CIO/CTO Perspective Policy and Regulation Defense in Depth Security Business Insights Voice and Collaboration Solutions IP Solutions
Virtualization & On-Demand

Home » Blogs » lippard's blog

Understanding information security threats: folk models

Wed, 03/30/2011 - 18:22 | by **Jim Lippard**

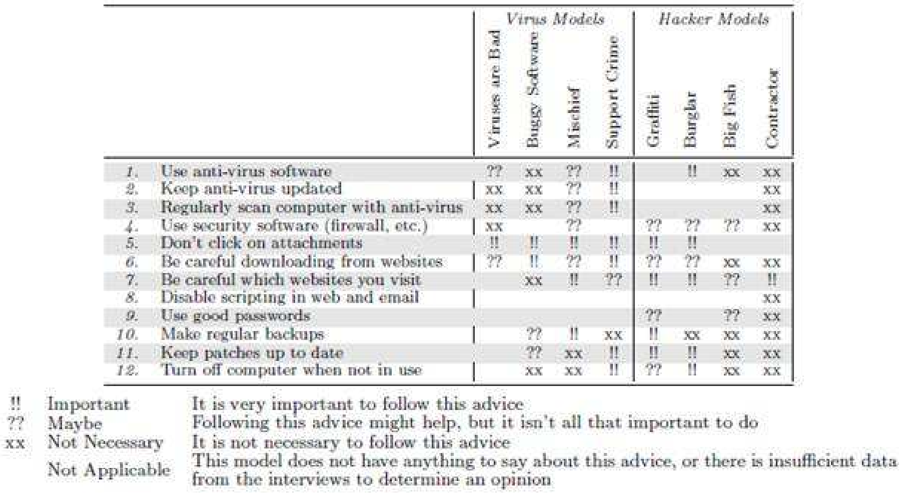
Like 6

"There's nothing on my computer anyone would want." This has been a common excuse for lack of concern about home computer security, given by users who think that the only relevant threat is theft of personal information stored on their computer. Such a person might add, "I don't use it for online banking or shopping online," or point out that they aren't a person of any particular significance to be targeted.

Rick Wash, assistant professor in the department of telecommunications, information studies, and media and at the school of journalism at Michigan State University, conducted research on non-expert computer users' mental models of the threats of viruses and hackers in a paper he presented at the 6th Symposium on Usable Privacy and Security (SOUPS). He identified four models each of "virus" and "hacker" which explained users' security decisions. For example, those who saw viruses as simply "bad" or "buggy software" didn't see the need for antivirus software—given their understanding, the way to avoid viruses is to not install such software by not downloading it and by not opening email attachments from people they don't know. Those who saw viruses as a source of "mischief" or as something used to "support crime," however, had a more complex understanding that recognized other modes of infection, and the latter recognized the importance of antivirus software and regularly scanning their machines.

Similarly, those who saw hackers as engaging in electronic "Grafitti" or akin to an Internet "Burglar," acting in an opportunistic fashion, understood the value of staying up-to-date on patches. Those who saw hackers as only going after "Big Fish" or as a "Contractor" working for criminals, on the other hand, were likely to say something like the opening quote—that hackers were only after specific information of value.

The following table from Wash's paper (Table 3, p. 10) summarizes the attitudes towards various recommended security practices held by those with these different "folk models" of the security threats from viruses and hackers:



		Virus Models				Hacker Models			
		Viruses are Bad	Buggy Software	Mischief	Support Crime	Graffiti	Burglar	Big Fish	Contractor
1.	Use anti-virus software	??	xx	??	!!		!!	xx	xx
2.	Keep anti-virus updated	xx	xx	??	!!				xx
3.	Regularly scan computer with anti-virus	xx	xx	??	!!				xx
4.	Use security software (firewall, etc.)	xx		??		??	??	??	xx
5.	Don't click on attachments	!!	!!	!!	!!	!!	!!		
6.	Be careful downloading from websites	??	!!	??	!!	??	??	xx	xx
7.	Be careful which websites you visit		xx	!!	??	!!	!!	??	!!
8.	Disable scripting in web and email								xx
9.	Use good passwords					??		??	xx
10.	Make regular backups		??	!!	xx	!!	xx	xx	xx
11.	Keep patches up to date		??	xx	!!	!!	!!	xx	xx
12.	Turn off computer when not in use		xx	xx	!!	??	!!	xx	xx

