BEHAVIOUR & INFORMATION TECHNOLOGY
https://doi.org/10.1080/0144929X.2020.1734087

# Understanding negotiated anti-malware interruption effects on user decision quality in endpoint security

Mark Khai Shean Tan, Sigi Goode and Alex Richardson

Research School of Management, Australian National University, Canberra, Australia

**ABSTRACT**
Anti-malware software must be frequently updated in order to protect the system and the user from attack. Makers of this software must choose between interrupting the user to update immediately or allowing them to update later. In either case, assessing the content of the interruption may still require cognitive investment. However, by allowing the user to negotiate a delayed response to these interruptions, users can instead focus on their work. This paper experimentally examines the effect of immediate and negotiated interruptions on user decision time and decision accuracy in multiple stage tasks. For complex tasks, decision performance is higher when the user can negotiate the onset of and response to interruptions. The option to defer response also results in greater subjective perceptions of control, improved task resumption and reduced feelings of interruption and distraction on the part of the user, even within a short period of time. These findings have practical implications for endpoint security and where there is a need to mitigate the effects of user interruptions from computer-mediated communication in complex task situations.

**ARTICLE HISTORY**
Received 29 August 2019
Accepted 19 February 2020

**KEYWORDS**
Anti-malware; endpoint security; interruptions; decision performance

## 1. Introduction

In the next five minutes, some 2,400 new strains of malware will be discovered (McAfee Labs 2018a). This malware aims to discretely infect and undermine the operational integrity of a user's computing environment, compromising the user's tasks, communications and confidential information, sometimes using seemingly innocuous messages to compel the user to inadvertently infect their own computer. At the desktop endpoint, the user's first line of defense against this malware is anti-malware software, also known as anti-virus or AV software, which must be kept up to date in order to effectively disrupt the myriad attack vectors of email, software and network vulnerabilities (Symantec Labs 2017). To this end, Sophos (2019, 13) argue,

> in contemporary malware attacks, the problem is not limited to a small number of executable file types that must be observed, tracked, and have their behavior monitored. With a wide range of file types that include several 'plain text' scripts, chained in no particular order and without any predictability, the challenge becomes how to separate the normal operations of a computer from the anomalous behavior of a machine in the throes of a malware infection.

The rate of new malware infections requires developers of anti-malware software to frequently update their software in order to keep abreast of new detection techniques (Gartner Research 2018). In many environments, it is the user's responsibility to keep such software up to date. Further, because most attack vectors are either not known or not reported (McAfee Labs 2018b), IT security departments must rely on good end user decision-making for effective defense. As a result, it is becoming increasingly clear that an understanding of the user's endpoint desktop security must involve an understanding of the user's approach to malware defense. However, desktop endpoint security updates can interrupt user activity, thereby disrupting the user's flow of work. To avoid disruption to their tasks, users may elect not to update their software, thereby diminishing the level of protection they receive, and putting their computing resources and personal data at risk. In the face of this user reluctance, anti-malware providers must choose how to interrupt the user to more effectively combat the threat of infection. On one hand, they can force the user to respond immediately to the update request, thereby ensuring the anti-malware software is operating effectively. On the other hand, the software can allow the user to defer or 'negotiate' the update to a more convenient time. However, the practical effects of this choice are not yet known.

Managers turning to the research literature for insight into this problem may be disappointed. The vast

**CONTACT** Sigi Goode ✉ sigi.goode@anu.edu.au Research School of Management, Australian National University, Canberra, ACT, Australia

majority of prior work into malware has examined user perceptions, damage resulting from infections, or organisational policies surrounding malware prevention. Very little work has examined the practical realities of how users defend themselves at the cognitive operational level (e.g. Doherty and Tajuddin 2018). Users are typically not waiting to upgrade – rather, they are engrossed in other tasks. Hence, any realistic approach to modelling the decision outcomes requires the user to be undertaking a primary task when responding to an anti-malware update request. However, most prior empirical research into the effects of interruptions on users' task performance (Avrahami and Hudson 2004; Cutrell, Czerwinski, and Horvitz 2001; Czerwinski, Cutrell, and Horvitz 2000a) have focused only on the immediate nature of user interruptions, with less emphasis on interruptions that allow users to delay their response. Knowledge of malware defense must hence be balanced against an understanding of how users respond while they are completing their tasks.

In this paper, we model two modes of user interaction in the anti-malware context. In the first mode, users must respond immediately to an interruption. In the second mode, users can defer responding to the interruption. We examine these modes against three indicators of decision quality, being decision comprehension time, decision response time and decision accuracy. Our findings indicate that anti-malware providers should encourage users to defer difficult decisions regarding anti-malware upgrades. The results of our modelling show that requiring an immediate response itself encourages users to make bad decisions.

This research makes two contributions to knowledge. First, the rise in malware threats requires a greater understanding of the operational level of malware defense in order to mount an effective response to malware threats. Despite much work into malware, mostly at a technical level, very little work has focused on the cognitive response state in which the user interacts with their anti-malware software in its practical role as the user's endpoint defense. Prior research has shown that users underestimate infection risk (Menard, Gatlin, and Warkentin 2014; Teer, Kruck, and Kruck 2007) and to date no study has yet identified the cognitive implications of this perception at the endpoint security level. To fill this gap, our experimental setup emulates the user's day-to-day operating circumstances in the face of an anti-malware interruption. Second, we identify the effects of negotiated interruptions in mitigating the disruptive effects of interruptions across simple and complex tasks. Our contribution in studying the anti-malware context is to identify the moderating effect of ongoing task complexity on interruptive effects, because users are typically engrossed in other tasks, and only encounter the anti-malware software interruption incidentally. We incorporate both multiple stages and multiple interruptions in each primary task with the inclusion of changes in task complexity. In this regard, the work addresses calls from Basoglu, Fuller, and Sweeney (2009) and Gupta, Sharda, and Greve (2011) to investigate the effects of interruptions across tasks with varying levels of cognitive burden on users.

This paper proceeds as follows. The next section provides background information, followed by an overview of prior work on interruptions. This leads to the study's research framework and hypotheses, followed by the research design and method. Analysis of the objective experiment and subjective questionnaire is then presented, followed by conclusions.

## 2. Endpoint security and anti-malware software

Operational security is an important issue for organisational and private user ICTs (Goode et al. 2015; Goode and Lacey 2011). Substantial prior research has highlighted the risks of malware threats to operational security. However, endpoint security from the perspective of the end user has received comparatively little attention in prior work (e.g. Doherty and Tajuddin 2018). To better understand current thinking regarding endpoint security in the end-user context, we searched for and reviewed all published journal articles that examined anti-malware and endpoint security at the user behaviour level. Table 1 presents the outcomes of this review.

The bulk of prior work has been either at a technical level or at the policy level. In the first group, research has been divided into two main streams: developing more effective anti-malware software by identifying the exploitation vectors of malware, and second in identifying new techniques for malware prosecution. These techniques have progressed from traditional techniques such as signature scanning (Liao and Wang 2006) and structural heuristics (Zenkin 2001) to more modern techniques such as data mining (Ye et al. 2017), machine learning, (Milosevic, Dehghantanha, and Choo 2017), and behavioural analysis (Faruki et al. 2014). The majority of such work has employed archival data, such as malware signatures (Sukwong, Kim, and Hoe 2011), or simulations (Abazari, Analoui, and Takabi 2016) to test empirical models.

Research in this stream has identified a number of concepts that are relevant to this research. A principal concept underpinning this work is that malware evolves quickly to exploit newly identified vulnerabilities in

**Table 1.** Prior studies on use behaviour with anti-malware and endpoint security.

| Source | Theory base | Methods | Participants | Findings |
|---|---|---|---|---|
| Peterson (1992) | | Conceptual | | This paper provides an overview of virus functionality as it relates to the MS-DOS operating environment. Compromise methods include the startup process and command file structure. Technical countermeasures, security awareness programs and response teams are seen as vital solutions |
| Herold (1995) | | Case Study | One company (Principal Finance Group) | This paper documents an anti-virus strategy at a large financial company. The strategy uses four components for endpoint security, being fileserver protection, workstation protection, anti-virus 'swat' teams and employee education and awareness |
| Bontchev (1996) | | Conceptual | | This paper discusses the novel threat of macro viruses in Microsoft Word documents and the ways in which macro viruses can gain elevated privileges on a user's desktop |
| Highland (1997) | | Conceptual | | This paper proposes a set of organisational rules for controlling endpoint virus risk, including software controls, employee access controls, and storage controls |
| Post and Kagan (1998) | | Survey | 115 Information security professionals | Barriers to anti-virus implementation include lack of financial support and lack of top management commitment to endpoint security initiatives. Organisations typically wait until they are attacked before implementing countermeasures |
| Zenkin (2001) | | Artefact development | | This paper proposes a method for detecting viruses using code fragments |
| Teer, Kruck, and Kruck (2007) | | Survey | 86 university students | Approximately one third of respondents do not operate or do not update anti-virus software, and approximately half of respondents had encountered a virus in the previous year |
| Bubaš, Orehovački, and Konecki (2008) | Adapted Protection Motivation Theory | Survey | 312 college students | Four factors of endpoint security were identified: user conscientiousness of their operating environment, engagement in risky behaviour, belief that malware threat was low, and lack of fear |
| Zhang and McDowell (2009) | Protection Motivation Theory | Survey | 182 college students across three US universities | Response cost, response efficacy and fear are positively related to strong password use. Perceived vulnerability and severity were not significant |
| Gurung, Luo, and Liao (2009) | Protection Motivation Theory | Survey | 232 university students | This paper examines factors that motivate consumers to adopt anti-spyware software when they are faced with security threats. The study found that perceived severity, self-efficacy, and response efficacy were positively associated with intention to adopt anti-spyware |
| Lee and Larsen (2009) | Protection Motivation Theory and Technology Acceptance Theory | Survey | 239 Small to Medium-sized Enterprise (SME) executives in the United States | Threat and coping appraisal predict executive intention to adopt anti-malware software. Adoption intention was affected by threat appraisal and social influence for IS experts, and coping appraisal and budget for non-experts |
| Anderson and Agarwal (2010) | Protection Motivation Theory | (1) Survey and (2) experiment | (1) 596 home computer users and (2) 101 experimental subjects | Conceptualises 'conscientious cybercitizens', a type of user that aims to secure their desktop. User intention is affected by cognitive, social and psychological components. Protection goal-framing and user self-view affect intention to protect using anti-malware software |
| Huang et al. (2010) | Communication theory and time orientation | (1) Survey; (2) Focus groups | (1) 83 undergraduate university students from China; (2) 20 undergraduate university students from China | Anti-virus notifications affect users in different ways. Users with low-context communication style use notification information better than high-context communication styles. Poly-chronic users perceive lower interruption than mono-chronic users |

(*Continued*)

**Table 1.** Continued.

| Source | Theory base | Methods | Participants | Findings |
|---|---|---|---|---|
| Okane, Sezer, and McLaughlin (2011) | | Conceptual | | This paper reviews malware mechanisms for obscuring damaging functionality to avoid detection by anti-malware. These techniques including packing, polymorphism and metamorphism. Anti-malware must stay up to date to adequately defend |
| Sukwong, Kim, and Hoe (2011) | | Archival data | 1115 malicious software files, tested against six anti-virus software applications | Anti-malware detected 60% of malicious software at zero day, with most of the remaining taking 30 days to detect. Some 10% were never detected |
| Warkentin, Johnston, and Shropshire (2011) | Social learning theory | Survey | 234 professionals working in healthcare | Security self-efficacy was positively affected by situational support, verbal persuasion and vicarious experience. Efficacy positively affected behavioural intention |
| Yoon, Hwang, and Kim (2012) | Protection Motivation Theory | Survey | 202 college students | Perceived severity, response costs, response efficacy and response efficacy are positively related to information security and protection behaviour. Perceived vulnerability and perceived social influence were not predictors |
| Furnell and Clarke (2012) | | Conceptual | | This paper examines a dialog box from an instance of user authentication and anti-virus. The paper argues that users often lack the skill and knowledge to immediately understand the content of these messages |
| Al-Saleh, Espinoza, and Crandall (2013) | | Software analysis | Symantec Anti-virus and Sophos | This paper examines the effect on operating system performance of two anti-virus software applications. The paper finds that anti-virus software makes significant demands on the operating system and time to complete processes |
| Yoon and Kim (2013) | Protection Motivation Theory | Survey | 162 organisational employees in Korea | Moral obligation, organisational norms and attitude toward computer security behaviour significantly affect employee attitudes to desktop security. Perceived threat severity, response efficacy, and self-efficacy significantly affect employee attitude |
| Ramachandran et al. (2013) | Culture | Semi-structured interviews | 40 business professionals | Perceptions of information security vary across professional cultures. Accountants reflected a strong security culture. IS professionals pursued productivity at the expense of security. Marketers saw limited involvement with security matters |
| Menard, Gatlin, and Warkentin (2014) | Protection Motivation Theory | Survey | 152 college students | Threat severity, threat susceptibility, automacicity and concurrency are positively related to behavioural intention to protect computer resources |
| Williams et al. (2014) | Security Belief Model | Survey | 237 business professionals in India | Perceived severity, perceived susceptibility and perceived benefits are positively related to intentions to perform preventative information security behaviours |
| Min et al. (2014) | | Artefact development | Operational proof of concept attacks on Avira, AVG, McAfee, Microsoft and Symantec anti-virus applications | This paper proposes an attack against the vulnerability that can occur when a PC's anti-virus definition library is being updated. The vulnerability is exacerbated the more frequently the anti-virus tool is updated |
| Leukfeldt (2014) | Routine activity theory | Archival data | 10,316 Dutch computer users | The currency of a user's anti-virus software has no relationship with the likelihood of email-borne malware (i.e. phishing) infection and hence user victimisation |
| Posey et al. (2014) | Protection Motivation Theory | Interviews | 22 business employees and 11 information security employees | Professionals see hackers and Internet threats (worms, viruses, Trojan horses), as the most likely security threat. Professionals understand that organisational assets require protection, but maladaptive behaviours (i.e. not behaving in a secure |

(*Continued*)

