PROFESSIONAL PRACTICE
Internet abuse and internet addiction in the workplace

Mark Griffiths
Nottingham Trent University, Nottingham, UK

Abstract

Purpose – This paper seeks to overview the issues, concerns and challenges relating to internet abuse and internet addiction in the workplace.

Design/methodology/approach – Using psychological literature, the paper outlines a number of important and inter-related areas including brief overviews of internet abuse, and the most extreme form of internet abuse in the workplace (i.e. internet addiction).

Findings – The paper reveals that internet abuse is a relatively neglected area of research and that internet abuse is a potentially serious cause of concern for employers. It also highlights that there are many different kinds of internet abuse in the workplace (e.g. cybersexual internet abuse, and online friendship/relationship abuse, internet activity abuse, online information abuse, criminal internet abuse). It is concluded that internet abuse has the potential to be a serious occupational issue.

Research limitations/implications – The empirical base for the paper was based on a relatively small number of peer-reviewed papers and relies heavily on the author's own work in the area.

Practical implications – Using the findings of the psychological literature, some guidance for managers on the issue of internet abuse in the workplace are presented.

Originality/value – Research on internet abuse and internet addiction is sparse and there is very little in the empirical literature concerning issues relating to internet abuse.

Keywords Internet, Addiction, Ethics, Communication technologies, Employee behaviour, Workplace

Paper type General review

The internet has become a fundamental part of many people's day-to-day working lives. As with the introduction of other mass communication technologies, issues surrounding use, abuse and addiction in the workplace have surfaced (Griffiths, 2002; Weatherbee, 2009). It is not uncommon for office workers to spend workplace time on various non-work activities (e.g. booking holidays, shopping online, bidding in online auctions, e-mailing friends/romantic partners, etc.). According to a survey by the International Data Corporation (Snapshot Spy, 2008), up to 40 per cent of internet access in the workplace is spent on non-work-related browsing, and 60 per cent of all online purchases are made during working hours. The same survey also reported that 90 per cent of employees felt the internet can be addictive, and 41 per cent admitted to personal internet surfing at work for more than three hours per week. Internet abuse at work can lead to a decrease in productivity, network clogging, and an increase in the incidents of security breaches at an organization (Pee *et al.*, 2008; Clayburgh and Nazareth, 2009; Weatherbee, 2009). Activities and consequences such as these highlight that internet abuse is a potentially serious cause of concern for employers.

Internet addiction: a brief overview

Previous writings in the area of internet abuse have concentrated on very excessive use of the internet (i.e. "Internet addiction"; Griffiths, 2002, 2004). It has been claimed that

excessive internet use can be pathological and addictive (Widyanto and Griffiths, 2006) and that such behaviour comes under the more general label of "technological addiction" (Griffiths, 1995, 1998). It has been argued that behavioural addictions are no different from chemical addictions (e.g. alcoholism, and heroin addiction) in terms of the core components of addiction such as salience, tolerance, withdrawal, mood modification, conflict, and relapse.

Internet dependency has most commonly been conceptualised as a behavioural addiction, which operates on a modified principle of classic addiction models, but the validity and clinical usefulness of such claims have also been questioned (Holden, 2001). Other studies have also supported the concept that problematic internet use might be associated with features of DSM-IV impulse control disorder (Shapira *et al.*, 2000). Young (1999) claims that internet addiction is a broad term that covers a wide variety of behaviours and impulse control problems. She claims there are five specific subtypes:

(1) *Cybersexual addiction.* Compulsive use of adult web sites for cybersex and cyberporn.
(2) *Cyber-relationship addiction.* Over-involvement in online relationships.
(3) *Net compulsions.* Obsessive online gambling, shopping or day trading.
(4) *Information overload.* Compulsive web surfing or database searches.
(5) *Computer addiction.* Obsessive computer game playing.

