

Managing OS Updates

What Are 'OS Updates'?

Microsoft (or any other Operating System Provider) regularly releases updates (or **patches**) for its products. Some of these are trivial; some of them only for specific users, but a large number of them are fixes for serious security flaws. At longer intervals, Microsoft collects all the updates together and releases a **Service Pack**, which greatly reduces the number of patches that need to be applied to a new or rebuilt computer. These Service Packs usually contain other, less critical patches, and should be applied to ensure your computer is as stable and secure as possible.

You may hear “horror stories” about patches or Service Packs that cause problems worse than the issues they are supposed to fix. This does happen, but not very often. The risk of leaving your computer un-patched is **far greater than the risk of applying the updates**. In almost all cases, even if the update causes a problem, it can be uninstalled until a resolution is found.

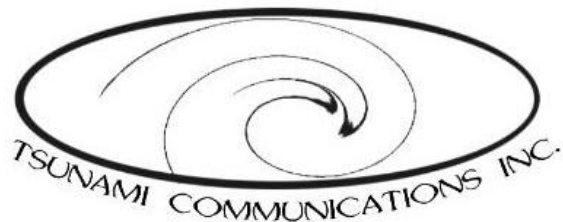
Why Should You Update?

In most cases, these flaws can allow strangers to have full access to your computers: either to disrupt your use of them, or more often, to allow your computers to be used for illegal/unethical purposes. A large portion of the Spam (unsolicited email) that fills your inbox is sent using individuals' computers that have been taken over specifically to hide the real senders, and make it difficult to block the unwanted messages. Others use infected machines to distribute music, movies, or other files, possibly causing your computer to break the law without your knowledge. Some individuals have only found out about this after receiving “cease and desist” letters from copyright holders.

Who Needs Updates and How Often?

If you never connect to the Internet, then you never need to worry about updates. However, even if you only use a dial-up connection, Security Updates should be a regular part of maintaining your system. Microsoft generally releases patches only once per month, but if a serious enough flaw is discovered, they will release the update as soon as they have a fix for it. You should check for updates at least once per week, and if you hear of an exploit (a worm or virus), check immediately to ensure that you are up to date. An un-patched computer will generally be infected within minutes of being directly connected to the Internet.

Everyone who owns, manages, or uses a computer should be aware of the need for updates. In a company, the IT department should have a process in place not only to apply patches, but to scan for missing patches as well. If you or your company do not have a process in place, you need to change that now. For individuals, the simplest option is to enable the AutoUpdate feature (in Windows 2000 and XP), or visit the Windows Update Website regularly.



Where Can I Get Updates and How Do I Apply Them?

Patches can be applied to your system in a number of ways; the most common is by visiting windowsupdate.microsoft.com, and allowing the web site to scan your computer. If you have enabled AutoUpdate, you will be notified of updates by a “globe” icon in the System Tray (next to the clock on your task bar). In corporate environments, the distribution of patches should be automated – either by using the free MS Software Update Services (www.microsoft.com/sus), or with a commercial product, such as Shavlik Software’s HFNetCheckPro (www.shavlik.com). In either case, the system must be managed on a regular basis to ensure that machines are as up-to-date as possible.

Remember that no Microsoft updates (or any other software updates) will be sent as email attachments – many people have been tricked into installing an “update” only to realize later that it was a virus or worm.

For more detailed information on how to protect your corporate environment, please contact Tsunami (contact@tsunami.ca).

This document is provided for general information and educational purposes only and is not intended to replace professional advice and services or the maintenance of any systems. In no event will Tsunami Communications Inc. be held liable for any decision made or action taken in reliance upon the information provided through this web site or any published documents.