11-1-2009

Snips, Snails, Truffles, Malware Warnings, and other Tidbits to Chew On

Pat McGregor

Follow this and additional works at: http://commons.pacificu.edu/inter09

Recommended Citation

This Article is brought to you for free and open access by the Interface: The Journal of Education, Community and Values at CommonKnowledge. It has been accepted for inclusion in Volume 9 (2009) by an authorized administrator of CommonKnowledge. For more information, please contact CommonKnowledge@pacificu.edu.
Snips, Snails, Truffles, Malware Warnings, and other Tidbits to Chew On

Rights
Terms of use for work posted in CommonKnowledge.

This article is available at CommonKnowledge: http://commons.pacificu.edu/inter09/64
Snips, Snails, Truffles, Malware Warnings, and other Tidbits to Chew On

Posted on November 1, 2009 by Editor

By Pat McGregor

Danger! Have your “Fans” been Checking you out on Facebook?

Your friends on Facebook may have been urging you to remove the increasingly popular “Fancheck,” which does the numbers and gives you some info about the totality of your friends, such as “most common name” and “average age”. But the malware is actually the interesting Facebook app “Removal Kits,” which many people have been buying and consequently giving fraudsters their personal info and credit card info.

Sophos Software Online expert Graham Cluley warns,
...hackers have set up websites pretending to be about the "Facebook Fan Check Virus", but which really host fake anti-virus software which display bogus warnings about the security of your computer in an attempt to get you to install fraudulent software and cough-up your credit card details. [1]

But, Facebook isn’t the only site plagued by this. Even the venerable New York Times had malware ads injected in the middle of September 2009.

![Warning: Visiting this site may harm your computer.](image)

Even worse, the Times says that the advertiser, posing as Internet phone company Vonage, sold the ads directly to them rather than through an ad vendor:

The creator of the malicious ads posed as Vonage, the Internet telephone company, and persuaded NYTimes.com to run ads that initially appeared as real ads for Vonage. At some point, possibly late Friday, the campaign switched to displaying the virus warnings.

*Because The Times thought the campaign came straight from Vonage, which has advertised on the site before, it allowed the advertiser to use an outside vendor that it had not vetted to actually deliver the ads, Ms. McNulty said. That allowed the switch to take place. “In the future, we will not allow any advertiser to use unfamiliar third-party vendors,” she said. Mr. Frons said it was unclear how many people saw the ads. [1b]*

This was a huge surprise to those of us who track these sorts of events. You’re more likely to see this on websites without such a scrupulous reputation, and generally with those using ad networks to manage what ads show up on their sites. (See my article last month on Behavioral Tracking for more info on how online ads work. [1c]

**In August, US Healthcare Debate Topped the Inbox Chart, But Then, Most Email Is Now SPAM**

According to Austin Modine in the online website The Register,

Health-care spam held a solid lead with 68.8 per cent of unsolicited emails. Miscellaneous offers accounted for 12.3 per cent, education 4.4 per cent, gambling 1.3 per cent, and foreign
language spam only 1.1 per cent. [2]

But, as you probably noticed, most of the email sent (and received) is now spam. Although your personal filters or your email provider may filter it out, spam now accounts for nearly 95% of the email whizzing around the Internet. [3]

Let’s do the Numbers

CSO Magazine always has an interesting column on “numbers” with InfoSec factoids or Trivia. This month’s:

- $704,610: Amount of money attackers siphoned out of bank accounts belonging to the Western Beaver County School District.
- 11: Number of vulnerabilities fixed in Firefox 3.0 in late July.
- 10: Number of Firefox flaws that were considered critical.
- 4: Approximate number of months remaining until Mozilla kills of Firefox 3.0 and forces users onto Firefox Version 3.5.
- 9: Number of security patches Microsoft released in August.
- 300: Number of companies attacked by the same malware that enabled the data security breach at Heartland Payment Systems (according to Heartland CEO Robert Carr) [4]

Antimalware: Not just about Viruses Anymore...