However, Griffiths (2000c) has argued that many of these excessive users are not "internet addicts" but just use the internet excessively as a medium to fuel other addictions. He argues that most of the individuals who use the internet excessively are not addicted to the internet itself, but use it as a medium to fuel other addictions. Griffiths says that there is a need to distinguish between addictions to the internet and addictions on the internet. He gives the example of a gambling addict who chooses to engage in online gambling, as well as a computer game addict who plays online, stressing that the internet is just the place where they conduct their chosen (addictive) behaviour. These people display addictions on the internet. However, there is also the observation that some behaviours engaged in on the internet (e.g. cybersex, cyberstalking, etc.) may be behaviours that the person would only carry out on the internet because the medium is anonymous, non face-to-face, and disinhibiting (Griffiths, 2000b, 2001).

In contrast, it is also acknowledged that there are some case studies that seem to report an addiction to the internet itself (Young, 1998; Griffiths, 2000a). Most of these individuals use functions of the internet that are not available in any other medium, such as chat rooms or various role playing games. These are people addicted to the internet. However, despite these differences, there seem to be some common threads, most notably reports of the negative consequences of excessive internet use (neglect of work and social life, relationship breakdown, loss of control, etc.), which are comparable to those experienced with other, more established addictions.

Research into internet addiction suggests that it does indeed exist but that it affects only a very small minority of users (Widyanto and Griffiths, 2006, 2009). These are usually people who use internet chat rooms or play fantasy role playing games – activities that they would not engage in except on the internet itself. To some extent, these internet users are engaged in text-based virtual realities and take on other social personas and social identities as a way of making them feel good about themselves. In such cases, the medium of the internet may provide an alternative reality to the user and allow them feelings of immersion and anonymity, feelings that may lead to an altered state of consciousness for the user. This in itself may be highly psychologically and/or physiologically rewarding.

There appear to be many people who use the internet excessively but are not addicted as measured by addiction criteria. Most people researching in the field have failed to use stringent criteria for measuring addiction (Widyanto and Griffiths, 2006). The main problems with much of the research to date is that the measures used have:

- no measure of severity;
- no temporal dimension;
- a tendency to over-estimate the prevalence of problems; and
- no account of the context of internet use.

Furthermore, the sampling methods used have been questionable (e.g. an over-reliance on self-selected samples), and there is no survey work to date that conclusively demonstrates that internet addiction exists (Griffiths, 2008).

Taking into account the diversity of the functions offered by the internet, it seems highly unlikely that "internet addiction" exists to any great extent. "internet addiction" implies that an individual is addicted to the experience of being online, despite whatever function they are using. What seems to be more probable is for an individual's addiction to be associated to a function that happens to be online. Making the distinction between viewing the internet as one general application and breaking it down into the specific functions available on it might have important implications on future research. The internet consist of so many diverse functions, with different uses and therefore, different types of user who have different reasons for using a particular function. Rather than focus on a unified concept of internet addiction, it may be more helpful to conceptualise and study disturbed patterns separately according to specific internet activities (Morahan-Martin, 2005).

Types of internet abuse in the workplace

It is clear that the issues of internet abuse and internet addiction are related but they are not the same thing. Furthermore, the long-term effects of internet abuse may have more

far-reaching effects for a company that internet abusers work for than the individuals themselves. Abuse also suggests that there may not necessarily be any negative effects for the user other than a decrease in work productivity. There have been few typologies of internet abuse in the scientific literature. Research by Blau *et al.* (2006) based on data collected from 415 medical technologists found that internet abuse fell into three distinct categories (browsing related, non-work-related e-mail, and interactive cyberloafing). A theoretical typology by Griffiths (2004) adapted Young's (1999) internet addiction typology to produce a typology of internet abuse within the workplace. These are cybersexual internet abuse, online friendship/relationship abuse, internet activity abuse, online information abuse, criminal internet abuse, and miscellaneous internet abuse. These are examined in more detail below:

