Computer abuse: vandalizing the information society

Steven M. Furnell and Matthew J. Warren

The authors

Steven M. Furnell is a Research Fellow with Network Research Group, University of Plymouth, UK.

Matthew J. Warren is a Lecturer at Plymouth Business School, University of Plymouth, UK.

Abstract

Examines the damaging effects that malicious computer abuse, such as hacking and viruses, can have on the development of an information-based society. Computing and telecommunications technologies are a key ingredient in the realization of this society, but are increasingly the targets of criminals and mischief makers. Highlights the apparent escalation in computer-abuse incidents, as illustrated by a number of recent surveys, and examines the effects that these may have on the public perception of technology (and, hence, the smooth transition to the information society). Also presents some broad recommendations regarding what can be done to address the problem. This considers both technical measures to help safeguard systems and revised attitudes to computer abuse, to insure that incidents can be dealt with more effectively.

Internet Research: Electronic Networking Applications and Policy
Volume 7 · Number 1 · 1997 · pp. 61–66
 · ISSN 1066-2243

Introduction

Global information networks are now an integral part of the way in which modern businesses and economies operate. One of the best examples of the trend, the Internet, is now estimated to extend to over one million computers, connecting 30 million users in more than 40 countries and is still increasing. A rudimentary comparison arising from this is that the "population" of the Internet now exceeds that of some industrialized nations. As a consequence there is now widespread dependence on computers and network technology, with the ability to communicate and receive information via these channels being recognized as an essential ingredient for competitiveness in the global market.

The transition to the information society is being driven by the reduction in the costs of computing power and telecommunications. These factors, in combination with advances in the core technologies, are making information resources available to an increasing number of people. Leading industry figures are excited by this revolution, some predicting that its effects will be as far reaching as the introduction of electricity (Gates, 1995). The concept has also received significant publicity and backing from national governments in various developed countries with (for example) the USA pushing the information superhighway, an open network of information that will be as accessible as the conventional telephone system. It is, therefore, clear that this route is perceived to be an important element in insuring future national development and competitiveness.

Unfortunately, within any sufficiently mature society there will always be a criminal or destructive element. The information society is no exception to this and the individuals involved have been collectively christened under various names, including "hackers," "cyberpunks" and "phreakers." However, a potential difference from the norm is that the undesirable element has been present from a relatively early stage, with a high degree of publicity being received in the process. As a consequence, many people know the information society as much for its problems as for its benefits. Outstanding issues are whether this will restrict the society's development and, if so, how the problem may be addressed.

Internet Research: Electronic Networking Applications and Policy
Volume 7 · Number 1 · 1997 · 61–66

The development of the information society

The fact that our lives are changing as a result of the spread of technology is widely accepted and the nature of the "society" that will result has been forecast by numerous authors (e.g. Martin, 1988; Toffler, 1981). While differing in many respects, all share the common vision of the computer as the foundation on which the society is built.

There is no doubt that, for the individual citizen, the formation of computer networks can represent an extension of conventional freedoms. They introduce the concept of an electronic presence, which offers the opportunity and ability to roam beyond the confines of one's physical environment, into what has become known as "cyberspace." However, we must not allow an individual's cyberspace existence, and their activities within it, to become entirely divorced from the responsibilities that would exist in the "real world." In order to gain a better perspective on how this may actually be the case, it is worth looking at an example which, while not directly related to the issue of computer abuse, may nevertheless provide an interesting rationalization for some activities in this area. In her book discussing the French Minitel system, Marchand (1987) examines the success of one particular aspect, namely the message service (or *messagerie*) where users could conduct conversations through the electronic medium. Marchand describes communication using the messagerie as "a game of masks" where one can slip into, and hide behind, different "identities" at will. The fact of an electronic presence is viewed with an air of detachment ("one is there without really being there"), with the implication that one is more at liberty to behave however one chooses. Indeed, Guillaume (Poster, 1990) views the computer screen as protection for the users in this context as they may, if they wish, remain totally anonymous in a "position beyond responsibility." This may be reasonable enough within the context of a Minitel or Internet Relay Chat (IRC) scenario, but an extension of this is that individuals may also feel less responsible for other activities within the electronic community; activities which they would not consider in other circumstances. For example, we may consider the traditional hacker activity of cracking passwords in order to obtain unauthorized access to someone else's system and files. Take the computer out of the equation and, regardless of the hacker's claimed motivation, the real-world equivalent would be an act such as going into that individual's office and taking a crow-bar to the filing cabinet; an activity which would be unlikely to appeal to the average hacker.

