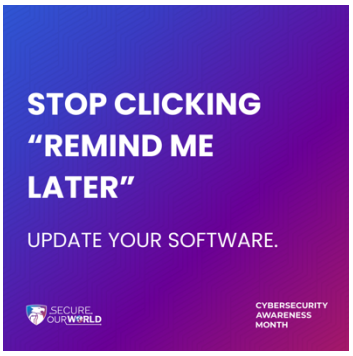
Don’t Hesitate. Automate or Click to Update!

Security updates are the best way to keep our devices protected from cyber threats. While our utility manages updates to workplace-owned devices, it’s up to each of us to keep our personal electronic devices (PC’s, laptops, mobile, home networking, Internet-of-things, applications, etc.) current with the latest “patches.” Even though phishing has become one of the primary cyber threats, malicious actors still seek to exploit technical vulnerabilities – *including old vulnerabilities that have been around for years.*

Security Updates are vital to fixing vulnerabilities and bugs discovered on the devices and software we use. Security updates or “patches” are the way organizations that create devices and software help keep these components from being “hacked.” Security updates are so important that the second Tuesday of each month has been accepted as “**Patch Tuesday**” and is when many organizations regularly release patches for their products. ***Fun Fact: Patch Tuesday has been around for over 20-years. Microsoft introduced Patch Tuesday in October 2003 (after dealing with the Blaster worm) to reduce the cost of distributing patches.***



Old, but not forgotten. If you haven’t always had automatic updates enabled or are using older technology that is no longer supported by the developer, **don’t assume it’s not important to apply older patches or upgrade your technology**. Threat actors know that we have historically been poor in our patching practices, and they do poke around for places to pillage for poorly secured programs and devices – *including workplace and personal* – that haven’t had vendor patches applied.

When it comes to security updates:

- **Automate.** The best option is to set updates to automatic. When security updates are automated, patches are downloaded and installed without user interaction whenever a new one is released. However, while it’s not as common these days, you may have to restart your device for some updates to fully install. It’s best to do this right away, but this can often be scheduled to happen during times when you aren’t using your device, like the middle of the night.
- **Update from the source.** It’s important to install updates as soon as possible to protect your computer, phone, or other digital device against attackers who would take advantage of system vulnerabilities. However, before downloading anything, especially software and application updates, be sure you know the source. Only download software to your computer from verified sources, and only download apps from your mobile device’s official app store. The device, software, or app developer should be sending you updates, not anyone else. And remember, pirated, unlicensed, or unofficial software can often spread malware, viruses, or other cybersecurity nightmares to your devices or network.
- **Don't fall for fakes!** You’ve probably come across suspicious pop-up windows that urgently demand you download a software update. These are especially common on shady websites or if there is malware already on your device. These pop-ups are always fake – they are attempts at phishing and are designed to scare us into clicking without thinking. **Don’t click any buttons on these pop-ups and immediately close your browser.** Many web browsers will warn you if you are attempting to visit an unsecure website address or one that could contain malware. Heed these warnings and don’t take the bait!

Known Exploited Vulnerabilities. While we don’t expect you to keep track of technical vulnerabilities, the Cybersecurity and Infrastructure Security Agency (CISA) maintains a very useful repository to help your network defenders understand which vulnerabilities are being actively exploited by the bad guys. It’s called the “*Known Exploited Vulnerabilities Catalog*” and it currently lists over 1200 vulnerabilities dating back to at least 2002 that we know threat actors are actively exploiting. If you are curious – *and want to feel bad for your IT folks* – you can learn more about it here or take a peek at the catalog here.

CYBERSECURITY AWARENESS MONTH