

DATA LINE



Published by Santa Clarita Valley Computer Club ... We're User Friendly
Serving the Santa Clarita Valley, CA since 1988

Volume XXII, Special
Editor: Judy Taylour

Meetings
SCV Senior Center
22900 Market Street
Newhall CA 91321
www.scvpcg.org

Page 1	October is National Cyber Security Month - Wilsker
Page 4	Facebook and Privacy Issues - Berger
Page 6	Bass Loves NIS2011
Page 10	7 Simple Steps to Keeping Your Account from Being Hacked - Notenboom
Page 12	What are users saying about MS Security Essentials?
Page 14	Beware of Phishing Schemes - IRS
Page 16	TrendMicro Titanium - A New Concept in Security - Wilsker
Page 18	What is Scareware? - Uniblue
Page 19	More Security Tips from Bass

October 2010 Special Security Edition

October is National Cyber Security Month

By Ira Wilsker, Member, Golden Triangle PC Club, TX; Columnist, The Examiner, Beaumont, TX; Radio Show Host, Mondays, 6-7pm CT, KLVI.com
iwilsker (at) sbcglobal.com

WEBSITES:

Microsoft Online Safety	http://bit.ly/2rzphb
Homeland Security	http://bit.ly/aCcq45
Internet Complaint Center	www. www.ic3.gov
About NCASM 2010	http://bit.ly/aefbJa
NCASM 2010 events	http://bit.ly/9TCAiK
NCASM Tip Sheets	http://bit.ly/cwHKmY
Additional Resources	http://bit.ly/cYljNt
Get Involved	http://bit.ly/cXTyaZ
Banners, Posters & More	http://bit.ly/bBAeeB



Organizations, employers, school teachers, computer clubs, senior citizen centers, and a variety of other institutions are often in search of some type of topic or event that they can use as a theme for meetings and presentations. For those looking for an October topic (but can really be done during any month), October has been declared by the president as National Cyber Security Awareness Month.

Someone may ask, "Why even have a National Cyber Security Awareness Month?" We all need to be aware of the risks involving our computers, and how those risks can impact us personally. The news is rife with stories about viruses and malware, such as the recent massive attack by the "Here You Have" trojan that wreaked havoc on millions of computers in a single day. Identity theft and other economic cyber crimes are depriving individuals and businesses of billions of dollars every year. Social networking websites are being utilized by pedophiles to lure thousands of children into dangerous, and even life threatening, liaisons with miscreants. Hackers and crackers will frequently try to break into our home and office computers for malicious purposes, trying to steal our private information, or otherwise hijack our computers to send out spam email or launch coordinated cyber attacks on other computers. Fraud of many types is rampant online, from phishing schemes designed to trick the user into giving his username and password to the crooks, to counterfeit products, get-rich-quick scams, political misinformation, and medical quackery. According to several cyber security companies, spam emails constitute over 90% of all email hitting our servers. As I type this, one security website has catalogued over 14 million different viruses, worms, trojans, and other forms of malware just waiting to infect our computers, with literally tens of thousands of new threats appearing every day. The average computer is unaware that we are currently engaged in an active cyber war, with foreign nationals hammering our government, military, and industrial computers looking for that hole that will grant them access to valuable information. Cyber espionage, the obtaining of military secrets or classified industrial projects, is rampant.



So, why have a National Cyber Security Awareness Month? While many of us are complacent, and compute with blissful ignorance, we are also all soldiers in the front lines of this battle, so we must first be aware of the threats, and then take appropriate actions to mitigate them.

National Cyber Security Awareness Month was first implemented by a Presidential Order from President Bush in 2001. The president declared that every October be National Cyber Security Awareness Month, a declaration recently ratified by President Obama. For 2010, the program is under the auspices of "The National Cyber Security Alliance (NCSA), a public-private partnership focused on educating a digital citizenry to stay safe and secure online. ... NCSA, along with the U.S. Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center, sponsors National Cyber Security Awareness Month." While the Department of Homeland Security is the primary public agency promoting this activity, several private companies provide much of the funding and manpower used for this project. These private companies include AT&T, Cisco, General Dynamics, Google, Lockheed-Martin, Microsoft, Symantec, McAfee, Verizon, and Visa. Dozens of other companies, organizations,

governmental agencies, and colleges have publically endorsed the project, and are actively participating in its promotion.

The NCSA has a "Get Involved!" website at <http://bit.ly/cXTyaZ> where different groups can get information on how to promote the event. Specific resources and instructions are available for home users, educators, businesses, college students, college administrators, libraries, local law enforcement, and local government. With the resources provided, these and other groups can easily present an audience appropriate presentation. Posters, flyers, pamphlets, brochures, bookmarks, and other printed materials are available in both PDF and Word formats, such that the presenter will have little original work to prepare.

Customized examples of the content for each constituency are freely provided, and easy to use on the "Get Involved!" website. For example, the home users are instructed to use a comprehensive security suite that provides frequent automatic updates, update their operating systems and browsers as soon as patches are released, use complex passwords, be cynical about giving others your personal information online, turn off your computer when not in use, know that security applies to mobile devices (such as smart phones) just as much as it does to a computer, know the symptoms of a compromised computer, teach his children about online safety, backup his data frequently, lookup himself and family members on the major search engines to see what is posted about them, and maintain vigilance and awareness of contemporary threats.

Teachers and college faculty should encourage good cyber security practices every time their students are online, as well as integrate cyber security and safety into lesson plans and course content; arrange for a competent cyber security professional to speak to classes and parents; incorporate cyber security and safety into faculty in-service training; require all students to change their password in October to one that is long, complex and not easy to guess. It should not only be the teachers that should be involved, but administration needs to also be involved. The NCSA has resources for administrators as well, at <http://bit.ly/9jRqaQ>

Local law enforcement needs to be involved, as our citizens are often victimized by online criminals. There is no net difference in the pain or loss suffered by a victim who has been robbed locally, or one robbed online. Too many of our children are victimized by pedophiles who troll for naive children online. Law enforcement should get on board with the program. Local law enforcement are looked to for security guidance and protection from criminal activity; that protection should not just be the traditional protection from street crime, but should also include community education on protection from cyber crime. Local law enforcement agencies should present cyber security topics at external community events, and internal training, including at roll call. The distribution of cyber security literature should occur along with other crime prevention literature. Departments should implement a written policy on dealing with citizens who have been cyber victimized (such as Internet fraud or identity theft), and encourage them to report it to the FBI's Internet Crime Complaint Center (www.ic3.gov). Appropriately trained and skilled officers should speak at local schools, businesses, religious institutions, and other organizations on cyber crime and cyber security; a police officer (or deputy sheriff) has a cache of authority that many other speakers may lack.