**Table 1.** Continued.

| Source | Theory base | Methods | Participants | Findings |
|---|---|---|---|---|
| | | | | manner) may be justified in response to perceived organisational injustice |
| Kim, Yan, and Zhang (2015) | | Archival data and artefact development | Corpus of webpages: 1,230 fake anti-virus, 210 popular security, 17,530 unpopular security, 538 irrelevant webpages | Users have difficulty identifying fake anti-virus software available online. This paper presents the development of a software artefact (DART) that identifies fake anti-virus software web pages with 90.4% accuracy |
| Safa et al. (2015) | Protection Motivation Theory and Theory of Planned Behaviour | Survey | 212 Information security experts and IT professionals in Malaysia | Users' security behaviour is positively affected by information security experience and involvement, information security awareness, threat appraisal, information security self-efficacy, information security organization policy, attitude towards information security, and subjective norms |
| Johnston, Warkentin, and Siponen (2015) | Protection Motivation Theory, Deterrence Theory and Fear Appraisal | Survey | 559 government employees in Finland | Sanction comments are associated with stronger intentions to comply with security policies and security threat warnings |
| Posey, Roberts, and Lowry (2015) | Protection Motivation Theory | Online survey | 380 insider employees from the United States | End user security education, training and awareness (SETA) improve security appraisals, which are also affected by response cost. Protection motivation theory does not necessarily apply in the user context as it does in the organisational context |
| Jansen et al. (2016) | Protection Motivation Theory | Survey | 1622 Dutch entrepreneurs | Coping behaviours, perceived effectiveness, positive user attitude and self-efficacy explain adoption of anti-malware measures |
| Ortiz de Guinea (2016) | | (1) Critical incident survey and (2) experiment | (1) 217 organisational employees (2) 12 university students | Users display negative emotions as they cope with negative desktop IT events. Users may eventually disengage and accidentally learn incorrect responses |
| Tsai et al. (2016) | Protection Motivation Theory | Survey | 998 Amazon Mechanical Turk users | This paper examines the security intentions (including use of anti-malware) of PC users. Coping appraisal, habit strength, response efficacy and personal responsibility predicted online safety intentions |
| Ifinedo (2016) | Deterrence theory and cost benefit analysis | Survey | 176 professionals (42 Canadian professionals, 51 IS professionals, 83 non-IS managers) | Information security compliance was positively affected by top management support and sanction severity, but negatively affected by s cost benefit analysis. Detection probability was not significant |
| Visinescu et al. (2016) | Protection Motivation Theory | Survey | 203 undergraduate students | Propensity to trust influenced users' perceived need for privacy and perception of the need to self-protect. Preventive measures, user self-efficacy, and acceptable cost of prevention positively affect users' need to develop a protection strategy. |
| Steinbart, Keith, and Babb (2016) | Cybernetic loop and Technology Threat Avoidance Theory | Experiment | 568 undergraduate students in the United States | Even if users initially use security behaviours, they may cease or reduce these behaviours if they become effortful. When login requirements are too strict, users develop work-around solutions that weaken security arrangements |
| Johnston et al. (2016) | Protection Motivation Theory and General Deterrence Theory | Survey | 317 organisational members | Users with strong stability meta-traits possess conscientiousness, agreeableness, and emotional stability. Users with strong plasticity meta-traits exhibit dominant openness and extraversion. These factors interact in end-user security related settings. |
| McGill and Thompson (2017) | Protection Motivation Theory | Survey | 629 users | This paper compares security intentions of computer and smartphone users. Use of anti-virus software was higher for PCs (85%) than for smartphones (44%) |
| White, Ekin, and Visinescu (2017) | Health Belief Model and Protection Motivation Theory | Survey (Qualtrics/ Online) | 945 computer users | This paper examines the factors affecting protective behaviour and perceived security incidents among home computer users. Self-efficacy, Cue to action and Perceived barriers to implement security tools are |

(Continued)

**Table 1.** Continued.

| Source | Theory base | Methods | Participants | Findings |
|---|---|---|---|---|
| | | | | positively related to Protection behaviour intentions (such as using anti-malware software) |
| Burns et al. (2017) | Protection Motivation Theory and Psychological Capital Theory | Survey | 377 employees in the United States | Psychological capital negatively affected threat severity, maladaptive rewards and response cost, but positively affected perceived security response efficacy. Protection motivation was positively affected by threat severity and response efficacy, but negatively affected by maladaptive rewards and response cost |
| Menard, Bott, and Crossler (2017) | Protection Motivation Theory and Self-Determination Theory | Online survey | 785 computer users with password manager software installed | Perceived relatedness, competence and autonomy positively affected threat severity, self-efficacy and response efficacy. Competence, response performance motivation and response efficacy positively affected behavioural intention to engage in security behaviour |
| Blythe and Coventry (2018) | Protection Motivation Theory | Survey | 526 employees | Ease of responding was positively related and cost of responding was negatively related to anti-malware behaviour |
| Jansen and van Schaik (2018) | Protection Motivation Theory | Survey | 1200 Dutch users of online banking services | Threat appraisal and coping appraisal, especially response and self-efficacy, predict precautionary behaviour in online banking |
| Dodel and Mesch (2018) | | Survey (archival) | 1850 Israeli internet users | Education, age, gender and quality of internet access are related to digital security skills which, along with frequency of online activities, predict anti-malware behaviours |
| Menard, Warkentin, and Lowry (2018) | Protection Motivation Theory | Factorial survey | 500 Amazon Mechanical Turk users from China and the United States | This paper examines user intention not to protect information, including use of anti-spyware software. Although psychological ownership was significantly associated with response efficacy and self-efficacy, efficacy was not associated with behavioural intention not to protect information |
| Yoo, Sanders, and Cerveny (2018) | Psychological ownership theory and flow theory | Survey | 327 Korean law enforcement professionals | A user's sense of flow is positively related to their level of psychological ownership and security education training and awareness (SETA) use. These in turn predict user intention to comply with security policy |
| Lévesque et al. (2018) | | Longitudinal experimental study | 50 household users over four months | Approximately a third of users were protected by an anti-virus application that blocked a malware attack, and 20% of users had become infected with a virus that was not detected by the anti-virus software (half of these users noticed no difference in operation of their software). Gender, age, area of expertise, and employment status were not related to malware attacks |
| Wachyudy and Sumiyana (2018) | Protection Motivation Theory and Coping Theory | Survey | 580 e-banking users from Indonesia | This paper examines threat perceptions of e-banking users. The study finds that threat perception and computer anxiety are both positively associated with intention to take protective action |
| Baskerville, Rowe, and Wolff (2018) | Vulnerability Points Theory | Archival data | Responses from 9,721 French companies | The use of self-protective cybersecurity measures is associated with higher degrees of internal and external system integration |
| Hanus, Windsor, and Wu (2018) | Technology Threat Avoidance | Quasi experiment and Survey | 74 municipal government employees in the United States | Security awareness is affected by self-efficacy, perceived severity, perceived susceptibility, perceived effectiveness, perceived cost and perceived responsibility |
| Martens, De Wolf, and De Marez (2019) | Protection Motivation Theory | | 1181 Belgian citizens | This paper examines end user propensities to secure their online activity. User perceptions of technical and social cybercrime differ. The paper finds that coping awareness (including awareness of anti-malware software) positively affects self-efficacy and response efficacy |
| | Protection Motivation Theory and Extended | Survey | 308 business employees | This paper applies an EPPM model to explain anti-spyware adoption. The study finds that |

(*Continued*)

**Table 1.** Continued.

| Source | Theory base | Methods | Participants | Findings |
|---|---|---|---|---|
| Chenoweth, Gattiker, and Corral (2019) | Parallel Processing model (EPPM) | | | users are not motivated to adopt anti-spyware when they appraise the malware threat as low. User efficacy then explains whether the user denies the threat or adopts spyware |
| Chen and Li (2019) | Person-organisation fit theory | Survey | 253 employees in China | This paper finds that perceived need–supply fit, demand–ability fit, and value fit motivate security commitment. Security commitment partially mediates demand-ability fit and need-supply fit and participation intention, and fully mediates value fit and participation intention. User apathy reduces motivation to engage in extra-role behaviour |

software. Accordingly, anti-malware software also requires frequent updating in order to maintain a strong defense against this malware. At a technical level, this updating may involve alterations both to malware definition files and anti-malware detection routines more directly. As anti-malware itself is often a malware target, most anti-malware software self-protects (Baskerville, Rowe, and Wolff 2018) and alterations to anti-malware applications require elevated user privileges in order to be updated: these elevated privileges frequently require user intervention and permission to update. Figure 1 illustrates several stylized examples of anti-malware pop-up modal dialog windows that require a user's response before they can resume their tasks. In this stream of work, keeping anti-malware definitions and functionality up to date is an accepted and expected part of endpoint defense.

Research in the second group has focused on two main areas. First, a substantial amount of work has examined the development of organisational security policies, especially with regard to policy effectiveness, completeness and structure (Bonny, Goode, and Lacey 2015). A key goal of this body of work lies in identifying effective techniques for compelling anti-malware use within organisational ICT resources and their users. The second body of work in this stream has focused on assessing the degree of policy compliance among end users, management, operational staff and, to a lesser extent, home and private users. Surveys of end users (Anderson and Agarwal 2010; Dodel and Mesch 2018; McGill and Thompson 2017) and employees (Blythe and Coventry 2018; Chenoweth, Gattiker, and Corral 2019; Williams et al. 2014) have been the dominant approach to empirical testing within this stream of research.

In contrast to evidence from the first body of work, an undercurrent of this research is that there is a gap between organisational expectations regarding endpoint security, and the degree to which users will adhere to endpoint defense policies. A core goal of these policies is to compel users to make good decisions regarding operational security in order to preserve operational assets: as a result, organisations strive to make their policies clearer (Herath and Rao 2009), more user-friendly (Höne and Eloff 2002; Safa, Von Solms, and Furnell 2016), for example by accommodating BYOD initiatives (Baillette, Barlette, and Leclercq-Vandelannoitte 2018), or more punitive by increasing penalties for non-compliance (Shropshire, Warkentin, and Johnston 2010). However, independently of the organisational context, private users also appear reluctant to adhere closely to endpoint security directives, such as those established by internet service providers (ISPs).

In both the organisational and private contexts, endpoint policies appear necessary because users may make operational decisions that benefit their immediate user outcomes, rather than those that relate to more distant possibilities such as a potential malware infection or a data breach (Goode et al. 2017). However very little work has offered an explanation for this reluctance at a cognitive decision level. There is hence an opportunity to study the effect of user decision making in the face of software interruptions while the user is involved in other tasks. A study into the effect of these interruptions must therefore take the user's other work processes into account when analysing these disruptive decision-making effects.

## 3. Interruptions

Interruptions are unpredictable stressors that require additional user effort and attention to address (Galluch, Grover, and Thatcher 2015). Interruptions are typically considered disruptive, hindering task performance and effectiveness, especially for interruptions that use the same sensory channels as the individual's working memory (Jett and George 2003; Nystrom et al. 2000). Interruptions test the user's cognitive abilities by forcing them to switch their attention from their primary tasks to another task (Bailey, Konstan, and Carlis

2001; Eyrolle and Cellier 2000; Hodgetts and Jones 2007).

Although extant literature has attributed differences in the effects of user interruptions on task performance to the type of interruptions and tasks that require varying levels of cognitive processing, few empirical studies have sought to provide an insight into the outcomes of such a research undertaking. To identify these effects, we identified prominent empirical studies of computer-mediated interruptions published in journals and leading conferences. Table 2 summarises the empirical studies on the effects of interruption in computer-mediated contexts.

Two types of interruptions emerge from prior literature, relating to the onset of the interruption and the amount of control available to the user over when and how to respond (Adamczyk and Bailey 2004; Hodgetts and Jones 2007; Robertson et al. 2004). On one hand, an *immediate* interruption is an event that demands user attention and expects them to suspend their tasks and interact with it at that time. Immediate interruptions burden people's cognitive limitations by drawing attention immediately (such as an urgent popup window that requires a quick response) (Altmann and Trafton 2004). On the other hand, a *negotiated* interruption gives a user control over when or whether to deal with the interruption, thus minimising disruptive effects (McFarlane and Latorella 2002).

Higher levels of concentration or cognitive effort involved in problem-solving tasks exacerbate the disruptive effects of interruptions (Eyrolle and Cellier 2000; Solingen, Berghout, and Latum 1998). Users will experience greater disruptive effects of interruptions to their task performance when they undertake complex tasks, due to their increased stress and inability to integrate a high number of information cues for accurate decision-making.

Interruptions can adversely affect tasks that require higher levels of concentration (Solingen, Berghout, and Latum 1998), are more difficult (Gillie and Broadbent 1989), or require greater involvement (Franke, Daniels, and McFarlane 2002).

When interruptions occur during simple tasks, stress increases and attention narrows, resulting in the exclusion of irrelevant information cues thus facilitating decision performance. However, as task complexity increases (Kelton, Pennington, and Tuttle 2010; Li et al. 2011), people's cognitive resources decrease and attention is narrowed, resulting in the exclusion of some information cues that may be needed for completing the task successfully. Adverse effects of these interruptions may occur at different stages (phases) in the task being undertaken.

### 3.1. Interruptions in the anti-malware context

Interruptions from anti-malware software are likely to arise while the user is engaged in other tasks. When anti-malware software issues an update dialog box appears that requires immediate decision-making (like those shown in Figure 1), the level of complexity in the interruption will be an important factor in determining how disruptive the interruption is. If the interruption allowed the user to delay their response to the interruption, the user might better manage their decision-making strategies to suit the current task, thereby minimising disruptive effects to their other work.

The anti-malware update process consists of two principal phases. The first stage is an announcement stage, which presents the user with a message calling them to action. This stage requires the user to understand and process the anti-malware announcement. The second stage is an action stage in which the user elects to obey or disobey the message. This stage requires the user to review their available options, given the content of the announcement, and to select their choice. Responding to an anti-malware dialog box is likely to involve *decision comprehension* (understanding and processing) and evaluation becomes *decision response* (option review and selection).

## 4. Research model and hypotheses

Synthesising prior literature, the effects of user interruptions will be different when users attend to interruptions immediately or when users negotiate a delayed response to the interruptions. Complex tasks exacerbate the differential effects of both interruption types on users' decision performance. The research posits that immediate interruptions are more disruptive than negotiated interruptions on users' decision performance in complex tasks, but there are no differential effects between both types of interruptions on users' decision performance in simple tasks. Figure 2 shows the research model.

Three hypotheses arose from the theoretical perspectives and are empirically tested in this study. First, interruptions may affect the overall time taken by the user to solve the problem and commit to a course of action (Marsden, Pakath, and Wibowo 2002). During the decision comprehension stage, the interruption may extend the time taken by a participant to identify and understand a problem task (Beynon, Rasmequan, and Russ 2002). This leads to the first major hypothesis concerning task complexity.

