Office of the Chief Information Security Officer
Risk Advisory: Update & Patch

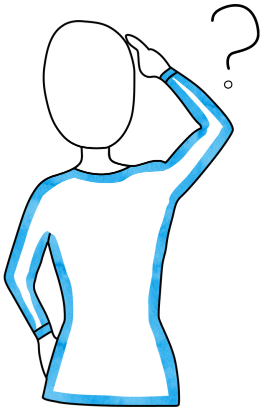
BACKGROUND

The majority of data breaches and incidents involving malware infections occur because of out-of-date applications or unpatched operating system (OS) vulnerabilities. Maintaining a current patch level for your personal or UW-owned desktop computer, laptops, and other devices is critical in maintaining the privacy and security of your personal and UW's institutional information.

EVALUATE

Patching is sometimes easier said than done. For UW-owned devices or personally owned devices used to access UW systems and data, identify who is responsible for patching the operating system and applications. The accountable person — whether it is you, your departmental IT support person, or a third party — should carefully evaluate the following when implementing a patching strategy:

- Is the technology or application too old to be patched?
- If your system cannot be patched, can it be updated?
- Is there a risk associated with patching? For example, will patching break the system (e.g. make the system not work, decrease functionality)?
- Do you have an obligation (grant, contract, law, or regulation) that requires you to patch your system in order to protect the data on the system?



THINGS TO DO

See the Information Security Guideline for more information. Below is a non-inclusive list of resource for patching. Consult with your IT support person or the vendor for specifics on how to patch your technology or applications.

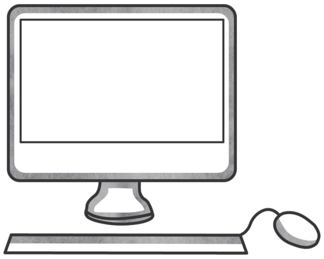
Office of the Chief Information Security Officer
Risk Advisory: Update & Patch

Please note that the list of operating systems, applications, browsers, and associated programs on this page is not exhaustive. It is important to run regular checks on any other applications running on your computer or device as well.

YOUR OPERATING SYSTEMS

For instructions on updating your computer's OS, click the appropriate link below:

Windows
MAC
Linux



ADOBE, JAVA AND OTHER SOFTWARE

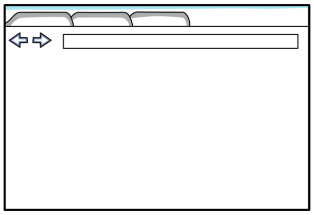
Many of the malware exploits in recent years have involved old versions of Adobe and Java products. You can check to see if you are running and up-to-date version and/or download the latest version by clicking on the links below:

Adobe
Java
Secunia Personal Software Inspector may be used to check other applications (PCs only).

BROWSERS

Check to see if your browser is up to date:

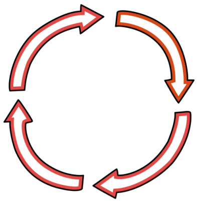
Browse Happy



PATCH TUESDAY

On the second Tuesday of each month, Microsoft and Adobe release security patches for their products. Oracle releases patches for Java and other software quarterly on the Tuesday closest to the 17th of each month

- Microsoft
- Adobe
- Oracle
- More Information



PLUG-INS

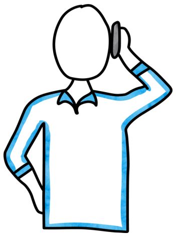
Check browser plug-ins:

- Qualys Browser Check

Some browsers check automatically for plug-in updates, but this functionality may not be enabled by default. Check your browser preferences for activation.

MOBILE DEVICES

For updates on mobile devices, such as Android, iPhone, and iPad, check with the vendor. For applications on mobile devices, regularly check for updates.



ANTI-VIRUS SOFTWARE

Even on an updated and patched system, malware infections may occur. It is always important to keep up-to-date anti-virus software on your machines and devices.

- Sophos Anti-Virus for UW Community
- Sophos Mobile Security (free)