Businesses, both small and large, have become the primary targets for many cyber thieves. These crooks are utilizing a variety of ingenious online tricks and tools to defraud businesses, many of which can be mitigated if only the employees (and management) are appropriately trained, and proper policies are implemented. Cyber security policies and procedures need to

be reviewed frequently, and updated as appropriate, as the threats are dynamic and constantly changing. The NCSA and Symantec published a small business cyber security study which shows what businesses are doing (<http://bit.ly/aAgOOG>). Hold periodic employee meetings, such as brown-bag lunches, where cyber security practices can be openly discussed. Post security tips in break rooms, work rooms, and company newsletters, as well as distribute handouts to employees. Businesses need to create an environment where employees can freely raise security concerns. Make sure that your customers and clients, including online customers, know that you are adequately protecting their personal and private information. Make it a policy that computers should be shut down at night and at other down times. Managers need to be kept informed in a timely manner of any evolving security threats that can impact the business.

Whatever the event or group, there is an abundance of educational and training materials freely available for cyber security training. There is a large assortment of cyber security "Tip Sheets" available from <http://bit.ly/cwHKmY> These Tip Sheets, available for free in both PDF and Word formats, include documents about gaming safety for kids and parents, Internet Safety and Security Tips For Parents, Mobile Safety Tips, and Social Networking Tips 2010. Under each of the groups listed at <http://bit.ly/cXTyaZ> (home users, businesses, law enforcement, etc.) are links to additional resources. Still more resources are available online at <http://bit.ly/cYIjNt>.

While October is indeed National Cyber Security Awareness Month, we need to make every day a security awareness day. We lock our cars, and we lock the doors to our homes; we need to lock our computers as well to prevent others from accessing them and doing harm to us and others.

Ira Wilsker is a member of the Golden Triangle PC Club as well as Director of the Management Development Program at Lamar Institute of Technology, in Beaumont, TX. He also hosts a weekly radio talk show on computer topics on KLVJ News Talk AM560, and writes a weekly technology column for the Examiner newspaper <www.theexaminer.com>. Ira is also a police officer who specializes in cybercrime, and has lectured internationally in computer crime and security.

Facebook and Privacy Issues

Written by Sandy Berger, CompuKISS

<http://www.compukiss.com> / [sandy\(at\)compukiss.com](mailto:sandy(at)compukiss.com)



When the Internet first started, no one worried about privacy. It was simply a joy to be able to communicate with others so easily and to be able to use the Internet as a tool to expand your horizons. Now, however, if you are on the Internet, you have to be concerned about privacy.

You see, the entire face of privacy has changed dramatically in just the last year. We used to be anxious about cookies and giving out information on insecure websites. Now we have to be concerned about every piece of information that we put on the Web.

facebook

Facebook helps you connect and share with the people in your life.



This situation was recently brought to the forefront when Facebook changed their privacy policies and gave third party websites the ability to mine data from Facebook accounts. Facebook, along with several partners, has developed a system that they call "Instant Personalization." Facebook says they did this to enable a "personal and social experience" on certain affiliated websites.

Here's an example of how it works. One of Facebook's first partnerships is with Pandora, a website that customizes music to your taste. Because of the new partnership, Pandora can pull your favorite musicians from your Facebook profile and automatically create a group of music that you will like. Now, that is not necessarily a bad thing. However, Pandora could also notify anyone on your friends list about the music that you are listening to and could notify you about the music they are listening to. Again, that is not necessarily a bad thing, unless you don't want others to know what you are listening to. Here's where it gets hairy. Facebook states that, "When you and your friends visit an instantly personalized site, the partner can use your public Facebook information, which includes your name, profile picture, gender, and connections." So you might see your picture and/or personal information in places that might surprise you.

Another portion of Facebook's new alliances that greatly affect our privacy is the "Like" button. This is a simple "thumbs-up" icon that Facebook users are very familiar with. But if you click on the Facebook "Like" button on an affiliated website you are authorizing Facebook to be able to put the fact that you like a certain website or activity on your Facebook profile which also appears on the newsfeeds of all your friends. Friends who also visit that website might be able to see that you have approved of that site. If you visit a porn site and press the "like" button, your minister, your spouse, and your mother might be immediately notified on their Facebook newsfeeds.

Basically, Facebook is weaving much of our web surfing and our likes and dislikes into Facebook for all our friends, and perhaps for everyone, to see. The ways that all this will be used are still being developed, but you can be sure that things you once thought you were sharing only with selected friends will now be posted blatantly in a variety of places on the web. Any sense of confidentiality, privacy or secrecy on Facebook is now gone.

One of the most aggravating things about the Facebook issue is that it was extremely difficult to adjust your own privacy settings on Facebook. You had to wade through pages and pages of privacy choices. Because the public outcry about Facebook's new policies was extremely loud, Facebook has revamped their privacy settings. Although in some ways it was a move forward, for the most part, it was simply a bone thrown to those concerned about privacy. Facebook reduced the number of separate pages of privacy options. There are now 8 pages instead of 13. There are also fewer options that need to be checked to make all of your information somewhat private. Previously there were 50 and now, by my count, there are only 15. The entire situation, however, is still problematic. It is difficult for the average person to understand what each of the privacy choices mean and there are still too many to juggle.

If you are on Facebook, however, I highly recommend that you visit the Privacy Settings Area to take a good look at what you may be sharing. Just click on "Account" from the top right of the Facebook page, then click on "Privacy Settings." Also remember that although you have some control over that is posted on Facebook pages, you still can't control the information that

Facebook transfers to partners and third party entities.

