WHY DON’T WE TRAIN FOR BETTER SECURITY?

Breaches of computer and network security are headline news. The mainstream press delights in the shock value of telling us that the data we all have stored on computers and transmitted across the Internet are exposed and exploited by mysterious forces, whom the media usually call “hackers.” In fact they are criminals, with the same motivation that many violent or white-collar criminals have. They are thieves who want to dispossess you, wrongly, of something you value so that they will have it instead.

How many people open an email attachment from a sender they do not know, and then are surprised when their computer becomes infected with a virus? How many people click on a link to a web site, fill in personal details on a form, and then are surprised to discover that their identity has been stolen? Even in the safest of communities we lock our doors at night, and yet when it comes to computers most people do not yet have this basic common sense.

The media does a great disservice by calling computer-based criminals “hackers” or sometimes, more accurately, “crackers.” They make it seem as if there is a particular sophistication in the nature of computer crime, in the face of which an ordinary user or even over-worked system administrator is defenceless. Most people find the operation of a computer system for a simple purpose to be overly complex, and so the added need to consider the security of that system while trying to figure out how to get it to work … the task can seem impossible. The threat implied by the media, which they never clearly define, doesn’t help matters.

In fact, computer-based criminals are not the evil geniuses cast as villains in Hollywood movies. Just like other criminals, the overwhelming majority of them are the equivalent of smash-and-grab thieves. They are “script kiddies” and not “elite crackers.” They can be defeated, or at least suppressed, just like unsophisticated criminals in any sphere of life: by taking common-sense precautions, and by being properly educated about what is a realistic threat.

If you leave your locked car in your garage at home, it is not very likely that an organized car theft ring will steal it from under your nose, without detection. If you leave your car unlocked and unattended, with the key in the ignition, in a parking lot at night, it is more likely that a joy-riding punk will steal it. Most people have the common sense to know these facts of life. But how many people open an email attachment from a sender they do not know, and then are surprised when their computer becomes infected with a virus? How many people click on a link to a web site, fill in personal details on a form, and then are surprised to discover that their identity has been stolen? Even in the safest of communities we lock our doors at night, and yet when it comes to computers most people do not yet have this basic common sense.

The only answer is education. By that, I mean broad education. A law-abiding society is not built by specialized people who are paid to know and enforce the law, whom we call police. Rather, a law-abiding society is built when all citizens have a general sense of what the rules are, and have the good will to abide by them. Computer and network security cannot come about when we only have specialized people, sometimes even given the title of “security administrator”, who enforce a security policy. The most debilitating breaches of security happen at the low-level. Computer hard drives are lost or improperly discarded, trust is granted naively to incoming data or network connections by ordinary users, fired employees vandalize the logic of computer systems — the list goes on and on, but none of it is very sophisticated stuff.

We have high-end course offerings that are aimed at system administrators seeking the expertise to specialize as security administrators. That’s like having medical schools to train doctors so that they can fight disease. It’s got to be done, of course. But what has history taught us has been of the most benefit in fighting disease and extending the human lifespan as a result? It has been public sanitation (building sewers) and overall cleanliness (washing your hands). When it comes to computer security, we’re missing the ordinary, mass education component. Most people don’t know how computers and the Internet work, so they have no idea how bad guys are exploiting its functionality for their ill purposes. They are victims without a means of defence. That has got to change. Computer security is for everybody, just like good health practices are for everybody and not something to be left only in the hands of doctors.

Who should go on computer security training? I think it should be everybody: end users, database administrators, storage specialists, developers, programmers, the office receptionist — everybody. These are the people that will be affected by the real crime, which is unsophisticated and which will reach them through ordinary web sites and emails and day-to-day practices with the physical pieces of their computerized and networked workplace environment. We “street-proof” our kids to live in the real world, but we’re not doing that with people who deal with computers every day of their working lives. The loss of efficiency, productivity, and business is enormous, and we should engage in mass security education at a lower level to reduce that loss.

Source : https://www.exitcertified.com/blog/michael/2012/why-dont-we-train-for-better-security/