Chapter XIII
Cyber Security and Anti-Social Networking

Malcolm Shore
Canterbury University, New Zealand

ABSTRACT

This chapter is about the way in which computer hackers invoke social networking paradigms to support and encourage their activities. It reviews the evolution of hacking as a form of social networking, from its roots in Bulletin Board systems to the current attacks on Second Life, and considers the motivation for hacking. Ajzen's Theory of Planned Behavior and Beveren's Flow Theory model are, when considered together, found to explain many of the observed characteristics of early hacker activity. The place of social networks in motivating hacking is explored, and some observations are made in relation to hacking and the Second Life environment. A number of control variables are identified which can be used to reduce the likelihood of people engaging in the hacking activity. Addressing the social network factors which motivate hacking provides an important early step in addressing cybercrime.

Laws are like cobwebs, which may catch flies but let wasps and hornets break through

—Jonathan Swift, *A Critical Essay Upon the Faculties of Mind*

INTRODUCTION

This chapter looks at how the many types of social networks and socio-technical systems can be used to enable and support the activity of computer hacking. A hacker was once the name given to a person who was able to rapidly and reliably change computer software to achieve new functionality, often using sophisticated coding techniques which were not generally known or used. Over time, however, the term became used to describe the more restricted group of people who exploit software vulnerabilities to gain unauthorized access to computers. Hackers have a strong networking culture—antisocial net-

working if you like, with online groups, magazines, and conferences characterizing their interactions and peer recognition rewarding their skills.

However, as with any computer system, socio-technical systems are at risk of attack from hackers. Understanding antisocial networking and the motivation that drives hackers is an important step in reducing the levels of disruption in socio-technical, and other, systems.

Computer Hackers and Bulletin Boards

Computer hackers are usually associated with the Internet, but hacking originated well before the Internet become popular. Early computer hackers attacked systems by accessing them through dial in modems. By the 1980s, phone and computer hackers had organized themselves into strong social networks in the form of hacker groups, one of the best known being the US-based Legion of Doom (LoD). LoD started out as a group of phone hackers, breaking into the operational systems used by telecommunications companies. However, it soon began to attract the more general computer hackers and eventually became notorious for its computer hacking. While much of this was focused on demonstrating their expertise, some hackers did use these skills to commit crimes.

At this time, computer hackers used dial-in bulletin boards to provide a means of sharing information on target vulnerabilities and exploits, and these boards were catalysts for the emergence of the early hacker social networks. Law enforcement agencies were poorly equipped to deal with this emerging field of anti-social computer activity, but some agencies did respond by establishing incognito bulletin boards. One example was the Underground Tunnel bulletin board created in 1985 in Austin, Texas by Sgt Robert Ainsley. Law enforcement boards were typically used as sting operations to catch hackers posting dial-in access codes and pirated software and to collect information that could be used to gain access to other hacker bulletin boards.

The early computer hackers tended to be bright college students with an average age of about 14, self-taught computer users with access to micro-computers and modems (Maxfield, 1990). These youngsters hacked for fun, but the leaders of the hacking groups were often older and sought financial gain from pirated software or using stolen credit card information.

Internet Crime

With the growth of the Internet, bulletin boards have been replaced with 'Warez' web sites. These sites operate in much the same way as the earlier bulletin boards but have a much wider audience thanks to the global nature of the Internet. There has been a corresponding increase in the opportunities for individuals and groups to access systems without authorization in order to cause disruption, damage systems, and commit crime. Examples of internet crimes include the $10,000,000 robbery from Citibank in 1994 and denial of service attacks on popular sites such as CNN and eBay (Slatalla, 2004).

There is a difference of opinion regarding the seriousness of hacking. Yar (2005) notes a convergence of thinking which aligns with traditional concepts of juvenile offending and offenders, and hacking has in many cases glamorized in the media. However, such views mask what has become a widespread and serious problem. PriceWaterhouseCoopers, in a multi-industry study of 897 companies from 19 Asian countries, revealed that 63% of respondents had suffered a security breach or attack over the previous twelve months (PriceWaterhouseCoopers, 2003) and it is not uncommon for home computers to suffer 50 attempted hacks or port scans a day (Furnell, 2004). This activity has far reaching effects on the national economies of developed nations, as it discourages the growth and widespread acceptance of eCommerce, eGovernment and eSociety. Further, a US Official involved with Critical Infrastructure Protection (Vatis, 2001) considers hacking to be a serious issue for the future reliability of cyberspace and cannot be ignored as just youthful exuberance: