

Security Mythology

Perhaps the biggest myth about security is security. This goes well beyond computers, but fundamentally, there is no security, there is risk management. If you stay in airplanes and never get into a car you are far less likely to die in an accident, however this is cost prohibitive and not very feasible. So you make concessions to go about living.



Randy Abrams

Computer security has its own share of myths. Here are some common myths.

1) "I have antivirus software so I can click on anything."

No antivirus product can detect everything. When you see "100% detection of in the wild viruses" it does not mean what you think. "In the wild" is an industry specific term that refers to detection of a very small subset of threats that are on a list called "The Wildlist". There is a good reason for this list, but it would take a whole article to explain. Simply put, it is unlikely that any antivirus product detects more than 80% of all of the threats that are really out there. When used properly, antivirus software helps to manage risk, not eliminate it. The proper use of antivirus software is as a layer of defense, not as a magic shield that absolves users of learning and using sound judgment.

2) "Macs can't get viruses"

There have been viruses that run on Macs for decades. Modern day Macs run on an operating system that is essentially a flavor of UNIX. The very first work to significantly disrupt the Internet only ran on some flavors of UNIX and would not run on DOS at all. That was the Morris Internet Worm. Viruses are not the big thing anymore, even on Windows. More than 80% of the threats we see are trojan horse programs. There has recently been increasing interest by the criminal element in creating this malicious software to run on Macs. Simply having a Mac does not make you secure. Currently there are far fewer threats for Macs, so using a Mac may help to manage risk, but it certainly does not eliminate it. There are also costs and conveniences to be factored into the use of any operating system.

3) "My router has a firewall so I don't need another one."

Most routers have a very rudimentary firewall at best. While useful, it is still a great idea to use either the Windows firewall, or an additional firewall. A firewall helps prevent bad things from coming in and in some cases prevents data from leaving improperly.

4) "I've done all of the above, so I am secure"

What you have done is a great start at managing risk, but it is never completely eliminated.

Feel free to email me at askeset@eset.com with any security related questions or topics you would like to see addressed in future columns.



Randy Abrams is Director of Technical Education for ESET

AskESET@eset.com

www.eset.com

610 West Ash Street, Suite 1900

San Diego, CA 92101 • 866.496-ESET

ESET paid for this space and is solely responsible for its content.