H1: Task complexity moderates the effects of immediate interruptions and negotiated interruptions on users' decision comprehension time

**Table 2.** Prior empirical studies on computer-mediated interruption.

| Source | Theory Base | Methods | System | Participants | Findings |
|---|---|---|---|---|---|
| Solingen, Berghout, and Latum (1998) | Task productivity | Ethnography (Goal / Question / Metrics) | E-mail client | An unspecified number of E-mail users among developers and project managers at two technology companies | Software developers were disrupted with the arrival of e-mails when they are in a state of focus or concentration and they take longer to reestablish their task context |
| Czerwinski, Cutrell, and Horvitz (2000a) | Relevancy, timing, task and temporal phase | Experiment | Instant messaging (MSN Messenger) | 23 experienced Microsoft Office users between the ages of 26–56 | Participants take longer to process irrelevant interruptions and it is more difficult to reestablish their task context following the interruption. Participants tended to delay switching to an IM until they had completed a subtask or an action, such as typing search terms |
| Czerwinski, Cutrell, and Horvitz (2000b) | Memory, timing, task type and task switching | Experiment | Instant messaging (MSN Messenger) | 16 experienced Microsoft Office users between the ages of 20–57 | The study examined immediate interruptions in simple search tasks. Participants were more susceptible to the disruptive effects of interruptions when evaluating and executing search tasks, where these tasks were less amenable to interruption than others |
| Cutrell, Czerwinski, and Horvitz (2001) | Information overload, divided attention and memory | Experiment | Instant messaging (MSN Messenger) | 16 experienced Microsoft Office users between the ages of 20–57 | The study focused on immediate Instant Messages. Participants were reliably slower overall after receiving an instant message, and the cost of the interruption was found to be higher when participants received instant messages earlier in their search tasks. The researchers suggested that the findings could be a result of participants having insufficient time to learn the task prior to receiving a message |
| Franke, Daniels, and McFarlane (2002) | Task context recovery, immediate and negotiated interruptions | Usability Test (Listen / Communicate / Show Paradigm) | 'Galaxy', a researcher-developed dialogue system | An unspecified number of US Marines (field testing) | Participants required assistance from intelligent agents to resume their task context after being interrupted in dialogue. The study noted that future work could focus on task complexity differences |
| Dabbish and Kraut (2003) | Awareness and task productivity | Experiment | Instant messaging | 72 participants assumed the roles of Helper and Asker (2-player communication) | Participants were disrupted by unanticipated instant messages and were distracted through increased awareness of the incoming message that added to their workload and deteriorated overall task performance |
| Jackson, Dawson, and Wilson (2003) | Task context recovery | Experiment | E-mail client (Microsoft Outlook) | 15 employees from an office-supplies technology company | Participants were found to view new e-mails within 6 s upon awareness of the e-mail. The researchers found a significant task recovery delay for participants after they finish reading an e-mail |
| Speier, Vessey, and Valacich (2003) | Decision-making and Task complexity | Experiment | E-mail and instant messaging | 136 undergraduate students | Participants were disrupted in their decision performance by interruptions in complex tasks, while their decision performance was facilitated by interruptions in simple tasks. Study focus was on immediate interruptions only |
|  | Intrusion, responsiveness and | Usability Test | Instant messaging (Trillian Pro) | An unspecified number of IM users and their | Incoming messages are distracting to users while they |

(*Continued*)

**Table 2.** Continued.

| Source | Theory Base | Methods | System | Participants | Findings |
|---|---|---|---|---|---|
| Avrahami and Hudson (2004) | immediate interruptions | | | respective IM 'buddy' contacts | are performing tasks and there is a tradeoff between responding to the message and staying on task. The problem of IM disrupting work can be alleviated by increasing the salience of messages that deserve immediate attention, and helping users to decide whether or not to stay on task |
| Rennecker and Godwin (2005) | Interruptions, personal control, disorganisation | Descriptive model and cross-level approach | Not specific | Not applicable | Synchronous and asynchronous communication modes were contrasted to show how the use of communicative technologies can both facilitate and detract from work organization at the individual level depending upon one's role in the interaction |
| Bailey and Konstan (2006) | Interruption, annoyance and task completion | Experiment | Variety of HTML-based tasks | 50 participants, comprising undergraduates and professionals | Interruption increases task completion time and annoyance. Participant affect and annoyance can be altered depending on timing of interruption |
| Moe (2006) | Online consumer behaviour and task interruption | Experiment | Informational Web site | 83,136 non-registered users over a four-day period | The study showed that within-page delay had an effect on click through rates, with a recommendation to minimize any delaying in showing the pop-up |
| Iqbal and Horvitz (2007a) | Interruption, attention, task switching and notifications | Field Study (DART Monitoring tool) | Email and Instant messaging | 27 users over a two-week period | Users prefer to enable alerts to be aware of incoming information, but still control when to switch tasks. The user's ability to perceive the length of time taken when responding to alerts is less than the actual time, with importance and visibility of the suspended task application reducing recovery time |
| Iqbal and Horvitz (2007b) | Interruption, disruption, recovery, conversation and cognitive models | Field Study (DART Monitoring tool) | Outlook and task specific applications | 16 users over a two-week period | Conversations cause users to interrupt their current task to participate and embark on other activities. The time until resuming the task depends on duration of the task activity before the interruption, with visibility of the suspended application positively related to faster resumption times |
| Russell, Purvis, and Banks (2007) | Interruptions, differing tasks/situations and Action Regulation Theory | Interviews | E-mail client (Microsoft Outlook and Lotus Notes) | 28 participants from three organisations | Qualitative content analysis found interviewees use a wide range of strategies for dealing with email in general, and adopt specific strategies when the task or situation changes |
| Bailey and Iqbal (2008) | Interruption effects on workload | Experiment | Proprietary email and document management tools | 24 participants | Participants' pupil dilation was monitored. Interruptions have reduced disruptive effects if they coincide with periods of reduced mental exertion. Workload changed during task and subtask completion |
| Garrett and Danziger (2008) | Interruption, effects on work communication | Survey | Instant Messaging | 912 respondents (272 IM users) | Results found IM use does not influence overall levels of work communication. Workers using IM in the workplace report being interrupted less frequently than non-users, and |

(*Continued*)

**Table 2.** Continued.

| Source | Theory Base | Methods | System | Participants | Findings |
|---|---|---|---|---|---|
| | | | | | more frequently engaging in computer-mediated communication, for both work-related and personal communication, than non-IM users |
| Basoglu, Fuller, and Sweeney (2009) | Interruption, cognitive state, effects on performance | Experiment | Not specific | 257 undergraduate students | The frequency of interruptions has a significant negative indirect impact on decision accuracy through cognitive load for tasks accuracy. The interaction between the order of performing tasks of varying complexity and interruption frequency also influences cognitive load, eventually performance |
| Mano and Mesch (2010) | E-mail features, work performance and side-effects | Secondary analysis of interview data | E-mail client | 354 respondents | E-mail communication in organisations carries important information for the completion of jobs, while personal e-mails neither contribute to work performance, nor are they detrimental. Workers check e-mails regularly and these interruptions are positive because they increase the acquisition of work-related information critical for getting the job done |
| Salvucci and Bogunovich (2010) | Interruptions, multitasking and mental workload | Experiment | E-mail and Instant messaging | 20 users | Most of the time users switched to the interrupting task during periods of lower workload rather than during those of higher workload. When interruptions can be deferred, users have a strong tendency to monotask until primary-task mental workload has been minimised |
| Li et al. (2011) | Interruption frequency, perceived task complexity and user satisfaction | Experiment | Instant messaging (Yahoo! Messenger) | 112 respondents | Poly-chronic individuals are more satisfied with the work process deploying interruptive IM technology than monochronic ones. Poly-chronicity moderates the effect of interruption dimensions on an individual's perceived task complexity and process satisfaction |
| Ou and Davison (2011) | IM use at work and group outcomes | Survey | Instant messaging | 253 working professionals | IM use is a significant predictor of work interruption, but it can contribute to communication performance in the workplace, where the benefits overwhelm the negative effects associated with work interruption |
| Sykes (2011) | Interruptions, employee effectiveness and satisfaction | Observations | Email and Instant messaging | 4 employees in the software development company | Participants were spending a considerable portion of their time serving interruptions. Companies should recognise the type and number of interruptions in the workplace and attempt to increase employee effectiveness and satisfaction as well as to reduce the cost of interruptions as methodologies identified in the study |
| | Task performance based on the degree | Experiment | | 30 undergraduate students | Participants who experienced an interruption by a task with |

(*Continued*)

**Table 2.** Continued.

| Source | Theory Base | Methods | System | Participants | Findings |
|---|---|---|---|---|---|
| Eatchel, Kramer, and Drews (2012) | of contextual similarity of an interruption | | A specialised computer programme developed for the experiment | | contextually identical information to the primary task made fewer errors following the completion of the interruption compared to a task with contextually dissimilar information |
| Marulanda-Carter and Jackson (2012) | E-mail addiction and interruptions | Experiment and survey | E-mail client | 7 employees for the experiment and 100 for the survey from a car rental company | E-mail interruptions have a negative time impact upon employees and show that both interrupt handling and recovery time exist. A method to capture addictive characteristics, both clinical and behavioral, in employees' e-mail communication behaviour was presented |
| Fonner and Roloff (2012) | Connectivity paradox | Online survey | face-to-face, videoconferencing, phone, instant messaging, and email | 89 high-intensity teleworkers and 104 office-based employees | The authors propose a model linking the core features of the connectivity paradox to organisational identification, with results indicating that connectivity increases stress from interruptions and indirectly diminishes teleworkers' identification |
| Wang et al. (2012) | Threaded cognition theory | Experiment | A specialised computer programme developed for the experiment | 32 university students | Communicating with a confederate led to a 50% drop in visual pattern-matching performance in the IM condition and a 30% drop in the voice condition. Visual fixations on pattern-matching were fewer and shorter during the communication task and a greater loss of fixations was found in the IM condition than the voice condition. The results suggest that distributing the work between the audio and visual channels reduces performance degradation |
| Mansi and Levy (2013) | Distraction conflict theory | Experiment | A specialised e-learning task developed for the experiment | 60 knowledge workers at a single institution | This study found that the time to complete a task for simple-spatial and complex-spatial of tasks are significantly affected by instant messaging interruptions |
| Adler and Benbunan-Fich (2013) | Flow Theory and Self-regulation Theory | Experiment | A specialised Sudoku computer programme developed for the experiment | 212 undergraduate US university students | This paper reports findings that negative feelings trigger more self-interruptions than positive feelings, and in general, more self-interruptions result in lower accuracy in all tasks. Furthermore, the results suggest that negative internal triggers of self-interruptions unleash a downward spiral that may degrade performance |
| Ou, Sia, and Hui (2013) | Social network theory | Social network analysis | Microsoft Sharepoint portal | 51 Global Bank employees | Both Email and IM use at work individually impact communication process, interactivity and relationship network, which are the antecedents that impact work performance. The social networks analysis suggests a linkage between using IM at work and the high level of degree and high level of closeness |

(*Continued*)

**Table 2.** Continued.

| Source | Theory Base | Methods | System | Participants | Findings |
|---|---|---|---|---|---|
| Gupta, Li, and Sharda (2013) | Distraction conflict theory | Experiment | Supply chain tasks interrupted by Yahoo messenger | 112 US university students | This paper reports that the effect of interruption on primary task completion time is dependent upon the hierarchical level of the message sender. Interruptions from a supervisor were found to reduce primary task completion time, whereas interruptions from a peer increased primary task completion time. On the other hand, interruptions from a supervisor aggravated the negative impact of interruptions on task quality |
| Chen and Karahanna (2014) | Cross-domain interruptions (personal and work) | Field study | Not specific | 137 knowledge workers of a Fortune 1000 technology firm | This study identified asymmetric effects for Work-to-Nonwork and Nonwork-to-Work interruptions on work and personal life. The frequency of WTN interruptions is found to be positively associated with work-life conflict and negatively associated with fulfilment of personal life responsibilities, whereas the frequency of NTW interruptions significantly affects fulfilment of work responsibilities but not work-life conflict |
| Lee, Son, and Kim (2016) | Person-environment fit model of stress and Transactional theory of stress and coping | Survey (online and offline) | Social networking services | 201 South Korean university students | Information, Communication, and System Feature overload were significant stressors that influence SNS fatigue. The characteristics of the SNS system significantly influenced the features of system overload, while information equivocality positively influenced information overload. However, information relevance was not a significant predictor of information overload and equivocality was not a significant predictor of communication overload |
| Levy, Rafaeli, and Ariel (2016) | Media richness theory | Online simulation experiment | A specialised computer programme developed for the experiment | 120 undergraduate social sciences students | This paper finds a significant effect of the richness of the message on cognitive performance quality, and the main effect of medium. Furthermore, required compensation time was greater among the groups using mobile phones with tasks performed with a mobile phone requiring more time than with the Internet application, and the mobile phone with MMS group had the longest recovery time of all the test groups |
| Stich et al. (2017) | Effect of computer-mediated communication use on workplace stress | Qualtrics survey panel | Email, video conferencing, audio conferencing or phone calls and instant messaging | 504 full-time US workers | Interruptions arising from computer mediated communications tools contribute to employee stress in the workplace, particularly for electronic mail. Qualitative evidence suggested a variety of computer-mediated tools |

(*Continued*)

**Table 2.** Continued.

| Source | Theory Base | Methods | System | Participants | Findings |
|---|---|---|---|---|---|
| | | | | | could have an effect if the employer desired their use |
| Stich, Tarafdar, and Cooper (2018) | Technostress | Conceptual | | | This paper reports an overview of current research and practice in technostress related challenges facing workplace communication. These manifest in the forms of technology overload, interruptions and work-home interferences. The authors surmise that organisations have to strike a balance between giving employees the technology they want and protecting them |
| Addas and Pinsonneault (2018) | Coordination theory used to develop multilevel theory for work interruptions | Conceptual | | | The paper examines literature to suggest that interruptions that target individuals can also affect other group members through various ripple effects and a cross-level direct effect. It also discusses how the usage of five communication technology capabilities during interruption episodes can moderate the impact of interruptions at the individual and group levels |

Interruptions also may lead to reduced efficiency and increased error rates (Hodgetts and Jones 2003; McFarlane 2002). During the decision response stage where the user reviews available options and makes their final selection, we posit that an interruption will lead to increased decision response time (Hypothesis 2).

> H2: Task complexity moderates the effects of immediate interruptions and negotiated interruptions on users' decision response time

We next posit that an interruption will reduce decision accuracy. This leads to our third hypothesis:

> H3: Task complexity moderates the effects of immediate interruptions and negotiated interruptions on users' decision accuracy

## 5. Research design and method

As in prior studies of interruption, we used a controlled laboratory experiment to test our hypotheses. As in prior studies of anti-malware, we then used a survey for post-hoc testing. Details of participants, measures and procedure are provided below.

