Mobile Device Risks and Best Practices

Cybercriminals employ a number of tactics to gain access to sensitive information such as logon credentials and banking information. *Please consider the following points when using your smartphone or tablet:*

- Be aware that cybercriminals embed fake mobile applications with malware that are then offered through app stores. Once installed, the **fake applications** can intercept mobile banking credentials or other sensitive information.
  - Only download apps from trusted places like iTunes or Google Play stores.

- Mobile users have a stronger tendency than online users to click through malicious links. This means they are more likely to connect to a phishing site which can lead to disclosure of sensitive information.
  - Remember, **"phishing"** is a criminal's attempt to acquire sensitive information by sending an email that appears to be legitimate; however, the email directs the user to follow a link and enter personal information that is then used for malicious purposes.
  - If you do not recognize an email sender or if the request seems out of the ordinary, do **NOT** click on any links. Instead, delete the email.

- Many users do not enable **passcodes** on their mobile devices, saying it is too much of a hassle, but it is actually quick and easy and goes a long way in protecting your device. To enable a passcode on your device, go to *Settings*.

- **Jailbreaking** (on Apple iOS devices) and **rooting** (on Android devices) removes restrictions to software installation. The restrictions are meant to improve the security of the device by preventing untrusted applications. (You cannot accidentally jailbreak or root your device; it requires an intentional download of software). Users are often unaware of the risks created by removing these restrictions. Hackers take advantage and install malicious apps to access sensitive information.
  - To ensure the security of your device, keep these restrictions in place.

For more information, please contact:
Mechanics Bank Information Security Department @ 419-524-0831