FBI alerts and instructs Android users about Malware

In addition to noting two dangerous forms of malware, the FBI offers advice for Android users to enhance mobile device protection.

In addition to noting two dangerous forms of malware, the FBI offers advice for Android users to enhance mobile device protection.

The FBI's Internet Crime Complaint Center (Internet Crime Complaint Center-IC3) has warned users about dangerous types of malware attacking the Android operating system. Two types of malware cited by IC3 are Loozfon - malware that steals user data - and FinFisher - malware that allows hackere to control mobile devices.

Loozfon can trick victims by sending emails promising jobs at home. If the user accesses the link with the email, the malware will steal the contact information from their address book.

FinFisher can assist hackers to control and monitor devices remotely. You may be infected with FinFisher after accessing a malicious link or a fake message is a software update notification.

In addition to the warning content about Loozfon and FinFisher, IC3 also offers some tips for Android users to protect mobile devices:

- When purchasing a smartphone, thoroughly understand the features of the device, including default settings. Turn off unnecessary features to minimize hacker attacks.

- Depending on the type of device, the operating system may have encryption mode. This mode can be used to protect personal data in case the phone is lost or stolen.

- With the development of mobile application repositories, users should preview the evaluation of the developer or the publishing company before downloading the application.

- Preview and understand the privileges you will grant to those applications after downloading.

- Protect the device with a password. This is the first physical measure to protect information on the device. Along with the password, activate the screen lock feature after a few minutes of no use.

- Use anti-virus software.

- Beware of applications that enable geo-location (geographic location determination). These applications will track the location of users anytime and anywhere and can be taken advantage of for marketing purposes, theft.

- Do not connect the device to strange Wi-Fi networks. These networks may be phishing access points that will steal the information transmitted between the device and the valid server.

- In case of purchasing or exchanging equipment, make sure you reset the device to its original factory default condition, to avoid missing personal data on the device.

- Smartphone needs to be updated to run apps and firmware, otherwise it will increase the risk of phones being hacked.

- Avoid accessing links or downloading software from unknown sources.

- When accessing the Internet on your phone, use security measures such as when accessing the Internet on your computer.