OPINION

THE END OF CYBERCRIME?

Eddy Willems
NOXS (formerly Data Alert) and EICAR, Belgium

I'm getting old. The idea of my 12-year-old son and his friends playing the latest version of 'Counterstrike' at a LAN party gives me an uneasy feeling. It is a very bizarre sight to see young people staring silently at TFT screens, as if they are in some sort of trance. After visiting a number of local organised LAN parties I discovered that it is not only gaming and the copying of games that interest our children. Now, it seems, their interests extend to the hacking and cracking of PCs, websites and so on.

MEGA LESSONS

My wife is a police officer, and a so-called 'MEGA' officer. MEGA is the European version of the US-based DARE (Drugs Abuse Resistance Education) project. MEGA officers visit local schools giving MEGA lessons to 12-year-old school children. The project has been created to raise children's awareness of the problems associated with drugs, alcohol, violence, and so on. One of the additional aims of the Belgian project is to make children aware of the dangers that reside on the Internet.

WHAT DO CHILDREN KNOW?

I decided to do some research to try to find out what really goes on in the minds of young people. I asked a number of MEGA officers and school teachers about the levels of computer security awareness they find in the children they meet. I also posed a set of basic questions about computer security to a small group of children. A selection of their responses is given beneath each question here:

1. *Do you know what a computer virus is?*
   "No"
   "It eats your emails"
   "It wipes out everything"
   "The computer is sick"
2. *Have you ever been infected by a computer virus?*
   20% said "Yes'"
   10% said "No"
   70% said "I don't know"
3. *What are the effects of a virus?*
   See answer 1. However, it became clear that none of the children really seemed to know what viruses do – none of them mentioned self-replication.
4. *Do you click on every link in an email and open every attachment you receive?*
   99% said "Yes"
5. *Do you use an 'easy' password, such as your first name, birthdate, etc.?*
   80% use a *blank* password if possible
   16% use an easy password
   4% use a difficult password
6. *How can you surf on the Internet safely?*
   "I surf to kids' sites" [laughing]
   "Isn't the Internet safe?!"
   "I use Google"
7. *What do you think of virus-writing or hacking?*
   "Cool"
   "Dangerous for your health"
   "Oh my father does it all the time…"

Of course this is not a scientific poll, and it reflects the ideas of only a small selection of children in one region of the world. However, together with other feedback and after discussions with MEGA officers, I arrived at several conclusions and opinions.

CONCLUSIONS AND OPINIONS

Children do not seem to know what computer security is. Some of them even find the idea of becoming a hacker or a virus writer 'cool'. Although some families use parental control mechanisms to secure their home computer networks, many children know how to bypass these mechanisms.

Generally, it seems that our children's knowledge of ethical computer behaviour and good 'netiquette' are a long way off target.

A suggestion as to how we may begin to influence students and young people is by using societal control. An example of how this has worked in the past is with the issue of drink-driving.

At one time, drinking and driving was a personal choice, but as society witnessed some of the consequences of the combination of the two activities, we began to pass laws which restricted such behaviour. Initially there was some resistance to these laws – people saw them as an infringement on their rights. However, as the laws became more widely accepted, people began to refuse to drink and drive on the principle that it is 'wrong' to do so.

Policy makers and law makers are very aware of this form of societal control. However, they are less aware of the societal structure of 'cyberspace', and for this reason there is the danger that the laws they make will not create the desired ethical model, and conversely will create a backlash or revolutionary movement. By taking time to develop realistic policies and effective laws, it is possible we can avoid such a reaction.

The speed with which global electronic communication is developing has brought with it an enormous benefit to all those fortunate enough to be able to exploit it. However, it has also brought opportunities to those who are willing to abuse it.

The way in which it has introduced relative and absolute anonymity for its users may encourage acts which would otherwise have appeared to be too risky to the perpetrator. Its very nature may encourage various kinds of anti-social activities, ranging from innocent pranks through serious malicious damage to data and individuals, and downright criminal fraud.

As a result of the fact that many of its principle users are relatively young, or people who may be impressionable or unprincipled, an ethos has developed in the Internet community, in which it is 'cool' to be an outlaw. Moreover, the inherent power embodied in being able to control the 'system' is potentially irresistible.

Resources that would enable us to emphasize and integrate ethical computing behaviour may provide a stabilizing influence. Our computing environments are very vulnerable regarding distribution of information – after all, it is what they were designed to do.

If we want to change people's behaviour and reduce the attractiveness of becoming a virus writer or hacker, we must start ethical computer education at a much earlier age. I think the way forward is to recognize the different factors introduced by computer technology – factors we have long ignored. If we don't, the technology may ultimately be self-destructive.

So why not incorporate this information into the MEGA lessons or the DARE project and start educating our children at a much earlier age?

This research project is definitely not finished and I would like to put more psychological elements into the project with the help of teachers, sociologists and psychologists. The research will be re-evaluated next year. In the meantime, I remain open to suggestions and comments from anyone who has experience in this field.

[*Readers interested in contributing to Eddy's research project can get in touch with him via the Editor of VB – email editor@virusbtn.com.*]