



NANAIMO COMPUTER CLUB NEWS

Oct 2009 Volume 6 Issue 8

Contents

Page ##

Greetings from the President

Message from the President- - - - - 03

Computer News

Firefox to run checks for Adobe Flash patch - - - - - 04

Starting with the upcoming releases of Firefox 3.5.3 and Firefox 3.0.14, Mozilla will warn users if their version of the popular Adobe Flash Player plug-in is out of date, according to Mozilla Human Shield Johnathan Nightingale.

AMD keeps things simple with vision - - - - - 04

In an attempt to wean customers away from worrying about clock speed, cores and cache, AMD has dramatically simplified its processor branding.

Google unlocks data restrictions, announces Data Liberation efforts - - - - - 04

Google is unlocking its data door by launching a new initiative called Data Liberation, an approach to engineering that allows users to move their data - be it pictures, mail or documents - from Google's servers to any other location.

Tests show Safari 4 "clearly the worst" for battery life- - - - - 05

AnandTech just published an interesting set of test results that shows the browser you pick can have a significant effect on your portable computer's battery life. Author Jarred Walton tested 5 major browsers on Windows:

Google exec calls for ISPs to get tough on botnets- - - - - 06

GENEVA — Head of Google's Anti-Malvertising team Eric Davis wants Internet Service Providers (ISPs) to look beyond profits and take a more proactive approach to dealing with malware-infested computers on their networks.

Modern banker malware undermines two-factor authentication- - - - - 07

Once pitched as an additional layer of security for E-banking transactions, two-factor authentication is slowly becoming an easy to bypass authentication process, to which cybercriminals have successfully adapted throughout the last couple of years.

what will the fallout be from Microsoft Security Essentials?- - - - - 08

Microsoft Security Essentials, the freeware security application from Microsoft, has only been available for download for a few hours and some of you have already been in touch wanting to know what I think the fallout will be from it.

Computer Tips and Tricks

Eight Tips for Super Searching- - - - - 09

Plain old Web searching doesn't do the trick anymore: It yields too much random data, or not what you need. Here's how to get what you want when you want it—sometimes before you ask for it. - Bill Dyszel

what Is Safe Mode? - Neil J. Rubenking - - - - - 10

Q: How do you start the computer, to see all the icons on the desktop, if Windows XP does not boot up? I see these options and don't know how to use them: Safe Mode, Safe Mode with Networking, Safe Mode with Command Prompt.—Wang Siewiew

- [Avoiding Adobe Flash Player Scams](#) - [Lockergnome](#) - - - - - 11
Q: Some of the sites I visit ask for Adobe Flash Player in order to run any videos etc. I have gone to the link as well as Adobe and downloaded the player, but it doesn't seem to be found by the Web sites when I try to run a video. What am I doing wrong? - Kathy
- [Net Jargon Translated](#) - [Newbies.com](#) - - - - - 12
Here's a translation of some of the Internet Jargon you come across and perhaps don't understand ...
- [10 Things You Should Know About Windows XP's System Restore Tool](#)- - - - - 12
System Restore is a great recovery tool that was introduced with Windows XP and has been carried over to Vista and Windows 7. It can be a lifesaver if you install a program or make a configuration change that causes your computer to crash or have other problems. Like magic, you can undo the change and take the operating system back to a previous state. Here are a few tips and tricks for using System Restore on XP most effectively

Greetings from the President

We certainly had an interesting meeting with John Borage from Black's Camera.

The one thing that was disheartening was the attendance. There were only 12 members in attendance. It seems that all the present executive does to improve attendance does not have the desired effects.

At the last executive meeting we reached a consensus that this would be our last year as a club. It is the wish of the present executive that we be replaced with a new executive with fresh ideas and approaches. Failing that, we see no other recourse but to end the existence of this club after June of this year.

We have enough money to continue for one more year. It was also suggested that there be no dues for all past members in order to wind down the affairs of the club. All assets would be donated to the Bowen Seniors Computer club when we dissolve our club.

With regrets,

Steve

Computer News

Firefox to run checks for Adobe Flash patch



Starting with the upcoming releases of Firefox 3.5.3 and Firefox 3.0.14, Mozilla will warn users if their version of the popular Adobe Flash Player plug-in is out of date, according to Mozilla Human Shield Johnathan Nightingale.

Once the browser is updated, Mozilla will present the user with a visual notice on its first-run Web site that the Flash Player plugin contains security and stability vulnerabilities.

Nightingale writes:

Old versions of plugins can cause crashes and other stability problems, and can also be a significant security risk. For now our focus is on the Adobe Flash Player both because of its popularity and because some studies have shown that as many as 80% of users currently have an out of date version.

