D.L. Evans | BANK

Mobile Device Security

We use mobile devices every day to make our lives easier; whether we are interacting with others on social media, checking email, surfing the internet, or playing games many of us carry a smartphone or tablet with us almost everywhere we go. It doesn't matter if you prefer Android or Apple smartphones or tablets each device has a great deal of valuable information about you in it. With this in mind we have brought together some tips to keep your information safe on these devices.

- Installing Apps
  - Only install apps from trusted sources. While no vendor can review every line of code trusted app sources, such as Apple's App Store on iPads and iPhones, or the Google Play Store on Android devices, provide a basic level of screening before allowing an application to be sold in their marketplace.

- Application Permissions
  - Each app installed must be granted permissions to access information contained in, or use resources on your device. Permissions requested may include access to your phones camera, contacts, location, ability to send and receive calls or SMS (text) messages, or accessing your phone's storage. Always closely review the permissions you are granting to an app before you install it. Ask yourself if it makes sense for the app to access that information (i.e. Does a game need access to send text messages by itself?). If a permission it is requesting doesn't make sense, think twice about installing the app.

- Anti-virus
  - While they are not nearly as effective as desktop or laptop anti-virus software, mobile anti-virus applications provide a layer of protection that help keep you and your information safe. A recent search in a reputable app store found more than 10 highly rated and reviewed anti-virus apps that were free or available for a modest fee from well know anti-virus software makers.

- Disposal
  - It's that time; you have your eyes set on the latest and greatest in new phones out there. You've made your decision, but what do you with your old phone? A factory reset of the device is not enough to protect your information. All those pictures, your social media accounts and even online banking data can be recovered from a factory reset device. Below are some steps you can take to protect your information when replacing your phone.

- Android Devices - One method to protect your information is to first encrypt the device, and then perform a factory reset. All the information will still be on the device; however it will be encrypted and unusable. You can go a step further by connecting the reset device to a computer and copying large files (that don't contain personal information) to the device. Then perform a second factory reset This will overwrite the previously encrypted data making it very difficult to recover.
- Apple Devices Apple provides instructions to securely wipe an iPhone or iPad at https://support.apple.com/en-us/HT201351.

Important Information

D.L. Evans Bank will not request personal or sensitive information (full Social Security Number, passwords, full Debit/Credit Card Number, or PINs) when contacting you. However, D.L. Evans Bank or our authorized Fraud Department may contact you regarding suspicious transactions on your account and request information to verify your identity. If you are suspicious of these automated phone calls, you are welcome to call us to ensure the phone call was indeed valid. We can be reached at 208-678-2552 or 1-866-661-5463, Monday through Friday from 8:00 am – 5:00 pm.