### 5.1. Participants

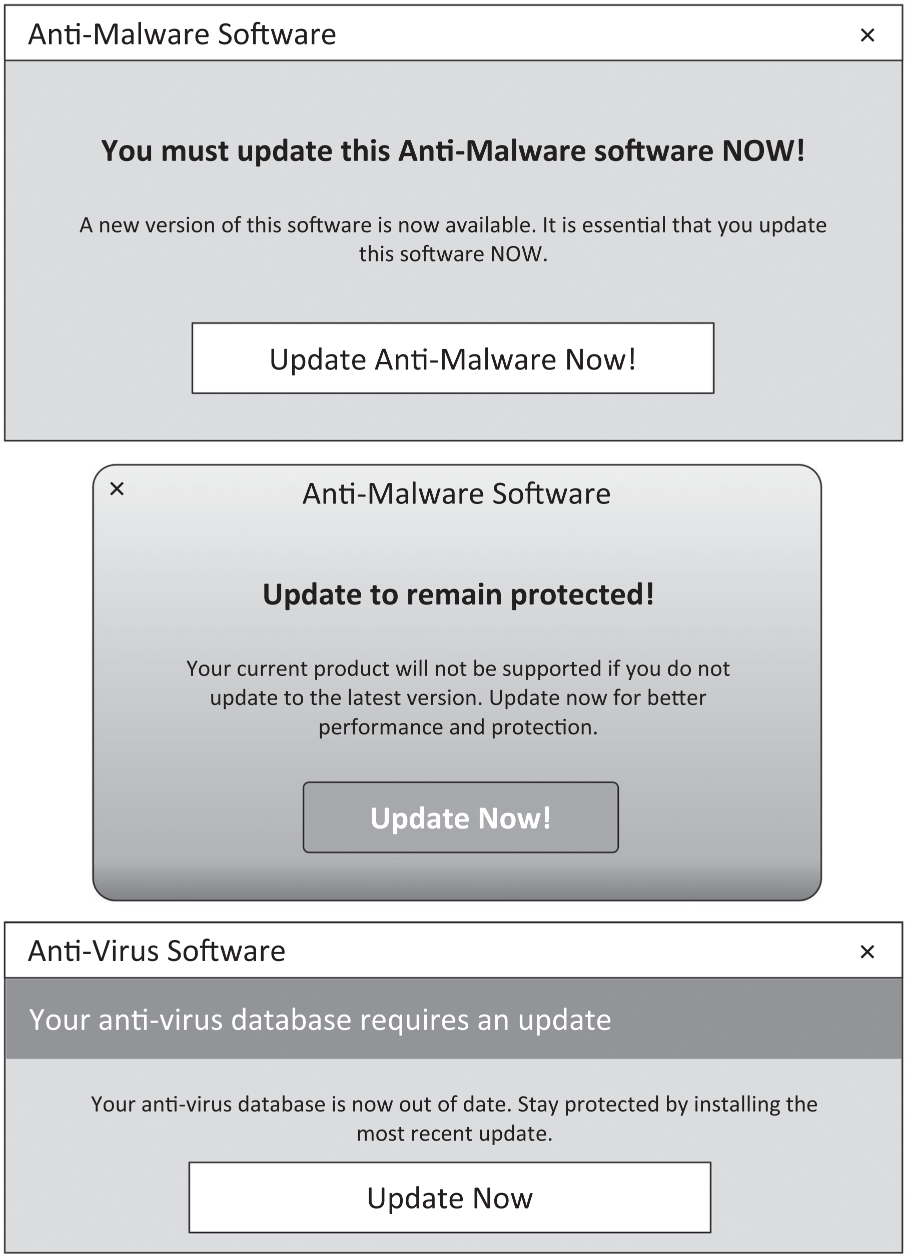
A sample size of 40 participants (Cohen's d = 0.8, $\alpha = 0.05$, power level 1-$\beta = 0.8$) was calculated to be sufficient and similar to previous experiments (e.g. McFarlane 1998). To ease cognitive dissonance and provide a more pragmatic experience for participants (Kim, Barua, and Whinston 2002), each participant received a fixed $10 cash payment as recompense for their time, of which they were aware before attending the experiment.

The 25 male and 15 female participants were between the ages of 18 and 37, with a mean age of 22 years. All participants were undergraduate students studying Information Systems, with skills ranging from intermediate to expert usage of computers and reasonable proficiency with computing tasks and general application software such as email.

Each participant was randomly assigned to one of four treatment order groups. Each of the four treatments was administered with a discrete combination of the two independent variables: interruption type (immediate and negotiated) and task complexity (simple and complex). Participants received all four treatments, and their decision performance was measured under the four treatment conditions. As shown in Table 3, a Kruskal–Wallis test revealed no significant differences in gender, age, level of proficiency and degree of involvement in computing tasks among participants across the treatment conditions.

### 5.2. Materials and measures

The tasks were performed on a standard PC (LCD monitor, keyboard and mouse) to emulate a standard home or office operating environment. The tasks were run in a



You must update this Anti-Malware software NOW!

A new version of this software is now available. It is essential that you update this software NOW.

Update to remain protected!

Your current product will not be supported if you do not update to the latest version. Update now for better performance and protection.

Your anti-virus database requires an update

Your anti-virus database is now out of date. Stay protected by installing the most recent update.

**Figure 1.** Example interruption dialog boxes from anti-malware software.

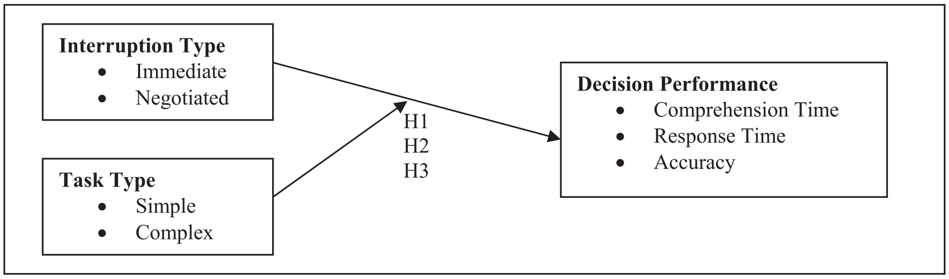


**Figure 2.** Research model.

**Table 3.** Means and standard deviations for participants' demographics across order groups.

| | | Treatment order group | | | |
|---|---|---|---|---|---|
| Variables | | 1 | 2 | 3 | 4 |
| Number of participants | | 10 | 10 | 10 | 10 |
| Male / female proportion | | 8 / 2 | 5 / 5 | 6 / 4 | 6 / 4 |
| Age of participants | Mean | 24.5 | 23.8 | 20.9 | 20.5 |
| | Std. Dev. | (5.6) | (4.0) | (3.8) | (2.2) |
| Degree of daily computer usage | Mean | 4.2 | 4.7 | 4.3 | 4.5 |
| | Std. Dev. | (1.0) | (0.5) | (0.9) | (1.0) |
| Level of proficiency with computing tasks | Mean | 3.5 | 3.9 | 3.6 | 3.3 |
| | Std. Dev. | (0.7) | (1.1) | (0.7) | (0.7) |
| Degree of e-mail usage | Mean | 4.6 | 4.3 | 4.2 | 4.7 |
| | Std. Dev. | (0.5) | (0.7) | (0.6) | (0.7) |
| Level of proficiency with basic e-mail functions | Mean | 4.4 | 3.9 | 4.4 | 4.0 |
| | Std. Dev. | (0.7) | (1.1) | (0.5) | (0.8) |
| Degree of instant messaging usage | Mean | 3.2 | 3.6 | 3.6 | 3.0 |
| | Std. Dev. | (2.0) | (1.3) | (1.2) | (1.6) |
| Level of proficiency with instant messaging functions | Mean | 3.5 | 3.5 | 2.9 | 3.2 |
| | Std. Dev. | (1.2) | (1.3) | (1.4) | (1.3) |
| Degree of being negatively affected by interruptions | Mean | 3.0 | 2.8 | 3.7 | 3.2 |
| | Std. Dev. | (1.2) | (0.8) | (0.8) | (1.2) |
| Degree of effort in avoiding interruptions when working | Mean | 3.8 | 3.3 | 3.2 | 3.4 |
| | Std. Dev. | (1.2) | (1.0) | (1.1) | (1.2) |
| Level of proficiency with multi-tasking | Mean | 2.8 | 2.9 | 2.7 | 3.2 |
| | Std. Dev. | (1.0) | (1.0) | (0.9) | (0.6) |

single browser window in the centre of the screen. Each interruption was triggered as a pop-up window in the style of an anti-virus update notification. The script was used to control how far the participant could progress before fully completing the current set of tasks. A script captured participant responses to a database unobtrusively in the background.

For the exit survey, we adapted measures of decision quality from prior research, such as comprehension and response time (Bailey, Konstan, and Carlis 2001; Burmistrov and Leonova 2003; McFarlane 2002), and decision accuracy (Eyrolle and Cellier 2000). As shown in Table 4, questions required the respondent to rank the conditions from easiest to hardest at different stages of the decision.

### 5.3. Design

**Table 4.** Exit survey decision quality measures and questions.

| Decision quality measure | Decision stage | Question |
|---|---|---|
| Preference (4 = most preferred, 1 = least preferred) | Comprehension | When you were at the phase of reading a question, could you rank the conditions, by how well you liked or preferred them? |
| | Responding | When you were at the phase of answering a question, could you rank the conditions, by how well you liked or preferred them? |
| Ease of Control (4 = easiest to control, 1 = hardest to control) | Comprehension | When you were at the phase of reading a question, could you rank the conditions, by how easily they allowed you to control your response? |
| | Responding | When you were at the phase of answering a question, could you rank the conditions, by how easily they allowed you to control your response? |
| Feeling of Interruption (4 = most interruptive, 1 = least interruptive) | Comprehension | When you were at the phase of reading a question, could you rank the conditions, by how interrupted you felt while responding to it? |
| | Responding | When you were at the phase of answering a question, could you rank the conditions, by how interrupted you felt while responding to it? |
| Feeling of Distraction (4 = most distracted, 1 = least distractive) | Comprehension | When you were at the phase of reading a question, could you rank the conditions, how deeply involved were you in reading when interrupted? |
| | Responding | When you were at the phase of answering a question, could you rank the conditions, how deeply involved were you in answering when interrupted? |
| Complexity of Task Resumption (4 = most complex, 1 = least complex) | Comprehension | When you were at the phase of reading a question, could you rank the conditions, by how complex the question was likely to be when you had to resume reading after being interrupted? |
| | Responding | When you were at the phase of answering a question, could you rank the conditions, by how complex the question was likely to be when you had to resume answering after being interrupted? |

A two factor, within-subjects Latin squares experimental design was selected because the dependent variables are measured repeatedly on the same participant under each of the different treatment conditions, thereby reducing error variance due to individual differences. This design also increases statistical power for a given number of subjects compared to a between-subjects design. Table 5 shows the diagram-balanced Latin squares ordering used as the counterbalanced grouping scheme in this experiment for simple and complex tasks and immediate and negotiated interruptions. This ordering was chosen

**Table 5.** Counterbalanced grouping scheme used in the experiment.

| | Treatment condition order | | | |
|---|---|---|---|---|
| | First | Second | Third | Fourth |
| Group 1 | SI | SN | CI | CN |
| Group 2 | SN | SI | CN | CI |
| Group 3 | CI | CN | SI | SN |
| Group 4 | CN | CI | SN | SI |

Note: SI = Simple Task, Immediate Interruption; SN = Simple Task, Negotiated Interruption; CI = Complex Task, Immediate Interruption; CN = Complex Task, Negotiated Interruption.

because it ensures that each condition follows every other condition exactly once, thereby controlling for possible carryover effects (Brooks 2012).

### 5.3.1. Tasks

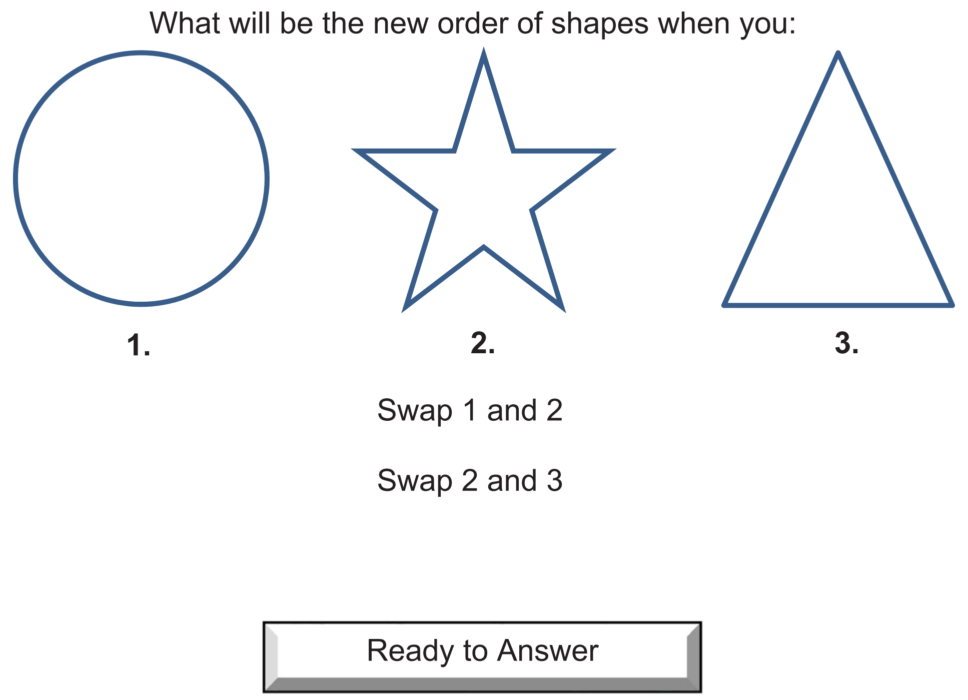
As in prior interruption research (e.g. Hodgetts and Jones 2007), we used process backtracking (Xia and Sudharshan 2002), and recursive reasoning (Anderson, Albert, and Fincham 2005) to authentically simulate user situations where cognitive load requirements are high, such as programming and business process analysis.

We presented each participant with a sequence of twelve question and answer-based tasks, comprising six simple and six complex tasks. Each task involved three discrete shapes and participants were given instructions to change the order of the shapes. After Bonner's (1994) definitions of task complexity, each simple task involved examining at least four information cues (two pairs) and required two transpositions during the comprehension process (Figure 3). Each complex task involved examining at least eight information cues (four pairs) and required four transpositions during the comprehension process (Figure 4). Both simple and complex tasks involved analysing six decision options during the decision response period (Figure 5).

Each task was presented to the participant on a new page. By default, each task had a duration limit of 2.5 min, with a maximum total completion time of 30 min for all tasks. Before commencement, each participant practiced two trial tasks to familiarise themselves with the cognitive requirements of the tasks. Task complexity was increased with the number of information cues about shape order (Jarvenpaa 1990) and number of consecutive transpositions required (Russell, Clark, and Stepney 2003). Participants were not able to write down or otherwise record the stages of their problem solving and so had to manage these information cues and transpositions mentally.