So whether you are on Facebook or not, there is one simple rule to live by when posting information on the Internet: If you don't want the world to know something, don't put it on Facebook or anywhere else on the Internet.

Bass Loves NIS2011

By Steve Bass, Publisher and Self-appointed Chief Content Officer, TechBite
www.techbite.com / [stevebass \(at\) techbite.com](mailto:stevebass@techbite.com)

Oh, Bass, What Did You Do?

On March 21, 1991, I stopped using Norton's security programs.

But I like to see what the dark side is up to, so I recently switched back to Norton. And I'm really happy I did.

Of course, knowing how you always like to hear the dirt, I'll tell you the back story.

Oh, Norton, What Did *You* Do?

It was at the March 21, 1991 user group meeting that a Norton rep was showing off the company's latest antivirus program. "Give these a spin," I said, handing the guy doing the demo a floppy disk filled with live viruses.

Not an unreasonable request, I thought. But that's just me.

He avoided making eye contact, wouldn't look at the floppy, and said "no." That's it. To a roomful of 350 computer users. "No."

And it was downhill from there.

Over the years, Symantec's Norton products grew popular; they also became bigger. They leapfrogged over Microsoft Office to obtain, and keep, the bloatware award. Norton products hobbled PCs by hogging computer resources and hard disk space. Like it or not, you got stuck with Live Update, a separate, massive, tool used to keep every Norton program in the world up-to-date -- even if you only owned one product.

And when you'd had enough of Norton, you needed special software and a small backhoe to uninstall it. Live Update stayed with you forever.

Symantec shot itself in the foot over and over--and what really fascinates me, is when it had spare time, it did it again.

Why I Switched Back to Norton

It's always been an open question whether I'm as smart as I look. It's a question you might be asking, because as I type this, I'm using Norton Internet Security 2011, better known as NIS2011.

I've used Kaspersky Internet Security for about four years. I haven't been happy for the last two. It's no longer an unobtrusive tool. Its interface has always been confusing; the recent redesign hasn't helped. It's a big program and in some spots, thunderously slow.

The upgrade to Kaspersky's new 2011 version is what killed the relationship: I lost too many brain cells configuring obscure exclusion settings to get a few online programs to work. If I had trouble, I'd guess you might, too.

Of course, synchronicity was waiting in the wings.

Brendon, a decade-long e-mail friend, works for Symantec. Every few months he pitches me to try a Norton security tool. "I'm pestering you about this not because it's my job (I'm not in product marketing or PR or sales or anything), but because I respect you as an educated power user and would like my product to have a fair shake."

My argument always starts with one word: *bloat*.

You'll like his testy, paraphrased reply.

Oh, that thinking is so 2006!

I'll admit the products had bad bloat problems in the 2004, 2005, and 2006 variants, and I totally understand the criticism and share in it.

We alienated a lot of the power-user base because of performance problems and focus on the wrong things, and it did a lot of damage to our reputation.

A big change in product management came, and we've been very aggressive in attacking performance and footprint, rewriting significant portions. I was game. It was off with Kaspersky (thanks to Revo Uninstaller) and on with Norton Internet Security 2011.

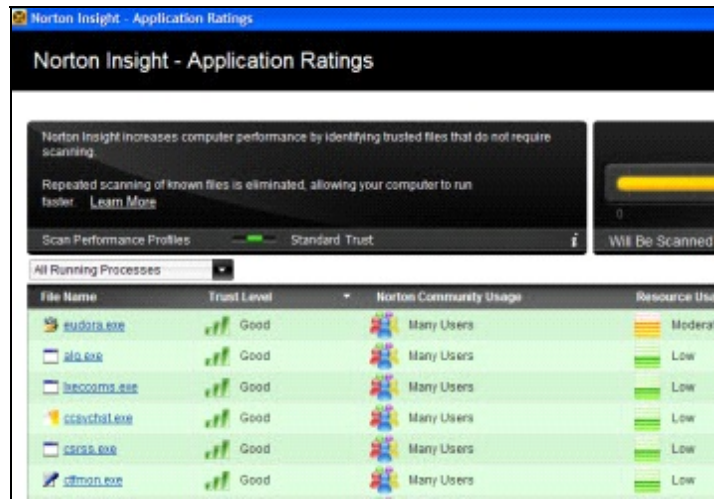
Norton? I Love Ya

I've had NIS2011 running for over a month, and it's surprised me. It's fast and keeps out of my way with no annoying alerts. It also found two embedded backdoor Trojans that Kaspersky missed.

Here are my impressions:

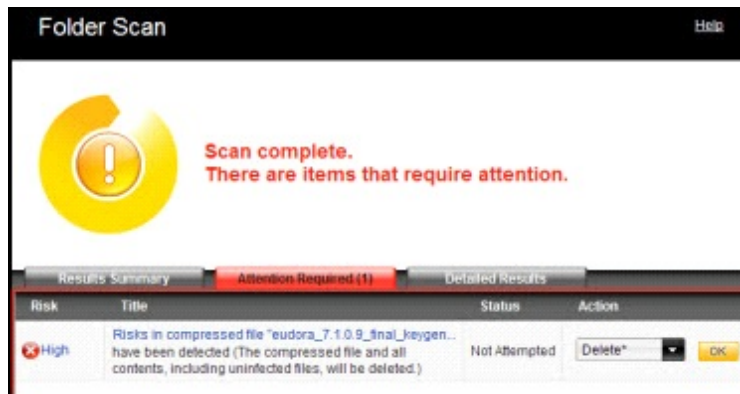
- NIS2011 installed in 57 seconds. Really.
- Every feature -- the built-in firewall included -- works fine using just Norton's defaults. No tweaking necessary.
- Programs load faster than with Kaspersky's Internet Security. I'm guessing that's because NIS2011 does a Reputation Scan on all the apps on my PC and approves them based on its massive user database of programs.