With these points in mind, it is now worth examining the nature of the abuse that can take place. This is outlined in the next section.

A summary of computer abuse

As networked systems have grown and matured, so too has the nature of abuse within the environment. In the earlier days of computing, abuse was largely restricted to fraud and theft-related activities, which simply represented the extension of traditional crimes into the electronic environment. However, as time has moved on, new and more advanced forms of abuse have emerged (e.g. computer viruses) which often appear not so much a means to an end, but an objective in themselves.

In actual fact, indications are that the public perception of malicious abuse is somewhat inflated. For example, a previous survey into computer security breaches (NCC, 1994) indicated that some 53 percent of respondents perceived a threat from hacking. However, in the same survey, hacking accounted for only 2.5 percent of reported incidents. Nevertheless, the fact that hacking (and other malicious abuse) may account for only a small proportion of computer security problems is, in a sense, immaterial because it is normally these cases that are seized on by the mass media. More often than not these are presented in a dramatic, and even scaremongering, fashion to the public, which may in turn influence public opinion of the activity. In some cases, it will reduce confidence in IT in general and impede progress, while in others it may unduly glamorize the concept of computer abuse (i.e. promoting the cyberpunk image) and thereby encourage others to enter the fray. It is in this sense that much damage may be caused.

Indeed, some publications present a favorable image of hackers as pioneering explorers who are contributing to a worthwhile goal

Internet Research: Electronic Networking Applications and Policy
Volume 7 · Number 1 · 1997 · 61–66

through their activities (Rushkoff, 1994). While it can be argued that, in some cases, the perpetrators may indeed be engaged in simple exploration of the computer network (and, therefore, feel that they are doing no real harm to anyone), it can increasingly be seen that hacking is being used as a means to achieve other ends. As evidence of this, it is possible to cite various incidents of commercial and political malpractice involving the use of IT. A number of cases have been well publicized, with the following examples providing good illustrations:

- malicious activities conducted by British Airways against its rival, Virgin Atlantic (Evans, 1994),
- alleged breach of the British Broadcasting Corporation's BASYS computer system by political parties attempting to acquire advance information on the content and running orders of news stories (Culf, 1996).

In these cases the use of IT was viewed as a definite means to an end, with the hope of gaining some commercial or political advantage. This kind of activity is far removed from that of the stereotypical teenage hacker operating alone in his bedroom, and the motivation more sinister than the straightforward vandalism that he may perpetrate (causing further adverse effects on the public opinion of technology as a consequence).

Another relatively recent survey into abuse incidents has been conducted by the UK Audit Commission (1994), with 1,073 responses from a variety of sectors (including government, health care, education and manufacturing). Of these, 36 percent reported some kind of abuse incident. Some of the principal results concerning malicious abuse incidents are reproduced in Table I (interested readers are referred to the report itself for further details).

While the figures in Table I are dwarfed by the combined losses from other aspects of abuse (e.g. fraud alone caused losses of over £3 million), they are nonetheless significant and the most likely to be remembered by the public.

By comparing the results from all of the related Audit Commission surveys since 1984 it can be seen that malicious abuse has increased dramatically in terms of both incidents and associated losses. Moreover, the increase in recent years is far more substantial than in those previously, indicating that abuse is becoming more widespread and that activities are moving away from merely curious exploration. These results are illustrated in Figure 1, which shows the total number of incidents reported in each surveyed year and the associated overall financial loss.

