# Cyber Security Games: A New Line of Risk

John Blythe, Lynne Coventry



# Cyber Security Games: A New Line of Risk

John M Blythe[1] and Lynne Coventry[2]

[1, 2] Department of Psychology, School of Life Sciences, Northumbria University, Newcastle-Upon-Tyne, UK
john.m.blythe@northumbria.ac.uk
lynne.coventry@northumbria.ac.uk

**Abstract**

Behaviour change is difficult to achieve and there are many models identifying the factors to affect such change but few have been applied in the security domain. This paper discusses the use of serious games to improve the security behaviour of end-users. A new framework, based upon literature findings, is proposed for future game design. The trust and privacy issues related to using serious games for improving security awareness and behaviour are highlighted.

**Keywords:** Information security, Behaviour change, Security games

## 1 Introduction

Organisations and individuals are becoming increasingly reliant on technology and the internet for the storage and processing of their information. Statistics reported by the Internet World Stats [1] indicate that the number of internet users worldwide has increased by 528.1% since 2000, and now represents 32.7% of the worldwide population. Whilst the globalisation of the internet and technology has brought many benefits for businesses and users, the increased dependency on cyberspace also creates vulnerability to security threats: for example, viruses, hacking attempts and malware. These threats present a major risk and so it is important that businesses and individuals protect themselves from the growing threats in cyberspace.

Attention has therefore been devoted to improving the security behaviour of end-users. In organisations, previous approaches have been adopted such as training, education and awareness campaigns. These approaches can take a number of different forms including presentations, newsletters, video games, and posters. A review of the existing literature on security interventions suggests that current approaches lack empirical evidence and a theoretical grounding with the majority of approaches being based upon practical experience [2]. To date, the use of serious games to improve security behaviour and awareness has received little attention, though the use of games for information security awareness has been proposed by researchers. However, in domains other than security, research into the use of serious games for behaviour change and knowledge impact has produced mixed results in research [3].

adfa, p. 1, 2011.

Serious games intending to change the behaviour of end-users need to incorporate models of behaviour change. Whilst there is relatively little research regarding behaviour change in security settings, there are a few examples. The research that exists has used behaviour models from health psychology literature. For example, one study used the Health Belief Model (HBM) to improve anti-phishing behaviour with the game 'Anti-Phishing Phil' teaching users to avoid phishing attacks. Using the HBM, this study manipulated participant's perceived susceptibility and found that tailored risk messages increased intentions to behave securely online regardless of whether participants were presented with at low risk or high risk message of being a potential victim of fraud. However, overall, the study found that the use of the game as a training program had no effect on actual secure behaviour [4]. Thus suggesting that intention to change did not lead to actual change. This study only manipulated one aspect of the HBM, perceived susceptibility, and generally more than one factor should be addressed simultaneously. Research from health has discussed the manipulation of behavioral determinants of models in great depth and meta-analyses have found behaviour change interventions for health behaviour to be efficacious [5].

We propose a framework based upon our current work investigating factors influencing security behaviour (see table 1).

**Table 1.** The behavioural determinants to be targeted in game design for behaviour change

| *Behavioural Determinants* | *Security context for the game player* |
|---|---|
| Perceived vulnerability | Assessment of the probability of an event occurring as the result of a breach |
| Perceived severity | The severity of the consequences of a security breach |
| Response efficacy | Belief as to whether the recommended action will actually avoid the threat |
| Response cost | Perceived costs of performing the security behaviour |
| Self-efficacy | Belief they have the knowledge and skills to perform the security behaviour |
| Attitude | Their positive or negative feelings toward security behaviour |
| Subjective norms | Relevant others to the user are performing the security behaviour |
| Locus of control | The extent to which they believe that they can control events that affect them |
| Psychological ownership | Perception that they own what they are protecting by performing the behaviour |

The framework is based upon two well-established theories of behaviour change; the protection motivation theory [6] and the theory of planned behaviour [7] with additional factors of locus of control and psychological ownership. We seek to address the practical efficiency of the framework in game design and argue that future serious game design should target the behavioural determinants (table 1) to increase the efficacy of behaviour change games. Games adopting this framework need concrete examples of how they are targeting each factor in the framework and how each determinant is manipulated in the game design. This will enhance the behaviour change effectiveness and further aid in the understanding of the use of serious games for behaviour change.

## 2 Security Games: A Double-Edge Sword?

Games designed to improve security behaviour have inherent trust and privacy issues. These games are designed with the intent to improve behaviour, yet they have the potential for people to expose their real life security behavior, its weaknesses and actual security data such as passwords. Firstly, users are pushed to a particular behaviour i.e. what the designers of the games target for a particular security issue. In the case of 'Anti-Phishing Phil', the game focuses on one generalized measure of behaviour which is the detection of fake URLs in phishing scams. In reality, users are more likely to face a range of phishing attacks so are required to use a number of heuristics to detect these attacks. Future security game design should ensure complete coverage of phishing attacks/security issues and required behaviour to ensure that a user is not left vulnerable.