### 5.3.2. Interruptions

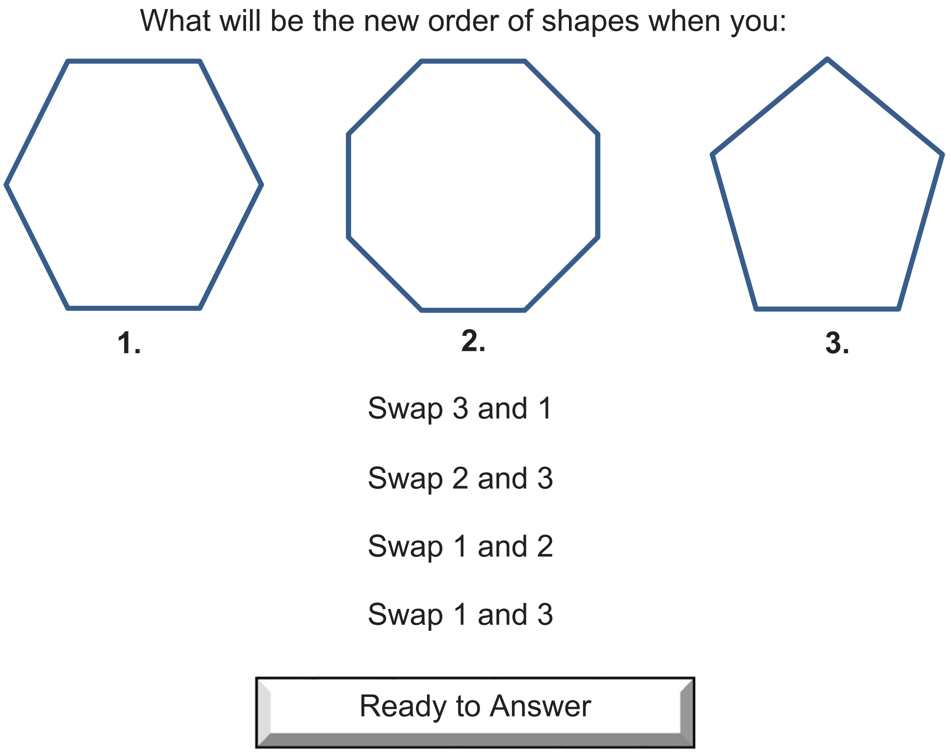
Interruptions were intermittently introduced while participants worked on their primary task. Immediate interruptions were administered as a pop-up window in the form of a modal dialog box in the style of an anti-malware notification, appearing without warning and positioned above the primary task. Negotiated


What will be the new order of shapes when you:

Swap 1 and 2

Swap 2 and 3

**Figure 3** . Simple primary task during the decision comprehension process.


What will be the new order of shapes when you:

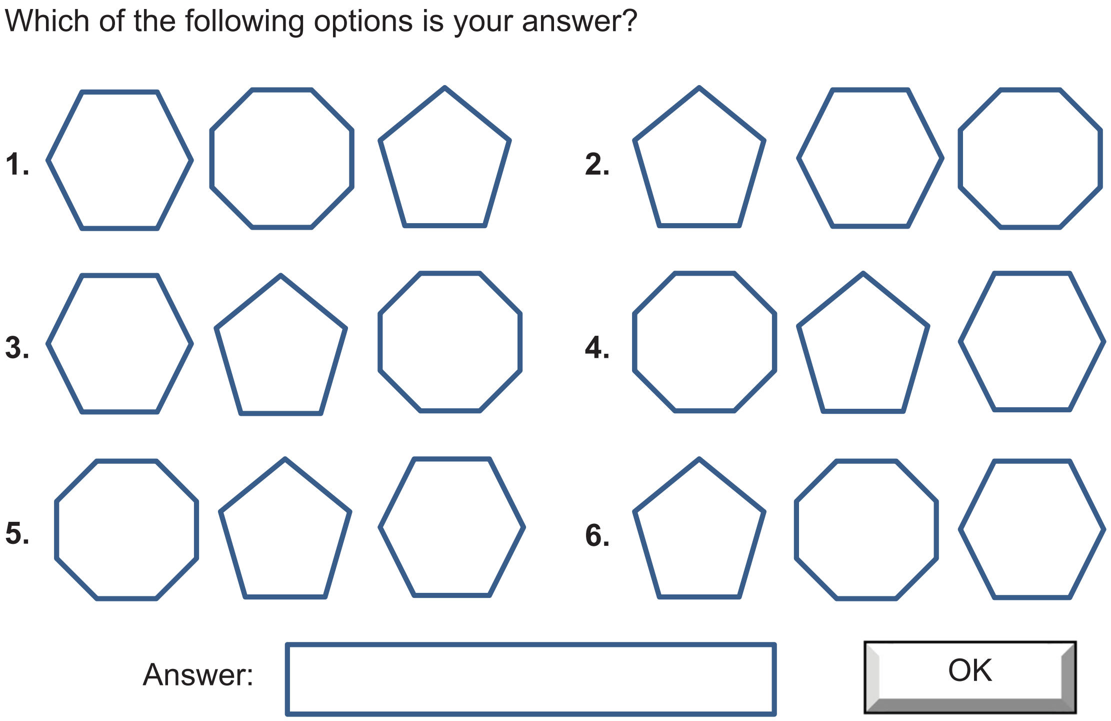
Swap 3 and 1

Swap 2 and 3

Swap 1 and 2

Swap 1 and 3

**Figure 4.** Complex primary task during the decision comprehension process.


Which of the following options is your answer?

Answer:

**Figure 5** . Complex primary task during the decision response process.

interruptions were administered as a pop-up window positioned at the bottom right corner of the screen. Participants responded to a notification by clicking the hypertext link, which closed the notification window automatically, and displayed a new message window on top of the primary task that the participant was working on. These simulated messages reflected the realism of interruptions from modern anti-malware software.

Both interruption types involved arithmetic tasks similar to the mental-arithmetic problems in prior interruptions studies (Gillie and Broadbent 1989), that place large demands on working memory (Seitz and Schumann-Hengsteler 2000) and can elicit the disruptive effects of user interruptions on task performance. Therefore, calculators were not permitted but the practice tasks and a pilot study were used ensure the mental arithmetic requirements were achievable. The interruption task required participants to add some two-digit numbers, with the numbers coded as letters. To decode the problem, a random displacement value (between two and nine) was given within the message body, indicating which letter represented zero for that task (for example, with a displacement value of two, letter B = 0, C = 1, D = 2, and so on). This random displacement value eliminated learning effects by ensuring that participants could not expect to dismiss each interruption with the same answers. The value range ensured a degree of comparative complexity. The alphabet was displayed in upper-case letters within the message body throughout the interruption task. Participants were required to enter the answer to the problem in digits, and were not expected to recode the answer into letters (Gillie and Broadbent 1989).

The pop-up dialog box featured a similar style to anti-malware dialog boxes that the user might encounter in an operational environment, but without being too similar to any existing anti-malware application so as not to bias responses. Figure 6 shows an example of this interruption task.

Participants were compelled to respond to messages immediately without delay, but they were given control over their responses to notifications. Both windows were identical in visual appearance, to eliminate extraneous variables that might influence task performance due to visual differences. After an interruption task was completed, the message window closed automatically, and participants were returned to the primary task that they were working on.

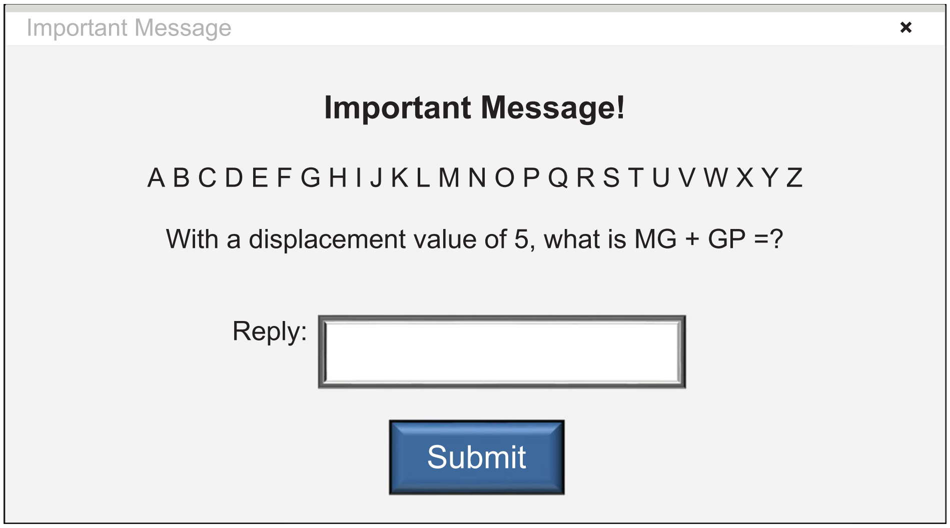
#### 5.3.3. Integrating tasks and interruptions

Interruptions were arbitrarily timed to occur five seconds into the decision comprehension process for simple tasks and 10 s for complex tasks. During the decision response process, participants were engaged in the stages of processing and output, as they analyse the decision options presented to them. Here, interruptions were timed to occur one second into the decision response process for the primary tasks to potentially interrupt before a selection was made. As both comprehension and response processes for problem tasks were displayed as separate pages, these timings appropriately reflect the amount of cognitive processing required by participants at the input, processing and output stages of information processing, and ensured that participants had sufficient time to be involved in the problem tasks for the interruptions to affect them.

Figure 7 summarises the problem tasks, illustrating how participants received their task sequences: four treatment conditions in order, with eight of the tasks administered with the treatments while four problem tasks as base-case control.

### 5.4. Procedure

The experimental tasks and treatment conditions were pilot-tested and refined using 15 participants, to verify task comprehension and relevance. Most pilot participants managed to perform the tasks within the default

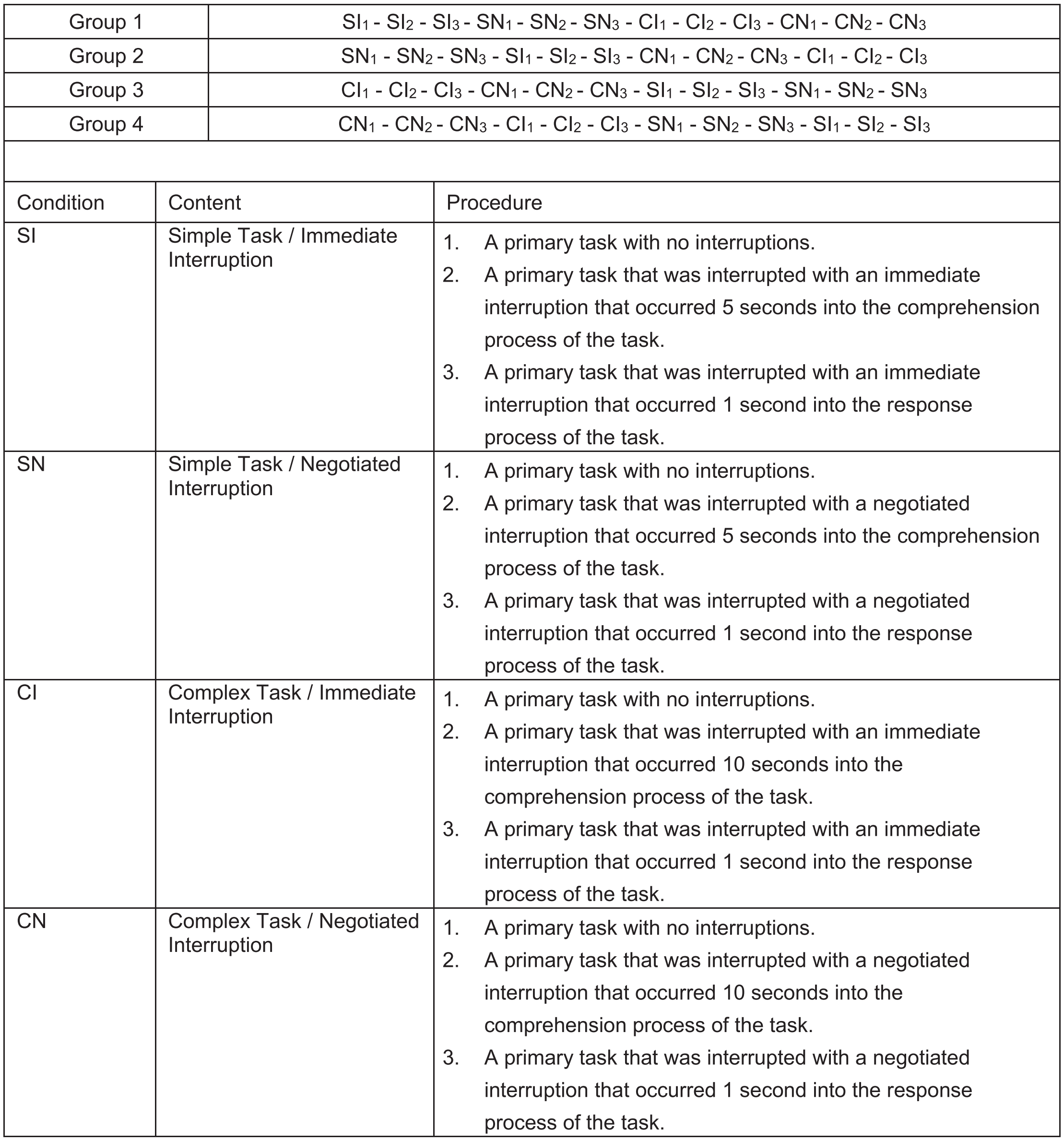


Important Message!

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

With a displacement value of 5, what is MG + GP =?

**Figure 6.** Interruption task by a pop-up message.



| | |
|---|---|
| Group 1 | SI$_1$ - SI$_2$ - SI$_3$ - SN$_1$ - SN$_2$ - SN$_3$ - CI$_1$ - CI$_2$ - CI$_3$ - CN$_1$ - CN$_2$ - CN$_3$ |
| Group 2 | SN$_1$ - SN$_2$ - SN$_3$ - SI$_1$ - SI$_2$ - SI$_3$ - CN$_1$ - CN$_2$ - CN$_3$ - CI$_1$ - CI$_2$ - CI$_3$ |
| Group 3 | CI$_1$ - CI$_2$ - CI$_3$ - CN$_1$ - CN$_2$ - CN$_3$ - SI$_1$ - SI$_2$ - SI$_3$ - SN$_1$ - SN$_2$ - SN$_3$ |
| Group 4 | CN$_1$ - CN$_2$ - CN$_3$ - CI$_1$ - CI$_2$ - CI$_3$ - SN$_1$ - SN$_2$ - SN$_3$ - SI$_1$ - SI$_2$ - SI$_3$ |

| Condition | Content | Procedure |
|---|---|---|
| SI | Simple Task / Immediate Interruption | 1. A primary task with no interruptions.<br>2. A primary task that was interrupted with an immediate interruption that occurred 5 seconds into the comprehension process of the task.<br>3. A primary task that was interrupted with an immediate interruption that occurred 1 second into the response process of the task. |
| SN | Simple Task / Negotiated Interruption | 1. A primary task with no interruptions.<br>2. A primary task that was interrupted with a negotiated interruption that occurred 5 seconds into the comprehension process of the task.<br>3. A primary task that was interrupted with a negotiated interruption that occurred 1 second into the response process of the task. |
| CI | Complex Task / Immediate Interruption | 1. A primary task with no interruptions.<br>2. A primary task that was interrupted with an immediate interruption that occurred 10 seconds into the comprehension process of the task.<br>3. A primary task that was interrupted with an immediate interruption that occurred 1 second into the response process of the task. |
| CN | Complex Task / Negotiated Interruption | 1. A primary task with no interruptions.<br>2. A primary task that was interrupted with a negotiated interruption that occurred 10 seconds into the comprehension process of the task.<br>3. A primary task that was interrupted with a negotiated interruption that occurred 1 second into the response process of the task. |

**Figure 7.** Task sequences, task treatment order and description of treatment conditions.

timings. Participants reported that the interruption task was too difficult, and the results of the pilot test showed that participants committed a relatively high mean error rate in the interruption task (*Mean* = 3.7, *s.d.* = 2.5). The level of difficulty of the interruption task had to be contrived so that it was complex enough for participants to feel disrupted when they attend to it, but not overly complex as to cause participants to despair of performing well (McFarlane 2002). The two problem task complexity levels were therefore deemed appropriate for manipulating task complexity and the instructions for participants were reworded for clarity.