NIS2011 recognized and gave every program an A-OK; with Kaspersky, I had to manually set complicated exclusions for four tools (including [SugarSync](#) and [Dropbox](#)). Kaspersky also needed for me to change permissions in order for a few online apps to run properly, including Java and Firefox. Crazy, no? NIS2011 handled all the apps with no interference.



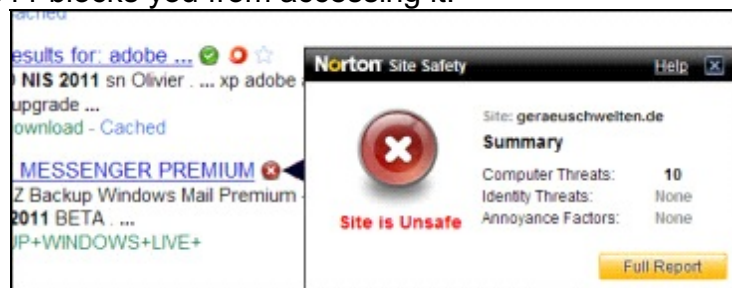
In the past, Norton's update system was a separate app (I hated that), but now it's integrated into the program. That's much better. And every few minutes, when the PC is idle, Norton's LiveUpdate checks and downloads updates quickly and quietly.

On NIS2011's initial scan, it found two Keygen backdoor Trojans that Kaspersky hadn't found. To be fair, if I'd tried to run them, Kaspersky would have blocked and removed them, too. But NIS2011 raises my comfort level considerably



Have Trojans? NIS2011 will find them.

- Until I checked the history, I never noticed that NIS2011 automatically does quick scans while my PC is idle. The default is every 10 minutes. Nice.
- Norton has a Web safety component, similar, but much stronger than WOT, that makes sure you don't land on a malware drive-by page. If you happen to land on a site that's dangerous, NIS2011 blocks you from accessing it.

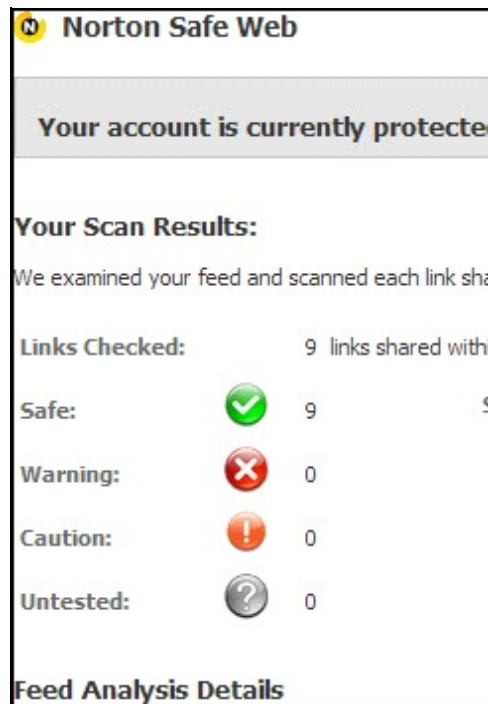


Hey, watch where you're going.



Let Norton watch out for you while you're surfing.

NIS2011 also makes sure the links on your Facebook account are safe.



Are you facing Facebook threats?

- NIS2011 shows how much memory and resources are used by running programs; it doesn't use any resources when it's not doing anything and about 3 percent while it's scanning. Bloated? Not at all.
- There are more things to like -- paternal controls and anti-spam, for instance -- but I'll leave it to you to explore the other features.

Should You Switch?

If you're happy with the performance of whatever you're using, stick with it. Of course, if you've been kvetching and need a change, or if the license on your existing security tool is coming up for renewal, consider giving NIS2011 a shot.

And if you've had a bad experience with Norton in the past (and who hasn't?), I'll tell you first-hand -- the current version's a treat to use.

You can download a 15-day free trial, but don't run two security programs simultaneously -- or even have them loaded at the same time. Make sure to uninstall the program you're currently using before installing NIS2011.

Amazon has NIS2011 for about \$60 for a one-year license for three PCs. (Don't have three PCs? It's probably a violation of the license, and I wouldn't do it, but if you have a buddy...)

I can predict the future: You're going to write and tell me about your favorite security tool. Save your bits and bytes, folks; while I'm always interested in what you have to say (well, okay, not always), I've tried nearly every major free and commercial security program there is. I've settled on Norton. So there.

Steve Bass is the publisher and self-appointed Chief Content Officer at TechBite; he continues to experience the cool feeling of having his own newsletter. Send him your feedback at TechBite <stevebass@techbite.com>. To sign up for TechBite's free Steve Bass Technology newsletter, head for our sign up page. <http://www.techbite.com/>

Steve's also the author of "PC Annoyances, 2nd Edition: How to Fix the Most Annoying Things About Your Personal Computer," available on Amazon. It covers XP, but not Vista. If you haven't purchased your copy today, don't wait, supplies always seem to be limited...

From Dick Beekman. I just upgraded my 3 computers from NIS 2010 to NIS 2011 for free because I have a subscription. Perhaps some folks forget, or don't realize that they can do this as long as the subscription is valid. Right now a 1 year renewal for 3 computers is going for \$59.00. I know Fry's has "deals" but sometimes it isn't worth the hassle, if you go there and its out of stock.

7 Simple Steps to Keeping Your Account from Being Hacked

By Leo Notenboom

<http://ask-leo.com/newsletter.html>

Article Source: http://EzineArticles.com?expert=Leo_Notenboom

By far the most common reason accounts get hacked is that they had easy to remember and simple - sometimes even trivial - passwords.

In other words, the accounts have easy to hack passwords. Passwords like a pet's name, a friend's name spelled backwards, a favorite movie catch phrase, a significant other's name (or "iheart" followed by that name), and so on.

Hackers are extremely resourceful at guessing and ferreting out those all-too-common password schemes. And sometimes it's not even the hackers that end up with your passwords.

Here are seven key steps to keeping an account from being hacked due to simple and common password theft.

