cbc.ca

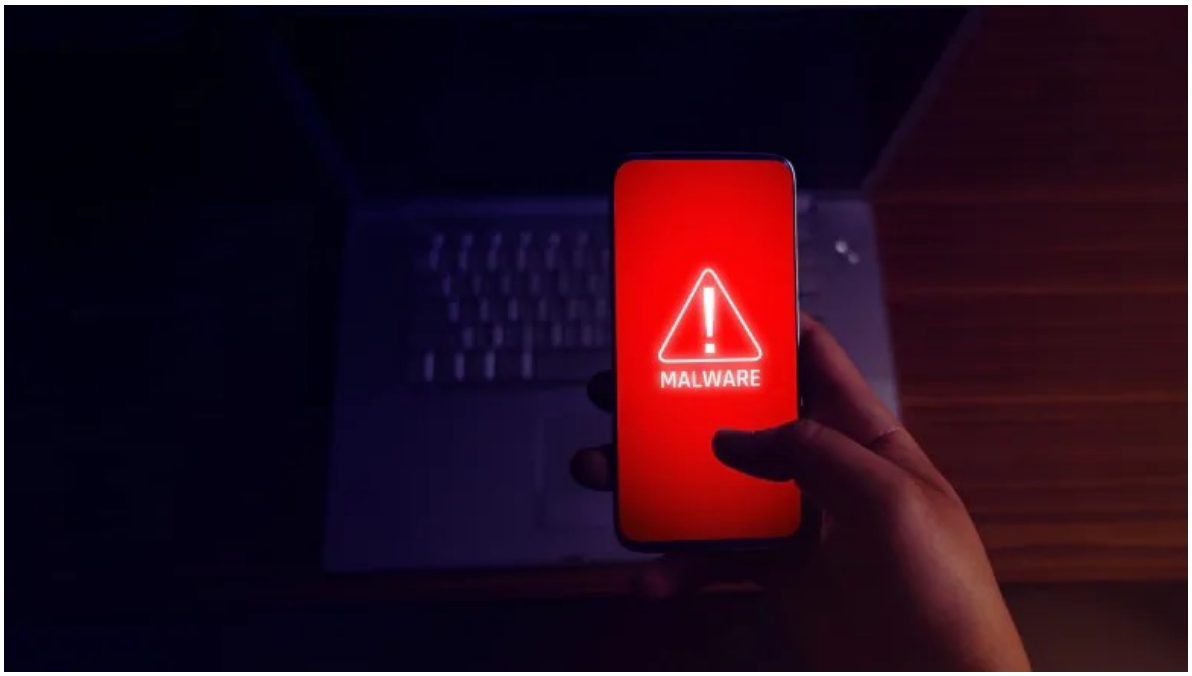
# Apple, Google not doing enough to fight app-store malware, say security experts | CBC News

*David Burke · CBC News · Posted: Nov 12, 2019 6:00 AM AT | Last Updated: November 12, 2019*

8-10 minutes

---

Companies like Apple and Google need to do more to protect malware from sneaking into their app stores and onto people's cellphones, say cybersecurity experts.




There's been a spike in the number of people being hit with malware on their cellphones, says David Shipley, CEO of Beauceron Security, a cybersecurity software company in

Fredericton. (Suttipun/Shutterstock)

The first sign Andre Pettipas had that anything was wrong with his cellphone was when his girlfriend texted him to ask about the message he wrote to her that simply said "Sexual assault allegations."

Pettipas didn't send that text from his Samsung Galaxy S9. The culprit was a PDF scanner app, which was actually malware he had downloaded from the Google Play store.

"I'm definitely worried about it," said the Port Hastings, N.S., man. "I'm going to be keeping an eye on my credit card statements and my banking information to make sure there's no money going [anywhere] as the days go by."

Pettipas isn't alone. He posted on Facebook about what happened and more than a dozen other people said they'd had similar problems.

Cybersecurity experts say companies like Apple and Google need to do more to protect malware from sneaking into their app stores.

Cape Breton musician Andre Pettipas is worried about his personal information being compromised after he discovered malware on his cellphone. (Travis Pettipas)

"In the last couple of months, we've seen a dramatic spike and particularly what happens is they're getting better at sneaking things into app stores," said David Shipley, CEO of Beauceron Security, a cybersecurity software firm based in Fredericton.

