Issue 18

November 2007

Page 1 of 2

THE M&H MONITOR

M&H CONSULTING

Benefits of Windows and Microsoft Updates

Adam Gadoury

Out amongst the end-user public, there seems to be a mixed feeling in regards to the cost benefit of doing Windows and Microsoft updates. Many people hear that it can be a bad thing to update Windows. They may hear from a friend that they had an awful experience when they downloaded a Windows update and that all kinds of things went wrong. While Microsoft updates certainly can cause issues, 99% of the time, there are no problems at all. When problems do occur, they can often be resolved very easily. Here is an explanation on how the benefits of keeping Windows updated far outweighs not updating a system.

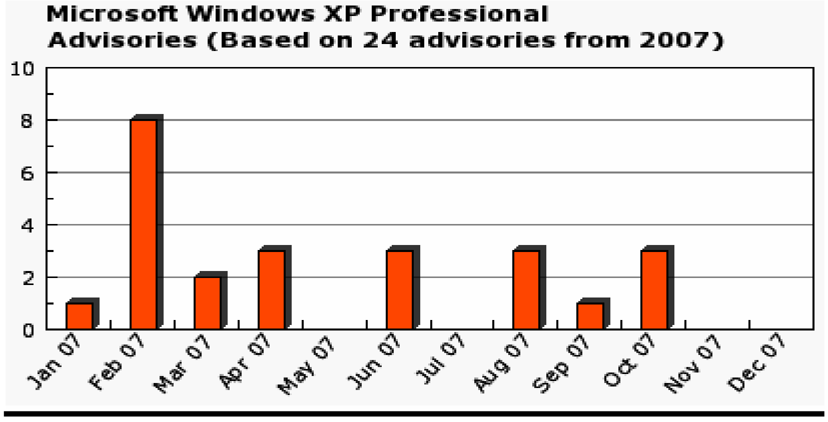
Like locksmiths and burglars, hackers and software manufacturers are engaged in an endless cat and mouse game. Hackers try to find and exploit bugs and loopholes in popular software in order to gain access into people's computers. Developers try to close these loopholes as they are discovered. If passwords are the key to get in a door and the firewall and anti-virus software is your alarm system, installing updates is like making sure that you don't leave any windows open. Essentially, having the best security does nothing if you leave an easy way to get in.

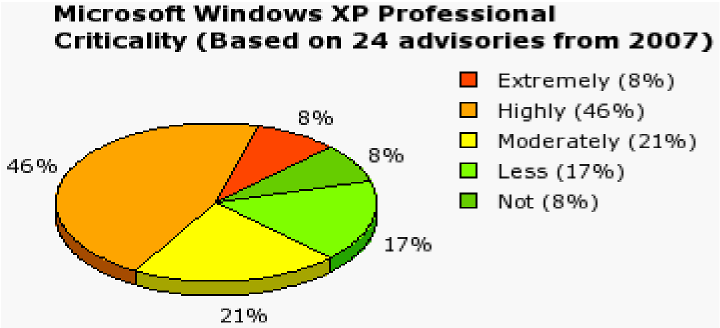
How do these important updates get onto your system? Well rather than distribute a new CD-ROM every time software is updated, software companies distribute updates using download patches or service packs. These updates can be downloaded over the internet.

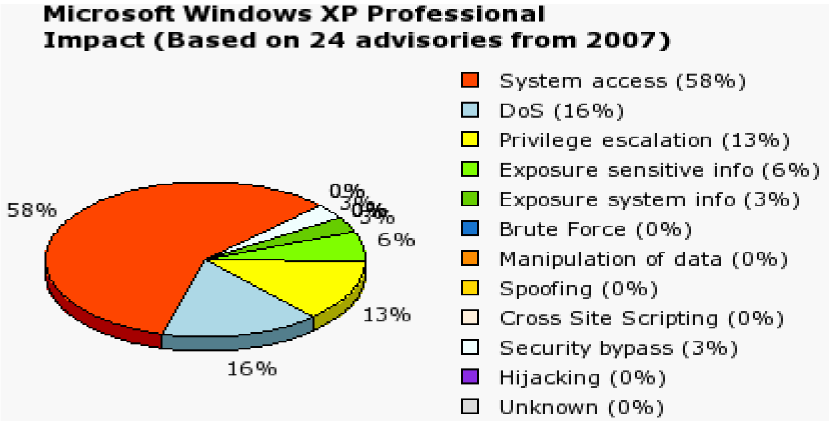
Updating your computer benefits you and your computer by protecting against viruses and hackers, improving performance, fixing bugs, and adding new features to the software. Windows and Microsoft updates must be combined with anti-virus, anti-spyware, and a firewall to be fully effective against all these threats. As new threats emerge, Microsoft updates its Windows operating system and Microsoft Office applications to block them. However, you would need to download the updates regularly to be sure of getting maximum protection. This is why M&H performs Windows updates as well as updating virus definitions and spyware definitions when doing regular maintenance on our clients' computers.

