CYBERSECURITY 101 FOR YOUR EMPLOYEES

UPDATE YOUR SOFTWARE

October is Cybersecurity Awareness month and this theme is “See Yourself In Cyber.” The month is dedicated to personal cybersecurity that we can all benefit from, especially employees who are often the first targets.

Employers should communicate effective cybersecurity hygiene beyond traditional security awareness training programs and each theme this month speaks well to that.

Week 4 is all about the importance of software updates.

WHY IS UPDATING YOUR SOFTWARE IMPORTANT?

While it may seem like an unimportant chore, keeping your devices, systems, apps, and software updated is crucial to minimize the risk of a compromise or vulnerability exposing your organization. Hackers and threat actors are always trying to find ways to get in, so security researchers try to find these vulnerabilities ahead of time in order to develop key fixes.

19,238

The number of critical vulnerabilities released in 2022 (as of September)

35%

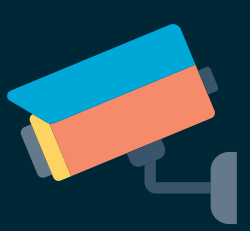
Increase in the number of CVEs released this year compared to 2021

These fixes are provided in the form of updates, and security and IT leaders should have a system and process in place to ensure they’re aware of what needs updating and how to effectively roll out updates.

As more employees work remotely and use their own devices, this makes patch management more challenging. Here’s what you can do.

HOW ORGS CAN DEPLOY EFFECTIVE PATCH MANAGEMENT

Pay attention to CVEs:
You can use a free, searchable resource like CVEdetails.com to make sure you haven’t missed critical vulnerabilities. Major vendors also release updates/patches as part of “Patch Tuesday” so you can plan around these scheduled updates.



Have asset visibility and monitoring systems in place:
To ensure you’re not missing a key update or device that may be outdated, it’s important to invest in monitoring and visibility tools that alert you to all the assets within your environment and may even tell you whether they need updates or not.

Be wary of downtime:
For company-wide updates, make sure you’ve planned in any necessary downtime and worked with the IT team for any mitigation controls or processes that would allow you to rollback updates in cases of errors.

HOW TO COMMUNICATE TO EMPLOYEES

When communicating to employees about software updates including patch management, make it clear that it’s a security/risk concern and that their devices are at risk, not just to the organization but to their own data and privacy. Recommend setting devices and apps to auto-update and consider having a “Patch Tuesday”-like engagement where all employees are encouraged to update their systems and devices on a regular basis.

For critical vulnerabilities or OS-based updates, you may want to send out specified communications to indicate urgency, particularly for any fixes released in response to any zero-day vulnerabilities.

To learn other ways to secure your organization, visit **solcyber.com**

SolCyber

solcyber.com