The Fulcrum Group, Inc.
(817) 337-0300

How To Reduce IT Risk While Still Running Windows XP

This White Paper is brought to you by your friends at The Fulcrum Group, Inc.

The Fulcrum Group, Inc. 5600 Egg Farm Rd., Suite 452, Fort Worth TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro

If You Still Run Now-Unsupported Windows XP Systems…

We've alerted our clients of the security deficits which may have already befallen their systems if they are still running Windows XP and Office 2003. The deadline for Microsoft's End of Support (or,"XPocalypse" as some have coined it) for those applications (April 8th) has come and gone. If your systems are still running XP PCs, your business is at risk for security flaws that will be unattended to by Microsoft.

For the safety and security of your business systems we recommend upgrading any Windows XP PCs to those currently supported by the manufacturer. In the meantime, we've compiled some tips for you to help mitigate the risks, in the case your Windows XP systems have not yet settled into comfortable retirement.

8 Tips To Help Mitigate Risks To Your Windows XP Systems

Some things you can do to help protect your systems until you can upgrade include:

1. *Replace XP PCs with Windows 8 or Windows 7 PCs.*
   Your best option is to simply retire all Windows XP PCs and **replace them with Windows 7 or Windows 8 PCs**. Windows 7 may be a good option to help avoid end-user confusion. The Windows 7 interface is comparable to Windows XP, and has a feature called **Windows XP mode** to run custom applications that require Windows XP.

If it isn't possible to retire all of your Windows XP PCs, these tips will also help you mitigate the risks in keeping Windows XP around.

2. *Be sure you've applied the last security update.*
   Businesses running the software past the April 8 deadline should ensure that the final update is applied.

3. Be mindful of your browsers.
   Security experts recommend that end users use the **Google Chrome or Mozilla Firefox** browsers rather than Internet Explorer, because cybercriminals are more likely to target the Microsoft browser running on Windows XP past the operating system's retirement date. Google and Mozilla will support Chrome and Firefox on Windows XP through 2015. Disable or uninstall browser plugins and set browsers to "always ask" when opening files, such as Adobe PDFs.

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5600 Egg Farm Rd., Suite 452, Fort Worth TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro

4. *Run Windows XP In A Virtual Machine.*
   A virtual machine can actually improve security. For some firms, client-based virtual machine workstations are a migration option. It gives IT more control and bolsters security by spinning up virtual instances for end users that can be quickly terminated if a threat is detected.

5. *Continue to run your Antivirus*
   Antivirus remains a valuable layer of protection. It will be critical for businesses to ensure that endpoint systems still running Windows XP past April 8 are running antivirus software, and that it is fully updated with the latest malware signatures. **Nearly all the top antivirus vendors will continue to provide anti-malware support for Windows XP PCs**. The software should be configured to provide the maximum level of protection on end-user systems.

6. *Update & Lockdown Microsoft Office*
   If Windows XP systems have Microsoft Office installed, ensure that the software is fully patched. Microsoft said it was also ending support for Office 2003. In its latest threat report, the firm advises businesses to **lock down the security options tightly in Office**. The ubiquitous Flash software will run by default if embedded in documents, and is often a technique used by cybercriminals to exploit vulnerabilities on PCs.

7. *Third Party Software Support*
   Third party applications and browser components are often poorly maintained and contain software vulnerabilities. To lower the risk of a successful attack, we recommend PC owners **uninstall unused software**.

8. *The Best Defense Is Educated End Users and a solid IT strategy.*
   Attackers often target the human element during the first phase. Many phishing messages can be challenging to spot but educated end users will be more suspicious of unsolicited email messages containing links and file attachments, according to security experts.

The Fulcrum Group is your IT Department. Our array of managed services assists businesses of all sizes in aligning IT needs with business strategy. The safety and security of your systems is important to us.

If you would like assistance with updating your Windows XP PCs, feel free to reach out to us sooner rather than later, at info@fulcrumgroup.net .

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5600 Egg Farm Rd., Suite 452, Fort Worth TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro