

Re: Your opinion matters

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2006-06/msg08235.html>

- *From:* "Vanguard" <vanguard.news@xxxxxxxxxxxxx>
 - *Date:* Sat, 24 Jun 2006 00:55:26 -0500
-

"Elmo" <none@xxxxxxxxx> wrote in message [news:Fc2ng.389\\$Tk.26@xxxxxxxxxxxx](mailto:news:Fc2ng.389$Tk.26@xxxxxxxxxxxx)

Vanguard wrote:

So you want us to volunteer to be unpaid documentation QA employees because you don't want to spend the money in-house or don't have the resources?

You must take reading classes before you answer. I asked for your opinion, not add-on.

No, your Subject asked for an opinion but the body of your post asked for comments. Comments are directed at the content of your document and may alter it. As yet, you have to explain why I would need reading classes. I read just fine. What you asked was so vague that anyone can construe whatever they want as regards to "commenting" on your document. If all you want is some overall rating of your document, well, it is too simplistic (i.e., it is not a comprehensive document) and wanders off on topics that have nothing to do with securing the *host*. Of course, this assumes your document is finished rather than a work in progress.

You mention programs that have nothing to do with the topic of your document: securing the host. You talk about security of e-mail but that doesn't secure your host. How does using OpenOffice improve security? It has its own macro language that can be abused as easily as the one in Word or Excel. It is not a security-related product. You make statement like "Considering the outrageous price of MS-Office, ..." which lends further to the non-professionalism of the entire document. Pricing can be mentioned but it should not dictate the value of a product on its merits alone. The free OpenOffice isn't anymore secure than MS-Office. Some users also consider almost all commercial anti-virus software to be outrageously priced, but then too often they are cheap bastards that aren't willing to pay the appropriate value for software and end up using the less effective freebies. Free is nice if it is effective, and even better if it is MORE effective than commercial solutions, but just because a product is commercialware doesn't disqualify it as being a viable choice. I'm not pro-Microsoft and, in fact, will probably switch to OpenOffice if I feel that my old Office 2002 is no longer a viable solution to my tasks. But if I were generating documents at home on my own computer that were absolutely required to be compatible with software used at my employer or by by customers, I'd probably qualify the cost of using Word over the free OpenOffice (as OO still isn't 100% compatible). Yet what does using OpenOffice over using Word have to do with security? What does discussing the tabbed pages in Firefox have to do with security? Too much is spent on discussing products or features of them that have nothing to do with security of a user's host. Those are preferences, not security measures.

Re: Your opinion matters

I get the general feeling that the document was written by some home computer users rather than by professionals within the industry. Too much bashing without qualification. You'll bash Microsoft as outrageously priced yet you recommend using Acronis which costs \$60 while there are free disk clone utilities plus there are problems with Acronis (you will not get the exact state of the hard drive after restoring an image as when the image was created). What does saving partition images have to do with security? They are for disaster recovery and may well themselves have the malware that you are trying to get rid of. If the host is infected then so are the backups made after that point. Using Acronis does nothing to secure your host.

Using GnuPG has nothing to do with securing your host. It secures the content of your [e-mail] communications against OTHERS from seeing it plus it helps identify the sender. It won't prevent the introduction of viruses in attachments or buffer overruns in the embedded images that utilize a weakness in the graphics engine (by using the e-mail client as a vector to the host) to deliver malware, and it won't eliminate web bugs (but, of course, has nothing to do with securing your host but then you wander off that topic, too). Why add on GnuPG when the e-mail client already supports x.509 certs? Encrypted e-mail has been around for a LONG time, like 8 years, but its presence goes ignored by home users even when they know of it. Again, home users are the ones that often reduce or circumvent security to increase ease-of-use. You mislead the readers into thinking that encrypting the content of their e-mails will somehow add to the security of their host. Data security is not the same as host security.

Under the section discussing Thunderbird, "Outlook is also known to be weak on security, especially for those who do not update their virus definitions on time." Huh? What has updating your anti-virus program have to do with the security features of an e-mail client? Outlook [Express] is configured, by default, to use the Restricted Sites security zone (which should be set at its default High setting) which will neuter all HTML-formatted e-mails. The user can even go further by configuring them to read in plain-text only mode. In Outlook, they could NOT use the Preview mode and instead use the AutoPreview mode that shows the first lines in plain text of each mail. Your regurgitate fallacies regarding security in Outlook without qualification. The only vulnerability (for HTML-formatted e-mails) not addressed by any security zone in Windows is for web bugs, but then Outlook [Express] has the option, again by default, to block linked images. However, again, web bugs are NOT related to host security. The rules in Thunderbird are more IMpotent than those in Outlook and even of those in Outlook Express. Please don't try to involve spam filtering since that also has nothing to do with host security, plus there are far better anti-spam solutions, even free ones, than what comes in Thunderbird.