The experiment was conducted in an isolated unallocated academic office to remove potential environmental distractions (McFarlane 2002). Participants attended one at a time, and each participant signed a consent form before commencing. Participants were briefed on what the research involved and what would be done with their data after the experiment. Participants completed an entrance questionnaire before commencement, documenting their personal demographics, educational background, proficiency and degree of involvement in computing tasks.

Participants were given written instructions containing pictorial examples of the primary and interruption tasks, as well as a description of the four treatment conditions. The treatment conditions were labelled with letters A to D so as not to imply numerical ranking (McFarlane 2002). Participants performed the primary tasks and interruption tasks with numeric key-presses and proceeded along each task with a mouse-click. On finishing, participants completed an exit questionnaire to record their perceptions on the treatment conditions.

## 6. Analysis of data

A repeated measures, two-factor Analysis of Variance (ANOVA) was used to analyse the data using interruption type and primary task complexity as within-subjects factors. For significant interactions, a post hoc analysis of the main effects using a repeated measures one-factor ANOVA was used to assess the effects of interruption type on each level of primary task complexity. Effect sizes for ANOVA analyses are reported using partial $\eta^2$ (Cohen 1973; Richardson 2011), which indicates the percentage of variance in the dependent variable that is attributable to the independent variable, and Cohen's $f$ (Cohen 1988). Cohen's $f$ values of 0.10, 0.25, and 0.50 (or greater) and Partial $\eta^2$ values of 0.01, 0.06, and 0.14 (or greater) suggest small, medium, and large effect sizes, respectively (Richardson 2011).

Without interruptions, participants took an average of 18.01 sec (*s.d.* = 5.77 sec) to comprehend simple primary tasks, and 42.82 sec (*s.d.* = 12.84 sec) to comprehend complex primary tasks. Without interruptions, participants took an average of 6.81 sec (*s.d.* = 1.83 sec) for decision responses in simple primary tasks, and 6.21 sec (*s.d.* = 2.07 sec) in complex primary tasks. Without interruptions, participants had an average decision error rate of 0.15 in 40 for simple primary tasks and 0.7 in 40 for complex primary tasks. Table 6 presents the means and standard deviations of decision comprehension time, decision response time and decision accuracy across the treatments, with graphical representations shown in Figure 8.

Table 6 shows a difference of 0.4% between immediate and negotiated interruptions on participants' mean decision comprehension time for simple primary tasks, but a difference of 19.1% between the interruption effects on mean decision comprehension time for complex primary tasks. There was a difference of 18.2% between the interruption effects on mean decision response time for simple primary tasks, and a 34.5% difference between the interruption effects on mean decision response time for complex primary tasks. Mean decision response time was extended for immediate interruptions compared to negotiated interruptions for both simple and complex primary tasks. There was a difference of 22.2% between the interruption effects on mean decision accuracy for simple primary tasks, and a difference of 75% between the interruption effects on mean decision accuracy for complex primary tasks.

**Table 6.** Means and standard deviations of comprehension time, response time and accuracy ($n = 40$).

| | | Interruption type | | | |
|---|---|---|---|---|---|
| | | Immediate | | Negotiated | |
| | | Mean | St. Dev. | Mean | St. Dev. |
| Decision comprehension time (seconds) | Simple tasks | 20.20 | 6.65 | 20.27 | 6.01 |
| | Complex tasks | 55.72 | 16.78 | 46.77 | 14.36 |
| Decision response time (seconds) | Simple tasks | 9.10 | 5.46 | 7.70 | 3.70 |
| | Complex tasks | 8.57 | 3.69 | 6.37 | 2.23 |
| Decision accuracy (no. of errors) | Simple tasks | 0.27 | 0.55 | 0.22 | 0.53 |
| | Complex tasks | 0.70 | 0.82 | 0.40 | 0.70 |

Table 7 shows the analysis of the interruption effects on decision comprehension time, decision response time and decision accuracy across primary task complexity. A significant interaction effect ($F_{1,39} = 9.811$, $p = 0.003$, Partial $\eta^2 = 0.20$, $f = 0.46$) was found between primary task complexity and interruption type, which indicated that the effect of interruption type on decision comprehension time depended on the primary task complexity. For decision response time, no interaction effect ($F_{1,39} = 0.519$, $p = 0.475$, Partial $\eta^2 = 0.01$, $f = 0.00$) was found between primary task complexity and interruption type. H2 was therefore rejected. For decision accuracy, a significant interaction effect ($F_{1,39} = 4.149$, $p = 0.048$, Partial $\eta^2 = 0.09$, $f = 0.28$) was found between primary task complexity and interruption type, which indicated that the effect of interruption type on decision accuracy was affected by primary task complexity.

The significant interaction effect permits a post hoc analysis on the main effects of interruption type on decision comprehension time and decision accuracy for each level of primary task complexity (see Table 8). For decision comprehension time, there was no significant difference between the interruption effects and decision comprehension time in simple tasks ($F_{1,39} = 0.004$, $p = 0.951$, Partial $\eta^2 = 0.01$, $f = 0.00$). The analysis revealed a significant increase in decision comprehension time ($F_{1,39} = 11.594$, $p = 0.002$, Partial $\eta^2 = 0.22$, $f = 0.50$) as participants received immediate interruptions compared to negotiated interruptions in complex primary tasks. H1 was therefore accepted. For decision accuracy, there was no significant difference between the interruption effects in simple primary tasks ($F_{1,39} = 0.494$, $p = 0.486$, Partial $\eta^2 = 0.02$, $f = 0.00$), but there was a significant decrease in decision accuracy ($F_{1,39} = 6.882$, $p = 0.012$, Partial $\eta^2 = 0.14$, $f = 0.37$) when participants received immediate interruptions compared to

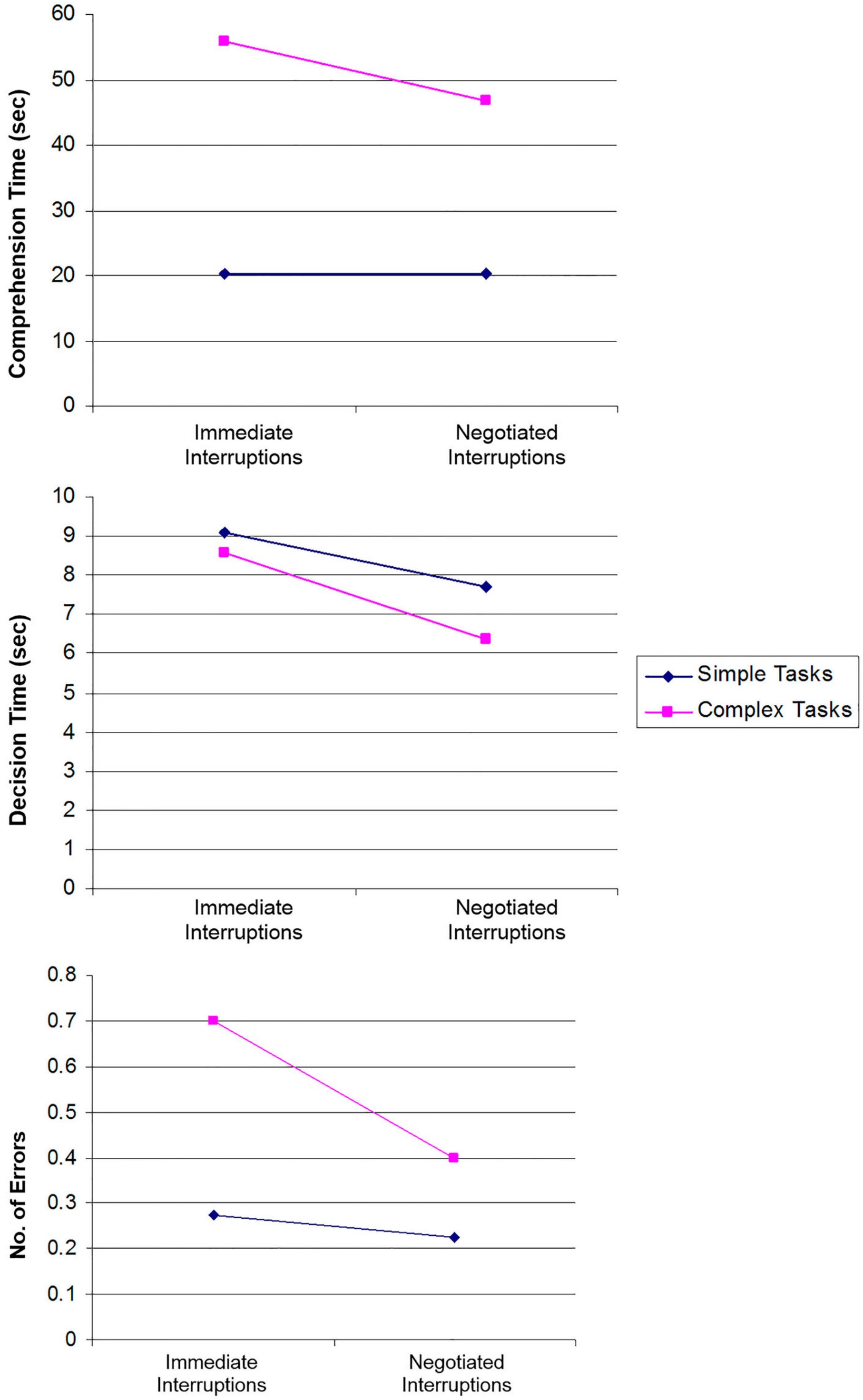


**Figure 8.** Variations of participants' mean decision comprehension, decision time and accuracy across experimental treatments.

negotiated interruptions in complex primary tasks. H3 was therefore accepted.

## 7. Tests of subjective effects

The subjective measurements were derived from participants' rankings of the treatment conditions based on their preference, ease of control, feeling of interruption, distraction and complexity of primary task resumption in the exit questionnaire. A one-way ANOVA was used to analyse the rankings of the treatment conditions for each level of primary task complexity during the comprehension process and decision-making process, to determine whether participants' perceptions of the

**Table 7.** Repeated measures ANOVA results for comprehension time, response time and accuracy with interruptions across primary task complexity.

| | | | Sum of | Mean of | | | *F* | Partial | |
|---|---|---|---|---|---|---|---|---|---|
| Decision variable | Effect | Source of variation | squares | squares | *F* | *p*-val. | Crit. | $\eta^2$ | Cohen's *f* |
| Comprehension time | Main effect | Task complexity | 38471.00 | 38471.00 | 178.01 | 0.00 | 4.08 | 0.82 | 2.07 |
| | | Interruption type | 787.65 | 787.65 | 9.24 | 0.04 | 4.08 | 0.19 | 0.44 |
| | Interaction effect | Task complexity × interruption type | 814.50 | 814.50 | 9.81 | 0.003 | 4.08 | 0.20 | 0.46 |
| Response time | Main effect | Task complexity | 34.22 | 34.22 | 2.53 | 0.119 | 4.08 | 0.06 | 0.19 |
| | | Interruption type | 129.60 | 129.60 | 16.12 | 0.000 | 4.08 | 0.29 | 0.60 |
| | Interaction effect | Task complexity × interruption type | 6.40 | 6.40 | 0.51 | 0.475 | 4.08 | 0.01 | 0.00 |
| Decision accuracy | Main effect | Task complexity | 3.60 | 3.60 | 7.84 | 0.008 | 4.08 | 0.17 | 0.40 |
| | | Interruption type | 1.22 | 1.22 | 5.77 | 0.021 | 4.08 | 0.13 | 0.34 |
| | Interaction effect | Task complexity × interruption type | 0.62 | 0.62 | 4.14 | 0.048 | 4.08 | 0.09 | 0.28 |

**Table 8.** Post-hoc analysis of main effects for comprehension time and decision accuracy.

| Decision variable | Source of variation | Sum of squares | Mean of squares | *F* | *P*-value | *F* Crit. | Partial $\eta^2$ | Cohen's *f* |
|---|---|---|---|---|---|---|---|---|
| Comprehension time | Simple tasks × interruption type | 0.11 | 0.112 | 0.00 | 0.951 | 3.96 | 0.01 | 0.00 |
| | Complex tasks × interruption type | 1602.05 | 1602.5 | 11.59 | 0.002 | 3.96 | 0.22 | 0.50 |
| Accuracy | Simple tasks × interruption type | 0.05 | 0.05 | 0.49 | 0.486 | 3.96 | 0.02 | 0.00 |
| | Complex tasks × interruption type | 1.80 | 1.80 | 6.88 | 0.012 | 3.96 | 0.14 | 0.37 |

interruption effects were consistent with the experimental findings. Table 9 presents the results of this testing, showing the outcomes of the subjective decision variables for each decision component.

The analysis revealed significant differences in participants' perceptions of distraction and interruption, ease of control and complexity of task resumption after immediate interruptions compared to negotiated interruptions in both simple and complex primary tasks during both the decision comprehension and response stages. The analysis also revealed significant differences in participants' rankings of these constructs for immediate and negotiated interruptions in both simple and complex primary tasks during the decision response stage. These findings corroborate the experimental process and results. As shown in Table 10, participants reported that negotiated interruptions mitigate their feelings of distraction and interruption, allow for greater ease of control and alleviated the complexity of primary task resumption compared to immediate interruptions.

