The Rochester Computer Society, Inc.
Since 1982

MONITOR

Vol. 30, No. 11 November 2012

Next Meeting
Tuesday, November 13

AVAST ANTIVIRUS 2013

Contents

More Free Utilities to Clean Hijacked PCs

by Ira Wilsker

Hardly a week goes by that I do not get a call from a friend or co-worker asking for help with a computer that had been hijacked by one of the thousands of variants of a type of malware generically known as 'Rogue AntiVirus." Last weekend was busy for me in this respect in that I received multiple frantic calls for help on Friday, Saturday, and Sunday. All of the computers I was asked to clean had been totally hijacked by this rogue antivirus operating under the names "Vista AntiVirus 2012," "Windows 7 Antivirus," and "Micro-soft Antivirus 2012."

While they all had different names, they all had the same modus operandi in that they infected a computer, displayed frequent popup windows alerting the user that the computer was heavily infected with viruses and spyware, offered to repair the problem for a fee, and totally took over the computer by not allowing most other programs to load. Often infecting the

computer via an email from a known acquaintance whose own computer had been hijacked and which sent out spam email with a link that would load the malware, or by visiting a legitimate or rogue website that injects the malware via the web browser, this rogue antivirus software is becoming more dangerous, and more difficult to remove.

As had been written here before, this rogue software generally protects itself from detection and removal by neutralizing the installed security software on the computer, and preventing other detection and repair software from executing. Most of the rogue software also blocks access to many of the websites with removal utilities, and prevents most programs on the computer from running by blocking almost all ".exe" files from opening.

What the user of the infected machine does not often see is that many of these rogue variants also disseminate their code to people whose email addresses are in the user's address book (both webmail and computer based address books), Facebook and Twitter friends. This spamming of illicit code is typically in the form of friendly emails apparently from you to your email buddies with a short polite message along with a link to a purloined website which will automatically load the malware code onto their machines. Facebook and Twitter have also become major vectors used to promulgate this malware, as the rogue software will post short messages apparently from you, with links to the malware; anyone clicking on those links will be hijacked as well, and the process repeats geometrically. In addition to propagating itself, this rogue software also often adds the hijacked computers as "zombies" to a massive "bot" of computers used to send out spam emails for a fee, payable to the crook that started this spider web of malware and hijackings. In addition to the revenues from sending countless spam emails from the "bot" (network) of "zombies" (hijacked computers), the purveyors of this malware also generate substantial revenues by charging a fee, typically $29 to $69, often payable only by credit card, for the rogue software to "clean" the infected computer. If the unfortunate victim pays this extortion, not just will the rogue software not clean the computer, but will also often sell the credit card number (along with its expiration date, and CVV security code) on other illicit websites, typically resulting in massive fraudulent charges on the credit cards.

In the past, I have had great success using the free portable version of SuperAntiSpyware (www.superantispyware.com) to detect and re-move the rogue antivirus infections. Using a clean computer, I download a fresh, updated copy of the portable version of SuperAntiSpyware to my USB flash drive, which I then take to the hijacked computer. I boot the infected computer into Safe Mode (F8), insert the flash drive, and run the SuperAntiSpyware, often in "full scan" mode. Once cleaned, I use the "Repair" button on the bottom of the SuperAnti-Spyware screen to undo many of the improper changes the malware had made to the computer. Because of its very frequenting updating, ease of use, and high success rate, SuperAntiSpyware portable version is still my first choice to clean an infected computer. The problem is that in this very rapidly evolving cat-and-mouse game between the malware code writers, and the security software companies, some of the recently released malware has become harder to detect and kill. I found this out last Friday when my normal battery of top-rated and updated malware detection and removal utilities that I carry on my flash drive (SuperAntiSpyware, Emsisoft Emergency Kit, and MalwareBytes) were unable to totally remove a persistent infection on a heavily compromised computer.

Knowing that a "Plan B" was necessary to defeat this stubborn mal-ware, I went home to download some other utilities that I have used in the past to remove stubborn malware that resisted the most common and popular methods of cleaning. I downloaded the latest versions of McAfee's Stinger, Kaspersky Rescue Disk, AVG Rescue CD, and Microsoft Standalone System Sweeper Beta. I downloaded the McAfee Stinger to my flash drive, and created fresh CDs with the Kaspersky, AVG, and Microsoft utilities. Be sure to implicitly follow the directions provided by these software companies for creating the bootable CDs or bootable USB flash drives necessary to load and run the utilities.

