Can we do anything to fight the waves of unsolicited commercial e-mail (spam) flooding into our electronic mailboxes? In this third of a three-part series, I look at some unusual ideas for improving our defensive posture.

In Common Law in the United States and Britain, there are well established precedents for assigning responsibility to the owners of resources that can become a danger to the public. The classic example is swimming pools in back yards. A long-established rule is that the owner of a property must protect children against attractive nuisances such as swimming pools. Swimming pool owners know that they must erect barriers to unauthorized access and use; fences, for example, are a typical mechanisms to prevent children from falling into unattended pools. Should someone leave the gate to their fence unlocked, they could very well become liable for damages if a child were to be injured by trespassing onto their property – clearly an act unauthorized by the property owner – and then falling into their pool.

The owner of a PC is in a situation analogous to that of the owner of a swimming pool in a residential neighborhood. Both benefit from their ownership and use of a tool or facility or resource; both ought to protect other people from the consequences of abuse of those systems by reducing the likelihood of abuse. Therefore, it seems reasonable to me that any owner of a PC should be obliged under law and presumably using technical constraints to have sufficient security in place on their PC to prevent it from being taken over by malware and suborned into becoming a zombie in a botnet that sends out spam.

At a technical level, today’s security and antimalware suites routinely protect systems against such subversion. Malware scanners quickly identity botnet code and quarantine or delete it; integrated firewalls and intrusion detection systems monitor traffic and – if not subverted by naïve users who may authorize everything they’re asked about – may even stop unauthorized outbound traffic, rendering even an infected machine useless for a botnet. Current versions of Windows operating systems (OSs) monitor their systems for the presence of antimalware and firewall functions; they pop up warnings to users if those functions are disabled or not present. How easy it would be to go one step further and have the OS itself block access to the computers – at least temporarily – instead of simply warning the user. Perhaps the OS could require some time-wasting process that would significantly annoy the user even more than usual, thus providing pressure that would encourage technological illiterates into installing the requisite security services. Yes, such a system could itself be abused; malware that escaped into an unprotected system could very well be written to activate a system lockout without warning using such facilities. We would have to think carefully about the functional specifications of any such system.

At a social level, perhaps the computer is reaching the same stage of social integration that the automobile reached in the US at the beginning of the 20th century, when state after state began requiring formal licenses for the operation of motor vehicles. Until then, anyone could run any kind of motor vehicle on a whim, without training and without regard for the possible
consequences of their inexperience and incompetence. As the number of automobiles increased, however, people realized that running them was not to be left to the untrained and the unqualified. Licensing began to include tests and then mandatory training.

Can we conceive of a time when a rite of passage for young people will be passing their Internet-connection license? Young Salil and Janet will be full of excitement as they take their computer-driver’s tests that show that they understand their responsibilities for maintaining a safe computing environment; that they are cognizant of laws that protect them and others against sexual predators on the ‘Net; that they are resistant to the blandishments of sociopathic scum intent on cheating them out of their resources; and that they won’t click on those cursed messages with the weird spelling in the subject lines.

What do you think? Would any such approaches make sense? Use the comment facility to post your own views and stimulate thought.

* * *


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.