How do we convince busy colleagues to pay attention to security?

I have argued for many years and in many columns that social psychology teaches us the value of getting people involved, even in a small way, in the activity we want them to integrate into their daily life – into their worldview. One of the best ways to integrate security into our employees working habits is to give them useful information that can help them personally or that they can use to help their families and friends stay safe in the ever-growing world of electronic communications. Every time an employee discusses or forwards a useful security tip – preferably one that has been professionally prepared, not a rumor about a Martian virus that will make computers explode into green goo – they actually subtly alter their own view of themselves: unconsciously, they come to think, “I am the sort of person who interested in security.” This change in self perception increases their willingness to cooperate with corporate security policies.

Recently I received word of a simple, short summary of some basic Web safety information freely available from Sophos that can serve our purposes in raising security consciousness and involvement. The “10 myths of safe web browsing” document (<http://www.sophos.com/security/topic/web-security-myths.html>) is only five pages long (the sixth page is just the company logo and copyright).

Chris McCormack, Product Marketing Manager at Sophos, introduces the booklet as follows:

“Are you suffering from misconceptions about safe web browsing? You might think you’re being safe, but with a newly infected webpage discovered every few seconds, it’s next to impossible to stay up to date on infected sites—no matter how educated or aware of the risks you are.

To start this assessment, ask yourself some questions.

Do you and your users practice safe web browsing? Avoid risky sites? Limit time spent online during work hours? Employ a rock-solid internet access policy? Use a secure browser? Have the experience to know a risky site when you see one?

If you answered ‘Yes’ to any of these questions, you need to read the rest of this report.”

I was surprised by the “Yes” in that last line (I immediately assumed it was a typographical error and should have been “No.” I queried the author, who responded as follows:

“The premise of this myths white paper is that most readers are likely aware that there are web threats... but have misconceptions about them. It’s assumed that most readers would answer ‘Yes’ to at least one of these questions, and thereby think they are protected, when in fact, they are clinging to a myth. If readers answer ‘No’ to all of these questions, then they are completely naive and this white paper about misconceptions is not for them.
They need more direct education of the threats and should probably study our Threat Report.”

I easily found several annual Threat Reports listed in the excellent collection of white papers available from Sophos<https://secure.sophos.com/security/whitepapers/index.html>, many of which will be equally helpful in raising employee security consciousness and self-identification.

In passing, I think the short paper, “Five tips to reduce risk from modern web threats”<https://secure.sophos.com/security/whitepapers/sophos-tips-to-reduce-web-threats-wpna> is particularly helpful for beginners.

In the next part of this two-part report, I’ll continue with a summary of Sophos’ ten myths.

* * *


Copyright © 2010 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.