If a person decided not to update Windows they would run the risk of being attacked by many various on-line threats, and they would also lose many beneficial improvements to Windows and Microsoft products. Yes, they may alleviate the 1 in 100 chance of having a bad update but they will then open themselves up to many more problems in the future. If you would like more information on how to ensure your computers are updated regularly, and you are not currently part of our Tech For A Day program, please call us at 866-9MH-Tech.

Inside the Numbers







If you would like to be removed from this newsletter, send an email to info@mhconsults.com with the word remove in the subject line.

Issue 18

November 2007

Page 2 of 2

THE M&H MONITOR

M&H CONSULTING

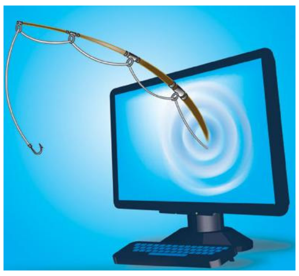
Beware of Phishers

Gavin Mish

Phishing… you may have heard of it before, and never really knew what it meant, but not being aware of how phishing works can cause you a very big headache, not too mention a lot of money. So what is it? Phishing is a cybercrime designed to get as much personal information as possible. By tricking you into giving your social security number, bank login information, or a variety of other personal information, the phishing scammers can open accounts under your name, or even worse, take money from existing accounts.

The most common phishing method is sending an email informing the user of some issue with their account, whether it be a bank account, credit card account, or any other type of financial account. There will often be a link in the email that directs you to a site that looks exactly the same as the website for the real financial institution. It has fields requesting your login information, and upon submitting it, you are not actually logging into your account, but instead you are giving your login credentials to the phishing scammers. Once this has happened, they now have your information, and your accounts are quite compromised. While there are certainly other phishing methods being used, this email method is the most common. This of course leads to the question of "How do I take care to not give my personal information to phishing scammers while still being able to confidently use my accounts online?"

There are a number of means of differentiating between your real financial institute and those being falsified by scammers. The best rule of thumb to remember, is that rarely, if ever, does a real financial institute ask you to fill out personal information via a link from an email. So if you get an email requesting something along those lines, your best bet is to either ignore the email, or call the institution to verify their request and to do it over the phone.



Another good method is to take a look at the web address that the link is going to bring you to. Your internet browser should have a bar on the bottom that shows you the link you will be going to before you click on it. If you are not 100% sure that the link is an authentic one for your financial institution, you should not click on it. Simply clicking on the link could even load "keylogger" software that records your keystrokes for when you eventually login to your real financial institution's website, and then sending that information back to the scammers.

So what do you do if you think you've been "phished"? If at any point you feel an account of yours has been compromised, you should immediately report it to the bank, and freeze or close the account. You should then also report it to a fraud alert agency by going to:

www.consumer.gov/idtheft

While contacting your local police department may seem like a useless endeavor, having the identity theft documented by local law enforcement can go a long way to help you recover funds down the road, so a call to your town's police department would be a good idea.

At M&H Consulting, we try to assist our clients to avoid phishing methods by recommending anti-malware software and anti-spam software that can help detect these scams. While our assistance can improve the chances of avoiding identity theft, the best way and the only guaranteed way to avoid it is by having the end user exercise extreme caution when entering personal information online. If you have any questions about phishing or would like to discuss methods of preventing identity theft, please call us at 866-964-8324.

If you would like to be removed from this newsletter, send an email to info@mhconsults.com with the word remove in the subject line.