5 Warning Signs of Malicious Apps - How To Get Rid of Them

Korin Miller

Malicious apps can be a big problem, and one you definitely want to avoid.
You download apps to your devices for a slew of reasons — to listen to music, do online shopping, check the weather and more. But malicious apps **can be secretly installed without you realizing it, and that can be dangerous for your personal information.** Norton recently revealed that hundreds of malicious apps that contain a specific type of malware called ***Dresscode*** are showing up at the Google Play store. **Dresscode is specially designed software that can infiltrate networks and steal your data**. It can even sign you up for spam email campaigns and infect other devices on your home network, causing issues for your computer, your tablet and your phone.

Basically, malicious apps can be a big problem, and one you definitely want to avoid.
One way to fend off malicious apps is to invest in powerful software like Norton Security Online — a leader in cybersecurity. One account can help protect up to five mobile devices from all kinds of cyber threats. Once it's downloaded, the software **helps find and get rid of existing malware, along with warding off future attempted attacks in real time**. It even helps shield your personal and financial data, and blocks malware that's created to steal your identity and, ultimately, your money.

Malicious apps are a type of malware that gets secretly installed on your device.
What exactly are they and how can you tell if you have these apps on your devices.
Cybersecurity experts break it down.

What are malicious apps?

Malicious apps are software or code that's specially designed to do something bad with your information or to your devices — and sometimes both. Malicious apps are a type of malware, which are viruses, spyware, ransomware and other unwanted software, that gets secretly installed on your device, according to the Federal Trade Commission (FTC). **Once malware is on your device, criminals can steal your sensitive information**, send you unwanted or inappropriate ads and make you vulnerable to even more issues.

What are the signs you have malicious apps?

There are certain clues that can tip you off that you have malware:

- **Ad pop-ups**. This is the most common sign, tech and cybersecurity expert Chuck Brooks, president of Brooks Consulting International, tells Yahoo Life. "This could be installed from adware or perhaps something more nefarious such as a Trojan horse," he says.

- **Slow operations**. You may notice this from apps you know are legitimate, Brooks says.

- **Shorter battery life**. When your battery suddenly isn't lasting like it used to, this can be a "telltale sign" of malicious apps, Brooks says.

- **Low levels of data**. If you notice that any of your applications are consuming "abnormal amounts of data," it could be a sign of a malicious app, Brooks says.

- **A new app you didn't authorize**. Notice a new app on your device that you're not familiar with? "It may be a sign that you have been breached," Brooks says.

How to get rid of malicious apps

"If you suspect that your device is running a malicious app, run mobile anti-malware software and remove any apps that you do not recognize," cybersecurity expert Joseph Steinberg, tells Yahoo Life.
(A good option: Norton Security Online, which is specifically designed to help hunt down and take out malware.)

If possible, Steinberg suggests wiping your device, restoring the factory settings and re-installing your go-to apps from trusted app stores. "Obviously, use Internet security software on your device going forward," Steinberg says.

Brooks says you shouldn't try to handle this alone if you're having a hard time removing suspicious apps. "**Unfortunately, if hackers have planted a malicious app, they can give themselves administrator privileges — meaning the app will not easily delete**," he says. "If this is the case, reach out to an IT or cybersecurity professional as soon as possible."

Going forward, keep this in mind, says Steinberg: "You should not install apps from anywhere other than trusted sources, such as the Google, Apple, or Amazon app stores, or the official app store of the vendor of your device." Sometimes malicious apps do make it into these stores, though, which is **why you should pay attention to how long an app has been in the store, how many people have downloaded it and what the reviews show**, he says. "Of course, fraudsters can manipulate such factors — but, often, they don’t expend the efforts to do so," Steinberg says.

Read more:

- What is spyware — and how can you protect yourself?
- Is identity theft protection worth it? Cyber security experts weigh in
- How to delete cookies from your computer—and why it matters