Our intent is to get the user's attention, and direct them to the Adobe web site where they can download the most up to date version.

Nightingale said Mozilla will work with other plugin vendors to provide similar checks for their products in the future.

AMD keeps things simple with Vision

In an attempt to wean customers away from worrying about clock speed, cores and cache, AMD has dramatically simplified its processor branding.



In fact, AMD has boiled down its processors to three different Vision levels:

Vision level PCs are designed for simple, easy tasks such as web browsing, email, and music playback. Premium Vision level systems can handle more demanding tasks such as video and gaming. Vision Ultimate level systems have the power to handle more demanding tasks such as audio and video editing and advanced photo manipulation.

Note: AMD is planning a fourth Vision level, called Black, which will be aimed at high-end gamers and enthusiasts. AMD usually uses the Black moniker to denote processors that offer a greater overclock potential to normal CPUs.

Now, the question is whether these Vision levels gives buyers the information they need, or it is an example of dumbing things down too much. Personally, I think that as long as consumers have access to the tech specs, then this system might actually make things easier for the average buyer. After all, most people buy PCs with a set of tasks in mind rather than a spec list, so a branding scheme that highlights the PC's capability might help buyers get the right PC.

Google unlocks data restrictions, announces Data Liberation efforts



Google is unlocking its data door by launching a new initiative called Data Liberation, an approach to engineering that allows users to move their data - be it pictures, mail or documents - from Google's servers to any other location.

In a blog post this morning, Data Liberation engineering manager Brian Fitzpatrick, uses a good analogy to explain why the company sees this is an important step:

Imagine you want to move out of your apartment. When you ask your landlord about the terms of your previous lease, he says that you are free to leave at any time; however, you cannot take all of your things with you - not your photos,

(Continued on page 5)

your keepsakes, or your clothing. If you're like most people, a restriction like this may cause you to rethink moving altogether. Not only is this a bad situation for you as the tenant, but it's also detrimental to the housing industry as a whole, which no longer has incentive to build better apartments at all. Although this may seem like a strange analogy, this pretty accurately describes the situation my team, Google's Data Liberation Front, is working hard to combat from an engineering perspective.

It wasn't so long ago that Facebook took a bit of a PR hit when the company changed its terms and services to basically give "ownership" of user data to Facebook - or at least that's how it was perceived. Since then, the idea of users keeping data behind a locked Internet door that they don't hold the keys to has become a buzz point. Yahoo, when it announced its new home page last month, was quick to note how it was enabling users to pull data from other Web properties and view it from the Yahoo home page.

Apparently, it's hip to be open these days. Fitzpatrick's post continues:

We think open is better than closed — not because closed is inherently bad, but because when it's easy for users to leave your product, there's a sense of urgency to improve and innovate in order to keep your users. When your users are locked in, there's a strong temptation to be complacent and focus less on making your product better.

The company has already liberated about half of its products - from Blogger to Gmail - and has plans to liberate Google Sites and Google Docs, with batch exports, in the coming months. The company has also launched a separate site to further explain its data liberation efforts

Cooter and Gomer...
Bubba died in a fire and his body was burned pretty badly...

The morgue needed someone to identify the body, so they sent for his two best friends, Cooter and Gomer.

The three men had always done everything

together.

Cooter arrived first, and when the mortician pulled back the sheet,

Cooter said, 'Yup, his face is burned up pretty bad. You better roll him over.'

The mortician rolled him over and Cooter said, 'Nope, ain't Bubba.'

The mortician thought this was rather strange.

So he brought Gomer in to confirm the identity of the body.

Gomer looked at the body and said, 'Yup, he's pretty well burnt up...

Roll him over.'

The mortician rolled him over and Gomer said, 'No, it ain't Bubba.'

The mortician asked, 'How can you tell?'

Gomer said, 'Well, Bubba had two assholes.'

'What? He had two assholes?' asked the mortician.

'Yup, we never seen 'em, but everybody used to say:

'There's Bubba with them two assholes.'

Tests show Safari 4 "clearly the worst" for battery life



AnandTech just published an interesting set of test results that shows the browser you pick can have a significant effect on your portable computer's battery life. Author Jarred Walton tested 5 major browsers on Windows:

IE8
Firefox 3.5.2 (with and without Adblock)
Chrome 2
Opera (versions 9.64 and 10.0b3)
Safari 4

(Continued on page 6)

IE8 provided the best battery life overall on the two Intel and AMD laptops tested, and second best (behind Chrome 2) in the netbook test. But the real surprise was how badly Safari 4 performed. On the AMD notebook, using IE8 increased overall battery life by a whopping 33%. Jarred wrote:

"Outside of Safari 4, which was clearly the worst browser choice for battery life under Windows, the major browsers offer similar battery life."