- *Cybersexual internet abuse.* This involves the abuse of adult web sites for cybersex and cyberporn during work hours. Such online sexual services include the conventional (e.g. internet versions of widely available pornographic magazines), the not so conventional (internet versions of very hardcore pornographic magazines). There are also pornographic picture libraries (commercial and free access), videos and video clips, live strip shows, live sex shows, and voyeuristic web-cam sites.
- *Online friendship/relationship abuse.* This involves the conducting of an online friendship and/or relationship during work hours. Such a category could also include the use of e-mailing friends and/or engaging in discussion groups, as well as maintenance of online emotional relationships. Such people may also abuse the internet by using it to explore gender and identity roles by swapping gender or creating other personas and forming online relationships or engaging in cybersex (see above).
- *Internet activity abuse.* This involves the use of the internet during work hours in which other non-work-related activities are done (e.g. online gambling, online shopping, online travel booking, online computer gaming, online day trading, bidding on online auctions, etc). This appears to be one of the most common forms of internet abuse in the workplace.
- *Online information abuse.* This involves the abuse of internet search engines and databases. Typically, this involves individuals who search for work-related information on databases, etc. but who end up wasting hours of time with little relevant information gathered. This may be deliberate work avoidance but may also be accidental and/or non-intentional. It may also involve people who seek out general educational information, information for self-help/diagnosis (including online therapy) and/or scientific research for non-work purposes.
- *Criminal internet abuse.* This involves the seeking out individuals who then become victims of sexually related internet crime (e.g. online sexual harassment, cyberstalking, and paedophilic "grooming" of children). The fact that these types of online criminal acts may have severe implications for employers.
- *Miscellaneous internet abuse.* This involves any activity not found in the above categories such as the digital manipulation of images on the internet for entertainment and/or masturbatory purposes (e.g. creating celebrity fake photographs where heads of famous people are superimposed onto someone else's naked body).

Why does internet abuse occur?

There are many factors that contribute to internet abuse in the workplace. It is clear from research in the area of computer-mediated communication that virtual environments have the potential to provide short-term comfort, excitement, and/or distraction (Widyanto and Griffiths, 2006, 2009). These reasons alone provide compelling reasons as to why employees may engage in non-work-related internet use. Lee *et al.* (2005) compared multiple theoretical perspectives in an attempt to explain internet abuse in the workplace using a combination of deterrence theory, theory of reasoned action, ethical decision making, and the technology adoption model. They found that perceived habits and perceived information systems accessibility as the most significant factors affecting non-work related computing. Research by Taneja (2006) found that attitude towards adverse usage, social influence, perceived behavioural control, and moral norms was significantly related towards internet abuse. Research by Lim (2002) has also shown that employees are more likely to rationalize their misuse of the internet in the workplace when they perceive that their employers do not treat them fairly. In addition to this empirical research, there are also other reasons that have been put forward in the psychological literature that appear to facilitate internet abuse among employees (i.e. opportunity, access, affordability, anonymity, convenience, escape, disinhibition, social acceptance, and longer working hours). These are briefly examined below:

- *Opportunity and access.* Obvious precursors to potential internet abuse include both opportunity and access to the internet. Clearly, the internet is now commonplace and widespread, and is almost integral to most workplace environments. Given that prevalence of undesirable behaviours is strongly correlated with increased access to the activity, it is not surprising that the development of internet abuse appears to be increasing across the population. Research into other socially acceptable but potentially problematic behaviours (drinking alcohol, gambling, etc.) has demonstrated that increased accessibility leads to increased uptake (i.e. regular use) and that this eventually leads to an increase in problems – although the increase may not be proportional.
- *Affordability.* Given the wide accessibility of the internet, it is now becoming cheaper and cheaper to use the internet. Furthermore, for almost all employees, internet access is totally free of charge and the only costs will be time and the financial costs of some particular activities (e.g. online sexual services, online gambling, etc.).
- *Anonymity.* The anonymity of the internet allows users to privately engage in their behaviours of choice in the belief that the fear of being caught by their employer is minimal. This anonymity may also provide the user with a greater sense of perceived control over the content, tone, and nature of their online experiences. The anonymity of the internet often facilitates more honest and open communication with other users and can be an important factor in the development of online relationships that may begin in the workplace. Anonymity may also increase feelings of comfort since there is a decreased ability to look for, and thus detect, signs of insincerity, disapproval, or judgment in facial expression, as would be typical in face-to-face interactions.
- *Convenience.* Interactive online applications such as e-mail, chat rooms, newsgroups, or role-playing games provide convenient mediums to meet