Returning to the location of the hijacked desktop computer, I booted it into safe mode (F8), inserted my flash drive and ran the McAfee Stinger. While McAfee Stinger detects far fewer

types of malware than many of the other utilities, it does an excellent job in detecting and killing some of the more stubborn infections, which it did on this victimized computer. After rebooting the computer, and rerunning the McAfee Stinger (it found no additional infections), there was very substantial improvement, but still some evidence of malware on the computer.

I inserted my newly created bootable Kaspersky Rescue CD into the drive, and was required to press the F12 key in order to boot the computer with the bootable CD (some computers require F10 or F2 in order to select a "boot from CD or flash drive" option). Since booting with a CD does not load the infected copy of Windows that is on the hard drive, but instead loads a clean operating system from the CD (usually some form of Linux or WinPE), the malware cannot load and protect itself from detection and removal. The Kaspersky Rescue CD detected and removed the remainder of the malware, proving itself as a very viable method of malware removal.

I removed the Kaspersky CD and inserted the Microsoft System Sweeper bootable CD, and rebooted the computer (F12). This Microsoft CD, very capable in its own right, did not detect any other malware on this computer, corroborating the fact that the computer was most likely clean of all forms of malware. If I still had any other problems, I know from past experience that the AVG Rescue CD, bootable the same way as the other CDs, had some very capable detection and system repair utilities which are often necessary to recover a badly damaged computer, but in this particular case, it was not necessary.

This badly infected and compromised computer had one of the major commercial security suites installed, but was still penetrated by the rogue antivirus, a common occurrence in that the rogue software is very well written by experts in security penetration. Rather than reinstall and update his current security software, which was near its expiration and renewal date, this computer owner wanted a different security suite than the one he had, in the hope that it would better protect his computer.

Whatever security software suite he would choose, it is absolutely imperative to install some comprehensive security suite immediately after cleaning the computer that had been hijacked, as the security software that was previously installed was totally dead, killed by the malware in the earliest stage of the takeover, which left the computer vulnerable to the inevitable follow-on attacks. While there are several excellent commercial and free comprehensive security suites available, in this case the user decided to try one of the popular freeware security suites, Outpost (free.agnitum.com), rather than purchase another commercial product; that was his informed choice.

Now, when I am called upon to clean an infected computer, I include McAfee Stinger in the arsenal of utilities on my USB flash drive, and bring the three bootable CDs that I created (Kaspersky, AVG, and Microsoft), just in case they are needed.

Ira is a member of the Golden Triangle PC Club, an Assoc. Professor at Lamar Institute of Technology, and hosts a weekly radio talk show on computer topics on KLVI News Talk AM560. He also writes a weekly technology column for the Examiner newspaper <www.theexaminer.com>. Ira is also a deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.

Websites:
http://www.mcafee.com/us/downloads/free-tools/how-to-use-stinger.aspx
http://support.kaspersky.com/viruses/rescuedisk?level=2
http://www.avg.com/us-en/avg-rescue-cd
https://connect.microsoft.com/systemsweeper
http://www.superantispyware.com
https://www.emsisoft.com/en/software/eek/
http://www.malwarebytes.org
http://free.agnitum.com

Debunking Some Common Myths

by Mindi McDowell

Here are some common myths that may influence your online security practices. Knowing the truth will allow you to make better decisions about how to protect yourself.

How are these myths established?

There is no one cause for these myths. They may have been formed because of a lack of information, an assumption, knowledge of a specific case that was then generalized, or some other source. As with any myth, they are passed from one individual to another, usually because they seem legitimate enough to be true.

Why is it important to know the truth?

While believing these myths may not present a direct threat, they may cause you to be more lax about your security habits. If you are not diligent about protecting yourself, you may be more likely to become a victim of an attack.

What are some common myths, and what is the truth behind them?

