Upgrade from Windows XP®

Microsoft has stopped issuing updates and patches for bugs in its Windows XP operating system, which was released in 2001 but still remains widely used. Approximately ten percent of government computers are still running on XP, is still installed on over 500 billion PCs and is being used by over a billion people.

Why is it important to upgrade from Windows XP to a newer version?

When Microsoft stops issuing updates and patches it means that people still using the Windows XP operating system will be left open to malicious activity with any new vulnerabilities discovered in the software. Those still on XP and who have not applied available patches leave their systems vulnerable to being used to run botnets or carry out DDoS (Distributed Denial of Service) attacks. These can be damaging because they may render a network resource unavailable for a period of time.

When Microsoft issues a new patch for one of its supported operating systems, hackers can simply reverse engineer the patch to figure out what it was designed to fix. Then armed with that information, they can see if the same vulnerability also exists in Windows XP, which will not be patched. Ultimately, this means that Microsoft will be providing the information needed by hackers to break into Windows XP systems throughout the world.

Tips and Advice

- All Windows XP users should upgrade to newer version as soon as possible.
- If upgrading is not an option at this time, remove any confidential information from that computer and store that data on an external hard drive as quickly as possible. Also, discontinue using Windows XP for any online activity that could put your identity and banking information at risk. This includes online purchases and online banking.

The use of trademarks is not intended to endorse any company, product or service. Trademarks are the property of their registered owners.

Get the lastest information from our website. Scan the QR Code to go directly to this page.