others without having to leave one's work desk. Online abuse will usually occur in the familiar and comfortable environment of home or workplace thus reducing the feeling of risk and allowing even more adventurous behaviours.

- *Escape.* For some, the primary reinforcement of particular kinds of internet abuse (e.g. to engage in an online affair and/or cybersex) is the sexual gratification they experience online. In the case of behaviours like cybersex and online gambling, the experiences online may be reinforced through a subjectively and/or objectively experienced "high." The pursuit of mood-modifying experiences is characteristic of addictions. The mood-modifying experience has the potential to provide an emotional or mental escape and further serves to reinforce the behaviour. Abusive and/or excessive involvement in this escapist activity may lead to problems (e.g. online addictions). Online behaviour can provide a potent escape from the stresses and strains of real life.
- *Disinhibition.* Disinhibition is clearly one of the internet's key appeals as there is little doubt that the internet makes people less inhibited (Joinson, 1998). Online users appear to open up more quickly online and reveal themselves emotionally much faster than in the offline world. What might take months or years in an offline relationship may only take days or weeks online. As some have pointed out (Cooper and Sportolari, 1997) the perception of trust, intimacy, and acceptance has the potential to encourage online users to use these relationships as a primary source of companionship and comfort.
- *Social acceptability.* The social acceptability of online interaction is another factor to consider in this context. What is really interesting is how the perception of online activity has changed over the last ten years (e.g. the "nerdish" image of the internet is almost obsolete). It may also be a sign of increased acceptance as young children are exposed to technology earlier and so become used to socializing using computers as tools. For instance, laying the foundations for an online relationship in this way has become far more socially acceptable and will continue to be so. Most of these people are not societal misfits as is often claimed – they are simply using the technology as another tool in their social armoury.
- *Longer working hours.* All over the world, people are working longer hours and it is perhaps unsurprising that many of life's activities can be performed from the workplace internet. Take, for example, the case of a single individual looking for a relationship. For these people, the internet at work may be ideal. Dating via the desktop may be a sensible option for workaholic professionals. It is effectively a whole new electronic "singles bar" which because of its text-based nature breaks down physical prejudices. For others, internet interaction takes away the social isolation that we all sometimes feel. There are no boundaries of geography, class or nationality. It opens up a whole new sphere of relationship forming.

Finally, in this section, it is worth noting that recent research into internet abuse has also shown that males are more likely than females to engage in internet abuse in workplace settings (Garrett and Danziger, 2008), particularly among younger men (Henle and Blanchard, 2008). Somewhat predictably, research has also found that individuals with low-impulse control are more likely to abuse the internet at work (Yellowlees and Marks, 2007; Higgins *et al.*, 2008).

What can be done about internet abuse in the workplace?

Mirchandani and Motwani (2003) report that employers are generally unaware of the full range of actions they can take to reduce problems such as internet abuse. They also claim that internet abuse can be viewed as a kind of systems risk (i.e. the likelihood that a firm's information systems are insufficiently protected against certain kinds of damage or loss). They propose the general deterrence theory, a criminological approach that applies sanctions and disincentive measures. This, they argue, can reduce systems abuse by making potential abusers aware that their unethical behaviour would be detrimental to their own good. According to deterrence theory, there are four strategies that can be adopted to reduce systems:

(1) deterrence;
(2) prevention;
(3) detection; and
(4) remedies.

