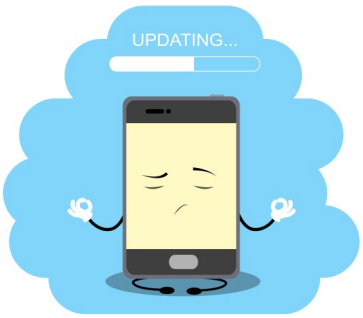
HOW UPDATES SECURE YOUR DEVICE

FEBRUARY 2020 ITSAP.10.096

Updating software addresses vulnerabilities and protects your device. When a software issue or vulnerability is identified, the vendor releases patches to fix bugs, address known vulnerabilities, and improve usability or performance. Although all patches are updates, not all updates are patches. For example, an update may be issued to upgrade software features whereas a patch may be issued to resolve a flaw that would leave you and your organization vulnerable to a data breach. If a vendor issues a patch to resolve a security issue, your organization should take steps to apply it as soon as possible.

WHAT ARE SOME TYPES OF PATCHES?

1. Bug fix patch: Repairs functionality issues in software (e.g. error that causes unexpected device behaviour)
2. Security patch: Addresses security vulnerabilities to protect the system from threats (e.g. malware infecting devices through security flaws)
3. Feature patch: Adds new functions to the software (e.g. enhancements to application performance and speed)



WHAT IS PATCH MANAGEMENT?

Patch management is your strategy and process for acquiring, testing, and installing patches and upgrades on your systems and devices. You can use automated patch management software to ensure your applications and software are kept up to date. The patch management process includes the following actions:

- Identifying when a new patch has become available for your device
- Testing the patch (when possible) to ensure it is compatible with your existing software and environment
- Reviewing additional requirements that may be necessary for the patch to be installed or function as expected
- Sending notifications when patches are available
- Installing the patches

For personal devices, setting up auto-updates is recommended as a form of patch management. Although auto-updating does not test patches, it keeps your device as secure as possible by taking the appropriate measures that are available to you as soon as possible.

ARE TEMPORARY WORKAROUNDS EFFECTIVE?

If an update is not available, you may want to use a temporary workaround to address issues. Workarounds are published by the vendor to disable or restrict access to the vulnerable service. Your IT department should track all temporary workarounds to ensure patches are downloaded to overlay and support each other (rather than workarounds overlapping each other). Workarounds are not a permanent solution. Once the patch is made available, you should apply it as soon as possible and the temporary workaround should be removed.

WHAT ARE THE RISKS TO NOT PATCHING?

Postponing or ignoring updates and patches can increase your organization's level of risk. Some of the risks include the following examples:

- System lags or crashes during use
- Unresponsive applications
- Vulnerabilities that are exploited to infect devices with malware
- Hackers gaining access to your sensitive information
- Inaccessible features on applications

WHAT ARE THE RISKS ASSOCIATED WITH PATCHING?

We highly recommend that you install patches and updates to ensure the ongoing, positive functionality and security of your systems and devices. However, there are some risks to be aware of when applying patches and updates. Some of these risks include the following examples:

- Installing a patch can interfere with the functions in other applications
- Rebooting devices for updates might interrupt other programs, resulting in loss of data or disruption of service
- Installing patches may reveal other issues with the program, including other security flaws (i.e. patching should be approached as a continual process for your organizations IT operations)

To avoid these risks, you should review and test patches before implementing them.

It is understandable that downloading patches may interfere with the functionality of your device (e.g. scheduled time for reboot). We strongly recommend that security patches be updated as regularly as possible, to ensure the safety of your device.

WHAT IF MY DEVICE IS UNSUPPORTED?

Unsupported devices are devices for which vendors no longer issue updates or patches. Legacy and unsupported devices are susceptible to vulnerabilities that will never be patched, which increases your organization's level of risk. We recommend that you ensure to replace systems and devices when the manufacturer no longer provides software support.

TOP 4 TIPS TO REMEMBER

1. Patching ensures the ongoing functionality and security of devices
2. Using a patch management system can help your organization keep devices and applications up to date
3. Testing and examining all patches before installing them is an important step in your patch management process
4. Using devices that are supported by the manufacturer ensures that your systems are patched and updated as necessary

Need help or have questions? Want to stay up to date and find out more on all things cyber security? Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**