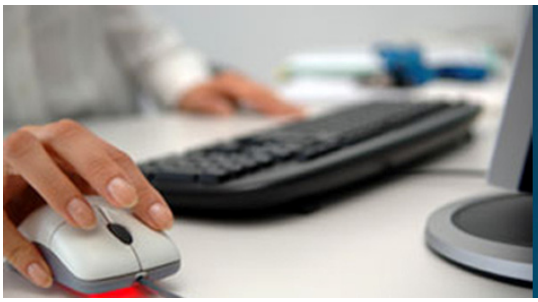

SANS OUCH!
SANS Institute Security Newsletter for Computer Users

May 2010

Get late-breaking security alerts at:

http://www.sans.org/newsletters/ouch/updates/

In This Issue:

- Countdown: Top Ten Computer Myths
- Patches and Updates Roundup

[Editor's Note: (Wyman) What you don't know can hurt you, and there's even greater danger in believing things that aren't true. This month we bust the Top Ten Computer Myths and offer some security tips that won't cost you a lot or take much of your time. And you don't have to be a tech guru to use them.]

Countdown: Top Ten Computer Myths

#10. Viruses and worms are created by sociopathic teenagers.

In days of yore, geeks sometimes went bad and vandalized computers to make a name for themselves. But in those days, if your system got infected it would act wonky, and you knew something was wrong. Today, well-financed, tech-savvy participants in international criminal conspiracies craft malware that keeps infections as quiet as possible for as long as possible so that they can continue making money and taking your money. They build botnets—armies of innocent computers, like yours, that have been hijacked and made to spew out spam or launch denial-of-service attacks. They steal usernames and passwords and credit card numbers by the score and sell them in lots on the black market.

#9. The Internet isn't safe. It's smart to use it as little as possible.

Does the potential for getting the flu prevent you from leaving your house? Have you stopped driving your car because of all the accidents lately? Did you give up hamburgers when Mad Cow Disease was discovered? Not likely. Yes, you can get into trouble using the Internet. The key is to be aware of the real risks and prepare for them so you can enjoy what the Web has to offer. While you can't eliminate all risk in the online world, any more than you can guarantee your safety in the real world, there are steps you can take to shift the odds in your favor.

#8. If it ain't broke, don't fix it.

What if it *is* broken, only you can't tell it is? Tales of woe abound about computer users who've been bitten in the past by applying a recommended patch to a piece of software, only to see that software break or foul up something else on their computers. Sounds like a good argument for skipping patches. There's just one problem. Today, a recommended patch is often, even usually, meant to close a security hole. Not installing it is tantamount to parking your car in a bad neighborhood at 2 a.m. with the windows rolled down.

#7. If my browser displays the locked padlock, the website is secure.
Chances are you've been hearing for years about how that padlock in your browser will keep you safe. But it won't. In fact, it never did. The padlock has to do with securing the *connection* between your computer and the website. Data sent via a secured connection is *encrypted* in both directions, but that does *not* mean the website or your computer is secure.

#6. I can tell a shady website by looking at it.
Not any more. Even websites that look professional and belong to established companies are not immune to the machinations of cybercrooks who hunt for security flaws and insert hidden code that attacks visitors surreptitiously. Case in point: The New York Times website was invaded last September by Bad Guys who smuggled in pop-up ads promoting bogus antivirus software. More insidious is malware implanted on websites that scans your computer quietly for security flaws while you are viewing a page. When it finds one, it dumps malicious software onto your system. This kind of "drive-by-download" can be rigged up on any website—big or small, slick or homely, official or unofficial—at anytime, anywhere in the world.

#5. If I go to a website, and don't do anything while I'm there, I'll be OK, right?
No! If a site or page has been rigged with the right malware, all you have to do is browse to it. If your computer is not protected, that is all a Trojan Downloader needs to get a foothold on your system. A cascade of crud can follow, as that Trojan goes about silently infecting your computer with more malware.

#4. If a friend on Facebook or Twitter posts a link, it's safe.
As Facebook and Twitter have grown in popularity, a swarm of attackers has come along for the ride. These are the same people who have been sending spam and spinning online scams for years. Today, they target social networks because, like con-artists and pickpockets, they follow the crowds. Standard in their bag of dirty tricks are ways to post messages that look like they are from your friends.