These are outlined in relation to internet abuse:

- *Deterrent measures.* In relation to internet abuse, these measures basically equate to policies and guidelines on internet abuse in the workplace. Such measures tend to be passive in that they have no inherent provision for enforcement and depend wholly on the willingness of system users to comply.
- *Preventive measures.* In relation to internet abuse, these measures could include locks on computer room doors and password access controls. Such measures are more active than deterrent measures and incorporate some kind of enforcement that may temper illegitimate and/or illegal internet use.
- *Detection measures.* These measures can be used when deterrent and preventive measures fail. In relation to internet abuse, such measures could include proactive security responses such as suspicious activity reports, system audits and virus scanning reports, or reactive responses such as detective work after a documented breach in security. Detection measures gather evidence of internet abuse and identify perpetrators.
- *Remedial measures.* In relation to internet abuse, these are measures that are used to correct the harmful effect of internet abuse and punish the perpetrators. Internal actions may include warnings, reprimands, and termination of employment. Legal actions include criminal and civil suits.

To overcome internet abuse in the workplace, Mirchandani and Motwani (2003) advise that a company can begin by deploying deterrent measures. If these are not successful, the company is then advised to use preventive and then detective measures. If these fail, then remedial measures are necessary. Despite a sound theoretical basis, there is limited empirical evidence of the effectiveness of such an approach so Mirchandani and Motwani (2005) carried out an empirical study. They examined 18 possible deterrent actions by companies to deal with internet abuse. They found that monitoring (a prevention measure) and blocking (a detection measure) were the only actions to have significant effect on internet abuse reduction in the workplace. Policies, contracts, and remedial action measures had considerably less impact.

As has been demonstrated, being able to spot someone who is an internet addict or an internet abuser can be very difficult. However, Griffiths (2004) reports some practical steps that can be taken to help minimize the potential problem:

- *Take the issue of internet abuse seriously.* Internet abuse in all its varieties is only just being considered as potentially serious occupational issues. Managers, in conjunction with personnel departments and employment counselors need to ensure they are aware of the issues involved and the potential risks it can bring to both their employees and the whole organization. They also need to be aware that for employees who deal with finances, some forms of internet abuse (e.g. internet gambling), the consequences for the company can be very great (Griffiths, 2009).
- *Raise awareness of internet abuse issues at work.* This can be done through e-mail circulation, leaflets, and posters on general notice boards. Some countries will have national and/or local agencies (e.g. technology councils, health and safety organizations, etc.) that can supply useful educational literature (including posters). Telephone numbers for these organizations can usually be found in most telephone directories.
- *Ask employees to be vigilant.* Internet abuse at work can have serious repercussions not only for the individual but also for those employees who befriend internet abusers, and the organization itself. Fellow staff members need to know the basic signs and symptoms of internet abuse. Employee behaviours such as continual use the internet for non-work purposes might be indicative of an internet abuse problem.
- *Monitor internet use of staff who are suspecting of having problems.* Those staff with an internet-related problem are likely to spend great amounts of time engaged in non-work activities on the internet. Should an employer suspect such a person, they should get their IT specialists to look at their internet surfing history as the computer's hard disc will have information about everything they have ever accessed.
- *Check internet "bookmarks" of staff.* In some jurisdictions across the world, employers can legally access the e-mails and internet content of their employees. One of the most simple checks is to look at an employee's list of "bookmarked" web sites. If they are spending a lot of employment time engaged in non-work activities, many bookmarks will be non-work related (e.g. online dating agencies, and gambling sites) (Griffiths, 2009).
- *Develop an "internet abuse at work" policy.* Many organizations have policies for behaviours such as smoking or drinking alcohol. Employers should develop their own internet abuse policies by liaison between personnel services and local authority technology councils and/or health and safety executives.