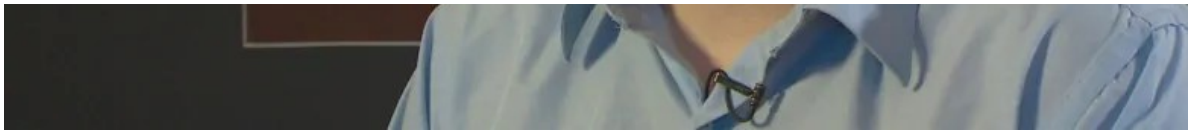
Often, malware steals a person's data, everything from their banking information to their contacts. That information is then either sold online or used by the person who made the attack.

Other times, ransomware encrypts the data on someone's phone and demands payment before the phone will be unlocked.

The problem is most app stores don't do a thorough security check on the apps they offer, said Arash Habibi Lashkari, a professor who studies malware at the Canadian Institute for Cybersecurity at the University of New Brunswick.

"They need to change their strategy," he said.

It's not clear how many cellphones across the country have been compromised by malware.

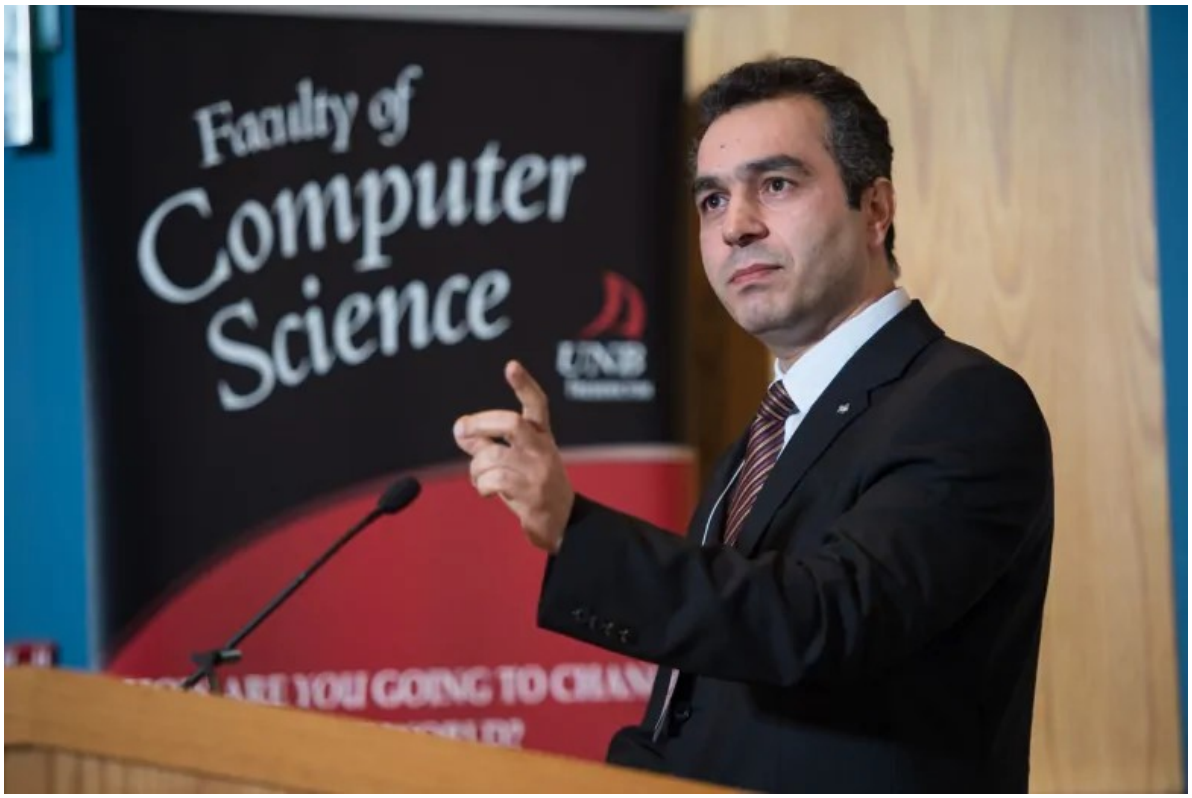


David Shipley is the CEO of cybersecurity software firm Beauceron Security. (Jonathan Collicott/CBC)

However, as part of Lashkari's research in 2015, he downloaded 5,000 apps from Google Play, tested them and found they were all legitimate. Then in 2017, he downloaded the same apps and discovered more than 200 of them had become malware.

