce your risk. Craft Bank is not responsible for losses related to security weaknesses within your personal Online Banking access devices such as your home computer, tablets, and mobile devices.