Poor Safari performance is being blamed on either a bad implementation of Adobe Flash, or inefficiencies in the code that does HTML parsing and rendering. Safari developers have not yet responded to the findings.

Google exec calls for ISPs to get tough on botnets

GENEVA — Head of Google's Anti-Malvertising team Eric Davis wants Internet Service Providers (ISPs) to look beyond profits and take a more proactive approach to dealing with malware-infested computers on their networks.



During a keynote presentation at the Virus Bulletin conference here, Davis said competitors in the ISP space must look beyond profits and partner on new initiatives to deal with the "parasites" that have taken control of the Internet landscape.

"Technology is only one part of security," Davis said, adding that the necessary countermeasures are currently undermined by structural issues. "We need to explore industry self-regulation, education and reputation systems, he argued.

Making it clear his statements were not necessarily the views of his employer, the Google executive chided ISPs for not doing enough to help users with infected machines.

"The ISPs are in the best position to detect infected machines. They're in the best place to do something about malware. They already

have monitoring systems that could be used to identify signs of malware and botnet activity. If they see abnormally high e-mail activity, that's most likely spam from a botnet," Davis said.

However, because ISPs have no monetary incentive to notify and help disinfect machines, the botnets live and thrive within ISP networks, he added.

"Detection is expensive and tech support is expensive so they don't do anything about it," Davis said.

He recommended ISPs use the Australia Internet Security Initiative (AISI) as a model to fight malware. The AISI group mandates minimum customer security levels and isolate infected machines into "walled gardens" until the malicious software is removed.

"The computer has to meet certain [security] standards for that ISP to grant access to the internet," Davis said.

At the basic minimum, he recommends that ISPs mandate that all computers connecting to the Internet be fully-patched (operating system and third party software) and have active anti-malware software running.

"We need to restrict computers that are not in good condition and maybe offer carrots to consumers — maybe provide some additional services, more disk space or free tech support as incentives for users to be strict about security."

Davis said this level of cooperation was also needed to combat the malicious advertising (malvertising) menace, where cyber-criminals buy text ads and redirect users to dirty sites or embed malicious code into multimedia (Flash) ads.

"Most malware ads today are made with Flash. There are some very dangerous things hidden in rich media, installing malware without any action on user's part, Davis said, warning that malvertising can leverage known brands and use sophisticated tricks to get malicious ads placed on high-traffic legitimate sites.

The New York Times and MLB.com are among

(Continued on page 7)

two known brands that have served malicious advertising in recent times.

"It's become big business. These guys [cyber-criminals] will approach and ad agency and say they're working with a company, have a pretty good spend planned out. They create shell brands that look respectable and, on the publishing side, there are very few incentives to do something about it."

"Part of the solution is a business decision. The players involved need to do better background checks, rather than just take a credit card. This underscores the larger theme that there's no single actor to take full responsibility for this problem. "It's a systemic problem," Davis added.

He challenged the anti-malware industry to do a better job of scanning SWF (Shockwave Flash) content to look for signs of malicious activity and called on online advertisers to partner on running background checks on advertisers.

"We should have a clearing house with information on advertisers, agencies. Does their nameserver host match the information on the credit card? Does that match the customer's contact information? We need to be on top of these things."

Modern banker malware undermines two-factor authentication



Once pitched as an additional layer of security for E-banking transactions, two-factor authentication is slowly becoming an easy to bypass authentication process, to which cybercriminals have successfully adapted throughout the last couple of years.

Modern banker malware, also known as crimeware, is now fully capable of bypassing the two-factor authentication obstacle by doing a simple thing - patiently waiting for the crimeware-infected victim to authenticate

himself in order to abuse the access in real-time.

A recently published article at MIT's Technology Review, details a case where cybercriminals managed to steal \$447K despite that two-factor authentication was in place:

Yet the manager's computer had a hitchhiker. A forensic analysis performed later would reveal that an earlier visit to another website had allowed a malicious program to invade his computer. While the manager issued legitimate payments, the program initiated 27 transactions to various bank accounts, siphoning off \$447,000 in a matter of minutes. "They not only got into my system here, they were able to ascertain how much they could draw, so they drew the limit," says Roy Ferrari, Ferma's president.

The theft happened despite Ferma's use of a one-time password, a six-digit code issued by a small electronic device every 30 or 60 seconds.

This incident, among the countless number of similar but largely under-reported ones, raises several important questions. Compared to a previous case where a bank was sued for not offering two-factor authentication, should Ferma's bank be sued for actually offering two-factor authentication, but allowing the fraudulent transaction to take place?