"It means someone repackaged them with the malicious code and uploaded [them]," said Lashkari.

Other programs start off benign and only become malicious after an update to the application turns it into malware. This helps malicious programs escape detection in the app store, said professor Ali Dehghantanha, director of the Cyber Science Lab at the University of Guelph in Ontario.



Arash Habibi Laskari is a research co-ordinator with the Canadian Institute for Cybersecurity at the University of New Brunswick. (Rob Blanchard/University of New Brunswick)

He said for the average citizen, the most common way for their cellphones to become infected is through app stores.

Lashkari said adding extra security to app stores is expensive. He said more people need to be hired to review apps or new programs need to be designed to detect malicious software, which is why he believes companies don't make more security improvements.

Both Apple and Google declined interviews with CBC News. Instead, the companies emailed links to online documents that outlined some of the security features of their app stores.

## What Apple says it's doing to fight malware

In its App Store Review Guidelines, Apple states all apps are reviewed by experts and an editorial team.

All third-party apps, meaning apps not developed by Apple, are restricted from accessing files stored by other apps or from making changes to a cellphone, according to Apple's IOS Security Whitepaper. These measures give "users industry-leading protection against viruses, malware, and other exploits."

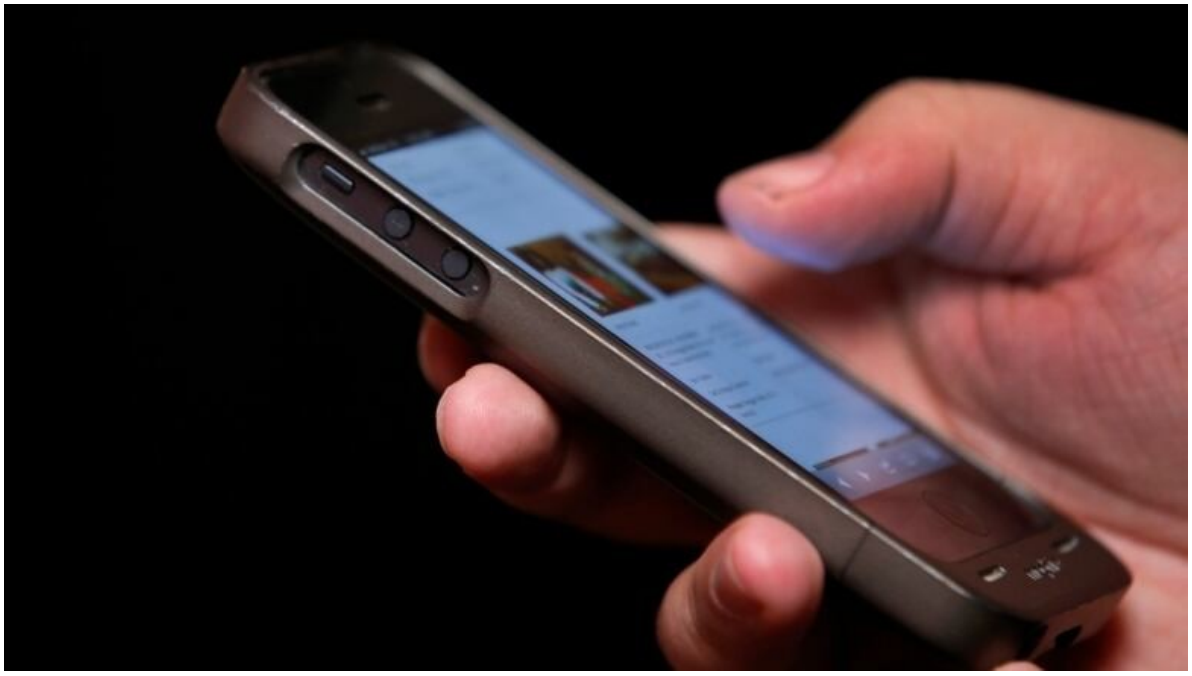
## What about Google?

Google said it has implemented new policies to stop malicious apps from entering Google Play. It said in 2018 its rejected app submissions increased by more than 55 per cent and it increased

app suspensions by more than 66 per cent. The company said in 2018 it rejected or removed "tens of thousands of apps" that didn't comply with the app store's policies related to user data and privacy.

"These increases can be attributed to our continued efforts to tighten policies to reduce the number of harmful apps on the Play Store, as well as our investments in automated protections and human review processes that play critical roles in identifying and enforcing on bad apps," said the Google post.