With all of these statistics it should be remembered that they only cover the reported incidents and many cases may still be either unreported or undiscovered.

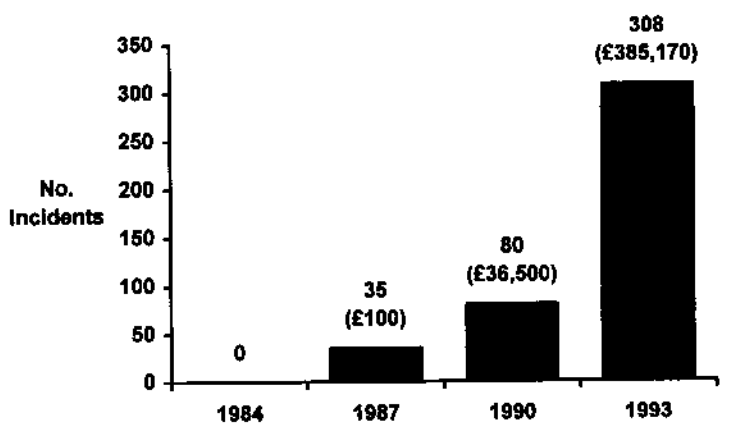
Effects on the information society

When a significant proportion of the population is still not at ease with technology, the widely reported incidents of computer abuse can do nothing but give the information society a bad reputation (or indeed worsen an already bad one – given that, in the eyes of many, computers are already perceived as job-slayers and the creators of a technological élite). It is off-putting enough for novices to be faced with the task of learning to use IT (along with overcoming the associated burden of terminology and jargon), without feeling that they are entering an unfriendly world where others will deliberately set out to damage their systems.

Table I Incidents of malicious abuse (1993)

	Hacking	Viruses	Sabotage	Invasion of privacy	Total malicious abuse
Number of incidents	15	261	16	16	308
Total losses	16,220	254,925	104,625	9,400	385,170

Figure 1 Total incidents of malicious abuse and resulting losses (1984-1993)



Internet Research: Electronic Networking Applications and Policy
Volume 7 · Number 1 · 1997 · 61–66

It can be argued that the one of the most significant signs of a progression toward an information society in recent years has been the popularity of the Internet and the World Wide Web. A great many commercial enterprises now use the latter as a means of promoting their products and services, with a quarter of the world's top 200 companies now having Web presence (Walker, 1996). This has the dual effect of recognizing the extent of the existing online population and increasing the breadth of information available on the network. However, even here there have been a number of high profile security incidents. For example, a great many people may have first heard of the Internet as a result of the "Internet Worm" incident (Hafner and Markoff, 1991), in which a university student released a self-replicating program that spread itself throughout systems on the network at an accelerated rate, slowing them down and eventually bringing the whole network to a temporary halt. More recently, there has been the breach of encryption on the Netscape browser by Berkeley students (Gornall, 1995). In terms of an organization debating whether to invest in IT or Internet connectivity, such bad publicity may count against the decision – potentially harming future productivity and competitiveness as a result.

Even restricting the discussion to existing Internet users, it can be argued that many have very little appreciation of the online world of which they are a part. They use their e-mail systems to communicate and this may be the full extent of their knowledge. They do not understand how the system works and they (quite rightly) have no wish to. They may also have little or no appreciation of the other groups with whom they share cyberspace. It will not be apparent to them that hackers have established their own communities on the Internet, within which they can explore and share their findings with others. The fact that hackers have far more of an appreciation of the "virtual world" in which they are operating than most other users, makes them better placed to take advantage of it.

While a detailed understanding of technology is not necessary for individuals to prosper in the information society, it important that there is adequate awareness and confidence. Rheingold (1994) makes the crucial point that potential opportunities can only be realized by an informed population.