#3. If I just view an email message without clicking on any attachments or links, I'll be safe.
Sometimes emails don't pass the "sniff" test, but we figure there's no harm in viewing them just to be sure. Bad idea. There are ways an attacker can launch an email attack that don't require you to click on a link, and these techniques can be just as dangerous as clicking on an infected attachment. Simply opening the email may be enough to confirm that your account is active and that makes your email address more valuable to sell to spammers.

#2. This email sure looks authentic.
Deception in cyberspace is as common as camouflage in nature. Has the Bank of America really placed a hold on your account? The email looks official. It even has the BofA logo. But stop and think. Doesn't your bank call you when there's been suspicious activity on your account? So, call the bank and find out what's up. Have you really overpaid your federal income tax? That email sounds like you are in line to get a gift, but only if you don't know that the IRS *never* communicates with taxpayers by email. Is that Amazon email cancellation notice legitimate? The embedded link promises a quick way to find out. The far safer way is to log into your account as you usually do and check the status of your order. Never use any of the contact information that's provided in the same message. Refer back to trusted information you already have or can get independently.

#1. This email is from someone I know.
How did Aunt Jennifer get stranded in London without any way to get home? Odds are she didn't. Spammers send out emails with forged "From" addresses because they know that a familiar name or address will make you give them a second look. That's the nibble. You may even open it just to make sure

it's not real. Another nibble. Now, what if Aunt Jennifer just happens to be traveling in Europe at the time? The coincidence may prompt you to read the message, perhaps take it seriously, and worst of all, act on it. You've taken the bait. Email messages, like envelopes, can be made to display any "From" address the sender chooses to use.

Tips!

- Remember, crooks are out for money, and they can make money by stealing anything from files to credit card numbers to passwords.
- To ward off drive-by-downloads and other attacks that exploit hidden software flaws, keep your software up-to-date.
- Be on guard against con jobs (a.k.a. social engineering). Double-check any email attachment or download you are not 100% sure about.
- Protect your passwords. If you have to enter one on a risky computer, like at an Internet café or other public place, change it as quickly as possible using a computer you can trust.
- Use a good-quality security suite and keep it updated.

More Information:

- http://www.pcworld.com/article/191999/top_6_security_myths_and_how_to_beat_them.html
- http://www.pcworld.com/article/156374/the_five_most_dangerous_security_myths.html

Patches and Updates Roundup

Operating Systems/Applications
Windows & PC Office: http://update.microsoft.com and http://www.microsoft.com/security/updates/bulletins/201004.aspx

Mac Office: http://www.microsoft.com/mac/help.mspx?CTT=PageView&clr=99-0-0&ep=7&target=ffe35357-8f25-4df8-a0a3-c258526c64ea1033

OS X: http://support.apple.com/kb/HT1338

iPhone/iPod: http://support.apple.com/kb/HT1414

iPod: http://support.apple.com/kb/HT1483

Windows Adobe Reader:
http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows
OS X Adobe Reader:
http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Macintosh

Flash Player: http://get.adobe.com/flashplayer/

Firefox: http://www.mozilla.com/en-US/firefox/update/

Safari: http://www.ehow.com/how_2033324_update-safari.html

Opera: http://www.opera.com/

Chrome: http://googlechromeupdate.com/updates.html

Java: http://www.java.com/en/download/manual.jsp

Windows iTunes: http://www.ehow.com/how_2016273_update-itunes-pc.html

OSX iTunes: http://www.ehow.com/how_2016270_update-itunesmac.html

Security Suites
Symantec: http://service1.symantec.com/SUPPORT/sharedtech.nsf/docid/2002021908382713

Norton:
http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=n95

McAfee: http://www.mcafee.com/apps/downloads/security_updates/dat.asp

Kaspersky: http://www.kaspersky.com/avupdates

AVG: http://free.avg.com/us-en/download-update

Panda: http://www.pandasecurity.com/homeusers/downloads/clients/

PC Tools: http://www.downloadatoz.com/pc-tools-internet-security/smart-update.html

BitDefender: http://www.bitdefender.com/site/view/Desktop-Products-Updates.html

Avast: http://www.avast.com/download-update

Webroot: http://support.webroot.com

Trend Micro: http://esupport.trendmicro.com/Pages/How-to-update-Trend-Micro-Internet-Security-Pro-2010.aspx

Microsoft Security Essentials:
http://www.microsoft.com/security/portal/Definitions/HowToMSE.aspx