A great many people figure that the Norton or Symantec suites that come on their pre-loaded machines will do the stuff — not realizing that it’s no longer just virus software. Information Security Magazine polled their readers for the best business-grade desktop and server antivirus and antispyware products. You won’t be surprised to find that many security-savvy home users use these products (or their single-user products) instead of the more familiar ones. But what may surprise you is the variety of apps you get rolled into one. Natalie Lambert, an analyst at Forrester Research, says:

Generally speaking, antimalware is antimalware; what you get from one vendor is not much different than what you get from another. Where the market is changing is that there are lots of components required to have a comprehensive strategy. Antimalware alone is not going to cut
It’s hard to buy antimalware alone; vendors are almost forcing you to buy a client suite. [5]

You may be surprised to find that the big players you may be most familiar with are not in the top three. Instead, we find:

**GOLD** Kaspersky Open Space Security, Kaspersky Labs

“Kaspersky Open Space Security is the company’s suite of antimalware protection for the gateway and endpoint. It includes: Work Space, which keeps workstations secure; Business Space, which adds file server protection; Enterprise Space, which adds mail server security; and Total Space, which adds gateway protection to the previous offerings. It received high marks for detecting, blocking and cleaning malware, and in the speed and frequency of signature updates.” [6]

I recommend you look at their home protection suites as well (Internet Security 2010, Anti-Virus 2010, Security for Ultra Portables, Mobile Security), as they have gotten high marks from fellow security geeks.

**SILVER** Sophos Endpoint Security and Data Protection, Sophos

“Sophos’ Endpoint Security and Data Protection wraps antivirus, firewall, network access control and encryption into a neat package that voters liked for its quick signature updates, and reporting and alerting capabilities. You can also centrally manage the security status of your endpoints from one console; the product supports Windows, Unix and Linux.” [6]

Sophos is not only hot software, but they maintain a terrific online source of threats, mitigations, and top-notch white papers and expert discussions.

**BRONZE** ESET NOD32 Antivirus, ESET

“ESET NOD32 Antivirus offers not only antivirus and antispyware protection, but a personal firewall and antispam capabilities. Voters were keen on the product’s ease of installation, configuration and administration. NOD32 requires 44MB of memory, less than other similar products. Voters also said they were able to get a significant ROI from this product.” [6]
ESET also received the CNET Editor’s Choice in April, 2009. I have just been learning more about them, myself, but these two selections make me advise that you take a look, too.

And, finally....

Even the President gets caught by the Law of Unintended Consequences...

President Obama, in an unguarded moment, referred to a recent spat between two music stars at MTV’s Video Music Awards, and said he thought one of the people was “a jackass.” Now, the unintended consequence wasn’t that someone heard him say it, or even that someone twittered away immediately with “Pres. Obama just called Kanye West a ‘jackass’ for his outburst at VMAs when Taylor Swift won. Now THAT’S presidential.” [7]

Nope, it was this small event that toppled big dominoes and caused a fuss:

Harwood [from CNBC. Ed.] had sat down with the president to tape an interview following his appearance on Wall Street on Monday. Although they are competitors, CNBC and ABC share a fiber optic line to save money, and this enabled some ABC employees to listen in on the interview as it was being taped for later use. [8]

I am certain that CNBC and ABC never thought when they made the deal that in sharing dark fiber (unused bandwidth) they would enable a competitor to listen in, and use a social media tool no-one had invented to immediately share an off-the-record remark in the warm-up to an interview. At some point later we can debate whether Twitter is going to be the final spike in the process that kills the ability to control one’s personal information.


Endnotes


http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1365969_mem1,00.html, Retrieved 14 Sept 2009


[8] Ibid.

This entry was posted in Uncategorized by Editor. Bookmark the permalink 
[http://bcis.pacificu.edu/interface/?p=3699]

22 THOUGHTS ON “SNIPS, SNAILS, TRUFFLES, MALWARE WARNINGS, AND OTHER TIDBITS TO CHEW ON”

**best charcoal grill**

on January 31, 2014 at 10:30 AM said:

I’ve been surfing online greater than three hours these days, yet I never found any fascinating article like yours.

It is pretty value sufficient for me. In my opinion, if all site owners and bloggers made just right content material as you probably did, the net will probably be a lot more helpful than ever before.

**lose weight using an elliptical**
Incredible! This blog looks exactly like my old one! It’s on a completely different subject but it has pretty much the same layout and design. Outstanding choice of colors!

Greetings! This is my first visit to your blog! We are a team of volunteers and starting a new project in a community in the same niche. Your blog provided us valuable information to work on. You have done an outstanding job!