- Myth: Anti-virus software and firewalls are 100% effective.
- Truth: Anti-virus software and firewalls are important elements to protecting your information (see Understanding Anti-Virus Software and Understanding Firewalls for more information http://www.us-cert.gov/cas/tips/ST04-005.html). However, neither of these elements are guaranteed to protect you from an attack. Combining these technologies with good security habits is the best way to reduce your risk.
- Myth: Once software is installed on your computer, you do not have to worry about it anymore.
- Truth: Vendors may release updated versions of software to address problems or fix vulnerabilities (see Understanding Patches for more information http://www.us-cert.gov/cas/tips /ST04-006.html). You should install the updates as soon as possible; some software even offers the option to obtain updates automatically. Making sure that you have the latest virus definitions for your anti-virus software is especially important.
- Myth: There is nothing important on your machine, so you do not need to protect it.
- Truth: Your opinion about what is important may differ from an attacker's opinion. If you have personal or financial data on your computer, attackers may be able to collect it and use it for their own financial gain. Even if you do not store that kind of information on your computer, an attacker who can gain control of your computer may be able to use it in attacks against other people (see Understanding Denial-of-Service Attacks http://www.us-cert.gov/cas/tips/ST04-015.html and Understanding Hidden Threats: Rootkits and Botnets for more information http://www.us-cert.gov/cas /tips/ST06-001.html).
- Myth: Attackers only target people with money.
- Truth: Anyone can become a victim of identity theft. Attackers look for the biggest reward for the least amount of effort, so they typically target databases that store information about many people. If your information happens to be in the database, it could be collected and used for malicious purposes. It is important to pay attention to your credit information so that you can minimize any potential damage (see Preventing and Responding to Identity Theft for more information http://www.us-cert.gov /cas/tips/ST05-019.html
- Myth: When computers slow down, it means that they are old and should be replaced.
- Truth: It is possible that running newer or larger software programs on an older computer could lead to slow performance, but you may just need to replace or upgrade a particular component (memory, operating system, CD or DVD drive, etc.). Another possibility is that there are other processes or programs running in the background. If your computer has suddenly become slower, it may be compromised by malware or spyware, or you may be experiencing a denial-of-service attack (see Recognizing and Avoiding Spyware http://www.us-cert.gov/cas/tips/ST04-016.html and Understanding Denial-of-Service Attacks for more information http://www.us-cert.gov/cas/tips/ST04-015.html).

Security Tip (ST06-002)
US-CERT
US Computer Emergency Readiness Team
www.us-cert.gov
Courtesy of APCUG.

How Do I Keep People From Finding Me on the Internet?

by Leo Notenboom

Do you wish you could erase yourself from the internet? In other words, do you want to stop your name and information from showing up when people Google or search for you on the internet? Sadly, you're not alone.

Not only is this disappointingly complex to do, ultimately… you can't.

What it boils down to is understanding how little control you have, what steps you can try, and how effective they may or may not be.

But first, you should know that prevention is the only real cure.

But even then it's not at all complete.

You need to assume that everything you place on the internet will remain there forever, and will be viewed in the worst light possible. To clarify, it may not be there forever, and may not be viewed in the worst light possible, but that's the safest way to look at how what you say, do and post in public might be used. You do have control over some of what goes up on the web before it goes up, so exercise caution.

Still feel like posting those party photos?

How about the example we hear about all the time: someone losing a job or job offer because they spoke their mind in a public post, posted unflattering photos of themselves, or otherwise made public information about themselves that they never should have. Information that their employer or potential employer eventually found.

It happens all the time.

It happens to those who have the freedom of speech mentality: "I should be able to post and say and do whatever I want."

Absolutely. You should be able to. Go ahead. Post and say what you like. In most countries you have the right to say pretty much whatever you like. Just remember that freedom of speech does not mean freedom from consequences.

Because chances are you're not going to get it removed from the internet once the day comes that you decide maybe it shouldn't be there.

Even preventing what you do and post may not be enough. What about other sources of information that relate to you?

You cannot control what others say or post about you. (Within the legal limits of harassment, libel and slander, of course, and even then within the limits of your own legal or justice system and your resources.) Been mentioned in a newspaper? Listed in publicly records? Do you participate in discussion groups that are visible and/or archived publicly?

All of these are ways you can show up online. And there are plenty more.

And more than likely, all are places from which you probably can't remove yourself.

Still want to try? Here's what you can do:

Your first thought may be to try to get in touch with the search engine, but here's the fundamental problem: the search engine has nothing to do with it. Even though people may use the search engine to find the information, that information is not in the search engine itself. It's on one of the thousands of other sites on the internet, and the search engine is merely in charge of finding it. The only way to truly remove yourself is to find each of those sites and ask them to remove the information that pertains to you.

