

## **Mobile Device Risks and Best Practices**

Cybercriminals utilize 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 <u>fake applications</u> can intercept mobile banking credentials or other sensitive information.
  - Only download apps from trusted places like Apple's App Store or Google Play store.
- 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.
- Unauthorized access can occur when using unsecured Wi-Fi or Bluetooth.
  - Avoid logging into accounts that contain financial or private information while using public Wi-Fi and disable Bluetooth when not in use.
- Enable a <u>passcode</u>, <u>Face ID</u>, <u>or Touch ID</u> on your mobile device to help protect data.
- <u>Install updates</u> issued by the device manufacturer. Regular updates help resolve security vulnerabilities.

For more information, please contact:

Mechanics Bank Information Security Department @ 419-524-0831