Conclusions

In this paper, major issues that surround internet abuse issues in the workplace have been highlighted. Internet abuse can clearly be a hidden activity and the growing availability of internet facilities in the workplace is making it easier to occur in lots of different forms. Thankfully, it would appear that for most people internet abuse is not a serious individual problem although for large companies, small levels of internet abuse multiplied

across the workforce raises serious issues about work productivity. For those whose internet abuse starts to become more of a problem, it can affect many levels including the individual, their work colleagues and the organization itself. Managers and specialist staff that they employ (such as employment counselors) clearly need to have their awareness of this issue raised, and once this has happened, they need to raise awareness of the issue among the work force. Furthermore, employers need to let employees know exactly which behaviours on the internet are reasonable (e.g. the occasional e-mail to a friend) and those that are unacceptable (e.g. online gaming, cybersex, etc.).

References

Blau, G., Yang, Y. and Ward-Cook, K. (2006), "Testing a measure of cyberloafing", *Journal of Allied Health*, Vol. 35 No. 1, pp. 9-17.

Clayburgh, C.C. and Nazareth, D.L. (2009), "Measuring severity of internet abuse in the workplace: creation of a thurstone scale", *Americas Conference on Information Systems (AMCIS) AMCIS 2009 Proceedings*, available at: http://aisel.aisnet.org/amcis2009/583 (accessed January 8, 2010).

Cooper, A. and Sportolari, L. (1997), "Romance in cyberspace: understanding online attraction", *Journal of Sex Education and Therapy*, Vol. 22, pp. 7-14.

Garrett, R. and Danziger, J. (2008), "On cyberslacking: workplace status and personal internet use", *CyberPsychology & Behavior*, Vol. 11.

Griffiths, M.D. (1995), "Technological addictions", *Clinical Psychology Forum*, Vol. 76, pp. 14-19.

Griffiths, M.D. (1998), "Internet addiction: does it really exist?", in Gackenbach, J. (Ed.), *Psychology and the Internet: Intrapersonal, Interpersonal and Transpersonal Applications*, Academic Press, New York, NY, pp. 61-75.

Griffiths, M.D. (2000a), "Does internet and computer 'addiction' exist? Some case study evidence", *CyberPsychology & Behavior*, Vol. 3, pp. 211-8.

Griffiths, M.D. (2000b), "Excessive internet use: implications for sexual behavior", *CyberPsychology & Behavior*, Vol. 3, pp. 537-52.

Griffiths, M.D. (2000c), "Internet abuse: time to be taken seriously?", *Addiction Research*, Vol. 8, pp. 413-8.

Griffiths, M.D. (2001), "Sex on the internet: observations and implications for sex addiction", *Journal of Sex Research*, Vol. 38, pp. 333-42.

Griffiths, M.D. (2002), "Occupational health issues concerning internet use in the workplace", *Work & Stress*, Vol. 16, pp. 283-7.

Griffiths, M.D. (2004), "Internet abuse and addiction in the workplace – issues and concerns for employers", in Anandarajan, M. (Ed.), *Personal Web Usage in the Workplace: A Guide to Effective Human Resource Management*, Idea Publishing, Hershey, PA, pp. 230-45.

Griffiths, M.D. (2008), "Internet and video-game addiction", in Essau, C. (Ed.), *Adolescent Addiction: Epidemiology, Assessment and Treatment*, Elsevier, San Diego, CA, pp. 231-67.

Griffiths, M.D. (2009), "Internet gambling in the workplace", *Journal of Workplace Learning*, Vol. 21, pp. 658-70.

Henle, C. and Blanchard, A. (2008), "The interaction of work stressors and organizational sanctions on cyberloafing", *Journal of Managerial Issues*, Vol. 20, pp. 383-400.

Higgins, G., Wolfe, S. and Marcum, C. (2008), "Digital piracy: an examination of three measurements of self-control", *Deviant Behavior*, Vol. 29, pp. 440-60.

Holden, C. (2001), "Behavioral' addictions: do they exist?", *Science*, Vol. 294 No. 5544.