It's common to want to have Google remove you from their index. There are two problems: 1. They won't. Google is a search engine, and their "job" is to report what can be found on other sites on the internet. They're simply showing you what's out there, but what's out there is not

in their control. 2. Google is not the only game in town. Google is perhaps the most popular, but there are literally thousands of search engines on the internet. From Bing to Yahoo, to many medium and smaller niche search engines, there are more search engines than you could ever count. Even if you could get Google to remove you from their results, which you cannot, you'd still be faced with all those other search engines that might also be returning the same results that show your information on the internet.

Look out for a growing service area called "reputation management." These services will promise to remove you from the search results. They can't. If they tell you that they can, they're wrong. The information cannot been removed. The best that they can hope to accomplish is to push whatever it is you want to hide further down the results list when people use common search terms for you. At best it's simply somewhat harder to find … which may, or may not, be valuable to you.

It would be nice to think that you have control over the information that is placed on sites and services that you control on the web. But you don't. This is another way that this issue gets so complicated.

You might think that if you wanted to remove something about yourself that's been posted on your own website, all you need to do is exactly that – remove it. Problem solved.

Not so fast.

The "problem" is that there are other sites that take copies of the pages on your site and preserve them as a kind of historical record. Archive.org is a good example, but in fact there could once again be any number of sites archiving or duplicating information- and many of them are doing it illegally. You can certainly remove the information from your site, but you have no control over what these other sites do with the information that they've already captured and made publicly accessible.

So what can you do?

- Well, you can use the search engines yourself to see where all the information about you is, and then contact all of those sites (not the search engines) and ask them to remove it.
- You can use a reputation management service to try and "bury" your information, making it harder, but not impossible to find. If that's enough for you.

And that's about it. Once something is on the internet, you can pretty much plan on it being there for good.

In fact, it might be easier to change you: move, change your name, change all of your identifying information, and then make sure that as little of that new you as possible gets on the internet.

But even then, you'll probably show up somewhere.

Real-World Warnings Keep You Safe Online

by Mindi McDowell and Matt Lytle

Many of the warning phrases you probably heard from your parents and teachers are also applicable to using computers and the internet.
Why are these warnings important?

Like the real world, technology and the internet present dangers as well as benefits. Equipment fails, attackers may target you, and mistakes and poor judgment happen. Just as you take precautions to protect yourself in the real world, you need to take precautions to protect yourself online. For many users, computers and the internet are unfamiliar and intimidating, so it is appropriate to approach them the same way we urge children to approach the real world.

What are some warnings to remember?

- Don't trust candy from strangers - Finding something on the internet does not guarantee that it is true. Anyone can publish information online, so before accepting a statement as fact or taking action, verify that the source is reliable. It is also easy for attackers to "spoof" email addresses, so verify that an email is legitimate before opening

an unexpected email attachment or responding to a request for personal information (see Using Caution with Email Attachments http://www.us-cert.gov/cas /tips/ST04-010.html and Avoiding Social Engineering and Phishing Attacks http://www.us-cert.gov/cas/tips/ST04-014.html for more information).