Also, could antivirus software have prevented (No security software, no E-banking fraud claims for you) the infection from taking place? Last week, Trusteer published an advisory entitled "Measuring the in-the-wild effectiveness of Antivirus against Zeus" according to which the most popular banker malware Zeus, is successfully bypassing up-to-date antivirus software :

Installing an anti-virus product and maintaining it up to date reduces the probability to get infected by Zeus by 23%, compared to running without an anti-virus altogether. The effectiveness of an up to date anti virus against Zeus is thus not 100%, not 90%, not even 50% - it's just 23%.

While disturbing, these results shouldn't come as a surprise due to the "value-added" services offered by a managed crimeware service, namely, the systematic release of undetected

(Continued on page 8)

Zeus samples. The popularity of Zeus has in fact contributed to the development of a monoculture within the crimeware market, prompting cybercriminals to look for, and actually find remotely exploitable vulnerabilities within outdated crimeware kits, allowing them to easily hijack someone else's misconfigured and outdated botnet.

Its popularity has also prompted the launch of such services as the the Zeus Tracker, which currently list 537 active crimeware domains, with the majority of them hosted in Russia, the U.S and China, followed by the Netherlands, Ukraine and Germany. The real-time blocklist it generates is in fact so useful, the service came under a DDoS attack in February, 2009.

With banker malware clearly able to operate even on PCs with up-to-date antivirus product, a logical anti-fraud move by a bank's customer would be to reclaim control of their bank account by assuming the worst.

In Ferma's case, depending on whether or not their bank offered such services — like it should — the ability to set daily, weekly or monthly account transaction limits may have mitigated the impact of the actual compromise. Moreover, issuing one-time passwords (OTP) over SMS is just the tip of the iceberg when it comes to offering additional alert services. Not only is the availability of SMS alert services (automatic SMS alert for each incoming and outgoing transaction) highly advisable, it can help a crimeware-infected victim quickly get hold of their financial institution's 24/7 fraud report center in order to freeze the transaction and the account itself.

Naturally, cybecriminals have found ways to adapt to these SMS alerts, by exploiting badly implemented processes within particular financial institutions allowing a customer to change the mobile number in any particular moment of time. Due to the fact that, for instance, a Chinese bank wouldn't accept U.S mobile number for SMS alert and one-time password services, cybercriminals are already using services offering to accept and forward any data sent to a particular mobile number within a country where they maintain local numbers for fraudulent purposes.

Multiple-factor authentication simply cannot prevent fraudulent activity if the user is operating from a compromised environment in the first place.

What will the fallout be from Microsoft Security Essentials?

Microsoft Security Essentials, the freeware security application from Microsoft, has only been available for download for a few hours and some of you have already been in touch wanting to know what I think the fallout will be from it.



A free antivirus applications isn't a new thing, but a big player like Microsoft making a security application available for free is bound to cause waves. So, what is the likely fallout?

While publicly the major security vendors have been playing things cool, privately they are scrabbling to come up with a decent response. The first response from the big security firms is likely to be a PR/white paper barrage telling us all how good their product is and how rubbish everyone else's is, especially Microsoft's. Following that, I think that a price war is inevitable, although price is a weak point for anyone trying to sell a product when going up against Microsoft's free offering. Still, looking at the price of security software nowadays, there's plenty of wriggle room.

Innovation ... you never know, this might be just the catalyst that the security industry needs to start innovating. I just hope it's not innovation that leads to pointless bloat.

One area that Microsoft Security Essentials is likely to have an effect on is free antivirus. People who provide unpaid tech support for family and friends are likely to turn to Microsoft Security Essentials as a quick and easy way to provide protection. With Microsoft Security Essentials there's no nag screens, toolbars, and other crapware to worry about.

Microsoft Security Essentials doesn't affect the enterprise market at all, so no one is affected

(Continued on page 9)

there.

Expect the security industry to start pushing “security suites” even harder than they do now. This could even be the end of the stand alone antivirus software as we know it.

Will Microsoft Security Essentials force some vendors to the wall? I doubt it.

Before I close, I do want to highlight one move that I think was bone-headed on Microsoft’s part, and that was requiring users to pass Windows validation before installation. The folks running pirated software are just the folks that need free antivirus. Microsoft shouldn’t look at it as giving something for free to those who aren’t paying, but as a way of making the web a safer place for those who do pay for their software.

Computer Tips and Tricks

Eight Tips for Super Searching

Plain old Web searching doesn’t do the trick anymore: It yields too much random data, or not what you need. Here’s how to get what you want when you want it—sometimes before you ask for it. - Bill Dyszel

Nobody “surfs” the Web anymore. Some 80 percent of all online sessions now begin with a search. Google proves the point by making over a billion dollars every quarter on search ads. Nobody ever made that kind of money selling browsers.

But plain old Web searching doesn’t do the trick anymore. Most Web searches either yield too much random data, or they don’t give you what you need when you need it.

