



State of Washington

DEPARTMENT OF FINANCIAL INSTITUTIONS
DIVISION OF BANKS

P.O. Box 41200 • Olympia, Washington 98504-1200
Telephone (360) 902-8704 • TDD (360) 664-8126 • FAX (360) 753-6070 • <http://dfi.wa.gov/banks>

February 24, 2014

All Bank and Trust Company CEOs

Subject: Microsoft Discontinues Support for Windows XP Operating Systems

Dear CEO:

As you are undoubtedly aware, Microsoft is ending its support for the Windows XP operating system after April 8, 2014. What does the end of support mean? According to Microsoft, it means Windows XP users should take action. There will be no new security updates, non-security hotfixes, free or paid assisted support options or online technical content updates after April 8, 2014.

Running Windows XP at your bank after April 8, 2014 may expose it to potential security risks, because unsupported and unpatched computer operating systems are vulnerable to security risks.

On October 7, 2013, the Federal Financial Institutions Examination Council (FFIEC) published a joint statement on the discontinuance of Windows XP. The FFIEC agencies expect financial institutions and their technology service providers to identify, assess, and manage the potential operational risks associated with the discontinuation of XP support to ensure safe and sound operations and to ensure their ability to deliver products and services is not compromised. The FFIEC statement can be downloaded at:

http://ithandbook.ffiec.gov/media/154161/final_ffiec_statement_on_windows_xp.pdf

At this point in time, your institution should have already assessed the potential risks that may threaten the confidentiality, integrity, and availability of information systems associated with continued use of the Windows XP operating system and formulated appropriate mitigating controls. Before April 8, 2014, your institution should:

1. Replace old Windows XP computers with new computers running on a currently supported operating system, or

2. Disconnect any remaining Windows XP computers from the internet and isolate them from your internal network.

In order to mitigate additional XP concerns post April 8, 2014, institutions should ensure they are taking the following steps to:

1. Block staff and volunteers who remotely access the institution's computer network using the Virtual Private Network (VPN) via a computer running Windows XP;
2. Ensure proper online banking authentication is in place to prevent possible fraud by hackers who have gained improper access to an Windows XP computer;
3. Prevent employees from accepting information, data or documents that have been created or stored on a Windows XP personal computer, especially via a thumb drive or other storage device; and
4. Verify that third party service providers have properly addressed the Windows XP concern, including ATM vendors. Management needs to determine that vendors with whom the institution shares member non-public personal information are appropriately addressing this issue to prevent unauthorized access and loss of the information entrusted to them.

We recommend that financial institutions update their customer security awareness program by alerting customers about the discontinuance of Windows XP support and the potential risks that they could be exposed to by continuing to use their computers that run Windows XP. Specifically, institutions should advise customers about the potential risks from cyber-attacks resulting in a compromise of the customer's online banking account. We suggest putting information on your company's website or in its newsletter regarding this concern.

If you have any questions regarding this Bulletin, please contact me at 360-902-8769.

Sincerely,



Susan Dumontet
Chief of Supervision and Enforcement
Division of Banks