Issue 22

August 2008

Page 1 of 2

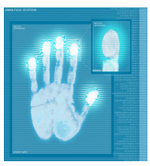
THE M&H MONITOR

M&H CONSULTING

Online Blunders That Threaten Your Identity

Consumer Reports

Many people are turning to the internet for most of their daily tasks, whether it is talking to friends through email, paying bills, shopping, looking for jobs, etc.



What many don't realize is the risk of having your identity stolen by doing so. Below are 7 things that Consumer Reports has found that could lead to you becoming a victim of identity theft.

1. Assuming Your Security Software Is Protecting You. Security software is fully effective only when activated and frequently updated. Last fall, McAfee found that nearly half the users polled who thought their software was protecting them hadn't updated it regularly. **What to do:** Renew the subscription when the software prompts you. Make sure your security software is active when you're online and that it has been updated within the past week .

2. Accessing an Account Through an Email Link. No matter how official an e-mail message looks, trying to access a financial account by clicking on embedded Web links is risky. If the e-mail message is fraudulent, a cybercriminal could use the account number and password you enter to steal your identity or empty your bank account. **What to do:** If an e-mail message asks you to update your account number, or other information, don't take the bait. Access an online account only by using your existing browser bookmark or typing in the institution's Web address.

3. Using a Single Password for All Accounts. 9% of home Internet users who responded to our State of the Net survey said they used a single password for all their accounts. Doing so lets someone who gets your password easy access all your accounts. **What to do:** Using different passwords need not be burdensome. Use variations on one password. A well-crafted password uses a combination of at least eight letters, numbers, or punctuation symbols.

4. Downloading Free Software. You couldn't resist that neat, free utility. Or your teenager couldn't resist those fish-tank screen savers. Now your computer runs more slowly than ever. That's because spyware was probably packaged with the freebies. **What to do:** Download freeware only from reputable sites.

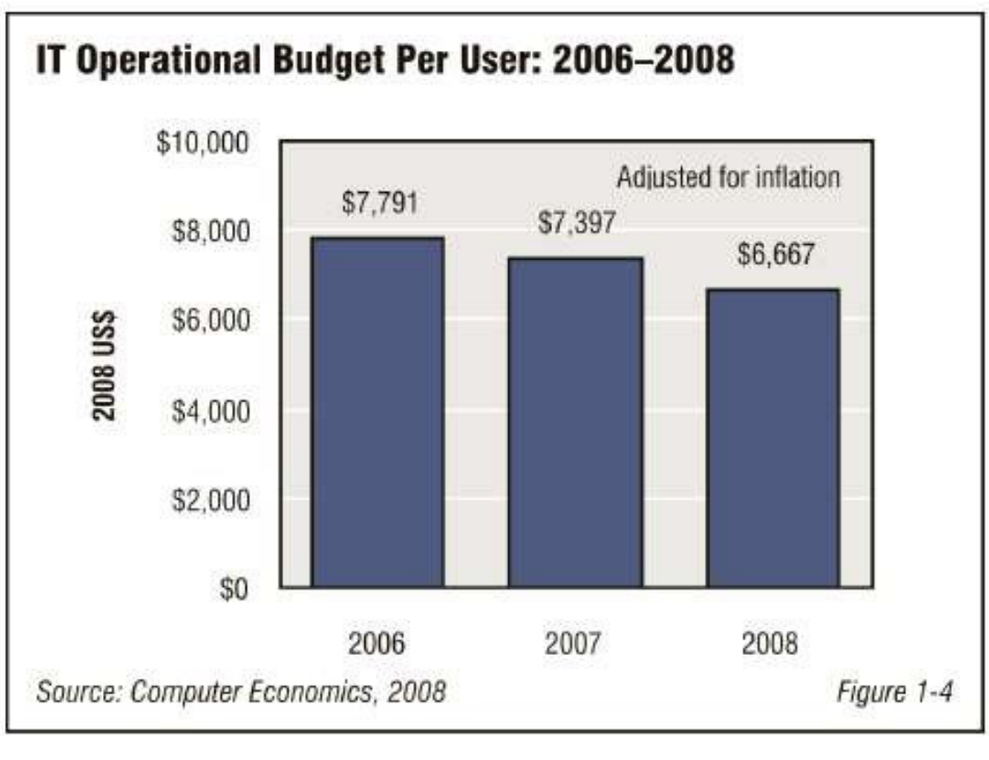
5. Clicking on a Pop-up Ad That Says Your PC Is Insecure. It's easy to click inside the ad by mistake and be transferred to a spyware site or, worse, have malware automatically downloaded onto your computer. **What to do:** When closing a pop-up carefully click on the X on the upper left or right corner, not within the window. To avoid pop-ups altogether, enable your browser's pop-up blocker.

6. Shopping Online the Same Way You Do in Stores. Online shopping has risks that are different than in a walk-in store: You can't always be sure who you're doing business with. **What to do:** Use a separate credit card just for your Internet shopping. Don't use a debit card. Sites that display "https" before their address when you're entering sensitive information and those displaying certification symbols from TRUSTe and other organizations are usually safe.

If you need help or have questions on how to handle any of these topics call **866-9MH-Tech** for help.

Inside the Numbers

Based upon 2008 figures from Computer Economics (www.computereconomics.com), per year IT spending for each user has declined slightly over the past couple of years. In 2007, the average M&H cost for our clients, per user, was $6,299. This cost was 15% less than that of the Computer Economics average IT cost per user of $7,397.



Issue 22

August 2008

Page 2 of 2

THE M&H MONITOR

M&H CONSULTING

Malware: The Next Generation

Robert Demers

As a technical services consulting company servicing a broad range of small to medium sized businesses, M&H Consulting tends to notice the trends that affect this market segment. One trend that is being noticed with alarming frequency is the rise in computers being infected with malware.

What is malware? It is an umbrella term that includes spyware, adware, and other software that invades your system and can install other applications or viruses that are at best annoying, and at worst system crashing. Many antivirus programs do not catch these rogue applications in time – they are written in such a way as to exploit vulnerabilities in the windows operating system and other software in order to bypass the antivirus application and behave like a trusted program. Antivirus protection is a necessity in business computing today; however it may not catch the thousands of new variants created each day.

How can one avoid becoming a victim? The best way to avoid these types of programs is to be very careful of where one surfs on the internet, what links are clicked on, and how updates to browser plug-ins are applied. A user may get an email from what looks like a trusted site - the author, for example, has received many emails from admin@microsoft.com. This email says to click on a link and download an 'upgrade' to some features installed in his web browser. If he were to click on that link, it would bring him to a webpage that could not load and would prompt for the install of a browser plug-in (which of course would infect his PC). For one thing, the author would never get a personal email from the Microsoft.com admin. He is certainly proficient in his technical ability, but a personal email from the administrator of a company and/or website on the scale of Microsoft is as likely as winning the lottery when the jackpot is around $250 million. Other emails may have interesting subjects (IBM going bankrupt, for example) and provide links for the story. This will bring up a page that will prompt for an install to your flash player or something similar, which will then infect your pc. The same may happen from a link clicked in a pop-up window. The longer a PC stays infected, the higher the chance there are other viruses being loaded. This can bring productivity to a screeching halt.

Bottom line: The best line of defense is smart browsing. Do not click on links in an e-mail unless the email was expected. Just like opening an attachment could infect a computer, so can a website these days. Do not click on any pop-up windows that are unsolicited. Also, if an update is needed for software, go directly to that site and do not follow a link from an e-mail. If there is ever any question, hold off on clicking and call M&H Consulting. The link can be verified or an alternative method of contacting the website for whatever is required can be found.