Cyber Security for small business: Is your software up to date?

In today's article, we will explore why it is important to keep operating systems (OS), application software and internet browsers up to date. Some of the main reasons are to provide security updates that plug holes in software, bug fixes that provide feature enhancements and minor fixes after the release date.

The world of technology is ever changing and software vendors constantly update their products to keep us safe. The operating systems on our devices usually update themselves — sometimes as if magically, without us noticing; other times, they painfully slow our devices (and us) down.

These updates are necessary for improving some functions, providing a security update or fixing an issue or bug in the software, OS or browser. When a new software version is released, it goes through extensive testing. However, minor flaws are usually found some time after its release. Some of these flaws can be cosmetic, while some can unwittingly provide hackers the opportunity to take advantage of that flaw. This is why software vendors must provide minor updates or security fixes known as 'patches' throughout the year as they find ways to improve your experience and safety.

Browsers are our window to the web and because they interact with the outside world through the internet, they become a potential target for hackers. Your safest bet is to stick to the more popular browsers: Chrome, Safari, Firefox and Internet Explorer. They are set to update automatically and will provide a line of defense against known browser vulnerabilities.

Periodically, your favorite software company will introduce a new version to include features that users have requested. Usually referred to as an upgrade, you don't have to download the latest version if the current feature set continues to meet your needs. For example, as of December 2016, almost 50 percent of Windows users used Windows 7 as their operating system. The latest version of the Windows OS is Windows 10, which comes with new features, a new interface and apps. If you are happy with your current version, there is no reason to move up. You should upgrade if you need one of the new features offered or if there are dependencies that no longer work with your older version, or if the software company no longer supports it.

When your software reaches its end of life, it becomes necessary for you to upgrade machines used for business. For instance, Windows XP reached end of life in 2014 and Microsoft no longer supports it. People who continue to use Windows XP (its user base is reported at 8 percent) will never get a patch or security update and are easy prey for anyone looking to exploit known security vulnerabilities.

OS updates are vital to keeping your machines healthy, secure and up to date. They are integral tools in your arsenal against hackers. You can find out more about keeping your OS up to date by clicking here for mac and here for Windows.

If you have any questions or comments, please reach out to us at info@misits.com or find me on twitter @jmlucien.

Cyber Security para pequeñas empresas: ¿Está actualizado su software?

En el artículo de hoy, exploraremos por qué es importante mantener actualizados los sistemas operativos (SO), el software de aplicación y los navegadores de Internet. Algunas de las razones principales son proporcionar actualizaciones de seguridad que tapen agujeros en software, correcciones de errores que proporcionan mejoras de características y correcciones menores después de la fecha de lanzamiento.

El mundo de la tecnología está cambiando y los vendedores de software constantemente actualizan sus productos para mantenernos seguros. Los sistemas operativos de nuestros dispositivos suelen actualizarse a sí mismos - a veces como si mágicamente, sin que nos demos cuenta; otras veces, ellos dolorosamente retardan nuestros dispositivos (y nosotros) hacia abajo.

Estas actualizaciones son necesarias para mejorar algunas funciones, proporcionar una actualización de seguridad o corregir un problema o error en el software, SO o navegador. Cuando se lanza una nueva versión de software, pasa por extensas pruebas. Sin embargo, los defectos de menor importancia se encuentran generalmente algún tiempo después de su liberación. Algunos de estos defectos pueden ser cosméticos, mientras que algunos pueden, sin saberlo, proporcionar a los piratas informáticos la oportunidad de aprovechar esa falla. Esta es la razón por la que los proveedores de software deben proporcionar pequeñas actualizaciones o soluciones de seguridad conocidas como "parches" a lo largo del año, ya que encuentran maneras de mejorar su experiencia y seguridad.

Los navegadores son nuestra ventana a la web y porque interactúan con el mundo exterior a través de Internet, se convierten en un objetivo potencial para los hackers. Su apuesta más segura es adherirse a los navegadores más populares: Chrome, Safari, Firefox e Internet Explorer. Están configurados para actualizarse automáticamente y proporcionarán una línea de defensa contra vulnerabilidades conocidas del navegador.

Periódicamente, su empresa de software favorita introducirá una nueva versión para incluir las características que los usuarios han solicitado. Por lo general se conoce como una actualización, no tiene que descargar la versión más reciente si el conjunto de funciones actual continúa cubriendo sus necesidades. Por ejemplo, a partir de diciembre de 2016, casi el 50 por ciento de los usuarios de Windows utilizan Windows 7 como su sistema operativo. La última versión del sistema operativo Windows es Windows 10, que viene con nuevas características, una nueva interfaz y aplicaciones. Si está satisfecho con su versión actual, no hay ninguna razón para subir. Debe actualizar si necesita una de las nuevas características ofrecidas o si hay dependencias que ya no funcionan con su versión anterior o si la empresa de software ya no la admite.

Cuando su software llega a su final de la vida, se hace necesario para que usted actualice las máquinas usadas para el negocio. Por ejemplo, Windows XP llegó al final de su vida en 2014 y Microsoft ya no lo soporta. Las personas que continúan utilizando Windows XP (su base de usuarios se informa en un 8 por ciento) nunca obtendrán un parche o actualización de seguridad y son presa fácil para cualquiera que desee explotar vulnerabilidades de seguridad conocidas.

Las actualizaciones del sistema operativo son vitales para mantener sus máquinas sanas, seguras y actualizadas. Son herramientas integrales en su arsenal contra los hackers. Puede

obtener más información sobre cómo mantener actualizado su sistema operativo haciendo clic aquí para mac y aquí para Windows.

Si tiene alguna pregunta o comentario, favor de comunicarse con nosotros en info@misits.com o en twitter @ jmlucien.

Google Translate for Business:Translator ToolkitWebsite TranslatorGlobal Market Finder