If you’re an efficient searcher, you know to hit the Web running. Here are some tricks that will help you get what you want when you want it—sometimes before you ask for it.

1. Go on the alert. Why search day after day for news about the next release of your favorite game? At Google Alerts you can tell Google to send you a daily, weekly, or up-to-the-minute e-mail that >sums everything up.

2. Alert Yahoo, too. Yahoo alerts don’t offer Google’s level of detail, but the menu-oriented

interface gives novices a clear idea of what options are available in the alerts that they create. On the other hand, Yahoo makes you sign in before you can create an alert, a task that could easily sidetrack distractable users.

3. Know an operator or two. You can create tightly defined searches for your alerts if you use search operators when defining your alert. For example, if you want to search only PCMag.com, append the operator site:pcmag.com to your search query. If you really want to geek out on all the search possibilities, peruse Google’s and Yahoo’s lists of search modifiers.

4. Live a little. Microsoft Live Search macros are easy to overlook. Live Search macros let you build and save frequent searches—for example, if you’re new to the Linux OS distribution Ubuntu and search the forums a lot, you can build a search (or use the already available macro) that includes those sites. When you’re ready to search, just plug in what you’re looking for and the search will automatically be limited to the sites you specified.

The macros are buried in the More menu at the right end of the main Live Search screen, and they can be really helpful. Go to the bottom of the More menu and choose See All. You’ll see two headings that refer to Macros: Edit Macros and Find Macros. The Find Macros menu lets you browse macros other people have created, while Edit Macros is your choice for creating menus yourself.—

5. Take a shortcut. Firefox launches a search when you right-click selected text and choose Search in Google from the shortcut menu. See “Firefox 3: 8 Things You Didn’t Know You Could Do” to learn how to get zippier performance from Firefox).

6. Get personal. Vanity surfing isn’t just an exercise in ego building. If you have a reputation to protect for any reason, you need to know what people can find out about you. Consider Google’s Profiles service, which allows you to set up a personal page in which you describe yourself to the world of Google searchers (you know, everybody) on a page that gets priority in Google search results. Google profiles don’t erase any nasty comments others may have

(Continued on page 10)

made about you on the Web, but they do give you equal time to make your case.

When you're looking for personal information about other people, Web searches are often too general, but if you go to www.pipl.com, you can find a slightly scary level of detailed personal information about yourself or anyone else. The information you find on Pipl is frequently much more detailed than what you'll get from Google. Even if you don't like bad news, it's usually better if you find the dirt on yourself before someone else does.

7. Troll Twitter for timely tips. Despite its reputation for disseminating drivel, Twitter is probably your best source for fresh, time-sensitive information, and an essential resource for ensuring that you're dealing with current information. It also delivers information of a different nature—search engines tell you what a machine thinks you're looking for, but a Twitter search tells you what other people are choosing to say about that topic right now. The mainstream search engines also conflate today's information with stuff that's been hanging around for years, while Twitter searches skew toward recent relevance. Twitter's plain old search box can deliver a mother lode of information about what's on the world's collective unconscious right this minute, as can the search tools in the most popular third-party services like Twitscoop and Twitterfall. You can also ferret out current trends through the search tools built into many of the free, downloadable helper applications for Twitter, including Tweetdeck, Seismic Desktop, and AlertThingy.

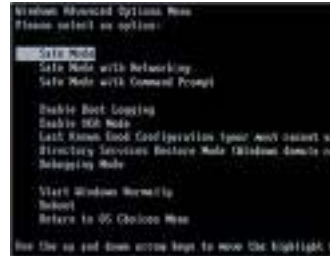
8. Tailor responses. The Internet makes more wrong information available to more people than ever before. Google now invites you to promote items from your search results (that is, move them up in the search ranking), or remove them altogether, by clicking the gray icons next to each returned link. As you repeat this action in different searches, Google's software learns to deliver results that are more reliable for you—more in line with what you tend to look for. So, for example, you might get recipes when you search on "chicken," while Farmer Pete gets items about the care and feeding of laying hens. In addition, Google now tries to deliver "personalized" results by taking into account

what you've clicked on in the past, so your own past search habits could affect the results you get as well.

If you can't have Web search results injected directly into your brain, that's only because Google's engineers haven't yet figured out how to push advertising up there, too. The minute they do, you'll know.

What Is Safe Mode? - Neil J. Rubenking

Q: How do you start the computer, to see all the icons on the desktop, if Windows XP does not boot up? I see these options and don't know how to use them: Safe Mode, Safe Mode with Networking, Safe Mode with Command Prompt.