You proselytize your favorite solutions rather than cover all available solutions and compare their weaknesses and strengths; i.e., you proliferate the same old trite content without qualification. The document becomes "what we like best" and wanders off onto non-security discussions. I'll be reading through your document and come across some opinion regarding a product or feature and wonder what the hell that has to do with securing the host. When they are on-topic, you'll make comments like, "By default, Microsoft Windows sets up all user accounts with Administrator privileges on any Microsoft desktop operating system that are initially created through the setup process." This is misleading. Only one account gets automatically created during the setup: the Administrator account. The other accounts are those created by the admin *user* and AFTER the install, so it up to the admin to decide who gets admin rights, not the setup program that isn't running anymore. Also, this is not something unique to MS Windows. Solaris does it, too. When you install Solaris 10 x86 on an Intel box, you aren't asked to create additional "user" accounts during the install, and when the install has completed the account you have for logging in is the root user. Obviously the install of the OS has to create the admin account so the admin can login and start creating accounts, adding devices, installing software, etc. It is after the install that the admin must create user accounts. Just because some boob can install Windows doesn't mean they are qualified to administer it. Therein lies the fallacy that Windows defaults to the Administrator account when, in fact, it is the ignorance of the user in not understanding the OS and not even reading a book or taking a class on it, like giving a child a loaded handgun and expecting them to know

Re: Your opinion matters

how to handle it. In corporate environments, the workstations are configured so users have restricted privileges (unless, say, they are developers). Imagine the outcry of home users that install Windows and then find they can't even install software because they haven't a clue that they got logged in under a restricted account. How many even know of the RunAs command so they get admin rights only temporarily to limit their exposure? In fact, the Administrator account itself should never be used for casual tweaking of the OS or installing software. That is, do not use the Administrator account for anything other than an emergency. You need to protect that account profile by not using it unless absolutely necessary. Create another admin-level account and use that one when you need admin rights. Use the Administrator account as an emergency backup when the profile for your normal admin account gets hosed.

Security is lax for home users because that is how they configure Windows and most even want it that way. Security and ease-of-use are the antithesis of each other, and security measures that are required in a corporate network don't make sense on a home computer. The major problem regarding security in Windows is not with Windows but in educating the users, especially those that think simply installing an OS qualifies them as having the expertise to administer it. There are problems regarding security that are innate to Windows. Unix and its variants tend to be more secure but then, from what I've seen, its users are also more educated than the typical Windows boob that can manage to slid a CD into the drive and manage get Windows installed. Look at all the posts asking how to subvert the security built into e-mail clients so users don't have to bother with that security and can willy nilly open any document and even do so automatically. You want Microsoft to hand-hold the users because the users don't want to be administrators or don't know how? Software vendors are not your parents. If you install the OS, it is your responsibility to administer it, so it is your responsibility to create the appropriate accounts for yourself and other users. Just because you can install an OS doesn't qualify you as being an administrator of it. Put a CD in their hand and they think they know everything about managing Windows, yeah, right. Just because you can weild a wrench doesn't qualify you as a car mechanic. Alas, the Windows install must be constructed in such a way that any boob can install the OS, so you get lots of boobs that haven't a clue how to administer the OS.

You make statements like the user not having anti-virus software makes them vulnerable to infection. No, their BEHAVIOR makes them vulnerable. No matter how much security you add to a host, users can and will undo or circumvent that security, if possible. Having anti-virus software doesn't guarantee that opening an e-mail attachment "from your friend" will not infect your host. You can add anti-virus software, intrusion protection software, heuristic software watching behavior of programs, database-driven anti-malware software (that checks a server for the latest definitions), and so on but the user can still say bypass every warning prompt or configure those protections to effectively disable them. Having the e-mail client configured to not automatically open attachments, even if just images, read in plain-text format or use the Restricted Sites security zone at its High setting, anti-virus software, IPS (like Prevx), and other protections only provides some security, but the user that decides to open the file or run the executable despite it all then obviates all those protections. They install a software firewall with app rules and yet they bitch about all the one-time prompts to authorize or not so they turn it off. They use Prevx or some other IPS software, don't want to figure out the prompts, and turn off those prompts (and let all apps make connections).

The copy right are there to prevent a case like we had in the past where someone took liberty to sell an old manual we had for integrating Novell clients into windows group policies.

So the "comments" you are looking for are not for corrections, spelling errors, regarding structure, corrections or suggestions for better descriptions, or for anything specific to the content of your document. Why not then simply ask for a rating scale of 1 to 5 as to the readers' opinion on the *value* of your document since they are not to address anything specific within?

Re: Your opinion matters