- If it sounds too good to be true, it probably is - You have probably seen many emails promising fantastic rewards or monetary gifts. However, regardless of what the email claims, there are not any wealthy strangers desperate to send you money. Beware of grand promises—they are most likely spam, hoaxes, or phishing schemes (see Reducing Spam http://www.us-cert.gov/cas/tips/ST04-007 .html, Identifying Hoaxes and Urban Legends http://www.us-cert.gov/cas/tips/ST04-009.html, and Avoiding Social Engineering and Phishing Attacks http://www.us-cert.gov/cas/tips/ST04-014.html for more information). Also be wary of pop-up windows and advertisements for free downloadable software—they may be disguising spyware (see Recognizing and Avoiding Spyware http://www.us-cert.gov/cas/tips/ST04-016.html for more infor-mation).
- Don't advertise that you are away from home - Some email accounts, especially within an organization, offer a feature (called an autoresponder) that allows you to create an "away" message if you are going to be away from your email for an extended period of time. The message is automatically sent to anyone who emails you while the autoresponder is enabled. While this is a helpful feature for letting your contacts know that you will not be able to respond right away, be careful how you phrase your message. You do not want to let potential attackers know that you are not home, or, worse, give specific details about your location and itinerary. Safer options include phrases such as "I will not have access to email between [date] and [date]." If possible, also restrict the recipients of the message to people within your organization or in your address book. If your away message replies to spam, it only confirms that your email account is active. This may increase the amount of spam you receive (see Reducing Spam http://www.us-cert.gov/cas/tips/ST04-007.html for more information).
- Lock up your valuables - If an attacker is able to access your personal data, he or she may be able to compromise or steal the information. Take steps to protect this information by following good security practices (see the Tips index page http://www.us-cert.gov/cas/tips/ for a list of relevant documents). Some of the most basic precautions include locking your computer when you step away; using firewalls, anti-virus software, and strong passwords; installing appropriate software updates; and taking precautions when browsing or using email.
- Have a backup plan - Since your information could be lost or compromised (due to an equipment malfunction, an error, or an attack), make regular backups of your information so that you still have clean, complete copies (see Good Security Habits http://www .us-cert.gov/cas/tips/ST04-003.html for more information).
- Backups also help you identify what has been changed or lost. If your computer has been infected, it is important to remove the infection before resuming your work (see Recovering from Viruses, Worms, and Trojan Horses http://www.us-cert.gov/cas /tips/ST05-006.html for more information). Keep in mind that if you did not realize that your computer was infected, your backups may also be compromised.

Tip (ST05-014)
US-CERT
US Computer Emergency Response Team
www.us-cert.gov *Courtesy of APCUG.*

Social Networks

by StaySafeOnline.org

Facebook, Twitter, Google+, YouTube, Pinterest, LinkedIn and other social networks have become an integral part of online lives. Social networks are a great way to stay connected with others, but you should be wary about how much personal information you post.

Have your family follow these tips to safely enjoy social networking:

- Privacy and security settings exist for a reason: Learn about and use the privacy and security settings on social networks. They are there to help you control who sees what you post and manage your online experience in a positive way.
- Once posted, always posted: Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research (http://www.microsoft.com/privacy /dpd/research.aspx) found that 70% of job recruiters rejected candidates based on information they found online.
- Your online reputation can be a good thing: Recent research (http://www.microsoft .com/privacy /dpd/research.aspx) also found that recruiters respond to a strong, positive personal brand online. So show your smarts, thoughtfulness, and mastery of the environment.
- Keep personal info personal: Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data, or commit other crimes such as stalking.
- Know and manage your friends: Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. Use tools to manage the information you share with friends in different groups or even have multiple online pages. If you're trying to create a public persona as a blogger or expert, create an open profile or a "fan" page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know and trust) more synched up with your daily life.
- Be honest if you're uncomfortable: If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let them know. Likewise, stay open-minded if a friend approaches you because something you've posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them respect those differences.
- Know what action to take: If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.

Protect Yourself with these STOP. THINK. CONNECT. Tips:

- Keep a clean machine: Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- Own your online presence: When applicable, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit how you share information
- Make passwords long and strong: Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- Unique account, unique password: Separate passwords for every account helps to thwart cybercriminals.
- When in doubt, throw it out: Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.
- Post only about others as you would have them post about you.

How Ants Invented the Internet

by IMT Staff | September 28th, 2012

Welcome to the Anternet

You may recall the moment during the opening ceremony of this year's Olympics when Sir Tim Berners-Lee popped up on screen — many folks recognized the inventor of the

World Wide Web by sight. However, according to recent research, the ceremony should have honored an ant hill instead.

Stanford biology professor Deborah Gordon studies ants. Her colleague Balaji Prabhakar is a computer science professor. They may not seem to have much in common, but when Gordon showed Prabhakar the research she'd conducted on ant colonies making decisions to dispatch foragers to collect food, a connection became apparent.

"It occurred to me, 'Oh wait, this is almost the same as how [Internet] protocols discover how much bandwidth is available for transferring a file!'" Prabhakar told Stanford Engineering. The Internet uses Transmission Control Protocol (TCP) to send packets of data to a receiver node. If these packets are acknowledged quickly, the sender speeds up delivery. If the acknowledgments are slow, the sender slows down.

Gordon's research revealed harvester ants operate on a comparable ratio: if foragers on the hunt return quickly with seeds, the colony knows to dispatch more ants faster; if the foragers are returning slowly, with little or no bounty, the search is slowed or ended.

