



SMARTPHONE SECURITY: PROTECT AGAINST HACK ATTACKS

by Texas Attorney General Greg Abbott

ALTHOUGH MOST COMPUTER USERS ARE aware that viruses can invade their home computers, it is generally less well-known that viruses can also target mobile telephones. Viruses and other malware can be particularly dangerous on phones and other mobile devices because users are less likely to be protected by anti-virus software. With more and more mobile phone customers conducting personal banking and other financial transactions on their unprotected mobile devices, these are increasingly attractive targets for criminals who develop viruses and malicious spyware.

Researchers estimate that more than 40 percent of American adults own a smartphone – the general term for mobile telephones that allow users to access the Internet. As these devices' processing power and data connection speeds continue to improve, their demand only increases. Thanks to these improvements, mobile phones today are used to perform the same tasks that just a few years ago required a computer. As a result, mobile devices are increasingly used to monitor email, store sensitive personal information and photos, and shop online.

Texans who want to protect their sensitive personal information, bank accounts and credit card numbers should only select and install mobile device applications from trusted sources. If a software developer or product is

not well-known, mobile phone users should research the product's rating and popularity. Positive user reviews and high-volume downloads often reflect a legitimate and well-received product.

To help secure their smartphones from unauthorized access, mobile device users should enable built-in security features such as passwords. If possible, mobile devices should be set to require a password or personally identifiable number (PIN) that must be entered before software is downloaded or installed onto a device. This feature can help prevent spyware or viruses from secretly being installed without the owner's knowledge. Smartphone owners should also install the latest security updates provided by their mobile phone service provider.

In addition to the measures outlined above, smartphone users should never respond to text messages or emails from an unknown source. Unsolicited text messages and emails actually may be phishing attacks that attempt to trick device owners into visiting malicious websites. Once an unsuspecting mobile device user clicks on a harmful link or downloads an attachment that contains a virus, it only takes seconds for mobile malware to secretly seize control of the phone and access its data.

Smartphone spyware can allow hackers to intercept text messages or gain unauthorized access to the device's photos, emails and other

sensitive personal data. Some malicious smartphone viruses can even allow hackers to log – and even record – incoming and outgoing calls without the device user's knowledge. As a result, these hidden mobile device viruses can not only compromise users' personal conversations, but also their calls to banks and credit card companies – which may involve sensitive account numbers and Social Security numbers. In short, mobile device viruses are uniquely poised to subject users to a high risk of identity theft.

In light of the significant risks posed by mobile device malware, smartphone users should consider installing security software to guard against the latest security threats. Just as personal computers always should be secured with up-to-date Internet security software, smartphones should be safeguarded against hackers and spammers. Further, once security software has been installed, it is important to keep it updated.

Just as computer owners know not to install software from unknown sources, careful smartphone users should delete suspicious or unsolicited text messages and emails without opening them. With these simple steps, smartphone users can talk, text and browse without having to worry about who is secretly reading, watching or listening to their private communications.

– October 2011

POINTS TO REMEMBER



KEEPING SMARTPHONES SECURE

- Only select and install applications from trusted sources.
- Never respond to unsolicited text messages.
- Never open unsolicited emails from an unrecognized sender.
- Utilize password protection to secure phones from unauthorized usage.
- Install smartphone security software.



For more information about cyber security, identity theft protection and other topics, visit the Texas Attorney General's Office online at www.texasattorneygeneral.gov.



ATTORNEY GENERAL OF TEXAS
GREG ABBOTT