1 - Pick a good password. "iHeartSue" is bad. "qicITcl}" is great! The problem's pretty obvious, though - if it's easy to remember, then it's probably a bad password. Instead, use a blended approach: never use full words or names; mix upper and lower case letters, use numbers. Use at least 8 characters. A password like "ILoveWindows" is bad, but a variation - "1luvwind00s" could be very good. "CorgiDog", not so good, but "Igroc7Pup" might be ok. Get creative, using a technique you can remember that no one else could possibly guess.



2 - Keep your password safe. Tell no one. Even in a close and presumably trusting relationship - if anything ever happens consider the damage that the person could do knowing your password. Too many account theft scenarios begin with trusting someone just a little too much, and then having the relationship go bad. Your friends are your friends until one day they're not. Especially if someone is pressuring you or if there's the least little bit of doubt, don't share your password.

3 - Use a "secret answer." Most systems use the answer to a "secret question" as a way to recover or reset a password. Unfortunately many people choose answers that anyone can guess, or easily research on the internet. Answers like where you were born or your pet's name are frequently easy to find out with a little searching. The good news is that your secret answer doesn't actually have to make sense. Pick something unrelated or bizarre instead; choose answers like "Pickle" as your city of birth, "Confusion" as your mother's maiden name, or perhaps "Flat Tire" as your favorite pet. As long as you can remember, it doesn't matter.

4 - Maintain that alternate email address. An "alternate email address" is used by many mail accounts as a place to send you a password reminder or reset. Be sure to set up an account on a different email system for your alternate email address (any other free email system will do), and then use that address as your alternate everywhere else. Of course, keep the alternate account active so as not to lose it, since without it you may be out of luck.

5 - Remember. Remembering sounds easy, but like we said earlier: if it's easy to remember, then it's probably a bad password. And yet remembering and being difficult to guess are both critical. You must remember your password, failing that your secret answer, and failing that your alternate email account. Forget or lose them all, and you're severely out of luck. If written down, be sure to keep it all in a secure place - not something like the almost cliché scenario of finding poorly hidden sticky notes containing passwords near your computer. It might be safe to keep something in your wallet, since you already treat that as secure. An encrypted file or password container on your computer might be another option.

6 - Don't get taken. There are shady services that will claim to be able to retrieve your passwords and account access. Many are simply scams to take advantage of you when you are vulnerable and only take your money or login information for another account that they can then breach. The only place trustworthy enough for password and account recovery help is the service you've lost access to itself. If they can't help, then neither can a reputable third party.

7 - Learn from your mistakes. Finally, if you now know that you have a weak password, if you've told it to someone you shouldn't have, or if you've not set up that secret question or alternate account, fix it. Now. Change your password to something stronger, set up the alternate recovery methods, and keep your information private. If you've been hacked and you don't have any of that set up, you're very likely out of luck. Make sure to take more secure care of your account password and information with your next one.

Get more free tech help and advice from Leo Notenboom by visiting <http://ask-leo.com> With over 30 years of industry experience, including an 18 year career as a software engineer with Microsoft, Leo gives real answers to real questions from ordinary computer users at Ask Leo! Subscribe to Leo's weekly newsletter now and receive a free ebook: "Internet Safety - Keeping Your Computer Safe on the Internet", a collection of steps, tools and concepts you need to know to keep your computer and your information safe.

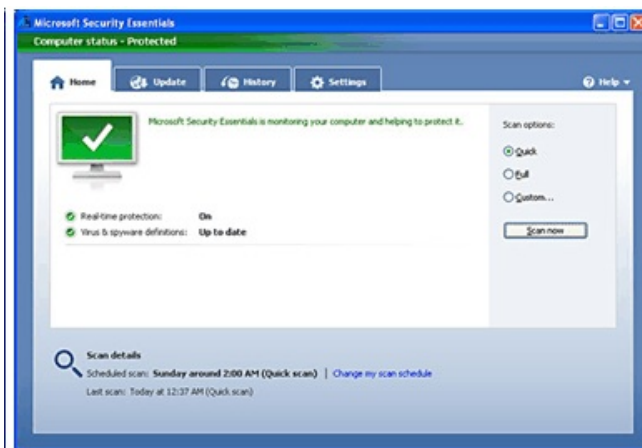
What are users saying about Microsoft Security Essentials?

October 2010 issue, Orange County IBM PC Users' Group nibbles & bits

Linda Gonse, Editor

www.orcopug.org / editor (at) orcopug.org

After half a year of real-life testing, Microsoft's Security Essentials anti-malware application is batting 1,000. All nine test computers - a mix of Windows 7, Vista and XP systems (including two portables with 20,000 miles of travel) - remain malware- and virus-free.



For my tests, I used Windows' built-in firewall (on XP, Vista, and Win7) and a copy of Microsoft Security Essentials, which I allowed to run with its default settings. Over the past six months, my main PCs have been online 24/7 and my two portables have logged over 20,000 miles (32,000 kilometers) of use in hotels, coffee shops, cars, planes, ships, and other assorted public venues.

All the machines have remained clean. They've suffered no malware or virus infections whatsoever.

Initially, I checked each PC's health and security every few days, using a variety of on-demand AV scanners from vendors such as McAfee (Freescan), Trendmicro (HouseCall), and Symantec (Security Check). The scans never found anything.

Over time, as it became clear that MSE was doing exactly what it was supposed to, I reduced the frequency of these just in case backup scans to once or twice a month. (That's good practice with any security tool. As the saying goes, "Trust, but verify.")

MSE is free and is available for every version of Windows (http://www.microsoft.com/security_essentials/). It's small and fast and consumes very little by way of system resources. I can detect no MSE-induced slowdowns on any of my PCs - even the low-horsepower netbook.

Very simply, it works.

So I highly recommend MSE. Combine it with a firewall (such as the one built into Windows), and verify it with periodic just-in-case scans with free third-party software (as listed earlier), and you'll have a free, efficient and self-maintaining security solution.

- Fred Langa, Windows Secrets (September 16, 2010)

I've been using this shortly after it came out. Steve Gibson recommends it. I have been using it on all my computers (2 XP's and 2 Windows 7). I have even put it on at work. Even though we have a corporate virus program that runs constantly, MS Security Essentials found a virus that the corporate program missed.