"Ants have discovered an algorithm that we know well, and they've been doing it for millions of years," Prabhakar said.

"So ant algorithms have to be simple, distributed, and scalable — the very qualities that we need in large engineered distributed systems," Gordon added. "I think as we start understanding more about how species of ants regulate their behavior, we'll find many more useful applications for network algorithms."

Why You Might be Sending Spam

by Leo Notenboom

As you probably already know there's a lot of spam – unsolicited and unwanted email – flying around on the internet these days. Some estimates say that well over 80 to 90 percent of all email is, in fact, spam.

That's bad enough, but when someone tells you that it looks like spam is being sent from your email address … well, then it gets personal.

The most common causes of spam being sent from your email address have nothing at all do with your computer.

In other words, while it's possible, it's not necessarily because your computer has a virus.

Your email account may have been hacked.

Actual account theft and hacking has risen dramatically in recent months.

The scenario is very simple: a hacker learns your password and logs in to your email account. Once in he starts using it to send spam. The hacker never even has to come close to your computer, and in fact often performs his activities from overseas.

The question, of course, is how did he learn your password?

Unfortunately there are many ways: perhaps your password is easy to guess, perhaps your so-called "secret questions" are easy to guess, perhaps you logged in to a public computer in a library or other public location that itself was compromised with malware or a keyloggers.

Perhaps you used your computer in an open Wifi hotspot, and the connection to your mail service was not encrypted and a nearby hacker was monitoring and saw your login information.

Perhaps you responded to a phishing attempt — an attempt to fool you into providing the hacker with your email login information including your password.

Perhaps you told a friend or family member who wasn't quite as careful about keeping it private as you are.

And, of course, there could indeed be malware on your machine. In my experience that's significantly less likely in this case than most of the possibilities above.

There could be absolutely nothing wrong.

One of the most frustrating aspects of this scenario is that it's very possible that there's nothing wrong at all.

The issue is simply this: it's trivially easy to make email look like it's from someone that it is not. So called "From spoofing" is used by spammers to hide their own identity. They pick email addresses at random – often email addresses to who they are also sending spam – and use those as the fake sender of the email.

In other words you may have had absolutely nothing do to with email that lists you as the sender.

And there's nothing you can do about it.

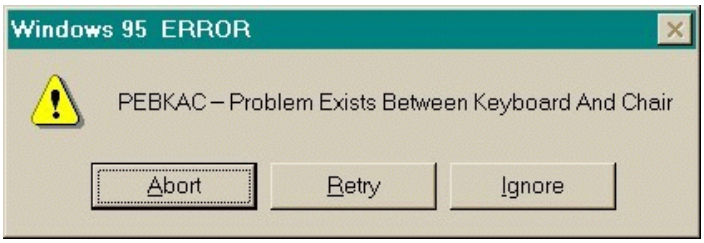
Before you assume this is the case, though, look at who's getting spam email "from" you.

If they are mostly people you know, then it's very likely that your email account has been hacked and your address book or contact list is being spammed. You need to take action right away by changing your email password.

In fact, you need to more than just change the password – you need to change or verify all the information in your account that could be used to recover your password. While the hacker had access to your account he had access to that too, and could have changed it or written it down so that he can easily come back and hack your account again.

You can certainly run up-to-date anti-malware tools on your computer if you like – you should be running those regularly anyway — but as we've seen, in all probability your computer wasn't involved.

Courtesy of APCUG.



"All in One" Free Windows Performance Utilities Updated

by Ira Wilsker

There are several excellent "all in one" Windows system cleaners available. These system cleaners may be able to improve system performance by cleaning the hard drive, managing the startup, tweaking internal Windows settings, cleaning and optimizing the registry (NOTE: cleaning the registry is controversial) improving internet speeds, and performing a host of other system maintenance functions.

What may be the most widely used free comprehensive system cleaner is IObit's Advanced System Care Free (www.iobit.com /advanced system careper .html), whose website claims that 130 million copies have been downloaded. IObit recently (October 10th) announced the release of a new Version 6 of its very popular Advanced System Care line. While the free version of Advanced System Care is very adequate for most users, some users will appreciate the increased functionality and features of the commercial version.

