Mobile Banking Best Practices

by The Henry County Bank

Your account and data security are important to us. Our mobile banking app and text message banking are provided in a secure environment. We are providing you these helpful tips to assist you in protecting your confidential and financial information. Implementing these practices may help reduce your risk.

Device

- Only download applications from trusted sources and approved App stores.
- Do not modify your device or access financial information from a modified device. (a.k.a. Jailbroken device)
- Password protect your mobile device using a PIN, password, pattern, fingerprint, or other methods available on your device.
- Enable the automatic screen-lock feature or always lock your device when not in use.
- Install reputable mobile security software such as anti-virus and anti-malware software.
- Keep your mobile device operating system and applications up to date with the latest patches.
- Consider enabling tools that allow you to remotely locate and wipe your mobile device if lost or stolen.
- Clear browsing history, cache, and temporary files regularly. Files stored in memory may contain sensitive information.

User

- Keep your password information safe and use strong passwords.
- Do not access banking or shopping applications or websites using a public Wi-Fi connection.
- Do not store financial information on your mobile device.
- Be aware of your surroundings when accessing your mobile banking account.
- Remember to log off of your mobile banking account when you are done.
- Never respond to “phishing” texts or emails requesting your financial information. The Henry County Bank will never request information this way.
- Never send financial information in emails or text messages to anyone for any reason.
- Monitor your accounts on a regular basis to help spot any suspicious activity.
- Set up transaction alerts to notify you of balance or other transaction information so you are aware of your account activity.

Lost or Stolen Device

- Immediately disable the device for mobile banking. You may change this by logging into your online banking account and selecting Mobile Settings.
- Request your wireless provider to suspend/deactivate your device until it is located.
- Change your online banking password.
- If previously enabled, use a remote location app to find your device and/or use the tool to wipe your device if recovery does not appear to be an option.
- Report stolen devices to your local law enforcement.