W a n g Siewsiw

A: When Windows has a problem and fails to boot properly, the next time you boot it will usually offer the options you have listed. Safe Mode starts Windows with the bare minimum of drivers and without any "launch at start-up" programs. It gives you a chance to investigate the problem even when you can't boot fully into Windows. If you have anti-malware software installed, you can try to run a scan in case the problem was caused by malware. Most anti-malware will scan in Safe Mode, though typically real-time protection is disabled.

Safe Mode with Networking is exactly what it says—Safe Mode with additional components enabled to make network connection possible. Safe Mode with Command Prompt give you only a Command Prompt to work with; it's rarely necessary.

Sitting on the side of the road waiting to catch speeding drivers, a state trooper sees a car pattering along at 22 mph. He thinks to himself, 'This driver is as dangerous as a speeder!' So he turns on his lights and pulls the driver over.

Approaching the car, he notices that there are five elderly ladies - two in the front seat and three in the

(Continued on page 11)

back, wide-eyed and white as ghosts.

The driver, obviously confused, says to him, 'Officer, I don't understand, I was going the exact speed limit. What seems to be the problem?'

The trooper, trying to contain a chuckle, explains to her that 22 was the route number, not the speed limit. A bit embarrassed, the woman grinned and thanked the officer for pointing out her error.

'But before you go, Ma'am, I have to ask, is everyone in this car OK? These women seem awfully shaken.'

'Oh, they'll be all right in a minute, officer. We just got Off Route 127.'

Avoiding Adobe Flash Player Scams - Lockergnome



Q: Some of the sites I visit ask for Adobe Flash Player in order to run any videos etc. I have gone to the link as well as Adobe and downloaded the player, but it doesn't seem to

be found by the Web sites when I try to run a video. What am I doing wrong? - Kathy

What you likely have done wrong is fall for one of the most common ploys by hackers these days to infect your computer with a worm.

Some time ago, we started seeing various ploys tricking people into installing malicious software into their computer under the auspices of needing an updated Adobe Flash player.

These clever 'social engineering' scams generally use salacious or provocative headlines in e-mails, on Web sites, through social media sites or instant messages to get folks to click on the links.

Often times, especially in the case of the 'KoobFace' worm commonly via social media sites, the message will suggest that the subject of the video is you, so that you are highly interested in viewing it. (ex: I can't believe they caught you on camera doing this!)

If they can get you overly concerned about seeing the video, then you'll likely be too distracted to realize that it's a scam.

For instance, if you were to look closely at a video that claims to be on Facebook or YouTube, generally speaking you will see a slightly stretched logo or a funny Web address.

The message that tries to hook you will often have misspellings or bad grammar or even broken English.

To make things look more realistic, they generally steal the official Adobe Flash button from the Adobe Web site, so it looks legit when you are told you need the new version of the Flash Player. And if you assume that it must be coming from Adobe since it is their button, they once again got you to let your guard down.

The problem is most folks are so worried about what's on the video that they blow right past the obvious 'red flags' that this may not be legit.

The fact that you go through the download and still can't see the video is a further indication that you have probably been had.

These infections are called worms, because once they make their way into your computer, they can 'worm' through the Internet without any help from humans.

Once you've been tricked, the possibilities for what they can or have been doing with your system are endless.

We have seen everything from key loggers to spam engines to botnet agents installed as a result of these scams and none of them are benign.

Make sure you have a technically savvy person examine and clean your system, especially if

(Continued on page 12)

you use this computer for online banking or other highly sensitive tasks. (If so, immediately change your pass codes from a different computer that you know is clean as a precaution against ID theft.)

In the future, if any site tells you that you need an updated program for ANYTHING, don't take the sites word for it and don't accept the sites offerings unless you absolutely trust the source. Remember, creating fake YouTube, Facebook or CNN pages is very easy, so don't let your eyes fool you!

Instead, manually go to the site for downloading your updates (in this case, you should have gone to Adobe.com to download the latest Flash Player yourself) so you know exactly what is being installed.

If, after you manually update your player, the same site still says you need an update, you'll know that it's a scam.

Net Jargon Translated - Newbies.com



Here's a translation of some of the Internet Jargon you come across and perhaps don't understand ...

Attachment... A file hooked to an e-mail message that gets sent to a recipient.

Bandwidth ... A measure of the amount of stuff that can get shoved through a limited transmission medium such as a cable or a phone line.

Blind courtesy (or carbon) copy (bcc) ... A copy of e-mail that gets sent to a recipient without the primary recipient's

knowledge.(always use with a group message)

Bounce ... The error message you read when your mail gets returned as undeliverable. Also, what happens to email that can't be delivered, causing the "undeliverable" message that's sent to you by the postmaster.

Filter ... A part of your e-mail program that scans incoming messages for predefined character strings (also known as words or sentences). You can set up a filter to automatically delete e-mail from a particular address.