Shipley said Apple devices are safer.



Cybersecurity experts say people should equip their cellphones with antivirus software to help protect against malware. (CBC)

"If you are an iOS user, you are in a little better shape because Apple has a lot more control over their hardware and software and they do a better job vetting stuff," he said. "That being said, there has still been malware that slips in there."

Dehghantanha said there's room for Apple and Google to improve,

but he said the malware getting into app stores these days is complex and well crafted.

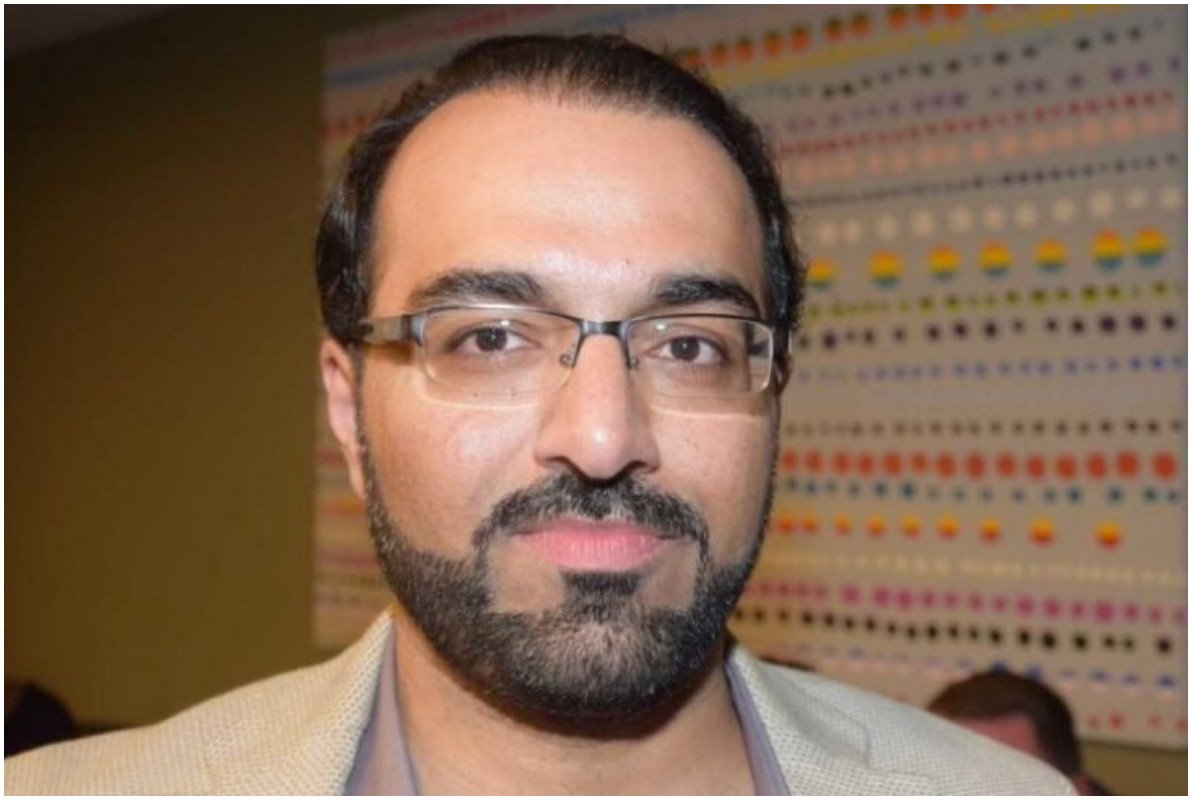
"Both Google and Apple are doing quite a fantastic job considering the scale and the size of apps that they are monitoring," said Dehghantanha.

## Stricter laws needed, says professor

But Shipley wouldn't praise the companies that much.

"Until Canadian laws catch up to actually have better consumer protection and privacy rights for Canadians, like they have in Europe, there's no real financial incentive for them to do so," he said.

Shipley said it's difficult to hold companies accountable for damages after malware tears through a cellphone because the terms of service for using the device say the companies aren't liable.