**Table 9.** One-way ANOVA results for participants' rankings for subjective effects.

| Subjective variable | Source of variation | Sum of squares | Mean of squares | *F* | *P*-value | *F* Crit. | Partial $\eta^2$ | Cohen's *f* |
|---|---|---|---|---|---|---|---|---|
| Preference | | | | | | | | |
| Comprehension process | Simple tasks × interruption type | 2.45 | 2.45 | 2.59 | 0.111 | 3.96 | 0.06 | 0.19 |
| | Complex tasks × interruption type | 12.01 | 12.01 | 13.58 | $p < 0.001$ | 3.96 | 0.25 | 0.55 |
| Response process | Simple tasks × interruption type | 15.31 | 15.31 | 16.23 | $p < 0.001$ | 3.96 | 0.29 | 0.60 |
| | Complex tasks × interruption type | 13.61 | 13.61 | 13.39 | $p < 0.001$ | 3.96 | 0.25 | 0.54 |
| Ease of control | | | | | | | | |
| Comprehension process | Simple tasks × interruption type | 24.2 | 24.2 | 30.56 | $p < 0.001$ | 3.96 | 0.43 | 0.84 |
| | Complex tasks × interruption type | 14.45 | 14.45 | 17.75 | $p < 0.001$ | 3.96 | 0.31 | 0.63 |
| Response process | Simple tasks × interruption type | 17.11 | 17.11 | 20.99 | $p < 0.001$ | 3.96 | 0.34 | 0.69 |
| | Complex tasks × interruption type | 30.01 | 30.01 | 39.89 | $p < 0.001$ | 3.96 | 0.50 | 0.97 |
| Feeling of interruption | | | | | | | | |
| Comprehension process | Simple tasks × interruption type | 24.20 | 24.20 | 42.9 | $p < 0.001$ | 3.96 | 0.52 | 1.01 |
| | Complex tasks × interruption type | 27.61 | 27.61 | 56.86 | $p < 0.001$ | 3.96 | 0.59 | 1.16 |
| Response process | Simple tasks × interruption type | 39.20 | 39.20 | 68.25 | $p < 0.001$ | 3.96 | 0.63 | 1.28 |
| | Complex tasks × interruption type | 22.05 | 22.05 | 31.88 | $p < 0.001$ | 3.96 | 0.44 | 0.86 |
| Feeling of distraction | | | | | | | | |
| Comprehension process | Simple tasks × interruption type | 13.61 | 13.61 | 29.84 | $p < 0.001$ | 3.96 | 0.43 | 0.83 |
| | Complex tasks × interruption type | 24.20 | 24.20 | 83.52 | $p < 0.001$ | 3.96 | 0.68 | 1.41 |
| Response process | Simple tasks × interruption type | 7.20 | 7.20 | 9.05 | 0.004 | 3.96 | 0.18 | 0.44 |
| | Complex tasks × interruption type | 9.80 | 9.80 | 12.05 | $p < 0.001$ | 3.96 | 0.23 | 0.51 |
| Complexity of task resumption | | | | | | | | |
| Comprehension process | Simple tasks × interruption type | 19.01 | 19.01 | 34.34 | $p < 0.001$ | 3.96 | 0.46 | 0.90 |
| | Complex tasks × interruption type | 23.11 | 23.11 | 46.13 | $p < 0.001$ | 3.96 | 0.54 | 1.04 |
| Response process | Simple tasks × interruption type | 23.11 | 23.11 | 54.01 | $p < 0.001$ | 3.96 | 0.58 | 1.13 |
| | Complex tasks × interruption type | 30.01 | 30.01 | 88.42 | $p < 0.001$ | 3.96 | 0.69 | 1.46 |

**Table 10.** Mean participant rankings of treatment conditions.

| | | Simple tasks | | Complex tasks | |
|---|---|---|---|---|---|
| | Process stage | Immediate interruption | Negotiated interruption | Immediate interruption | Negotiated interruption |
| Preference (4 = most preferred, 1 = least preferred) | Comprehension | 2.8 | 3.2 | 1.5 | 2.5 |
| | Response | 2.4 | 3.3 | 1.6 | 2.7 |
| Ease of control (4 = easiest to control, 1 = hardest to control) | Comprehension | 2.5 | 3.6 | 1.5 | 2.4 |
| | Response | 2.5 | 3.4 | 1.4 | 2.6 |
| Feeling of interruption (4 = most interruptive, 1 = least interruptive) | Comprehension | 2.4 | 1.2 | 3.7 | 2.6 |
| | Response | 2.8 | 1.2 | 3.6 | 2.5 |
| Feeling of distraction (4 = most distracted, 1 = least distractive) | Comprehension | 2.1 | 1.2 | 3.8 | 2.6 |
| | Response | 2.2 | 1.6 | 3.6 | 2.6 |
| Complexity of task Resumption (4 = most complex, 1 = least complex) | Comprehension | 2.3 | 1.3 | 3.6 | 2.6 |
| | Response | 2.3 | 1.2 | 3.8 | 2.5 |

## 8. Conclusions

Anti-malware software must be kept up to date in order to be effective. Notifications of anti-malware software updates can disrupt a user's tasks and thought processes. We simulated a personal desktop processing environment to investigate whether immediate interruptions are more disruptive than negotiated interruptions to users' decision-making performance.

The results showed that both immediate and negotiated interruptions disrupt user's decision processes and outcomes. Immediate interruptions exhibited poorer decision performance than negotiated interruptions for decision comprehension time (H1 is supported) and decision accuracy (H3 is supported), but not in decision response time (H2 is not supported). Task complexity exacerbated these negative effects. The results also suggest that these disruptive effects are mitigated when users can negotiate when or whether to deal with the interruptions. Subjective effects in post-hoc analysis also indicate that negotiated interruptions were perceived to be less disruptive, affording both control over interruption effects and mitigation of task complexity. Importantly, because respondents had only 20 min to complete the exercise, it can be seen that these outcomes appear even within a short period of time. Table 11 summarises the experimental findings for each decision variable.

Practically, the results indicate that immediate interruptions disrupt and degrade users' decision efficiency and accuracy in complex decision processes. Users also found negotiated interruptions to be more desirable than immediate interruptions in their decision processes. Anti-malware application designers should incorporate features that enhance existing negotiation mechanisms. The findings suggest that if anti-malware software manufacturers want users to make good decisions regarding matters of endpoint security, they should allow users to negotiate anti-malware updates and notices. Although this finding may seem counter-intuitive, we argue that this poorer decision-making with regard to endpoint security might undermine the user's ability to make other decisions regarding the security of their desktop environment. Forcing a user to update without considering the implications of this update may undermine the user's ability to make other decisions regarding endpoint security.

More broadly, a key implication of this work is that forcing users to update their anti-malware software immediately in effect replicates the pressure techniques employed by malware authors (Symantec Labs 2017) to compel users to make bad endpoint security decisions. An extension of our findings is that while denying users the ability to negotiate their anti-malware update might result in more immediate operational security, the user's decision-making ability suffers. As malware

**Table 11.** Summary of findings from the experiment.

| Hypothesis | Variable | Finding | Significance | Effect size interpretation |
|---|---|---|---|---|
| H1 | Comprehension time | An interaction effect was found between primary task complexity and interruption type | Significant ($p < 0.01$) | Large |
| | | For simple tasks, there was no differential effect between immediate and negotiated types of interruptions on participants' comprehension time | | Large |
| | | For complex tasks, immediate interruptions increase participants' comprehension time compared to negotiated interruptions | | Large |
| H2 | Decision time | No interaction effect was found between task complexity and interruption type | Not significant | None |
| H3 | Decision accuracy | An interaction effect was found between task complexity and interruption type | Significant ($p < 0.05$) | Medium |
| | | For simple tasks, there was no differential effect between immediate and negotiated types of interruptions on participants' decision accuracy | | Medium |
| | | For complex tasks, immediate interruptions decrease participants' decision accuracy compared to negotiated interruptions | | Large |

attacks are becoming more sophisticated, it is likely to be increasingly important to ensure that users feel sufficiently empowered to make good endpoint security decisions that is compatible with their primary task commitments. By allowing users to negotiate their anti-malware response, our evidence shows that users feel greater ease of control and lower feelings of distraction and interruption.

A theoretical implication of this research is that task complexity negatively moderates the differential effects between immediate and negotiated types of interruptions on decision efficiency and accuracy. The differential effects between both interruption types widen as cognitive task complexity increases, across decision stages. These findings point to the importance of task complexity as a factor in explaining the differential effects between immediate and negotiated types of user interruptions on users' decision performance. The findings suggest that interruption effects should not be studied independently of task complexity.

Another implication of this research is that the disruptive effects of immediate interruptions on users' efficiency and accuracy for complex decision processes can be mitigated by the use of negotiated interruptions. The findings show that it should be possible to alleviate the burden on users' cognitive limitations with negotiated interruptions, thereby mitigating reduced efficiency and accuracy of their decision performance that might result from these interruptions. This implication reinforces the notion that negotiated interruptions are more desirable for users in complex situations than immediate interruptions.

The study may be open to two limitations. Although the use of controlled experimentation permitted reliable inferences to be made about the findings, the increased control afforded by a laboratory experiment was weighed against limitations of realism and generalizability of problem tasks. Although the tasks were aimed at maximising the external validity by defining the way in which users are cognitively engaged (Bonner 1994), the generalizability is limited to where an individual systematically engages their cognitive ability in decision processes. In a real-world setting, tasks and decision processes may not be as well-defined as in the experiment, thereby requiring varying levels of cognitive processing by users. Second, we did not impose any skill requirements on participants beyond their technology ability (Plumlee 2002). Users with greater skepticism or risk aversion may approach updating their anti-malware software differently.

The findings suggest several avenues for future research. First, future research could examine the effects of the task resumption process that is experienced by users following an interruption in order to identify the optimal time at which to remind users of their anti-malware updates. In particular, study of the resumption process would provide understanding of the precursors to the disruptive effects. It would also be valuable to examine how and why users would utilise the negotiation mechanism afforded by task-relevant interruptions and whether there are subsequent effects on their decision processes and outcomes. Second, it would be interesting to examine the potential effect of security interruption alerts on user anxiety and mental wellbeing, particularly in the context of ongoing workflow. Research in this space could also examine the degree to which users are avoiding flow disruption by acquiescing to endpoint security notifications. A third area for future research could involve understanding security interruptions across user modalities in different device contexts. If mobile devices afford the user a greater variety of task environments than personal computers, then it is also possible that users exhibit different security-related avoidance/conformance behaviours. We selected a modal window design to reflect a general endpoint security software dialogue box. However, changes to the appearance of these dialogue boxes as a result of operating system updates may have an effect on user propensity to comply with or defy the instruction.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## References

Abazari, F., M. Analoui, and H. Takabi. 2016. "Effect of Anti-Malware Software on Infectious Nodes in Cloud Environment." *Computers & Security* 58: 139–148.

Adamczyk, P. D., and B. P. Bailey. 2004. "*If Not Now, When? The Effects of Interruption at Different Moments Within Task Execution*." In *Proceedings of the ACM Conference on Human Factors in Computing Systems CHI 2004*, edited by Elizabeth Dykstra-Erickson and Manfred Tscheligi, 271–278. Vienna.

Addas, S., and A. Pinsonneault. 2018. "Theorizing the Multilevel Effects of Interruptions and the Role of Communication Technology." *Journal of the Association for Information Systems* 19 (11): 1097–1129.

Adler, R. F., and R. Benbunan-Fich. 2013. "Self-Interruptions in Discretionary Multitasking." *Computers in Human Behavior* 29: 1441–1449.

Al-Saleh, M. I., A. M. Espinoza, and J. R. Crandall. 2013. "Antivirus Performance Characterisation: System-Wide View." *IET Information Security* 7: 126–133.

Altmann, E. M., and J. G. Trafton. 2004. "*Task Interruption: Resumption Lag and the Role of Cues*." In *Proceedings of the 26th Annual Conference of the Cognitive Science Society*, edited by Kenneth Forbus, Dedre Gentner, and Terry Regier, 43–48. Chicago, IL, United States: Lawrence Erlbaum Associates, Inc..

Anderson, C. L. and R. Agarwal. 2010. “Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions.” *MIS Quarterly* 34: 613.

Anderson, J. R., M. V. Albert, and J. M. Fincham. 2005. “Tracing Problem Solving in Real Time: fMRI Analysis of the Subject-Paced Tower of Hanoi.” *Journal of Cognitive Neuroscience* 17: 1261–1274.

Avrahami, D., and S. Hudson. 2004. “*QnA: Augmenting an Instant Messaging Client to Balance User Responsiveness and Performance*.” In *ACM Conference on Computer Supported Cooperative Work CSCW’04*, edited by Jim Herbsleb and Gary Olson, 515–518. Chicago, IL, United States: Association for Computing Machinery.

Bailey, B. P., and S. T. Iqbal. 2008. “Understanding Changes in Mental Workload During Execution of Goal-Directed Tasks and its Application for Interruption Management.” *ACM Transactions on Computer-Human Interaction* 14: 1–28.

Bailey, B. P., and J. A. Konstan. 2006. “On the Need for Attention-Aware Systems: Measuring Effects of Interruption on Task Performance, Error Rate and Affective State.” *Computers in Human Behavior* 22: 685–708.

Bailey, B. P., J. A. Konstan, and J. V. Carlis. 2001. “*The Effects of Interruptions on Task Performance, Annoyance and Anxiety*.” In *Proceedings of INTERACT’01*, edited by M Hirose, 593–601. Tokyo, Japan: IOS Press.

Baillette, P., Y. Barlette, and A. Leclercq-Vandelannoitte. 2018. “Bring Your Own Device in Organizations: Extending the Reversed IT Adoption Logic to Security Paradoxes for CEOs and End Users.” *International Journal of Information Management* 43: 76–84.

Baskerville, R., F. Rowe, and F.-C. Wolff. 2018. “Integration of Information Systems and Cybersecurity Countermeasures: An Exposure to Risk Perspective.” *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 49: 33–52.

Basoglu, K. A., M. A. Fuller, and J. T. Sweeney. 2009. “Investigating the Effects of Computer Mediated Interruptions: An Analysis of Task Characteristics and Interruption Frequency on Financial Performance.” *International Journal of Accounting Information Systems* 10: 177–189.

Beynon, M., S. Rasmequan, and S. Russ. 2002. “A New Paradigm for Computer-Based Decision Support.” *Decision Support Systems* 33: 127–142.

Blythe, J. M., and L. Coventry. 2018. “Costly but Effective: Comparing the Factors That Influence Employee Anti-Malware Behaviours.” *Computers in Human Behavior* 87: 87–97.

Bonner, S. E. 1994. “A Model of the Effects of Audit Task Complexity.” *Accounting, Organizations and Society* 19: 213–234.

Bonny, P., S. Goode, and D. Lacey. 2015. “Revisiting Employee Fraud: Gender, Investigation Outcomes and Offender Motivation.” *Journal of Financial Crime* 22: 447–467.

Bontchev, V. 1996. “Possible Macro Virus Attacks and How to Prevent Them.” *Computers & Security* 15: 595–626.

Brooks, J. L. 2012. "Counterbalancing for Serial Order Carryover Effects in Experimental Condition Orders." Psychological Methods 17:4 600-614

Bubaš, G., T. Orehovački, and M. Konecki. 2008. “Factors and Predictors of Online Security and Privacy Behavior.” *Journal of Information and Organizational Sciences* 32: 79–98.

Burmistrov, I., and A. Leonova. 2003. “*Do Interrupted Users Work Faster or Slower? The Micro-Analysis of Computerized Text-Editing Task*.” In *Human-Computer Interaction: Theory and Practice (Part 1) – Proceedings of HCI International 2003*, edited by J. Jacko and C. Stephanidis, 621–625. Crete, Greece: Lawrence Erlbaum Associates.

Burns, A. J., C. Posey, T. L. Roberts, and P. Benjamin Lowry. 2017. “Examining the Relationship of Organizational Insiders’ Psychological Capital With Information Security Threat and Coping Appraisals.” *Computers in Human Behavior* 68: 190–209.

