



## Beware downloading some apps or risk "being spied on"

CBS NEWS *February 24, 2016, 7:00 AM*

Popular apps on your smartphone can be convenient and fun, but some also carry malicious software known as malware, which gives hackers easy access to your personal information.

A security firm found that between 75 and 80 percent of the top free apps on [Android phones](#) or [iPhones](#) were breached. The number jumps as high as 97 percent among the top paid apps on those devices.

Whether these apps help advertisers target you or help [hackers](#) rip you off, you'll want to do your homework before downloading apps, reports CBS News correspondent Anna Werner.

California's Susan Harvey said she was a victim after she used a debit card to download a slot machine game app to her cell phone through a Google Play store account.

"It was something you purchased once, for like \$15," Harvey said.

When she went to reload the game, she found hundreds of purchases had been made -- by her math, more than \$5,000 worth of transactions.

"My heart sank, I just sat there looking at it... I physically, I was sick, because I didn't know what they were," Harvey said.

That story's no surprise to [cybersecurity](#) expert Gary Miliefsky, whose company SnoopWall tracks malware. He said certain apps are designed to steal your personal information.

"What are the consequences for me as a consumer?" Werner asked.

"You're gonna lose your identity. You're gonna wonder why there was a transaction. You're gonna wonder how someone got into your bank account and paid a bill that doesn't exist," Miliefsky said.

Miliefsky said when you download an app, you also give permission for it to access other parts of your phone, like an alarm clock app that can also track phone calls.

"You think an alarm clock needs all those permissions? Access to the Internet over wifi, your call information, calls you've made, call history, your device ID? This to me is not a safe alarm clock," Miliefsky said.

And there's the weather and flashlight apps that he says exploit legitimate banking apps to capture information, as he showed us in a demonstration of what could happen when someone takes a photo of a check to send to their bank.

"The flashlight app spies on the camera and noticed the check and grabbed a copy of it. Shipped it off to a server somewhere far away," Miliefsky said.

Last year the group FireEye discovered 11 malware apps being used on iPhones that gathered users' sensitive information and send it to a remote server, including text messages, Skype calls, contacts and photos Apple fought back by removing the apps and putting stricter security measures in place.

"They get at your GPS, your contacts list...to build a profile on you," Miliefsky said.

Some apps are simply collecting information for advertising purposes. In 2014, the Federal Trade Commission settled a lawsuit with a company over its popular Brightest Flashlight app, alleging it transmitted consumers' personal information to third parties without telling them.

But Miliefsky said he's found another flashlight app that can do much more troubling things.

"This one turns on your microphone in the background, listens in on you, and sends an encrypted tunnel to a server we discovered in Beijing," Miliefsky described.

"You're saying that they're actually listening to people's conversations and sending that audio back to Beijing?" Werner asked.

"Yeah, we've tracked it. I can show you where it does it," he said.

Miliefsky said it can be traced to a few blocks from Tiananmen Square on Information Drive in Beijing.

He gave a report on that app to the FBI.

"Because to me, it's spyware at the nth degree," Miliefsky said.

His recommendation?

"We really have to look at our phone and say, 'This is really a personal computer that fits in our pocket. Let's shut down all the apps we don't use. Let's delete apps that don't make sense and reduce the risk of being spied on,'" Miliefsky said.

The creator of the Brightest Flashlight app settled with the FTC, agreeing to change its policy and delete all the information it had gathered.

Harvey sued Google over her alleged hack, but a judge recently dismissed it, saying she and her attorney filed too late. Google said fewer than one percent of Android devices got bad apps in 2014.

<http://www.cbsnews.com/news/mobile-phone-apps-malware-risks-how-to-prevent-hacking-breach/>