

Skills for a brighter tomorrow

Teaching new technologies can help Britain compete in a global market and contribute to its economic future. **Janet Murray reports**

In any episode of Spooks or CSI, you are likely to see a sinister figure hunched over a laptop, cleverly hacking their way into a website or file they are not supposed to see. Hacking seems mysterious, subversive and illegal.

What, then, can we make of mild-mannered Elliott Frost? An IT systems administrator at a Leeds-based engineering company, he regularly exploits the vulnerabilities of websites and computer networks. But his actions are not malicious. Frost, who works for Harvard Engineering, which specialises in retail and street lighting, is merely practising on a custom-built "virtual" computer – complete with "mock" websites and computer networks – on his PC.

Frost recently attended a five-day course in certified ethical hacking at Leeds City College's Network Academy, where he learned about common tools and techniques used by hackers and how they avoid detection, and gained hands-on experience of hacking.

The course, which combines theory and practice, is designed to help students (usually IT professionals from small and medium-size businesses in the area) to make sure their company's computer systems are secure. Immersing themselves in the world of the

hacker helps them gain a unique insight into what could go wrong.

Knowing how and what hackers are most likely to attack helped Frost identify "a few low-risk vulnerabilities" and do something about them; it has also highlighted less obvious ones.

"A lot of companies don't think about what is known as 'passive' hacking, which is more about eavesdropping and monitoring information," says Frost. "For example, a company might place a job advert in the public domain which asks for applicants with experience of different operating

'A company making public what operating systems it uses makes it vulnerable to attack'

systems. That's intelligence for the potential hacker. A company publicising what operating systems they are using might make them vulnerable to attack."

Frost also learned about social engineering, where potential hackers manipulate people or situations to gain information that could give them unauthorised access to systems or information, with the ultimate

aim (among other things) of committing fraud, network intrusion, identity theft, or simply to disrupt the system or network. "The typical scenario is someone getting a job as an office cleaner. They find out user names and passwords to get into the system, which creates a security hole they can exploit." In today's multimedia world, an understanding of IT security is vital for us all, Frost says. "If someone gets into your email, it can wreak havoc on your life. On a professional level, many companies make themselves vulnerable to hacking because they set their systems up in a rush, leaving a big hole the hacker can exploit. Others don't update software which can cause vulnerabilities. Since doing the ethical hacking course, we've changed our mindset. We're now scanning, testing and securing our own systems on a regular basis. 'Practising' hacking is part of that."

Leeds City College has been running the ethical hacking course for two years now. "IT systems are central to the running of most businesses nowadays," says Paul Titman, business manager at the college's Network Academy. "Any business with a web presence is at risk of being hacked, and the damage caused can have a devastating effect on the business. The more people know about how it's done, the better equipped they are to prevent it."