Attitudes for the future

There are plenty of things that can be done in terms of introducing proper safeguards in our computer systems. At a basic level, a large degree of "people-based" abuse could be prevented by ensuring that sufficient user authentication procedures are incorporated – if people cannot gain access, then that rather limits the amount of damage that they can do. Although frequently maligned, traditional passwords are entirely adequate for many contexts if implemented correctly. However, problems do occur in that passwords are often:

- badly selected (and, therefore, potentially easily guessed), which includes passwords that are too short, based on dictionary words or derived from personal data,
- infrequently changed,
- only used at the start of a session and, thereby, grant subsequently unrestricted access to user resources.

If these problems were addressed, with users being properly educated in password principles and system administrators incorporating appropriate mechanisms to monitor/control their use, then passwords would provide a much more effective measure of authentication.

However, passwords are no defense against the scenario where the legitimate user is also the abuser. A valid account holder acting within his privileges may still perform undesirable activities (e.g. deliberately introducing a virus into the system). The traditional approach to discovering such behavior is to maintain audit trails of user activity. Unfortunately, this is more of a reactive measure (i.e. shutting the stable door after the horse has bolted) and, in addition, will normally require some measure of human intervention in order to identify anomalies. The solution may lie with more advanced techniques that monitor user activity in real-time (Mukherjee *et al.*, 1994). These could, for example, compare user activity against historical patterns of behavior (or profiles) for the individual in question and/or against generic rules that might help identify abuse scenarios. Profiles could maintain information on factors

Internet Research: Electronic Networking Applications and Policy
Volume 7 · Number 1 · 1997 · 61–66

such as typical access times/locations and applications most frequently used, whereas the rules would compare behavior against more general indicators (e.g. access outside of normal working hours may be suspicious). Such supervision would also act as an ongoing means of user authentication, in that departures from the behavior profile might also indicate that an impostor has accessed the system. For this purpose, some further behavioral factors (e.g. monitoring of user keystroke rhythms) could also be incorporated into the profiles. In this way, it would both supplement and strengthen the protection afforded by the password system.

With regard to other technical measures, circumstances unfortunately dictate that virus scanners must now be a standard feature on all systems. They must also be regularly updated if they are to remain effective and combat the new virus strains that are constantly emerging. Internet users are particularly at risk from the spread of viruses, owing to the frequent downloading of information from other sources which also provides a path for virus transmission. While network archives should ideally insure that their files are virus free, this may place an unrealistic demand on system administrators in many cases. As such, end-users should still be vigilant and assume some level of responsibility for their own defense.

In addition to the adoption of such safeguards, there must also be a shift in attitude on the part of the victims of computer abuse. It is often conjectured that the majority of computer abuse cases may not be reported, as a result of organizations' desires to avoid adverse publicity and thereby risk losing the confidence of the public or their shareholders (Parker, 1989). An example of this can be cited in terms of a recent headline news story in the UK claiming that various financial institutions, including those in the City of London and New York, have given in to blackmail by "cyber terrorists" at a cost of some £400 million (*The Sunday Times*, 1996). Such attitudes will not be acceptable if the information society is to fulfill its full potential. With the computer as the very hub of operations, any nefarious activities will have to be policed effectively if the society is to succeed. There should, therefore, be the same moral obligations to assist in the prevention and punishment of offenses that are encouraged in conventional society.

In some cases, the dangers from abuse are already recognized but the organizations do not consider the introduction of security to be cost-effective (i.e. the cost of a breach is less than that of installing comprehensive safeguards) and, therefore, prefer to adopt a reactive stance. However, given the increasing dependence on our information networks, a proactive attitude may become increasingly essential.

Technological changes are occurring faster than either the law or the general population are able to appreciate. There is consequently a strong argument that we should not attempt to impose controls and legislation on a society that is not yet fully understood (Rheingold, 1994). However, we must at least be adequately prepared to take action when necessary. Unfortunately, the signs are that currently this is not the case. For example, the level of specialist computer-crime training in the UK police force is rather low and computer-crime cases are perceived as being less interesting to investigate (Collier and Spaul, 1992). In addition, even where legal provisions do exist, the judiciary frequently do not possess a sufficient understanding of IT to appreciate the crucial details of cases. For example, after a two-and-a-half year investigation, one of the first prosecutions under the UK Computer Misuse Act ended with the defendant being acquitted on the grounds of computer addiction (Grossman, 1993). It has since been suggested that because the unauthorized access was to a computer system (as opposed to a physical property) it was not viewed in such a serious manner and that an IT-literate jury would have had more difficulty in accepting the line of defense that was offered.

Such apparent weaknesses will obviously have to be overcome as an increasing proportion of crime becomes technology-related. In the meantime, it is worrying that we are so reliant on technology and yet frequently appear ill-prepared to deal with problems.

Conclusion

Computer abuse is by no means the only barrier to the success of the information society – unfriendly technology, unreliable software and

Internet Research: Electronic Networking Applications and Policy
Volume 7 · Number 1 · 1997 · 61–66

many other such factors will also provide genuine reasons for doubt (Stoll, 1995). However, computer abuse is different in the sense that it represents a deliberate attempt by one party to inflict damage on others.

It would be unrealistic to expect to be able to remove the criminal element from the information society – within any society there will always be an element that is unethical or disruptive. However, we must modify our attitudes and give the issue a similar level of consideration to that which we already give to other types of crime (e.g. theft from our properties).

In general, an increase in the instances of computer crime must been seen as inevitable, as technology itself becomes more pervasive and hence the most natural environment in which criminal opportunities will be perceived. The widespread acceptance of this fact will be the first step in ensuring that the information society is a safe place to be.

References

Audit Commission (1994), *Opportunity Makes a Thief – an Analysis of Computer Abuse*, HMSO Publications Centre, London.

Collier, P.A. and Spaul, B.J. (1992), "The Woolwich Centre for Computer Crime Research: addressing the need for UK information," *Computer Fraud & Security Bulletin*, August, pp. 8-12.

Culf, A. (1996), "BBC acts to thwart political hackers," *The Guardian*, February 9, p. 1.

Evans, D. (1994), "BA in dock over hacking," *Computer Weekly*, April 28, p. 6.

Gates, B. (1995), *The Road Ahead*, Viking Press, New York, NY.

Gornall, J. (1995), "Netscape plugs latest leak," *The Times: Interface Supplement*, September 27, p. 4.

Grossman, W.M. (1993), "Hacked off," *Personal Computer World*, June, pp. 286-90.

Hafner, K. and Markoff, J. (1991), *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Simon & Schuster, New York, NY.

Marchand, M. (1987), *La Grande Aventure du Minitel*, Larousse, Paris.

Martin, W.J. (1988), *The Information Society*, Aslib, London.

Mukherjee, B., Heberlein, L.T. and Levitt, K.N. (1994), "Network intrusion detection," *IEEE Networks*, Vol. 8 No. 3, pp. 26-41.

NCC (1994), *IT Security Breaches Survey Summary*, National Computing Centre Limited, Manchester.

Parker, D.B. (1989), "Consequential loss from computer crime," in Grissonnanche, A. (Ed.), *Security and Protection in Information Systems*, Elsevier Science Publishers B.V., North-Holland, pp. 375-9.

Poster, M. (1990), *The Mode of Information: Poststructuralism and Social Context*, Polity Press, Cambridge.

Rheingold, H. (1994), *The Virtual Community – Finding Connection in a Computerized World*, Secker & Warburg, London.

Rushkoff, D. (1994), *Cyberia – Life in the Trenches of Hyperspace*, HarperCollins, London.

Stoll, C. (1995), *Silicon Snake Oil – Second Thoughts on the Information Highway*, Macmillan General Books, London.

The Sunday Times (1996), "City surrenders to £400m gangs," June 2, pp. 1-24.

Toffler, A. (1981), *The Third Wave*, Pan Books, London.

Walker, C. (1996), "Brand leaders embrace Web," *Computer Weekly*, January 11, p. 6.