The Power of Updating

Overview

Cyber attackers are constantly looking for and finding new vulnerabilities in the software you use every day. A vulnerability is a mistake or weakness in how software was developed. This software may run your laptop, the mobile apps on your smartphone, or perhaps even the software in your thermostat. Cyber attackers take advantage of and exploit these software vulnerabilities, allowing them to remotely break into systems, including the ones you use. At the same time, the vendors who create the devices and software are constantly developing new fixes for these vulnerabilities and pushing them out as software updates. One of the best ways you can protect yourself is to ensure that the technologies you use always have these latest updates. These updates not only fix known vulnerabilities, but often add new security features, making it much harder for cyber attackers to hack into your devices.

How Updating Works

When a software vulnerability is known, the developer or vendor will create a software fix for the vulnerability (called a patch) and release the update to the public. Your system then downloads and installs this update, fixing the vulnerabilities. Examples of software you need to update are:

- The operating systems that run your laptop (such as Microsoft Windows or Apple OSX) or run your smartphone (such as Android or iOS)
- Home networking equipment such as your Internet router or Wi-Fi access points or home smart devices such as thermostats, doorbells, home appliances, or security cameras
- Programs that run on your devices, such as your laptop's web browser or your phone's mobile apps

This is why whenever you want to purchase a new device or install a new computer program or mobile app, check first to be sure the vendor is actively updating the program or device. The longer software goes without any updates, the more likely it has vulnerabilities that cyber attackers can exploit. This is why many vendors, such as Microsoft, automatically release new patches every single month.

In addition, if you are no longer using a certain computer program, software, or mobile app, remove it from your system. The less software you have installed, the fewer potential vulnerabilities you have and the more secure you are. Finally, if any of your devices or applications are old and no longer supported by the vendor, we recommend you replace them with newer versions that are actively updated and supported.

How to Update

There are two ways to update your systems.

1. **Manual (the hard way)**: When an update is available, you manually download and install the update. This gives you more control over what and when updates are installed. The disadvantage of manual updates is that it is much more work, as you not only have to track when each of your devices or programs have to be updated, but you must update them manually, which makes it easy to forget to update them.
2. **Automatic (the easy way)**: You enable automatic updating on all of your devices, which means whenever a new patch is released your device automatically downloads and installs it. The advantage of automatic updates is that most of the work is done for you. The disadvantage of automatic updates is the updated program could cause a problem, resulting in the loss of functionality or data. This is rare for personal devices, but can happen for more complex environments, like within large corporations. When you enable automatic updates, be sure to double check your system regularly to ensure the updates are happening.

Of the two approaches, we highly recommend you enable and use automatic updating on all your personal devices. This ensures that all the technologies you are using, from your smartphone and laptop to your baby monitor and door locks, have the latest software. Up-to-date devices and software make it that much harder for any cyber attackers to hack you and your systems.

Guest Editor

Dr. Janell Straach is a faculty member at Rice University where she teaches cybersecurity and artificial intelligence. Janell is Chair of the Board for Women In CyberSecurity (WiCyS). Dr. Straachl can be reached at janell@wicys.org.

Resources

Cyber Digital Spring Cleaning: https://www.sans.org/newsletters/ouch/digital-spring-cleaning-7-simple-steps/
Do I Need Security Software?: https://www.sans.org/newsletters/ouch/security-software/
Emotional Triggers: How Cyber Attackers Trick You: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/