I haven't had any problems with my computers at home and one of the XP machines I use for test and I'm not always that careful about sites I don't know or testing downloaded programs. I have recommended this at our meeting and I obviously agree with the author. The other thing I like about it is that it sits in your tray and will tell you when you need to refresh the signature file. It's a great solution to recommend to non-technical users.

- Mike Lyons, ORCOPUG president

This gentlemen is having the same results that I have encountered. All 11 systems that I have installed this program onto-using the Windows Firewall in conjunction with it-have been threat-free since that installation.

You're going to see firms like Norton, McAfee, AVG, etc. crying, "Monopoly!" before very long-if they have not done so already.

- Darry D Eggleston, darryd.com

A reader recently asked us if she needed Windows Defender, antispysware software from Microsoft that comes with Windows Vista and Windows 7, if she had downloaded Microsoft Security Essentials (free antivirus and antispysware software).

If you use Microsoft Security Essentials, you don't need Windows Defender. When you download Microsoft Security Essentials, it will turn off (but not uninstall) Windows Defender automatically. It does this so that you don't have two programs on your computer that are doing the same thing. If you ever decided to uninstall Microsoft Security Essentials, Windows Defender will be turned back on again.

- Marcelle Amelia (Security Tips & Talk, MSDN blog, <http://bit.ly/c7op6w>)

I just switched from McAfee to Microsoft Security Essentials yesterday and so far I'm very impressed. McAfee's latest update was constantly consuming hogfulls of CPU resources, whereas MSE is just sitting quietly whilst I'm writing this, for example, and is consuming just about zero resources. My PC is noticeably faster overall now with MSE rather than McAfee, and scanning individual files or groups of files is much more speedy too.

- Paul J, Online Dating Services.org
(comment at <http://www.reviewguy.net/downloads/microsoft-security-essentials.html>)

Beware of Phishing Schemes

www.irs.gov

What is phishing?

Phishing is the act of sending an e-mail to a user falsely claiming to be a legitimate enterprise in an attempt to scam the user into surrendering private information that could be used for identity theft. According to the Federal Trade Commission, phishers send e-mails or pop-up messages that claim to be from a business or organization, for example, an Internet Service Provider, a bank, an online payment service or even a government agency. The message may ask you to update, validate or confirm your account information. Some phishing e-mails threaten dire consequences if you don't respond. The messages direct you to a Web site that looks just like a legitimate organization's site—but it's not. It's a bogus site whose sole purpose is to trick you into divulging your personal information so operators can steal your identity and run up bills or commit crimes in your name.



Remember these tips:

- If you get an e-mail or a pop-up message that asks for personal or financial information, do not reply or click on any links in the message. Legitimate companies don't ask for this information via e-mail.
- If you are concerned about your account, contact the organization in the e-mail by using a telephone number you know or open a new Internet browser session and type in the company's correct Web address yourself. Don't cut and paste the link from the message into your Internet browser — phishers can make links look real, but it actually sends you to a different site.
- Use anti-virus software and a firewall and keep them up-to-date. Some phishing e-mails contain software that can harm your computer or track your activities on the Internet

without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files.

Beware of phishing schemes involving the IRS

Although the FTC has reported that the IRS has a low number of identity theft crimes, phishing schemes using the IRS name have been escalating in number and sophistication. The current phishing scheme attempts to convince the users that they are receiving an e-mail from the IRS. The e-mails use an official IRS seal and ask recipients to provide personal information, such as Social Security numbers, credit card numbers and bank PINs. You should only respond in writing or by phone to the phone number listed on an IRS notice.

Remember, the IRS does not initiate communication with taxpayers through e-mail.

What if you believe you've been a victim of a scam?

File a complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site at www.ftc.gov/idtheft. Victims of phishing can become victims of identity theft. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early by ordering a free copy of your credit report from any of the three major credit bureaus. See www.annualcreditreport.com for details on ordering a free annual credit report.

What if you become aware of an IRS-related phishing scam?

If you receive an unsolicited e-mail communication claiming to be from the IRS, please forward the original message to: phishing@irs.gov. Find complete instructions at www.irs.gov.

How do I report other IRS scams?

You may report misuse of the IRS name, logo, forms or other IRS property to the Treasury Inspector General for Tax Administration at 800.366.4484.

How do I report tax fraud?

Don't fall victim to tax scams. Remember, that if it sounds too good to be true, it probably is. Report suspected tax fraud activity by sending a completed Form 3949-A, Information Referral, to Internal Revenue Service, Fresno, CA 93888. You can download the form or call 800.829.3676 to order by mail.

For more information about identity theft prevention and victim assistance, visit www.irs.gov(keyword: identity theft).



TrendMicro Titanium - A New Concept in Security

**By Ira Wilsker, Member, Golden Triangle PC Club, TX; Columnist, The Examiner, Beaumont, TX; Radio Show Host, Mondays, 6-7pm CT, KLVI.com
iwilsker (at) sbcglobal.com**

WEBSITES:

<http://www.trendmicro.com>

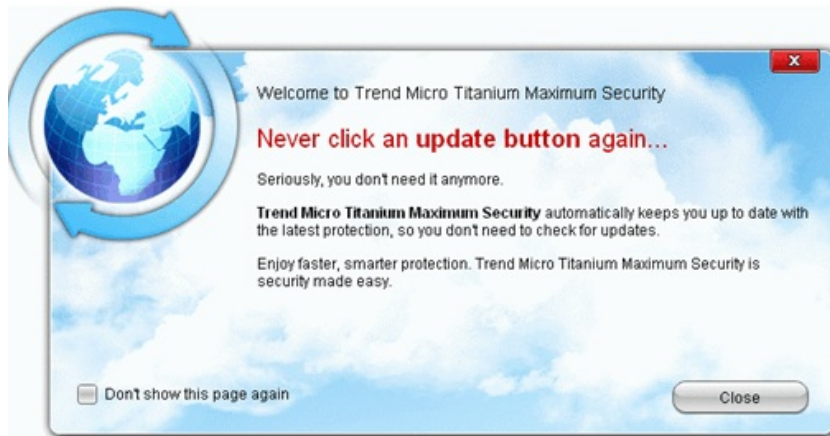
<http://www.soluto.com>

As I have said in this column many times before, I am a software junkie. I like trying new software, often seeking out the gems that can improve performance, or increase security. Recently, I installed a most intriguing product that promised both the epitome of online security along with a noticeable increase in performance due to the utilization of less system resources. This product is the newly released TrendMicro Titanium Maximum Security.