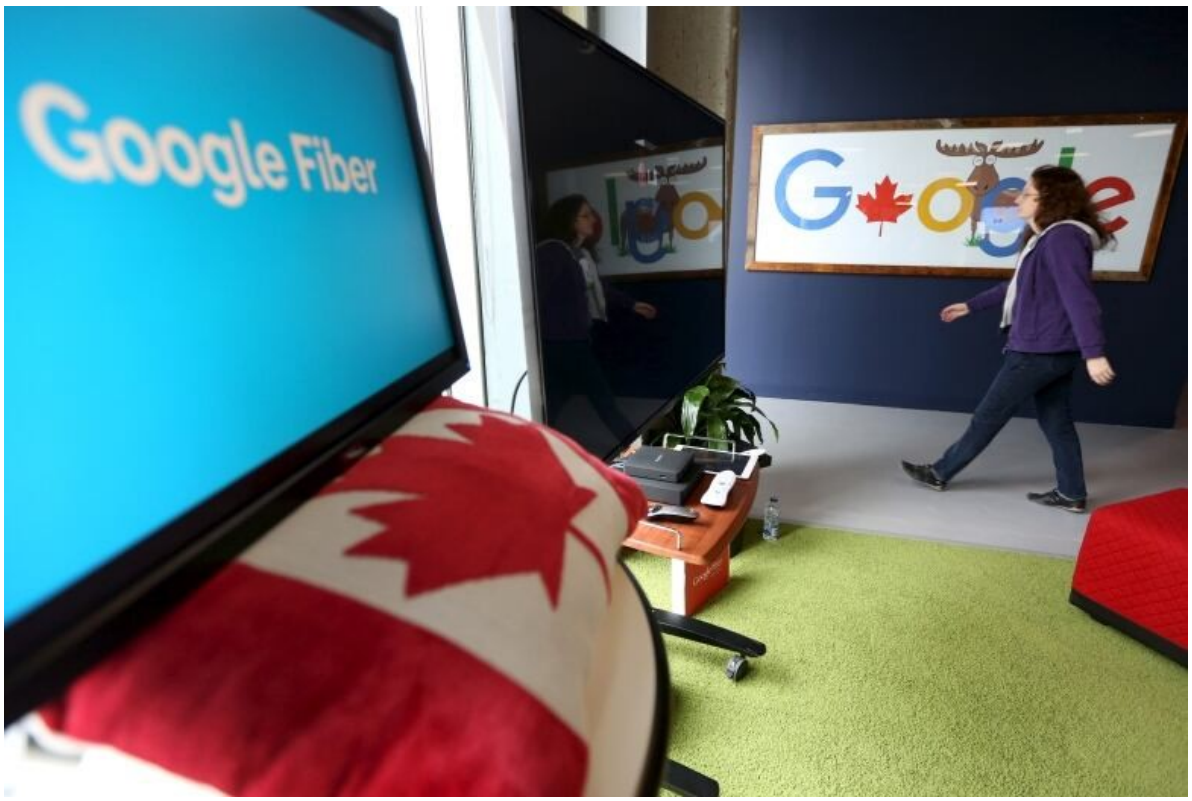


Ali Dehghantanha is the director of the Cyber Security Lab at the University of Guelph. (University of Guelph)

"They don't really face many consequences if malware gets on your phone from the app store," he said.

Canadians can protect themselves by installing antvirus software on their cellphones.

Lashkari said people should avoid downloading apps that have free and pay versions available, especially if the free version has exactly the same features as the one you buy. He said it's likely the free version has been compromised by malware.




Google's Canadian engineering headquarters in Kitchener-Waterloo, Ont. (Peter Power/Reuters)

Dehghantanha said before installing an app, people should think about what systems the app is asking for access to. For example, if a calculator program wants access to your camera, location

services and contacts, people should ask why.

"That would prevent many issues," he said.

Dehghantanha said some app developers will initially ask for all access so they can later make the app malicious.

He said people should pay attention to apps that continuously crash or have technical problems because that can indicate they have become malware.

An aerial view of the new Apple headquarters on April 28, 2017, in Cupertino, Calif. (Justin Sullivan/Getty Images)

Lashkari said people should also back up their cellphones so they have access to important information in case their phone becomes locked by ransomware.

Shipley said a phone's operating system needs to be kept up to date because updates often contain important security fixes. As well, users should never accept messages from unknown people

or click on suspicious links.

"A lot of people think that cybercrime is something that happens to big organizations, governments, somebody else. It happens to a lot of everyday people," said Shipley.

"It's incredibly lucrative to do these kinds of crimes and more and more people with just average skills are engaging in cybercrime, so be careful, you can be a target."

**MORE TOP STORIES**