A further issue surrounding the use of security games is that they can maintain logs of user behaviour, for example, the security resource management game cyber-CIEGE [8]. The game requires the user to take the role of a decision maker for a fictional IT-dependent organisation and they must make choices regarding technical, procedural and physical security. Their role is to ensure that the organisation's employees are happy and productive whilst ensuring that security measures protect information. The game creates a log of the choices made by the user which can be viewed to provide summaries of progress and details of individual gameplay.

The content of these logs could potentially be very sensitive as they could provide information about the security behaviour of the individuals. For example, if a security game requires the development of more effective passwords, studies have shown that users manage around 8 passwords [9] and have on average 25 accounts protected [10]. When combined they have on average 25 accounts that require a password but only have 8, therefore they are more likely to re-use current passwords. In games, users are also likely to re-use and disclose their real world passwords in a scenario that requires them to develop more secure ones. Those who have access to these logs could therefore use this information for malicious intentions.

It is important that the access to these logs is reflected in the policies of the games and acceptable usage by organisations using security games for improving awareness in employees. Wrongful access to logs of behaviour can give indication of weak aspects of users' security practice and what resources individuals may protect (in the case of a resource management game). This could potentially highlight weak areas in organisational infrastructures which could then be comprised by hackers. The acceptable use of security games should also be addressed as the competitive nature of some of these games may mean that organisations may wish to create a leaderboard in which employees may compete with each other to achieve higher scores. Such an approach may improve engagement and the potential effectiveness of the game. However, in the context of organisations, this may lead to many trust and privacy issues. For example, if an employee is particularly careless regarding their security then a leaderboard could present them a negative manner. An employee could perceive this as being procedurally unfair and this can have implications for their productivity and their psychological contract with their company.

These issues are more concerning when games adopt a social media framework as they leave players vulnerable to social engineering attacks. For instance, researchers have designed a prototype security awareness game with a social media framework [11] that uses a leaderboard, so users have the ability to view their friend's scores and thus their friend's progression. They can share badges and achievements on their profile which can be viewed by friends. Users can select topics such as password security and social media security. A major issue with this sort of framework is that it leaves individuals open to a social engineering attack. By displaying an individual's security behaviour on their social network, it has the potential to highlight weak aspects of their security and those who score low could be the target of an attacker who could identify where to exploit based upon their score. Social engineers are known to use social media to gain information about users which they can then use to exploit them.

Phishing could also be potentially developed for security games, in which the user is tricked into thinking they are learning how to improve their security behaviour when the game is actually used to gather information regarding their security practice. It is therefore important that this sort of issue is addressed in future practice.

In conclusion this paper has presented a new framework for designing future games for security behaviour change based upon previous research findings. The paper has also identified potential trust and privacy issues with serious security games. In future work the framework presented will be validated and developed.

## 3 References


1. Internet World Stats. (December 2011). *Internet usage statistics: the internet big picture*. Retrieved June 22nd, 2012 from http://www.internetworldstats.com/stats.htm.
2. Puhakainen, P., Siponen, M.: Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quart, 34,* 757-778 (2010)
3. Connolly, T.M., Boyle, E.A., MacArthur, E., Hainey, T., Boyle, J.M.: A systematic literature review of empirical evidence on computer games and serious games. *Comput Educ. 59(2),* 661-686 (2012)
4. Davinson, N., Sillence, E.: It won't happen to me: Promoting secure behaviour among internet users. *Comput Hum Behav, 26*, 1739-1747 (2010)
5. Johnson, B.T., Scott-Sheldon, L.A.J., Carey, M.P.: Meta-Synthesis of Health Behavior Change Meta-Analyses. *Am J Public Health, 100 (11)*, 2193-2198 (2010)
6. Maddux, J.E., Rogers, R.W.: Protection motivation theory and self-efficacy: A revised theory of fear appeals and attitude change. *J. Exp. Soc. Psychol. 19*, 469-479 (1983)
7. Ajzen, I.: The theory of planned behavior. *Organ Behav Hum Dec*, 50, 179–211 (1991)
8. Thompson, M.F., Irvine, C.E.: Active Learning with the CyberCIEGE Video Game. *4th CSET workshop*, San Francisco, CA (2011)
9. Grawemeyer, B., Johnson, H.: Using and managing multiple passwords: A week to a view. *Interact Comput, 23 (3),* 256-267 (2011).
10. Florencio, D., Herley, C.: A large-scale study of web password habits. *Proceedings of the 16th WWW '07*, 657-66 (2007)
11. Labuschagne, W.A., Burke, I., Veerasamy, N., Eloff, M.M.: Design of cyber security awareness game utilizing a social media framework. *10th Annual ISSA Conference ISSA 15-17* (2011)