!!	Important	It is very important to follow this advice
??	Maybe	Following this advice might help, but it isn't all that important to do
xx	Not Necessary	It is not necessary to follow this advice
	Not Applicable	This model does not have anything to say about this advice, or there is insufficient data from the interviews to determine an opinion

Noticeably absent from these models is a recognition of the most common actual use of a home computer user's system by hackers—as an intermediary platform for further activities. A hacker can install bot software on a system that doesn't produce any obvious effects to the end user, but allows it to be controlled along with other similarly compromised systems. This gives the hacker access to a large base of computing power—a botnet—which can be used to send spam, launch attacks, distribute malware, collect and store data, and so forth. An understanding of this sort of threat may motivate more of the recommended security actions in the table above, if the risks are understood.

There is perhaps no better illustration of the potential harms and inconvenience that can arise from allowing unknown third parties to gain access to and use one's home computer network as a base of operations than a recent news story from Buffalo, NY. On March 7, police broke down the front door of a Buffalo businessman's home and seized his computer,

Follow Global Crossing

Subscribe to our Level 3 Blog

Languages

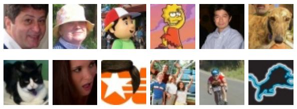
English

Search

Search

Connect on Facebook

Like Luiz Carlos Damasio, Erica Palmer Erkkila and 1,809 others like this.



Cloud Services Suite

Click Again for Full Screen

User login

Username: *

Password: *

Log in

Log in using OpenID

Create new account

accusing him of downloading child pornography. It quickly became apparent, however, that the problem was his open wireless connection being used by a neighbor, who was subsequently arrested. But had the access been through the businessman’s computer, not just his WiFi, he might be in jail today. As knowledge of cases like this spreads, it is likely to result in more complex folk models of home computer security.

Tomorrow: ***Expert threat models***

More information:
Rick Wash, "Folk Models of Home Computer Security"
Buffalo News: "Open WiFi leads to child porn raid"
Jim Lippard, "Botnets, Zombies, and Remote Control Attacks"

Like

Add New Comment

Login

Type your comment here.

Showing 0 comments

Sort by oldest first

M Subscribe by email S RSS

Trackback URL http://disqus.com/forur

Jim Lippard's blog Português Español
Tags: Defense in Depth Security Folk Models hackers Rick Wash SOUPS

Request new password

Recent blog posts

- Global Crossing Genesis Solutions International Events Part 2 of 2 - "Operationalizing the deal"
- Global Crossing Genesis Solutions International Events Part 1 of 2 "Winning the deal"
- IPv4 Addresses for Sale?
- Recap at IBC 2011 - Global Crossing Genesis Solutions
- Regional and global bandwidth expansion boom
- Tips to prevent voice communications systems fraud
- PSN Cost Savings in the UK Government Sector
- Advanced Cyber Attacks Require Sophisticated Technology
- Application management on Data Center critical enviroments
- Crowning glory for Global Crossing (UK) Telecommunications Limited

more

Legal Disclaimer

Disclaimer: Opinions expressed here and in any corresponding comments are the personal opinions of the original authors, and do not necessarily reflect the views of Global Crossing. The content is provided for informational purposes only and is not meant to be an endorsement or representation by Global Crossing or any other party. This site is available to the public. No information you consider confidential should be posted to this site. By posting you agree to be solely responsible for the content of all information you contribute, link to, or otherwise upload to the Website and release Global Crossing from any liability related to your use of the Website.