SAINT ROSE OF LIMA
CATHOLIC SCHOOL
SIMI VALLEY, CALIFORNIA
OFFICE: 805-526-5304 FAX: 526-0939 EMAIL: OFFICE@SRLS.ORG

iPad Safety

The information age has brought its fair share of headaches, including viruses, malware, trojan horses, worms, spyware and dozens of other hacks that can expose your private information or simply infect your data. However, the iPad does a great job of combating viruses, malware, and the dark side of the Internet.

If you see a message on your iPad saying you have a virus, don't panic. **There are no known viruses that target the iPad.** In fact, *a virus may never exist for the iPad*.

In a technical sense, a virus is a piece of code that replicates itself by creating a copy within another piece of software on your computer. But iOS doesn't allow one piece of software direct access to the files in another piece of software, preventing any would-be virus from replicating.

If you visit a website and see a message pop up informing you that your device is infected by a virus, you should immediately exit the web site. This is a well-known scam that attempts to install malware on your device under the guise of helping your device become more secure.

An iPad Virus May Not Exist, But That Doesn't Mean You Are Out of the Danger Zone!

While it may not be possible to write a true virus for the iPad, malware – which is simply a term for apps that have bad intentions, such as tricking you into giving up your passwords – *can* exist on the iPad. Luckily, there is one major obstacle malware must overcome in order to get installed on your iPad: the App Store.

One of the great benefits of owning an iPad is that Apple checks every app that is submitted to the App Store. In fact, it takes several days for an iPad to go from a submission to a published app. It is possible to sneak malware through the app store, but this is rare. In these cases, the app is usually caught within a few days or a few weeks and is quickly removed from the store.

But while rare, this means you should still be a little vigilant. This is especially true if an app asks for financial information such as credit cards or other personal information. It is one thing for the Amazon app to ask for this type of information and quite another when it comes from an app you'd never heard of before and downloaded on a whim while browsing the App Store.

The Best Protection Is an Updated iPad

Have you ever wondered why Apple seems so focused on keeping us updated with the latest version of the operating system? While it might sometimes seem annoying how often Apple will pop up a message telling us a new update is available, the truth is that the easiest route for the dark side of the Internet to use to enter our iPad is through exploiting security holes in the operating system. These issues are often fixed rather quickly by Apple, but you need to keep on top of operating system updates.

Apple has made this rather easy for us. When prompted with a message about a new operating system update, simply tap "Later" and then plug your iPad in before going to bed. The iPad will schedule an update for that night, but it needs to be plugged into a power source (a computer or a wall outlet) to download and run the update.

Do Not Jailbreak Your iPad

There is one big hole that can lead to possible infections of malware: jailbreaking your device. Jailbreaking is the process of removing the protections Apple has in place that restrict you from installing apps anywhere but their App Store.

Normally, an app needs a certificate to download, install and run on your device. It gets this certificate from Apple. Jailbreaking gets around this protection and allows any app to be installed on your iPad.

And if you are thinking that allowing any app to be installed means malware can be installed, you are correct. If you jailbreak your device, you need to be extra careful on what you install on the device.

Luckily, most of us don't jailbreak our iPad. In fact, as the iPad has gained more features, it has become less popular to jailbreak the device. Most of what can be done through apps on Cydia and other third-party stores can now be done with apps downloaded through the official App Store.

Is There an Anti-Virus App for the iPad?

The iOS platform got its first official anti-virus program when VirusBarrier went on sale in the app store, but this anti-virus program is for checking files that may be uploaded to your Mac or PC. McAfee Security exists for the iPad, but it simply locks your files in a secure "vault," it doesn't detect or clean "viruses."

Apps like VirusBarrier are preying on your fear of viruses in hopes that you will install them without reading the fine print. Yes, even McAfee Security is hoping you are scared enough not to realize that there are no known viruses for the iPad and that malware is actually much more difficult to acquire on the iPad than on the PC.

But My iPad Told Me It Has a Virus!

One of the most common scams for the iPad is the iOS Crash Report and variations of it. Phishing is an attempt to trick users into giving up information. In this phishing scam, a website displays a pop-up page that informs the user that iOS has crashed or the iPad has a virus and informs them to call a number. But the people on the other end aren't Apple employees and their main goal is to trick you out of either money or information that can be used to hack into your accounts.

When you receive a message like this, the best course of action is to quit out of the Safari browser and reboot the iPad. If you get this message often, you may want to clear out the cookies and web data stored on your device:

1. **Open Settings**. (Find out how.)
2. **Scroll down** the left-side menu.
3. **Tap Safari**.
4. In the Safari settings, **scroll down and tap Clear History and Website Data**. You will need to confirm this choice. Unfortunately, you will need to enter any saved passwords again, but this is a small price to pay to keep your Safari browser clean and secure.

So Is My iPad Safe?

Just because it is difficult for malware to get on your iPad doesn't mean your iPad is completely safe from all intrusion. Hackers are great at finding ways to either disrupt devices or to find their way inside of devices.

Here are a few things everyone should do with their iPad:

1. Turn on **Find My iPad**. This will allow you to lock the iPad remotely or even erase it completely if it should ever become lost or stolen. *How to Turn on Find My iPad.*
2. Lock your iPad With a **Passcode**. While it may seem like a waste of time to input a 4-digit code every time you want to use your iPad, it is still the best way to keep it secure. *How to Lock your iPad With a Passcode.*
3. Disable **Siri and Notifications** from your lock screen. Did you know Siri can still be accessed by default when your iPad is locked? And, with Siri, anyone can do anything from checking your calendar to setting reminders. You can disable Siri on the lock screen in your iPad's settings. *Learn How to Turn Siri Off on the Lock Screen.*