Good answer back in return of this matter with genuine arguments and telling everything on the topic of that.

Great post.

I hardly leave remarks, but I looked at some of the comments here Snips, Snails, Truffles, Malware Warnings, and other Tidbits to Chew On | Interface. I do have 2 questions for you if it’s alright.
Could it be simply me or do some of these comments appear like they are written by brain dead folks? 😊 And, if you are posting at additional online social sites, I would like to follow you. Could you list of the complete urls of all your social networking sites like your Facebook page, twitter feed, or linkedin profile?

**induction cooktop reviews**

*on February 3, 2014 at 10:27 PM said:*

Sweet blog! I found it while surfing around on Yahoo News. Do you have any tips on how to get listed in Yahoo News? I've been trying for a while but I never seem to get there!
Cheers

**best robotic pool cleaner**

*on February 3, 2014 at 11:05 PM said:*

Your style is very unique in comparison to other folks I've read stuff from.
Thank you for posting when you have the opportunity, Guess I will just bookmark this blog.

**best vacuum sealer**

*on February 3, 2014 at 11:24 PM said:*

I do trust all the ideas you have presented in your post. They're really convincing and can certainly work. Still, the posts are too quick for beginners. May just you please prolong them a little from next time? Thanks for the post.
infrared grill reviews

on February 4, 2014 at 12:12 AM said:

This website was… how do you say it? Relevant!! Finally I have found something that helped me.
Kudos!

best jig saw

on February 4, 2014 at 12:37 AM said:

Hey I know this is off topic but I was wondering if you knew of any widgets I could add to my blog that automatically tweet my newest twitter updates. I’ve been looking for a plug-in like this for quite some time and was hoping maybe you would have some experience with something like this. Please let me know if you run into anything.

I truly enjoy reading your blog and I look forward to your new updates.

humidifier reviews

on February 4, 2014 at 1:56 AM said:

I was wondering if you ever thought of changing the layout of your site? Its very well written; I love what you’ve got to say. But maybe you could a little more in the way of content so people could connect with it better. Youve got an awful lot of text for only having 1 or two pictures. Maybe you could space it out better?

Gregorio

on February 4, 2014 at 3:11 AM said:

I am really inspired together with your writing abilities and also with the layout on your
weblog.
Is that this a paid theme or did you modify it yourself?

Either way stay up the excellent high quality writing, it is rare to look a nice blog like this one nowadays..

rifle scope reviews
on February 4, 2014 at 3:42 AM said:

This paragraph is in fact a pleasant one it assists new internet visitors, who are wishing for blogging.

best vacuum for hardwood floors
on February 4, 2014 at 5:11 AM said:

Wonderful goods from you, man. I have understand your stuff previous to and you are just extremely magnificent. I really like what you’ve acquired here, certainly like what you are stating and the way in which you say it.

You make it entertaining and you still take care of to keep it wise. I can’t wait to read much more from you. This is really a tremendous site.

best shoes for crossfit
on February 4, 2014 at 5:13 AM said:

I constantly emailed this web site post page to all my contacts, since if like to read it after that my friends will too.

table saw reviews
Hmm is anyone else having problems with the images on this blog loading?

I’m trying to figure out if its a problem on my end or if it’s the blog. Any feed-back would be greatly appreciated.

Sheena

Hey there! I realize this is somewhat off-topic however I needed to ask. Does operating a well-established website such as yours require a large amount of work?

I am brand new to writing a blog but I do write in my journal every day. I’d like to start a blog so I can easily share my own experience and feelings online. Please let me know if you have any ideas or tips for brand new aspiring blog owners. Thankyou!

Hi, its fastidious article concerning media print, we all understand media is a wonderful source of facts.

Hi there! This article could not be written much better! Going through this post reminds me of my previous roommate! He always kept preaching about this. I most certainly will forward this article to him. Pretty sure he will have a good read. I appreciate you for sharing!
Teresa
on February 6, 2014 at 7:23 AM said:

You really make it appear really easy along with your presentation but I in finding this matter to be actually one thing which I feel I would never understand. It sort of feels too complicated and extremely vast for me. I'm having a look forward on your next post, I will attempt to get the cling of it!

Nicole Shotton
on February 6, 2014 at 12:54 PM said:

Ciao a tutti, appena iniziato oggi. Web forum Nizza!