

It all comes down to YOU - The User



Peter Silva, 2009-14-12

One of my favorite Security writers, [Bruce Schneier](#), had an interesting entry last week called [Reacting to Security Vulnerabilities](#) where he discusses the recent reports about the [security flaw in the SSL protocol](#) and how we as users should relax and essentially, 'do nothing.' "What?!? – *Do nothing??*" Yup, and he has some good reasons why. Usually, new exploits, threats, breaches and the typical security stuff that garners the headlines, makes security folks jump. Jump to search the internet for anything related, jump to see if our systems are infected or vulnerable, jump to put an action plan in place to reduce the risk. These are reactionary behaviors when gloom gets delivered and we fully don't understand the risk. I'm not saying ignore warnings or plan for the worst, but since several new 'weaknesses' seem to get published on a monthly basis, you do need to prioritize and put some context around it.



With anything in life, there are certain things we have control over and others we do not. For many years now, we've been warned that it is risky to click on [embedded links in a suspicious email](#) or dangerous to [click through the certificate warnings](#) from your browser and hopefully many people have changed their behavior. That's within our control. But when a researcher finds a specific vulnerability in a particular protocol, potentially affecting several vendors, there is really not much an individual user can do. Sure, you or the IT department can check with their vendor to see if it applies to their product but would you immediately stop using something when it's a critical part of your infrastructure. Once again, which is usually the case for security, you must weigh the risks and determine if it's within your control. Bruce points out that many of the vulnerabilities affect systems that are out of our control and if your data is already out there, unplugging your computer will not lessen the potential exposure.

What you can do is simply stick to your general security practices (AV/FW, OS patch, Auto updates, backups, common sense), which already protect you from a slew vulnerabilities but let the experts/vendors figure out the best way to handle new exposure(s) since they must deal with them on a daily basis. If the risk is too great and your infrastructure is vulnerable, push your vendor for an answer. Most vendors, especially with security products, are fairly reasonable and typically move fast when it comes to security holes – their reputation and revenue are at risk. You can also report to [CERT](#) if you're not getting a response but most vulnerability 'finders' alert the vendor first and give them a chance to fix or respond to it.

Protecting yourself from the multitude of threats on the internet can be daunting, never ending, and always changing so you do need to be vigilant with the things you can control but as you peruse the [Top 9 Beaches of 2009](#) or the [Top 15 Most Common Attacks](#), you find there was/is little you could do to avoid them.

ps

- #25 out of [26 Short Topics about Security](#)
- Previous stories: [24](#), [23](#), [22](#), [21](#), [20](#), [19](#), [18](#), [17](#), [16](#), [15](#), [14](#), [13.5](#), [13](#), [12](#), [11](#), [10](#), [9](#), [8](#), [7](#), [6](#), [5](#), [4](#), [3](#), [2](#), [1](#)

**For the record, F5 is listed on the US-CERT site as being potentially vulnerable but we have tested our products/versions and are not vulnerable to this issue. F5 Networks has published a security advisory in the past to cover similar vulnerability and provide best practice recommendations. These best practice recommendations can be found at the F5 support site:*

<https://support.f5.com/kb/en-us/solutions/public/6000/900/sol6999.html>

<https://support.f5.com/kb/en-us/solutions/public/10000/700/sol10737.html>

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113