Software updates can be maddeningly inconvenient—and downright disruptive. Prompts pop up right when you need to open an important application like Outlook or Word. Patches install right when you need to log in to a video meeting. Or, worst of all, a system restart rolls out right when you're in the middle of a critical project.

These security patches and updates are necessary, however. Cybercriminals often take advantage of vulnerabilities in older programs to break into your devices or steal your data. So reliable software maintenance and regular updates actually reduce your risk of cyberattacks, identity theft, and privacy breaches.

Take this recent scenario as an example: an accounting firm uses QuickBooks every day for account management, financial management, and employee payroll. Hoping to prevent the inevitable interruptions that come with software updates, the company has declined to upgrade its QuickBooks license for the last two years—saving a little money along the way.

Then, one day, QuickBooks stops working entirely. The business is completely crippled, bringing daily operations to a complete halt. Employees are frustrated that they can't get their regular work done, while the accounting firm's clients who need help are left hanging. After just one day of downtime, the combined costs of lost productivity, lost revenue, and IT assistance far outweigh the recurring cost of the QuickBooks subscription that could have prevented all these problems in the first place.

So how can you protect your business and keep your software updated, without breaking the bank or disrupting regular operations? A trusted partner can help you with the following steps to ensure continued success:

1) Enable automatic updates with the help of an IT provider. Many people are nervous to turn on automated updates, worried that they'll install at the wrong time or go too far in changing the way applications work. But a trusted partner can manage automatic updates for critical software (like operating systems or antivirus protection) and review any updates that require extra attention—all while making sure updates roll out during off-hours when employees won't be interrupted.

2) Rely on the subscription-based Software-as-a-Service (SaaS) model. This format is most commonly used with popular software suites like Microsoft Office 365 or Adobe Creative Cloud. Important applications like Excel, PowerPoint, or Photoshop are installed on your computer but then receive regular maintenance, trusted support, and frequent version control from cloud-based connections that are always on and running in the background. Many businesses looking to save a few bucks download their apps this way before falling behind on maintenance plans or forgetting to pay subscription fees. In the long run, this can lead to bigger problems like lost functionality or steep costs to restore access.

3) Balance the desire for something new with the need for security enhancements. Software and hardware companies love to push fresh versions of their apps or devices, always promising that "the new" is better than the old. But smart IT providers and tech support partners always recommend waiting before installing and upgrading, especially if the main desire is just to be an early adopter. If the latest software or newest device includes a critical security fix or privacy enhancement, however, it might be smart to upgrade quickly—even if you've never been hacked before. That's a situation where the extra knowledge of a trusted IT partner like CMIT Solutions can pay big dividends for small and medium-sized businesses.

4) Routers and hardware deserve attention, too. Most of us set up our Wi-Fi router once and never think of it again (unless, of course, we forget the password). But since routers serve as the front door to all Internet traffic flowing to and from your business, it's especially important to keep them up to date with security patches and regular updates. Everything else runs on some kind of firmware or software these days: TVs, speakers, cameras, printers, dishwashers, and even new cars. Think of how important regular connectivity is for each of those items—and then extend that to the PCs, Macs, tablets, and phones that your employees use every day.

5) A proactive partner ties the whole thing together. A proactive approach to software maintenance and security updates ensures uninterrupted use and smooth performance, no matter when, where, or how the device is being used. Just as important is a proactive IT provider to ensure that things run smoothly on the back end so software can be updated at the right time and on the right device. At CMIT Solutions, we work with every client to outline the importance of software updates before problems arise. Many applications can be set up to deliver behind-the-scenes automated alerts to IT technicians so we can quickly address issues and identify software vulnerabilities that may leave your systems exposed.

With 25 years of experience working with every type of operating system, industry software, and hardware vendor under the sun, CMIT Solutions understands that patches and updates make up just one layer of a comprehensive cybersecurity strategy.

Succeeding with this one single layer won't prevent every malicious attack. But it will provide your business with one important step toward safety and security. We take an "It's not if, but when" approach to cybersecurity, preparing our clients' systems in advance for every possible problem so we're ready when they do occur.

Our proactive IT monitoring and maintenance services perform around-the-clock system scans, identifying vulnerabilities and updating applications before hackers can. We protect mission-critical systems and the integrity of your data so that normal operations can continue, even in the face of a cybersecurity issue. If you want to build this kind of resiliency for your data, your devices, and your business, contact CMIT Solutions today.

GO TO CMIT SOLUTIONS FOR MORE INFO AND TIPS