I have been an avid user of antivirus software since the earliest days of the internet, switching to more comprehensive software as the threat matrix evolved. The threats started as simple viruses, and then worms, Trojans, and other forms of spyware. Malware of other varieties started to appear and then became endemic, including other forms of spyware, keyloggers, rogue antivirus, online scams, compromised but otherwise legitimate websites, identity theft schemes, and a panoply of other newly created cyber threats. As the threat landscape increased, the traditional antivirus software started to become technically obsolete as it could not protect from the myriad of threats, and security suites evolved into comprehensive protection that depended on bloated software which inevitably degraded computer performance. Some of the recent security suites created such a drag on performance that boot times became excessive, and opening files would be so slow that user frustration set in. The security software publishers were well aware of this predicament, and worked hard to produce software that provided comprehensive protection without dramatically sacrificing computer performance. TrendMicro has accomplished this most worthy goal with its new Titanium series of security suites.

A few weeks ago I installed the newly released TrendMicro Titanium Maximum Security. It installed quickly and smoothly with a minimum of user intervention. After rebooting the computer immediately following the install, I was pleasantly amazed that my computer seemed to boot much faster than it had with my previous security suite. Using the Solutio boot management and monitoring software (www.soluto.com), my boot time was reduced by about half, meaning my computer was booting up twice as fast, the only difference being uninstalling my previous security suite, and installing the Titanium Maximum suite.

Being one who likes to explore the features of any new product, the first thing I wanted to do was update the malware signatures, but was surprised that there is no such button or link on the software console (main software window). When right-clicking on the red ball TrendMicro icon in the task bar, and opening the control console, I was greeted with a popup that said, "Never click an update button again ... Seriously, you don't need it anymore. TrendMicro Titanium Maximum Security automatically keeps you up to date with the latest protection, so



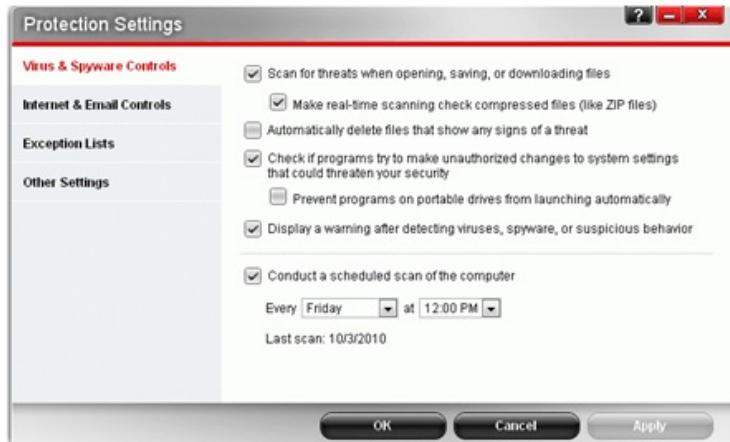
you don't need to check for updates." This lack of frequent signature file updating may have been an acute disadvantage with earlier security products, where failure to update frequently would leave the computer vulnerable to new threats, but it actually is an advantage with this new product since it uses "Cloud Technology" to continuously keep the signatures updated without the need for periodic signature

updates. This also acts to enhance protection since there is minimal lag time between detection of new threats, the development of countermeasures, and the protection on the computer. With previous products, many users had a false sense of security for which they sometimes paid dearly, as they did not download the latest updates in a timely fashion; this is not a problem with TrendMicro's Cloud Technology. To be fair, there is a selection that says "Check for program updates" on the program icon, but these are software updates, and not new malware signature files. To the credit of TrendMicro, they do frequently push software updates and improvements to the user.

The main console offers a Security Summary, a System Tuner, Parental Controls, and Subscription Information. The security summary displays the threats that have been detected and neutralized, with the option of preparing periodic graphical reports, or exporting the results to a CSV file that can be utilized by database and spreadsheet programs. The results can also be exported to a plain text (.txt) file if desired.

The Parental Controls, System Tuner, and other features can be accessed by clicking on the Tools button. Some of the other features accessible in this manner are a Secure Erase utility, Data Theft Prevention, Trend Micro Vault, and a Free Tool Center. The Parental Controls utility is intended to protect children from inappropriate websites, control access and online time, and provide detailed reports to the parents on the child's online activity. The System Tuner can clean junk files freeing up hard drive space, manage what loads at boot in order to improve startup performance, clean history files, schedule tune-ups. The System Tuner also includes a comprehensive registry cleaner, and a feature that protects internet privacy. The Secure Erase offers an option to securely delete files such that they are unrecoverable, and complies with government data security standards. Data Theft Prevention protects sensitive data including credit card numbers, passwords, and email addresses from hackers and spyware, which may attempt to steal such vital personal information. The Trend Micro Vault is an encrypted, password protected Windows folder that can protect sensitive files; in the event the computer is lost or stolen (a common occurrence for laptop and notebook computers), the Vault can be sealed remotely, preventing illicit access to those sensitive files. If the computer is recovered, the authorized user can unlock the directory. The Free Tool Center opens a webpage that offers online backup services (10 gb provided free, up to 100 gb available); Housecall free online security scanning; Guarded ID Standard version which encrypts keystrokes to defeat keyloggers; SafeCentral, a fee based security system that protects online activities such as online banking; and DriveClonePro, a comprehensive backup utility.

Users should periodically perform a scan of their computers, and this product offers a very fast Quick Scan, a comprehensive Full Scan, and a selective Custom Scan. In independent speed tests, TrendMicro Titanium Maximum Security completed a full scan of a hard drive in half the time of the next fastest name-brand security suite, in one-fourth the time (four times faster) than another top-selling competitor. In addition to being the fastest scanner tested among the major brands, Titanium also had the smallest memory footprint (least resources used), fastest file copy, and took up the smallest amount of hard drive space.



