Camryn Tanner

Dr. Bai

Technology 101

October 16, 2014

Mobile Device Protection

The consequences of losing a smartphone or other mobile device are significant because these devices store personal and business data. The goal, therefore, for mobile device users is to make their data as secure as possible. Techniques include avoiding unsafe links, using caution when downloading apps, turning off GPS tracking, and installing mobile security software.

A higher percentage of users follow unknown links, which can lead to a malicious website. Malicious links can inject malware on a mobile device. The malware may steal personal information or create toll fraud, which secretly contacts wireless messaging services that impose steep fees on a monthly bill. Users should avoid tapping or clicking unknown links.

Any device that connects to the Internet is susceptible to mobile malware. Popular games are likely candidates to house malware, and it often is difficult to distinguish the legitimate apps from the fake apps. Users should check the reliability of the seller, the descriptions and reviews of the app, and the requested permissions before downloading.

GPS technology can track the mobile device’s location as long as it is transmitting and receiving signals to and from satellites. Although this feature may be helpful, serious privacy concerns can arise when the technology is used in malicious ways, such as to stalk individuals or trace their whereabouts. It is best to keep this feature disabled until needed.