Fall 11-15-2010

Hacked Off in the Web

Mark Y. Herring
Winthrop University, herringm@winthrop.edu

Op Ed — Little Red Herrings

Hacked Off in the Web

by **Mark Y. Herring** (Dean of Library Services, Dacus Library, Winthrop University)
<herringm@winthrop.edu>

Column Editor's Note: *An earlier version of this article appeared on the* ***Dacus*** *blog at* ***http://dacuslibrary.wordpress.com/category/bookmarks/****. — MH*

According to a new report (*http://tinyurl.com/2g6ghps*), if you are on the Web at all, you're not safe from hackers, phishers, and spammers (oh my!). The *Norton Cybercrime Report: The Human Impact* (*http://cybercrime.newslinevine.com/*) of 7,000 Web users tells us that 65% of all users globally, and 73% of U. S. users, have been hacked in some sort of cybercrime. Globally, the U.S. ranks very high but in this case we're not first in line. China wins Number One with 83% of its users Web-abused in some manner. These are figures to give one pause.

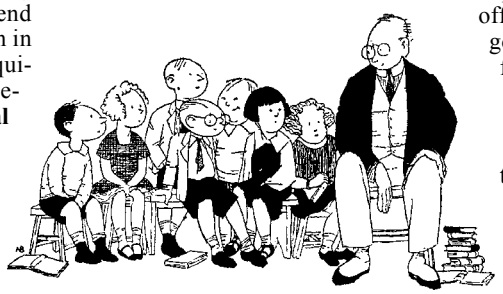
And there isn't much we can do about it, either. In a recent article (*http://nyti.ms/9gASVb*) in the *New York Times*, we are reminded that even strong passwords aren't the solution and neither is changing them or garbling them with letters and numbers. In fact, there are no certain safeguards. Apparently folks like **Scott McNealy** (*http://bit.ly/iX8Y*) and **Mark Zuckerberg** (*http://rww.to/4LSyfR*) are right after all. We all have no privacy anymore: it's dead, so get over it.

Plenty of blame for these privacy breaches exists to go around. But there are at least two places that shoulder much of it: our own stupidity and the nature of the free and open Web.

First, our own stupidity. We all — yes, even we brilliant academics — do really stupid online tricks. We reply, open, or follow emails from individuals we do not know. Some of us click on emails that tell us our email address is worth millions, and proceed to give the miscreants access to our thousands. Still others of us have passwords so simple even a caveman (my apologies to Neanderthals everywhere) could guess. Others of us still send passwords and security information in response to authentic-seeming inquiries. We also shop online where security leaks are the weakest. **PayPal** and **Amazon** — two favorite such places — appear to be the worst for allowing weak passwords and security loopholes.

The most recent and celebrated case of stupid human online tricks comes from a most unlikely example: **Duke** graduate, **Karen Owen** (*http://bit.ly/axMNri WARNING: very graphic*). **Owen** wrote up a 42-page mock thesis (which she subtitled "excelling in horizontal academics") about her sexcapades while in college. Complete with graphs and charts, detailing both the types of sex engaged in and the amount of alcohol consumed that powered these adventures, **Owen** sent the "joke" to a couple of friends. Not only was the story covered on the *Today* show, but it also went viral on the Web. Of course, **Owen** will likely get a book deal, but she flunks both propriety and basic computer privacy.

Then there are the social networks we join. **Facebook** (*http://www.facebook.com/*), in particular, has been among the most egregious in allowing security breaches. (With now more than a half billion people using it, perhaps the above-quoted cybertheft figures seem low upon reflection.) **Facebook** is allergic to privacy, or so it would seem. Privacy on **Facebook** has eroded over its existence, and in considerable ways (*http://bit.ly/9cTtYk*). An excellent discussion of that loss of privacy appears here (*http://www.deobfuscate.org/?p=166*). In order to protect your privacy in at least some manner on **Facebook**, you have to follow a number of steps (*http://read.bi/bfukbT*), meaning that **Facebook** privacy isn't exactly intuitive. Last month, without fanfare, the social networking giant changed its follow feature (*http://tcrn.ch/bvdamz*) so that now a two-step process to fully block a person is required. Of course, **Facebook** isn't the only culprit. **Twitter** (*http://twitter.com/*), **MySpace** (*http://www.myspace.com/*) and other social networks all have varying degrees of privacy problems. **Google's Buzz** (*http://tinyurl.com/2daghb4*), you may recall, was pulled after only a couple of months because its privacy had been handled so cavalierly.



Part two of the blame is the free and open Web. In addition to our less than brilliant online tricks, the other half of the blame goes to the Web itself. Web security came about almost as an afterthought. Even today, those twentysomethings creating the next latest and greatest application aren't thinking about security and/or privacy as a first, second or even third consideration.

And that is why security and privacy issues will never really be treated with anything other than contempt in our brave new world. I don't mean to sound petulant, or like a grumbling, old curmudgeon (which, of course, I am, and do sound like), but treating an individual's privacy in this manner is unacceptable. To talk about it at all is to reveal my age (*http://rww.to/clqbOt*). Apparently, only those of us over 50 care about online privacy (unless of course you're under 50 and have been a victim of cybertheft). Even the courts now tell us that you have no right to an expectation of privacy (*http://tinyurl.com/29jwhag*) when you go online. Those working in this industry do not understand privacy issues, and many think it much ado about nothing. The farther down the information superhighway we go, the more often we'll see little bits (and bytes) of personal privacy roadkill along the way.

So, seriously, what *should* we do? All sign off? Perhaps. But before you do, keep your security up-to-date when at home, don't surf to places where information is asked without knowing what the security certificate is, and never, never, never give out information to anyone whom you do not know personally — and even then, call them just to be sure. If you must order online, do so but not before you check the security certificate to see if it measures up, or ask someone who would know. I wish I could be more optimistic and give easy-to-follow steps, but none exist (beyond signing off) that I can think of. It's even a good idea to use a separate computer for all your checking needs and for nothing else.

Allow the moral of this story to be simply this: if you don't want to be a victim of cybertheft or have your personal information in the hands of those who can harm you, don't put enough of it online for anyone to use … ever.