Flame ... An insulting, caustic, or otherwise unpleasant response to an email.

Dictionary flame ... Criticizes someone for a misspelling or grammatical gaffe.

Forward (FW) .. To pass along a message to another e-mail address. Just don't forward already forwarded messages. They're no fun to receive or read.

Mail Bomb ... To send a huge message or groups of messages to an e-mail address, causing an explosive reaction from the recipient.

Mailbox ... The place on a mail serving computer where your e-mail is stored. You may create individual mailboxes in your email client to distribute your mail to as well.

Postmaster ... The person who gets to troubleshoot the mail server, and make sure everything is running smoothly.

Sig quote or sig file ... A quotation or closer message added to the end of an e-mail message. Often used to promote a cause or business. Short for signature quote or signature file.

10 Things You Should Know About Windows XP's System Restore Tool - Greg Shultz

System Restore is a great recovery tool that was introduced with Windows XP and has been carried over to Vista and Windows 7. It can be a lifesaver if you install a program or make a configuration change that causes your computer to crash or have other problems. Like magic, you can undo the change and take the operating system back to a previous state. Here are a few tips and tricks for using System Restore on XP most effectively



was introduced with Windows XP and has been carried over to Vista and Windows 7. It can be a lifesaver if you install a program or make a configuration change that causes

your computer to crash or have other problems. Like magic, you can undo the change and take the operating system back to a previous state. Here are a few tips and tricks for using System Restore on XP most effectively

(Continued on page 13)

Windows XP's System Restore lets you restore your computer to a previous time if a problem occurs. To accomplish this feat, System Restore continuously monitors your system looking for significant changes to the operating system, such as an application or driver installation procedure, automatically creating a restore point when it detects an impending change.

System Restore will also create restore points every 24 hours. Restore points are essentially snapshots of your system state, which comprises crucial system files, including certain parts of the registry. System Restore maintains multiple restore points, which gives you the choice of restoring your computer to any number of previously saved states. Here are 10 things you should know about getting the most from Windows XP's System Restore tool.

1: Data files and System Restore

Because System Restore is described as a tool that allows you to restore your computer to a previous time, many people mistakenly assume that they will lose any data files they've created since the restore point was created. However, System Restore doesn't monitor or save the contents of the My Documents folder, any files that use common data filename extensions, such as .doc or .xls, e-mail message stores, browsing history, or even password files. Those files will remain intact when you restore your system.

Keep in mind that the Desktop is not a protected folder, and any files that exist there could be lost during a restore operation. So before you perform a restore operation, you should move any crucial files you have saved on the Desktop to the My Documents folder.

2: Undoing a restore operation

If you perform a restore operation and then determine that the problem still exists, you can undo the operation. To do so, you must immediately run System Restore. When you see the Welcome To System Restore screen, select the Undo My Last Restoration option and click Next. On the Confirm Restoration Undo screen, click Next. System Restore will restore the previous system state and restart the computer.

When the system restarts and you log on, you'll see System Restore's Undo Complete screen, which lets you know the operation was successful.

If you perform a restore operation and then determine that you selected the wrong restore point date, simply run System Restore again and select the restore point date you wanted.

If you perform a successful restore operation and discover that your computer won't boot Windows normally, you can still undo the restore operation. First, boot the system into Safe Mode. After you log on, a Warning dialog box will appear, allowing you to launch System Restore and select the Undo My Last Restoration option.

If the restore operation fails, the Restoration Was Unsuccessful screen will appear, and your computer will automatically return to the same state it was in when you activated the restore operation. In other words, no changes will be made to your computer.

3: Running System Restore from a command prompt

If your computer won't boot Windows normally and won't boot into the Safe Mode GUI, you can still access System Restore. Start by booting the system using the Safe Mode With Command Prompt option. After you log on, type the following at the command prompt:

```
%systemroot%\system32\restore\rstrui.exe
```

Press [Enter], and System Restore will run as it normally does. You can follow the steps in the wizard to perform a restore operation.

4: Purging restore points

System Restore by default claims a maximum of 12 percent of the available hard disk space to save the restore points. (The amount of storage space will depend on the size of your hard disk.) Once the 12 percent mark is reached, System Restore will purge the oldest restore points in its database to make room for new ones. However, there may be situations where you need or want to purge restore points to free up disk space.

(Continued on page 14)

Fortunately, the Disk Cleanup utility will allow you to delete all but the most recent restore point.

You can launch Disk Cleanup from the Start | All Programs | Accessories | System Tools menu. Once Disk Cleanup is running, select the More Options tab and click the Cleanup button in the System Restore panel. You'll then be prompted to confirm the delete operation.

