Increase in smartphone hacking raises concerns

By Eliza Molk
Via uWire

As smartphone data usage continues to rise, so does the security risk.

The world's largest technology security company, McAfee Inc., reported a significant increase in iPhone and Android hacking in 2011. Additionally, 42 percent of cellphone users said their data use has increased within the last year, while only 32 percent of those users feel their information is secure, according to an Oracle Communications survey. Students should be concerned about their smartphones' security because once an application or password-free Internet hotspot is used, information on their smartphones could easily become available to hackers, according to Kelley Bogart, a senior information security analyst at the U. Arizona Information Security Office.

Bogart said often times, students don't want to pay for certain applications on their phones, so they circumvent the legitimate application downloading source and find a fake source for that same application. The hackers that created the fake application, she said, can collect information users type into their phones and can sell that data, such as personal banking accounts, on the black market or use it for themselves.

"It's a risk balance and a trade off," she said. "If you're going to download an app without researching the source, you need to think about that."

It's also important to read the application agreement before downloading, Bogart said, because the fine print often times says what the application owners will have access to. For example, the Flashlight application for the iPhone and Android acts as a flashlight on a user's phone, yet the agreement says that it grants access to a user's contacts and video camera.

"Why on earth would a flashlight need to have your contacts and enable your video camera? It's kind of scary," Bogart said.

Caleb Tellez, a UA journalism senior, said his second-generation iPhone is "jailbreaked" in order to find apps like Nintendo games, which he said he couldn't find through his iPhone's app store. Jailbreaking, or modifying a smartphone's firmware to access the internals of its operating system to install third-party applications, often occurs when smartphone users want to find particular apps, wallpapers or programs for free. Tellez said it was easy to find out how to jailbreak his iPhone — he simply Googled it.

The problem with jailbreaking, he said, is that once an iPhone is jailbroken, Apple no longer covers that iPhone's warranty. Tellez said he isn't concerned about his smartphone getting hacked, because it has yet to happen.

"I'm not worried about it, I've never really thought about it," he said.

But Bogart said a lack of foresight is a problem among students who use smartphone — because students grew up using technology, they are almost too comfortable with it, she said.

"Students need to step back and think, 'How might a hacker use this? Why might they want this information? People trust too easily,'" Bogart said.

Nick DePratti, an architecture freshman at UA, said that although personal information has never been stolen from his iPhone in the two years has had it, he will not consider buying protection software for it until he is a victim of hacking.

"I hope it (hacking) will never happen," he said. "If a stranger gets a hold of my information, who knows what that person might do. Everything from private text messages to bank information is held on my smartphone."

Smartphone users can take protection measures to keep information from being hacked, Bogart said. Users should research applications prior to downloading, update their smartphones to the most up-to-date software, install anti-virus and anti-spyware software, read application license agreements thoroughly and use password-protected Internet hotspots instead of free Wi-Fi.

"We've got to break down that trust barrier," Bogart said. "It's the Internet — you don't know who's on the other line."