Issue 23

October 2008

Page 1 of 2

THE M&H MONITOR

M&H CONSULTING

How can I get a virus if I have Anti-virus Software?

Tim Clarkin

Computer virus infections are still among one of the most common computer problems that can affect a home or business. They cause downtime, threaten data security and integrity, and can be expensive to repair. While it is essential to have valid, working anti-virus software on all PCs in the office, many people operate under the misconception that having this software will prevent any chance of virus infections. In reality, the only way to make sure a computer is 100% virus proof would be to keep it off the internet and not use it.

The first reason why even the best antivirus solutions on the market today can and will occasionally fail is the simple fact that it's impossible to protect against something that has not yet been created. Anti-Virus software uses a variety of detection methods and none is more important than the actual virus definitions. This list of currently known viruses allows the program to immediately identify infected files and prevent them from doing damage. While there are other safeguards in place, these definitions work similar to vaccinations for living beings in that they're effective when they're kept up to date, and they can only protect you from the diseases that are known and specifically made to prevent.

The next logical question is "Why does this antivirus software that I paid money for not know about all viruses?" The main reason is that there are tens of thousands of people creating new viruses across the globe. Unfortunately for the rest of us, these viruses aren't being sent to Anti-Virus companies before being unleashed on the internet. The result is a situation where security software is always playing catch-up with new viruses and new variants.

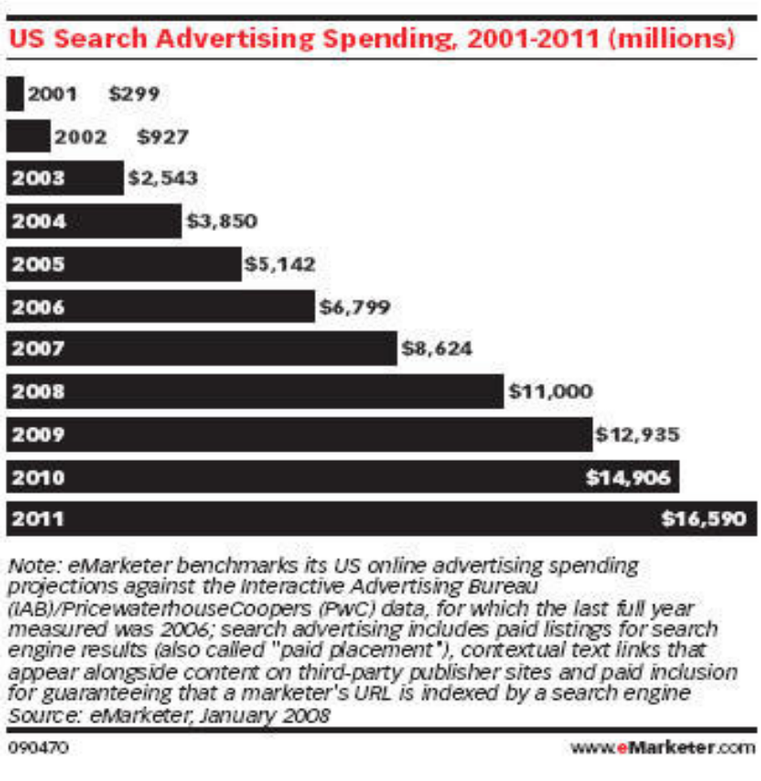
The final reason why computers can still get infected is due to user errors. Having the best security software installed on a workstation will certainly help prevent problems, but it can't protect a user from opening an infected file, or going to a infected website. It is very important that users do not alter any anti-virus settings. Users must also take the extra time to review the address of a link before clicking on it, especially if it is in an email, and ensure that email attachments are legitimate before opening them. Even the best security software can't save users from their own mistakes.

With all this information, you might be wondering if a virus infection is inevitable. It is possible to seriously reduce your risks of a costly infection. You must make sure you use a current Antivirus software solution with a valid subscription that is regularly updating itself. If you're unsure of these details or don't have the time to make sure that every system is up to date, regular Tech for a Day maintenance done by M&H is a great way to make sure the software is fully functional. Remind users that just because there is working security software installed on the computer, it does not mean that their system is immune to infections.

Following these steps can go a long way to ensure that you are well-protected and will have minimal issues with viruses.

Inside the Numbers

eMarketer has released their 2008 search marketing report highlighting user and spending trends. The report paints a very rosy picture for search in the next three / four years with spending doubling from $8 billion last year to a projected $16 billion in 2011. These types of growth numbers clearly indicate we're still in the growth phase of the s-curve. Could the looming recession impact these numbers? You bet. But, it's also likely MORE marketing dollars are poured into search. The savvy marketer will turn the screws on their campaigns and spend their marketing dollars on the most effective marketing channels that have a direct and measurable impact on their business's bottom-line (i.e. search).



Issue 23

October 2008

Page 2 of 2

M&H CONSULTING

THE M&H MONITOR

The Importance of a Strong Password

Adam Gadoury

More often we hear stories of people who have had their accounts hacked or heard about people that have had their infrastructure compromised by someone hacking into their server. Having an easy password is like handing your house keys to a stranger. It is vital that people not make these dangerous mistakes.

Mistake #1: *Using the same password for your accounts.*

Please don't do this. Use different passwords for every email account, and definitely use unique passwords for websites where you'd enter your credit card.

Mistake #2: Using s*hort passwords*.

The risk of someone guessing your password is increasingly difficult the more characters are in it. So, go for the gusto and make your passwords long. It makes it much harder to guess a password that is 10 characters rather than 3 characters.

Mistake #3: *BradPitt, Charlie, Sarah, Princess, Barbie -- Did I guess it?*

Do not use kids' names, pet's names, nick-names, characters in books or celebrity names. Even if I didn't guess it in my list, someone who knows you could.

Mistake #4: *Using easy to remember words.*

Easy to remember is also easy to guess. Passwords should not contain English and Non English words found in a dictionary. Hackers tend to use software that will perform scans of common English words. If your password is "password" or "test" then it's a wonder you haven't been hacked yet!

Mistake #5: *Using numbers.*

Seriously, stay away from birthdays, anniversaries, addresses, social security numbers or telephone numbers. They are all too easy to guess.

Below we will discuss how to create strong and secure passwords.

Think of a sentence that you can remember. This will be the basis of your strong password. Use a memorable sentence; such as "My sister Anne has three kids." You can simply use the first letter of any phrase you can remember. For this example the password could be “MsAhtk”.

Add complexity by mixing uppercase and lowercase letters and numbers as well as symbols. It is valuable to use some letter swapping or misspellings as well. For instance, in the pass phrase above, consider misspelling Anne's name, or substituting the word "three" for the number 3. There are many possible substitutions, and the longer the sentence, the more complex your password can be. Your password might become "M$@h3K."

Test your password with a Password Checker. It can be found at Microsoft’s website at http://www.microsoft.com/protect/yourself/password/checker.mspx

These are just a few ways to create a strong password. After someone has created a strong password it is vital to keep the password secret. Treat your passwords and pass phrases with as much care as the information that they protect. We at M&H always try to create passwords that are easy to remember but also are strong passwords when setting up a client network. We feel your information is invaluable and we want to ensure it is secure. We are willing to check the strength of a password or the overall security in place.