5: Reining in System Restore's disk space usage

To perform its operations, System Restore requires at least 200 MB of available hard disk space. However, if more disk space is available, System Restore will claim up to 12 percent of it to save the restore points. Although System Restore can use that full 12 percent if it's available, this chunk of disk space is not reserved. System Restore will yield disk space back to the system if it's needed. Furthermore, restore points more than 90 days old are automatically purged by default.

If you want to see how much hard disk space System Restore has potentially set aside on your system, press [Windows][Break] to bring up the System Properties dialog box and then choose the System Restore tab. Next, select your hard disk from the Available Drive list and click the Settings button. When the Drive Settings dialog box appears, you'll see a number in the Disk Space Usage panel that represents the amount of space in MB that System Restore is using to amass restore points.

For example, on a system with an 80GB hard disk, System Restore's 12 percent amounts to nearly 9 GB. If you feel that System Restore has the potential to take up too much disk space, move the slider to the left to specify a more reasonable amount of hard disk space for System Restore to store its multiple restore points.

6: Manually creating a restore point

System Restore will automatically create restore points, but you can manually create one anytime you want. To do so, launch System Restore and then follow along with the wizard. If want to save yourself a few steps, you can simplify

the launching process by copying the System Restore shortcut from the Start | All Programs | Accessories | System Tools menu to the desktop

7: Bypassing the System Restore Wizard

If you want to be able to manually create a restore point without having to go through the wizard, you can create a simple two-line VBScript file that uses WMI (Windows Management Instrumentation) to instantly create a restore point. Just launch Notepad and type these two lines:

```
Set IRP = getobject("winmgmts:\\.\\root\default:Systemrestore")
```

```
MYRP = IRP.createrestorepoint ("My Restore Point", 0, 100)
```

Then, save the file as MyRestorePoint.vbs. Now, you can easily create a restore point by double-clicking the script's icon. When you do, System Restore will run in the background without displaying its interface and will create a restore point called My Restore Point.

8: Steps to avoid restoring viruses

If you know that your system is infected by a virus, you should temporarily turn off System Restore. Otherwise, the virus could be saved along with other system files in a restore point and reintroduced to your system during a restore operation at a later date.

To turn off System Restore, press [Windows][Break] to bring up the System Properties dialog box. Then, choose the System Restore tab, select the Turn Off System Restore check box, and click OK. As soon as you do, you'll see a confirmation dialog box warning you that turning off System Restore will delete all existing restore points. Click Yes to continue.

You can now use your antivirus software to clean up your system. When the virus has been eradicated, access the System Restore tab again and clear the Turn Off System Restore check box. Click OK to re-enable System Restore.

9: Disabling System Restore for data drives

(Continued on page 15)

If you have additional hard disks connected to your computer, System Restore will automatically add them to its list of monitored drives. If these additional drives just store data or data backups, there's no reason to have System Restore monitor them.

To disable System Restore for data drives, press [Windows][Break] to bring up the System Properties dialog box. Then, choose the System Restore tab. Next, select your hard disk from the Available Drive list and click the Settings button. When the Drive Settings dialog box appears, select the Turn Off System Restore On This Drive check box and click OK. You'll see a confirmation dialog box warning that by turning off System Restore on this drive, you won't be able to track or undo harmful changes on it. Click Yes to continue. Then, click OK to close the System Properties dialog box.

10: Determining the actual amount of space System Restore is using

You can easily determine how much disk space System Restore can potentially use, but you may also want to determine how much disk space System Restore is actually using. If you're running Windows XP Professional and the hard disk is using NTFS, you can find out.

You'll begin by making a few configuration changes from an Administrator account that will allow you to investigate the hidden and protected folder called System Volume Information, located in the root directory of your hard disk. Keep in mind that this information is meant only for investigative purposes. Making any changes to the files in the System Volume Information folder will disrupt or otherwise damage System Restore's ability to do its job.

From within Windows Explorer, access the View tab of the Folder Options dialog box. Then, select the Show Hidden Files And Folders option, deselect the Hide Protected Operating System Files check box, and click Yes in the Warning dialog box. (If the system is in a workgroup, you'll need to deselect the Use Simple File Sharing check box as well.) Click OK to close the Folder Options dialog box.

Now, access the root directory of the hard disk,

right-click on the System Volume Information folder, select Properties, and access the Security tab. Then, click the Add button, enter your user account name in the Select Users Or Groups dialog box, and click OK twice to close both dialog boxes.

At this point, you can open the System Volume Information folder, right-click on the _restore folder, and select Properties. Once Windows XP finishes tallying, check the Size On Disk value to see the exact amount of space System Restore is using for restore points. To ensure the security of the restore point files, you should remove your user account from the System Volume Information folder once you finish your investigation