Mobile Device Security and Best Practices

Best Practices

- Always apply system updates when available
- Regularly check for App updates
- If you didn't go looking for an application, don't install it!
- Uninstall Applications you are no longer using
- Only install applications from official app stores
- Always check the app permissions before installing, e.g. if an app shouldn't need access to your camera or microphone don't install it
- Maintain a regular backup of your device, in the event of an infection you will need to restore to a good known state

Warning signs that your device may be compromised

- Browser redirects to random destinations
- Additional login forms/prompts being displayed that usually aren't
- Unexplained high data usage
- Poor phone performance
- Reduced battery life

What to do if you think your device has been compromised

- Use another device (or alternate means such as calling customer support)
- Change your passwords for all services that you use on the device: Web banking, Email,Social media, App store i.e. Apple ID or Google Play ID
- Review online banking/credit card statements for unauthorized activity
- Restore your device to a known working backup
- If a backup isn't available restore device to factory settings

MemberDirect® PaymentStream™ C1 Central 1®