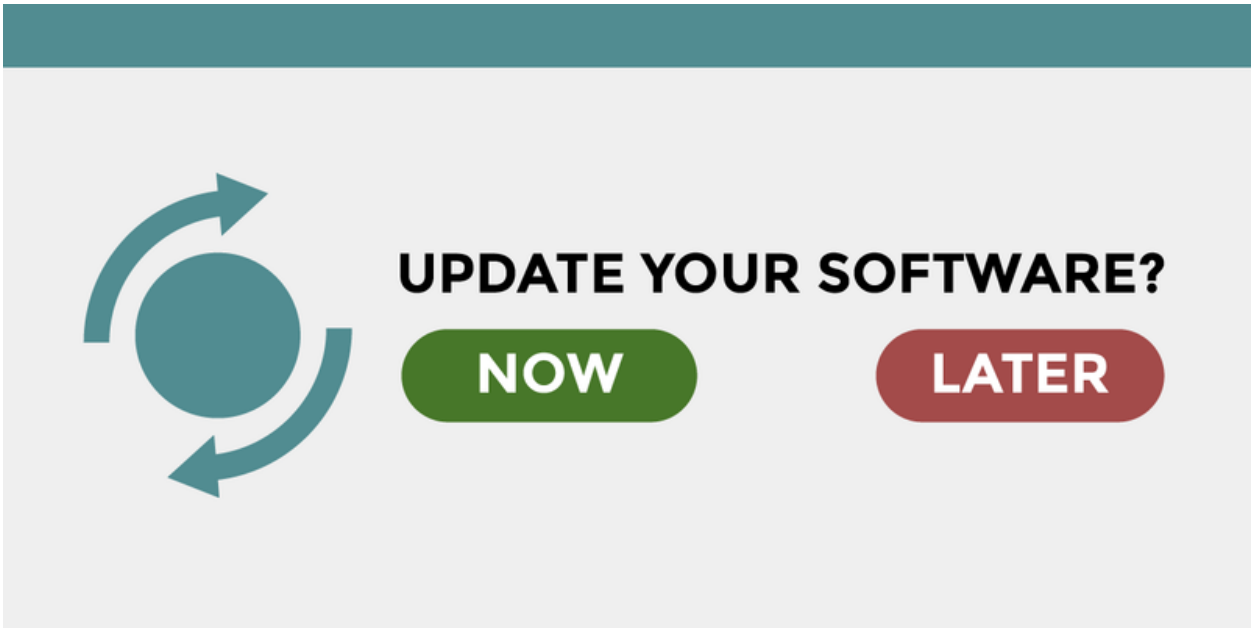
Software Updates and Why They're Important



“Keep your software updated!” is the closest thing we have to security advice that will work for everyone. But the reasoning behind it can be counterintuitive, and even quick updates can intolerably interrupt people’s workflows. Below are several common questions about why it is so important to update one’s software, as well as tips for how to talk about it with people new to digital security.

Updating your software makes you more expensive to hack.

No software is perfect. Programmers make mistakes, best practices get updated, and security problems are discovered over time.

Sometimes, security researchers will discover security bugs and *not* report them to the developer. This kind of bug is called a “zero day” or “0-day,” because the company that could fix it does not know about it and has had “zero days” to address it. These kinds of bugs can be hard to find and expensive to purchase, and are sometimes used in targeted malware or phishing attacks on very high-value targets. Most people do not have to worry about these kinds of bugs.

When you update your software, you are no longer a “target of opportunity” for cheap attacks that try to catch people running out-of-date software.

More often, it will be amateur or professional security researchers, academics, or employees at the company itself who discover such problems, and report them back to the developers to get fixed. When that’s the case, the company can release updates (also known as “patches”) to correct the problem. If you update your software as soon as that pesky “Update!” notification pops up, you are staying current with the best available protections.

But what happens if you *don’t* update your software immediately? Once a company releases a security update to fix a bug, the bug is somewhat “old news.” It may be commonly known and understood in the security research community, or, over time, people will be able to reverse-engineer the security update to figure out the details of the

bug. Unlike a “zero day,” these bugs are easy to learn about and cheap—or free—to buy exploits for. They are often used in broad phishing and malware schemes to target people who have devices with out-of-date software on them.

When you update your software, you are no longer a “target of opportunity” for cheap attacks that try to catch people running out-of-date software.

“But the update might break my software or include new features that I don’t like!”

This is a valid concern. Although it’s a best practice to separate security updates from updates that include new features and other changes, not all vendors and companies do so consistently.

However, if your software needs a security update, it is *already broken*. A problem has been found, and the update is there to address it. Updating takes you from software that is definitely broken to software that has a lower likelihood of breaking.

“But you just told me *not* to click on urgent-sounding messages so I don’t get phished!”

This is where the advice to update one’s software is at its most counter-intuitive. People are told to scrutinize unsolicited links or pop-ups and avoid clicking them if possible—but then told to always, without fail, click on particular kind of unsolicited pop-up!

Here it’s important to consider context and trade-offs. First, the context: an update will never show up in your email, texts, or other messages. It will generally be a system notification, which will look like a notification on your phone, or a stylized pop-up on your device or inside an app. If something doesn’t look quite right to you, you can investigate the operating system or app to find out what version you are running and compare it to the most recent version listed on their website.

And now the trade-off: we can’t rule out the possibility of a malicious bug pretending to be a normal software update. However, that kind of attack is quite rare compared to other kinds of things a normal user might encounter. That slim possibility should not deter you from updating your software. For every attack that might try to look like a security update, there are one hundred attacks that will take advantage of you not updating your software.

By keeping your software up to date at all times, you’re staying one step ahead of all but the most advanced threats.