While the default settings are entirely adequate to provide reasonable security, the user can control the virus and spyware settings, degree of protection from web threats, set protection from malware spread through instant messaging, select comprehensive spam filtering, and configure some other forms of protection.

In the few weeks that I have been using TrendMicro Titanium Maximum Security, I have been very impressed with the

improved performance of my computer, the comprehensive protection that has been provided, and the additional performance, tools, and security enhancements available. For those users who want a modern and technologically advanced commercial security suite, I can recommend TrendMicro Titanium Maximum Security. The Maximum suite which I have been using, retails for \$79.95, and includes a one-year license for up to three computers. For those who may not need all of the extra tools, there is a Titanium Internet Security for \$69.95 retail, also for use on up to three computers. For those only needing basic security from malware, there is a \$39.95 TrendMicro Titanium Antivirus+, but that is only for use on a single computer. Bargain hunters can find these products locally in the big-box stores and online at significant discounts from the retail price, which only enhances the return on the investment. At whatever price, TrendMicro Titanium Maximum Security would be a wise choice for a security suite.

What is Scareware?

Uniblue

Free resource libraries by Uniblue

www.liutilities.com/articles / www.uniblue.com

Scareware is a name given to different types of scam software, which can infiltrate your PC, ironically, with your consent. These are actually software packages, which often have limited or no functionality, and may even severely harm your PC in certain rare circumstances. These software programs are always marketed using illegal “scare” tactics.

Have you ever visited a webpage and seen a flashing banner stating that your hard disk may be infected with a dangerous computer virus, or that your Windows registry has errors in it, and you should click on the banner to get your PC scanned? If yes, then you have already seen the

ugly face of scareware. These banners are usually the gateway of scam software into your PC. When you click on the banner, you will usually see a small pop-up window and a progress bar inside it. The progress bar will fill up gradually, to give you an impression that your PC is being scanned. When the progress bar fills up completely, you will see another message that several errors were found in your PC, and that you should purchase some software to get rid of the error. Be careful, this is where you may fall victim to the scam software vendor.



First of all, if you see a warning like this from a flashing, or colorful banner on a website, do not worry. Your PC is not infected by anything. Do not click on these banner ads; these are often hoaxes, designed to trick you into purchasing some software that may in fact be just a bunch of malware.

If you accidentally click on any of the banners, then immediately close the pop-up window that comes up. Scan your PC with a good malware remover to make sure your PC has not been infected.

Even if it has been infected, the malware remover should be able to stop it dead in its tracks, and remove it from your hard disk.

Install good antivirus software in your PC, and keep it updated to the latest version. Any good antivirus software can provide decent protection against most scareware around. Also, for greater safety, install good malware remover in your PC, and keep it updated as well. These two should be able to keep your PC safe from almost anything scareware banners can throw at you, even if you accidentally click on the flashing banners.

More Security Tips from Bass

You're the Target!

This just in: Somebody out there is trying to trick you into clicking a link in an e-mail. Do it and you'll be delivered to a Web site ready, willing, and absolutely able to damage your PC, steal your passwords, and use your address books.

Just this week, PandaLabs (www.pandasecurity.com) warned of a massive iTunes phishing campaign. E-mails are sent with a well-designed, authentic-looking receipt for \$895. Alarmed -- and unsuspecting -- victims click to see how it happened and they eventually get tagged with the Zeus Trojan.

But I'm Protected

Okay, yes, you already have a security tool. But I have three smart, free, no-fuss browser tools that'll give you an extra edge against cyber criminals.

I sense you might be resisting. Go along with me for a minute.

You're asking, legitimately, why I'm suggesting you need more help when I went on so long in the last newsletter about Norton Internet Security 2011. Two reasons: One, I'm not taking any chances with my PC, and I don't think you should either. And two, if Norton somehow skips a

beat -- or you forget to update your security program for a week -- I want someone else to watch both our backs.

Up in the Clouds

My friend Alex (Eckleberry), from Sunbelt Software (Vipre Antivirus Premium) just released ClearCloud, a valuable, free tool that monitors your online activity in three ways: In your browser and e-mail program, or if a program's trying to send details about you to their servers.

ClearCloud works by making a small, benign change to your PC's Internet settings. When you head for a Web site -- by clicking a link in e-mail, typing a URL in your browser's address bar, or clicking a link on a Web page -- ClearCloud looks over the link. If the site's dangerous, it blocks access.

ClearCloud: Under the Hood

Technically, ClearCloud changes the DNS server settings so traffic is routed through its servers first. I like how I can turn the ClearCloud service on and off, and it uninstalls without doing any damage. ClearCloud is still in beta, a testing phase. Read the ClearCloud FAQ www.clearclouddns.com/FAQ/. If you're interested in this technology, you can also look at Norton DNS, which is in beta as well. <http://nortondns.com/>

As with any tool that changes your system's DNS settings, ClearCloud still blocks sites for a couple of hours after it's disabled or unloaded. You can manually flush the DNS cache by typing "ipconfig /flushdns" at a command prompt (this feature will be included in the final product).

ClearCloud is similar to SpywareBlaster , also a freebie, a tool I used to recommend. But SpywareBlaster uses a static list that's on your computer and needs to be updated. ClearCloud has a substantially larger database of hazardous URLs--and the list is Web-based and dynamic, so nasty URLs are constantly being added.

ClearCloud versus OpenDNS

ClearCloud and OpenDNS have lots in common. (Read my take on OpenDNS / <http://bit.ly/d1QnBG>) The difference is that OpenDNS focuses more on letting you filter sites you don't want to see, say porn, politics, parked domains, dating, and so on. In the last few weeks, OpenDNS has upped the ante to block more phishing sites than it has in the recent past.

Me, I'm switching to ClearCloud for a few months to try it out. It's not likely to happen, but I wish OpenDNS would partner with ClearCloud and integrate its list of dangerous sites.

