us.norton.com

5 reasons why general software updates and patches are important

Written by Steve Symanovich for NortonLifeLock

4-5 minutes

Revised Jan. 23, 2021

You're probably no stranger to those little pop-up windows. They tell you software updates are available for your computer, laptop, tablet, or mobile device.

You might be tempted to click on that "Remind me later" button. Don't do it. Or, at least don't put off updating your software for long.

Software updates are important to your digital safety and cyber security.
The sooner you update, the sooner you'll feel confident your device is more secure — until the next update reminder.

Why are software updates so important? There are a lot of reasons. Here are 5 that show why it's important to update software regularly.

1. Software updates do a lot of things

Software updates offer plenty of benefits. It's all about revisions. These might include repairing security holes that have been discovered and fixing or removing computer bugs. Updates can add new features to your devices and remove outdated ones.

While you're at it, it's a good idea to make sure your operating system is running the latest version.

2. Updates help patch security flaws

Hackers love security flaws, also known as software vulnerabilities. A software vulnerability is a security hole or weakness found in a software program or

operating system. Hackers can take advantage of the weakness by writing code to target the vulnerability. The code is packaged into malware — short for malicious software.

An exploit sometimes can infect your computer with no action on your part other than viewing a rogue website, opening a compromised message, or playing infected media.

What happens next? The malware can steal data saved on your device or allow the attacker to gain control over your computer and encrypt your files.

Software updates often include software patches. They cover the security holes to keep hackers out.

3. Software updates help protect your data

You probably keep a lot of documents and personal information on your devices. Your personally identifiable information — from emails to bank account information — is valuable to cybercriminals.

They can use it to commit crimes in your name or sell it on the dark web to enable others to commit crimes. If it's a ransomware attack, they might encrypt your data. You might have to pay a ransom for an encryption key to get it back. Or, worse, you might pay a ransom and not get it back.

Updating your software and operating systems helps keep hackers out.

4. It's not all about you

OK, cyber security is mostly about you, but you've got other people to think about, too. If your device gets a virus, you could pass it on to your friends, family, and business associates. That's why you want to keep your software and systems updated.

A trusted security program such as Norton 360™ can help keep your devices secure. And that can potentially help all those people you interact with online. But it's also important to know anti-virus protection isn't enough to protect your devices against all cyberthreats

5. You deserve the latest and greatest

Updates not only patch security holes, they can also add new features and improve existing ones. You don't want to fall behind the times, right?

In that way, software updates really are all about you. Your software program may get a new shot of stability — no more crashing. Or an update might boost program performance — more speed. You deserve no less.

You could ignore those reminders to update your software, but you might be missing out on a lot, starting with your cyber security.

Another option? If you're still not keen on clicking "Update now," you may be able to configure your devices to update automatically.
If so, your problem is solved.