Written by **C. Mitchell Shaw** on April 22, 2016

Colleges Fail to Prepare Students for Life in Digital Age

Little could be more valuable in the digital age than to have at least a basic knowledge of how to protect one's data. Sadly, colleges are not teaching those skills to students. The result is that many of today's young people are not as tech-savvy as they may think. And their lack of knowledge is dangerous to them and the institutions where they work and go to school.

A recently published study conducted last year illustrates part of the problem in startling clarity. In the study, 297 USB flash drives were dropped in various locations around the University of Illinois, Urbana-Champaign campus during the week of April 27, 2015. The drives were marked (or unmarked) in different ways: Some had labels with contact information for the "owner," some had labels marked "confidential" or "final exam solutions," some had keys attached, and some had neither label nor keys.

But all of the drives had one thing in common: buried in the normal types of files one would expect to find on such drives were HTML files containing an embedded img tag that allowed the team conducting the study to track when a file was opened on each drive. The HTML/img file would "call home" from any Internet-connected device into which it was inserted when any of the files were accessed. The "finder" was then contacted and asked to complete a survey to help the team better understand both the participants' understanding of technology and their reasons for inserting the drives into computers.

The result? As the authors of the study wrote in their final report:

> We find that users pick up and connect an estimated 45%–98% of the drives we dropped. Further, the attack is expeditious with a median time to connection of 6.9 hours and the first connection occurring within six minutes from when the drive was dropped.

So, on a university campus populated by educated (or at least in the process of *being* educated) young men and women who have grown up using computer technology, the first drive was inserted into an Internet-connected computer *within six minutes*. By the end of the week, 45–98 percent of the drives were connected to a device (the range takes into account those who connected the drive to a device that was not connected to the Internet at the time the drive was inserted). Surprisingly, the appearance and labeling of the drives had no real impact on whether the drives were inserted.

Furthermore, while the study revealed that the majority of people who found the drives acted out of a desire to locate the owner of the drive, "nearly half" accessed photos and other files on the drives

before opening the conspicuously placed resumé that would likely contain the contact information of the owner of the drive. Curiosity, it would seem, trumps altruism.

Most shocking, though, is the fact that more than two-thirds of the participants said "they took no precautions when connecting the drive." Of those who did take precautions, most were either inadequate or worse. Some admitted that rather than insert the drives into their own devices, they "sacrificed" a university computer. "In the end, all but a handful of the users who took precautions did so in an ineffective manner," the studies authors wrote, adding, "the majority took no precautions at all."

Luckily, this was only a study. If that same experiment had been conducted by hackers, the university's network would certainly have been compromised. The same is true for any office where any of the participants are employed. And as the study observed, "The students and staff that connected the drives were not computer nor security illiterate and were not significantly different than their peers at the University of Illinois." Since the University of Illinois is not unique, this experiment would likely have the same results anywhere. And this writer imagines many more scenarios where people unschooled in the protection of systems and data would likewise jeopardize themselves and those around them.

Beyond the fact that the majority of college students finding a stray USB drive will connect it to a computer, many (read: nearly all) teens and young adults seem also to miss the point of privacy. Perhaps they are only so much to blame for that: Fish don't know they are wet. Having grown up in a culture of surveillance where the expectation of privacy is at or near zero, they don't even have the nostalgia to look back on and miss.

As a consequence, today's college students are ripe for the data-mining. And tech companies from Google to Facebook to Microsoft are only too happy to profit from the privacy many of those students don't even realize they are losing. The companies that have made data-mining into a multi-billion dollar industry have a very real and vested interest in keeping the status quo exactly as it is. But some college students and administrators are pushing back and asking that colleges begin teaching their students about how to safely navigate the dire straits of the digital world.

In a letter to the editor of *The Chronicle of Higher Education* in February, Tracy Mitrano, academic dean of the University of Massachusetts Cybersecurity Certificate Programs wrote about "the difference between 'consent,' as in a checked box, and 'informed consent,' which … would take a course in information literacy for an upper-level high-school or college student to understand."

That type of course is exactly what Thomas Briggs called for in a recent article for a student newspaper of The College of William and Mary. Briggs wrote:

> Data is itself a product. Tracking people's online activity gives profitable insights into all types of consumer information, allowing corporations to build detailed digital profiles on potential customers. Because there are so few regulations that limit this type of profiling, corporations have every incentive to collect as much information as possible, which they use to both predict and influence every action we take online. Targeted advertisements and personalized search engine results are just two of the many ways in which our experience online is molded by forces other than our own choices. This commodification of data has led many to demand a greater degree of "informed consent" — the knowledge that a service is collecting our data should be made explicit, not hidden in a bloated terms of use agreement.

Since college is traditionally a place where young men and women are supposed to learn the skills

necessary to succeed in life, isn't it reasonable to expect that colleges would teach students about the basics of data security? I am not suggesting that every student must major in Network Security Management, but a one-semester class on how to protect your data (and the data of the college and your employer) would go a long way toward a well-rounded education in the 21st century.

As Briggs put it:

> If the College's mission truly is to mold us into informed citizens and consumers, an excellent place for it to start would be with this issue of data security and online privacy. Even a brief session during orientation would be an improvement; if not to teach us how to be fully secure in our data, then simply to let us know that it is not, by itself, fully secure.

As a father and self-professed crytpo-nerd, I could not agree more. In the digital age, computers (and the data they produce and store) play such a large role in our daily lives, that for colleges to ignore this educational need while issuing degrees would be the equivalent of colleges in the early 20th century turning out graduates who couldn't read or write.