The new version 6 is an 18.2 mb download, and will uninstall any previous versions of the program that may have been on the computer. After downloading and installing the new version 6, the opening window displays the current health of the machine, an option to select "Quick Settings", "Smart Scan", and "Expert Mode." The "Quick Settings" mode offers a wide selection of security, performance, and cleaning options, as well as a selection of automatic options.

The "Security - Full Detection" setting allows the user to perform a security scan and remove malware from the computer, as well as provides some protection from future infections. Also under "Security" is an option that will provide substantial security while surfing the web, a major vector for malware infections. The "Performance" group pro-vides system performance

monitoring, active optimization, intelligent drive optimization (defragmentation), and an "Ultimate TuneUp" which optimizes Windows performance and maximizes internet speed by implementing revised browser settings. The cleaning choices include "Deep Cleaning" of the registry (some users do not recommend cleaning the registry), and secure file deletion. The "Automatic" settings will provide the selected services anytime that the computer is idle, remove privacy threats, and keep Advanced System Care updated.

In the center of the opening Advances System Care screen is a large "Smart Scan" button, which will invoke a series of scans, including malware detection and removal, registry repair and cleaning, a privacy sweep (removes tracking cookies and other privacy threats), deletes junk files from the hard drive freeing up space, boosts the internet speed, and repairs any broken shortcuts. My personal choice is to implement the "Expert Mode" which includes all of the basic cleaning functions already listed, as well as a "Toolbox" with over two dozen helpful utilities, and a "Turbo Boost" function which will optimize and speed up the computer. On the expert window is also the option of changing the "skin" or appearance of Advanced System Care between the classic view, and a black or white background.

Slim Cleaner (slimcleaner.com) is a well regarded system cleaner, with a 5-Star "Spectacular" rating from the CNET editors, and a 4-Star average users' rating. Slim Cleaner, updated October 4th, and rated #4 in downloads from the CNET Maintenance and Optimization category with nearly a million downloads, is a very strong contender. In order to install Slim Cleaner, a small 700k installer is downloaded, which in turn downloads the complete program (6.5 mb). Slim Cleaner is a very comprehensive cleaning and optimization utility that offers features in one program that are competitive with the combined features of several other programs.

One of the several Slim Cleaner features includes virtually all of the cleaning capabilities of CCleaner, the world's most widely used hard drive cleaner. Under the "Optimize" menu is an excellent startup manager that uses cloud computing and community ratings to indicate which programs are necessary in startup, which are optional, and which should be removed from the startup in order to speed the boot process and improve overall performance.

If a suspicious program is found in the startup (or other optimize functions), clicking on the "View Results" will display the risk factors using Cloud AV (anti-virus); if a program in startup is not determined as malware by Cloud AV, it will be marked with a green check. The Optimize - Services displays the services (programs and Windows com-ponents) that are currently running, their risk as determined by Cloud AV, and includes the ability to control which systems are running, another performance and security benefit.

Other menu selections in Slim Cleaner include "Software" which displays the community rating of all programs installed on the computer, publisher information, and an uninstall link for each pro-gram. The "Browsers" menu displays information on the internet browsers installed on the computer including Internet Explorer, Fire-fox, Chrome, Opera, and Safari browsers. Clicking on the browser displays information on the startup page, extensions, and plugins, as well as the community ratings for each item displayed. The "Disk Tools" menu includes several hard drive utilities including a smart defragmentation utility, disk analyzer, disk wiper, file shredder (securely deletes files), and a duplicate file finder to free up hard drive space. The "Windows Tools" offers 15 system utilities, as well as a speedometer type display that shows CPU usage and RAM utilization.

The "Hijack Log" is a strong competitor to the industry leading "Hijack This" from EmsiSoft, which is used to determine if any running programs or other items are malware. The Hijack Log displays all of the items in the startup, browser toolbars, browser helpers (BHO), and Active X, along with the community ratings for each, the Cloud AV results (displays if malware), the path, and the publisher of the item. In summary, Slim Cleaner is well deserved of its "Spectacular" rating from CNET.

Clean Genius (www.easeus.com/cleangenius) is somewhat of a newcomer to the all in one cleaning and optimization category, even though it listed as a version 3, dated October 2nd. Its publisher, the well regarded EaseUS, is known for its excellent utilities, and Clean Genius

is one of the newest utilities in its large stable of software utilities. As with most other cleaning utilities, there are both free and commercial versions available. According to the EaseUS website, the free version of Clean Genius offers optimized computer speed and performance, a quick scan and deep scan for computer issues and problems, and a comprehensive hard disk cleaner.

The Quick Scan includes a junk files cleaner, registry cleaner (some users recommend against cleaning the registry), shortcut repair, system optimizer, and a privacy sweeper. The Deep Scan does all of the above, plus includes a system optimizer, network optimizer, and disk defragmenting utility. In addition to the automated functions, there are an even 20 individually selectable utilities available from a scrolling menu at the bottom of the program window; some of these utilities are a RAM manager, a hard drive checker, a file splitter, and uninstall manager, driver backup function, file encryption, and several other useful functions.

While there are countless other free and commercial all in one optimizers and cleaners, any one (or more) of these three comprehensive free utilities would serve PC users well.

Websites:
http://www.easeus.com/cleangenius
http://slimcleaner.com
http://www.iobit.com/advancedsystemcareper.html

Some Picks from Gizmo:

Protect Your Online Privacy with This Terrific New Extension for Chrome and Firefox

Are you concerned about all the tracking that goes on while you surf the Internet? Users of the Chrome and Firefox browsers have a new weapon against the invasion of their privacy.

It is an extension called PrivacyFix just launched and makes it really easy to configure the privacy settings for Google, Facebook, and many other sites. If you try it, let us know what you think.

http://www.techsupportalert.com/content/protect- your-online - privacy-terrific-new-chrome-extension.htm

Do You Know How Many Apps Have Access To Your Google Account?

The web is full of great free services. To save you having to create a new username and password every time you sign up, many of them allow you to optionally sign in with your existing account. But over time, you tend to forget just how many of these services you have tried. In the case of Google, check this out how to review and deny access to any of those with a single click.

http://www.techsupportalert.com/content/do-you-know-how-many-apps- have-access-your-google-account.htm

Society News

Help's Half Hour Notes
Led by a team of members
October 9, 2012
by Jan Rothfuss

Q: One member is getting a new computer. Which security software should he install?

A: You will need an anti-virus program. If you have Road Runner, they will give you McAfee free. Spybot will provide help, too. Malicious Removal Tool is available through Windows 7. The Microsoft anti-virus program is good. Be sure to set up notifications so that you will know when updates are available.
Q: TechSoup is available for non-profits. Members can then download software for really low prices.
A: Steve is going to check into this option for our members.
Q: One member's computer will not shut down (maybe once a month). D3D9 window message is displayed. How can he tell why?
A: Try Googling the error message. There may be a process running in the background that is causing this problem.

The Lighter Side

"Prediction is very difficult, especially if it's about the future." --Niels Bohr (1885-1962), Danish physicist, first to apply the quantum theory, won the Nobel Prize for Physics in 1922.

In 1966, Time Magazine predicted, "By 2000, the machines will be producing so much that everyone in the U.S. will, in effect, be independently wealthy." In that year too CoCo Chanel said about miniskirts: "It's a bad joke that won't last. Not with winter coming."

In 1954, a concert manager fired Elvis Presley, saying, "You ought to go back to driving a truck." In 1962, Decca Records rejected the Beatles, "We don't like their sound, and guitar music is on the way out."

In 1894, A.A. Michelson, who with E.W. Morley seven years earlier experimentally demonstrated the constancy of the speed of light, said that the future of science would consist of "adding a few decimal places to the results already obtained."

After the invention of the transistor in 1947, several US electronics companies rejected the idea of a portable radio. Apparently it was thought nobody would want to carry a radio around. When Bell put the transistor on the market in 1952 they had few takers apart from a small Japanese start-up called Sony. They introduced the transistor radio in 1954.

Irish scientist, Dr. Dionysius Lardner (1793-1859) didn't believe that trains could contribute much in speedy transport. He wrote: "Rail travel at high speed is not possible, because passengers 'would die of asphyxia' [suffocation]."

In 1943, Thomas Watson, the chairman of IBM forecast a world market for "maybe only five computers." Years before IBM launched the personal computer in 1981, Xerox had already successfully designed and used PCs internally … but decided to concentrate on the production of photocopiers.

Ken Olson, founder of Digital Equipment Corporation, said in 1977, "There is no reason anyone would want a computer in their home."

(Courtesy of didyouknow.org)