Chen, A., and E. Karahanna. 2014. “Boundaryless Technology: Understanding the Effects of Technology-Mediated Interruptions Across the Boundaries Between Work and Personal Life.” *AIS Transactions on Human-Computer Interaction* 6: 16–36.

Chen, H., and W. Li. 2019. “Understanding Commitment and Apathy in is Security Extra-Role Behavior from a Person-Organization Fit Perspective.” *Behaviour & Information Technology* 38: 454–468.

Chenoweth, T., T. Gattiker, and K. Corral. 2019. “Adaptive and Maladaptive Coping With an It Threat.” *Information Systems Management* 36: 24–39.

Cohen, J. 1973. “Eta-Squared and Partial Eta-Squared in Fixed Factor ANOVA Designs.” *Educational and Psychological Measurement* 33: 107–112.

Cohen, J. 1988. *Statistical Power Analysis for the Behavioral Sciences*. New York, NY: Routledge.

Cutrell, E., M. Czerwinski, and E. Horvitz. 2001. “Disruption and Memory: Effects of Messaging Interruptions on Memory and Performance.” In *Human-Computer Interaction: INTERACT’01*, edited by M. Hirose, 263–269. Tokyo: IOS Press (for IFIP).

Czerwinski, M. E., E. Cutrell, and E. Horvitz. 2000a. “*Instant Messaging: Effects of Relevance and Time*.” In *People and Computers XIV: Proceedings of HCI 2000*, edited by Sharon McDonald, Yvonne Waern, and Gilbert Cockton, 71–76. Sunderland, United Kingdom: British Computer Society.

Czerwinski, M. E., E. Cutrell, and E. Horvitz. 2000b. “*Instant Messaging and Interruption: Influence of Task Type on Performance*.” In *Proceedings of OZCHI 2000: Interfacing Reality in the New Millennium*, edited by C. Paris, N. Ozkan, S. Howard, and S. Lu, 356–361. Sydney, Australia: The University of Technology, Sydney.

Dabbish, L., and R. Kraut. 2003. “*Coordinating Communication: Awareness Displays and Interruption*.” In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI’03): Extended Abstracts*, edited by Gilbert Cockton and Panu Korhonen, 786–787. New York: ACM Press.

Dodel, M., and G. Mesch. 2018. “Inequality in Digital Skills and the Adoption of Online Safety Behaviors.” *Communication & Society* 21: 712–728.

Doherty, N. F., and S. T. Tajuddin. 2018. “Towards a User-Centric Theory of Value-Driven Information Security Compliance.” *Information Technology & People* 31: 348–367.

Eatchel, K. A., H. Kramer, and F. Drews. 2012. “The Effects of Interruption Context on Task Performance.” *Proceedings of* *the Human Factors and Ergonomics Society Annual Meeting* 56: 2118–2122.

Eyrolle, H., and J. M. Cellier. 2000. “The Effects of Interruptions in Work Activity: Field and Laboratory Results.” *Applied Ergonomics* 31: 537–543.

Faruki, P., A. Bharmal, V. Laxmi, V. Ganmoor, M. S. Gaur, M. Conti, and M. Rajarajan. 2014. “Android Security: A Survey of Issues, Malware Penetration, and Defenses.” *IEEE Communications Surveys & Tutorials* 17: 998–1022.

Fonner, K. L., and M. E. Roloff. 2012. “Testing the Connectivity Paradox: Linking Teleworkers’ Communication Media Use to Social Presence, Stress from Interruptions, and Organizational Identification.” *Communication Monographs* 79: 205–231.

Franke, J. L., J. J. Daniels, and D. C. McFarlane. 2002. “*Recovering Context After Interruption*.” In *24th Annual Meeting of the Cognitive Science Society*, edited by Wayne Gray and Christian Schunn, 310–315. Fairfax, VA: Lawrence Erlbaum Associates.

Furnell, S., and N. Clarke. 2012. “Power to the People? The Evolving Recognition of Human Aspects of Security.” *Computers & Security* 31: 983–988.

Galluch, P. S., V. Grover, and J. B. Thatcher. 2015. “Interrupting the Workplace: Examining Stressors in an Information Technology Context.” *Journal of the Association for Information Systems* 16: 1–47.

Garrett, R., and J. Danziger. 2008. “Interruption Management? Instant Messaging and Disruption in the Workplace.” *Journal of Computer-Mediated Communication* 13: 23–42.

Gartner Research. 2018. *Magic Quadrant for Endpoint Protection Platforms*. Stamford, CT: Gartner Research Inc.

Gillie, T., and D. Broadbent. 1989. “What Makes Interruptions Disruptive? A Study of Length, Similarity and Complexity.” *Psychological Research* 50: 243–250.

Goode, Sigi, Hartmut Hoehle, Viswanath Venkatesh, and Susan A. Brown. 2017. “User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach.” *MIS Quarterly* 41 (3): 703–727. 10.25300/MISQ.

Goode, S., and D. Lacey. 2011. “Detecting Complex Account Fraud in the Enterprise: The Role of Technical and Non-Technical Controls.” *Decision Support Systems* 50: 702–714.

Goode, S., C. Lin, J. C. Tsai, and J. J. Jiang. 2015. “Rethinking the Role of Security in Client Satisfaction With Software-as-a-Service (SaaS) Providers.” *Decision Support Systems* 70: 73–85.

Gupta, A., H. Li, and R. Sharda. 2013. “Should I Send This Message? Understanding the Impact of Interruptions, Social Hierarchy and Perceived Task Complexity on User Performance and Perceived Workload.” *Decision Support Systems* 55: 135–145.

Gupta, A., R. Sharda, and R. A. Greve. 2011. “You’ve Got Email! Does it Really Matter to Process Emails Now or Later?” *Information Systems Frontiers* 13: 637–653.

Gurung, A., X. Luo, and Q. Liao. 2009. “Consumer Motivations in Taking Action Against Spyware: An Empirical Investigation.” *Information Management & Computer Security* 17: 276–289.

Hanus, B., J. C. Windsor, and Y. Wu. 2018. “Definition and Multidimensionality of Security Awareness: Close Encounters of the Second Order.” *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 49: 103–133.

Herath, T., and H. R. Rao. 2009. “Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations.” *European Journal of Information Systems* 18: 106–125.

Herold, R. 1995. “A Corporate Anti-Virus Strategy.” *International Journal of Network Management* 5: 189–192.

Highland, H. J. 1997. “Procedures to Reduce the Computer Virus Threat.” *Computers & Security* 16: 439–449.

Hodgetts, H. M., and D. M. Jones. 2003. “*Interruptions in the Tower of London Task: Can Preparation Minimize Disruption?*.” In *47th Annual Meeting of the Human Factors and Ergonomics Society*. Denver, CO: Human Factors and Ergonomics Society.

Hodgetts, H. M., and D. M. Jones. 2007. “*Reminders, Alerts and Pop-Ups: The Cost of Computer-Initiated Interruptions*.” In *Human-Computer Interaction: Interaction Design and Usability – Proceedings of HCI International 2007, Part I (Lecture Notes in Computer Science)*, edited by Julie Jacko, 818–826. Berlin: Springer.

Höne, K., and J. H. P. Eloff. 2002. “What Makes an Effective Information Security Policy?” *Network Security* 2002: 14–16.

Huang, D.-L., P.-L. P. Rau, H. Su, N. Tu, and C. Zhao. 2010. “Effects of Communication Style and Time Orientation on Notification Systems and Anti-Virus Software.” *Behaviour & Information Technology* 29: 483–495.

Ifinedo, P. 2016. “Critical Times for Organizations: What Should Be Done to Curb Workers’ Noncompliance With IS Security Policy Guidelines?” *Information Systems Management* 33: 30–41.

Iqbal, S. T., and E. Horvitz. 2007a. “*Disruption and Recovery of Computing Tasks: Field Study, Analysis, and Directions*.” In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI’07)*, edited by Mary Beth Rosson and David Gilmore, 677–686. New York: ACM Press.

Iqbal, S. T., and E. Horvitz. 2007b. “Conversations Amidst Computing: A Study of Interruptions and Recovery of Task Activity.” In *Proceedings of 11th International Conference on User Modeling (UM 2007), (Lecture Notes in Computer Science)*, edited by C. Conati, K. McCoy, and G. Paliouras, 350–354. Berlin: Springer.

Jackson, T., R. Dawson, and D. Wilson. 2003. “Reducing the Effect of E-mail Interruptions on Employees.” *International Journal of Information Management* 23: 55–65.

Jansen, J., and P. van Schaik. 2018. “Testing a Model of Precautionary Online Behaviour: The Case of Online Banking.” *Computers in Human Behavior* 87: 371–383.

Jansen, J., S. Veenstra, R. Zuurveen, and W. Stol. 2016. “Guarding Against Online Threats: Why Entrepreneurs Take Protective Measures.” *Behaviour & Information Technology* 35: 368–379.

Jarvenpaa, S. L. 1990. “Graphic Displays in Decision Making – The Visual Salience Effect.” *Journal of Behavioral Decision Making* 3: 247–262.

Jett, Q. R., and J. M. George. 2003. “Work Interrupted: A Closer Look at the Role of Interruptions in Organizational Life.” *Academy of Management Review* 28: 494–507.

Johnston, A. C., M. Warkentin, M. McBride, and L. Carter. 2016. “Dispositional and Situational Factors: Influences on

Information Security Policy Violations." *European Journal of Information Systems* 25: 231–251.

Johnston, A. C., M. Warkentin, and M. Siponen. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric." *MIS Quarterly* 39: 113–134.

Kelton, A. S., R. R. Pennington, and B. M. Tuttle. 2010. "The Effects of Information Presentation Format on Judgment and Decision Making: A Review of the Information Systems Research." *Journal of Information Systems* 24: 79–105.

Kim, B., A. Barua, and A. B. Whinston. 2002. "Virtual Field Experiments for a Digital Economy: A New Research Methodology for Exploring an Information Economy." *Decision Support Systems* 32: 215–231.

Kim, D. W., P. Yan, and J. Zhang. 2015. "Detecting Fake Anti-Virus Software Distribution Webpages." *Computers & Security* 49: 95–106.

Lee, Y., and K. R. Larsen. 2009. "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software." *European Journal of Information Systems* 18: 177–187.

Lee, A. R., S.-M. Son, and K. K. Kim. 2016. "Information and Communication Technology Overload and Social Networking Service Fatigue: A Stress Perspective." *Computers in Human Behavior* 55: 51–61.

Leukfeldt, E. R. 2014. "Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization." *Cyberpsychology Behavior, and Social Networking* 17: 551–555.

Lévesque, F. L., S. Chiasson, A. Somayaji, and J. M. Fernandez. 2018. "Technological and Human Factors of Malware Attacks: A Computer Security Clinical Trial Approach." *ACM Transactions on Privacy and Security* 21: 1–30.

Levy, E. C., S. Rafaeli, and Y. Ariel. 2016. "The Effect of Online Interruptions on the Quality of Cognitive Performance." *Telematics and Informatics* 33: 1014–1021.

Li, H., A. Gupta, X. Luo, and M. Warkentin. 2011. "Exploring the Impact of Instant Messaging on Subjective Task Complexity and User Satisfaction." *European Journal of Information Systems* 20: 139–155.

Liao, H.-C., and Y.-H. Wang. 2006. "A Memory Symptom-Based Virus Detection Approach." *International Journal of Network Security* 2: 219–227.

Mano, R. S., and G. S. Mesch. 2010. "E-mail Characteristics, Work Performance and Distress." *Computers in Human Behavior* 26: 61–69.

Mansi, G., and Y. Levy. 2013. "Do Instant Messaging Interruptions Help or Hinder Knowledge Workers' Task Performance?" *International Journal of Information Management* 33: 591–596.

Marsden, J. R., R. Pakath, and K. Wibowo. 2002. "Decision Making Under Time Pressure With Different Information Sources and Performance-Based Financial Incentives—Part 1." *Decision Support Systems* 34: 75–97.

Martens, M., R. De Wolf, and L. De Marez. 2019. "Investigating and Comparing the Predictors of the Intention Towards Taking Security Measures Against Malware, Scams and Cybercrime in General." *Computers in Human Behavior* 92: 139–150.

Marulanda-Carter, L., and T. W. Jackson. 2012. "Effects of E-mail Addiction and Interruptions on Employees." *Journal of Systems and Information Technology* 14: 82–94.

McAfee Labs. 2018a. *McAfee Labs Threats Report, December 2018*. Santa Clara, CA: McAfee Labs.

McAfee Labs. 2018b. *McAfee Labs Threats Report, March 2018*. Santa Clara, CA: McAfee Labs.

McFarlane, D. C. 1998. "Interruption of People in Human-Computer Interaction." PhD., George Washington University.

McFarlane, D. C. 2002. "Comparison of Four Primary Methods for Coordinating the Interruption of People in Human-Computer Interaction." *Human-Computer Interaction* 17: 63–139.

McFarlane, D. C., and K. A. Latorella. 2002. "The Scope and Importance of Human Interruption in Human-Computer Interaction Design." *Human-Computer Interaction* 17: 1–61.

McGill, T., and N. Thompson. 2017. "Old Risks, New Challenges: Exploring Differences in Security Between Home Computer and Mobile Device Use." *Behaviour & Information Technology* 36: 1111–1124.

Menard, P., G. J. Bott, and R. E. Crossler. 2017. "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory." *Journal of Management Information Systems* 34: 1203–1230.

Menard, P., R. Gatlin, and M. Warkentin. 2014. "Threat Protection and Convenience: Antecedents of Cloud-Based Data Backup." *Journal of Computer Information Systems* 55: 83–91.

Menard, P., M. Warkentin, and P. B. Lowry. 2018. "The Impact of Collectivism and Psychological Ownership on Protection Motivation: A Cross-Cultural Examination." *Computers & Security* 75: 147–166.

Milosevic, N., A. Dehghantanha, and K.-K. R. Choo. 2017. "Machine Learning Aided Android Malware Classification." *Computers & Electrical Engineering* 61: 266–274.

Min, B., V. Varadharajan, U. Tupakula, and M. Hitchens. 2014. "Antivirus Security: Naked During Updates." *Software: Practice and Experience* 44: 1201–1222.

Moe, W. W. 2006. "A Field Experiment to Assess the Interruption Effect of Pop-Up Promotions." *Journal of Interactive Marketing* 20: 34–44.

Nystrom, L. E., T. S. Braver, F. W. Sabb, M. R. Delgado, D. C. Noll, and J. D. Cohen. 2000. "Working Memory for Letters, Shapes and Locations: fMRI Evidence Against Stimulus-Based Regional Organization in Human Prefrontal Cortex." *NeuroImage* 11: 424–446.

Okane, P., S. Sezer, and K. McLaughlin. 2011. "Obfuscation: The Hidden Malware." *IEEE Security & Privacy Magazine* 9: 41–47.

Ortiz de Guinea, A. 2016. "A Pragmatic Multi-Method Investigation of Discrepant Technological Events: Coping, Attributions, and 'Accidental' Learning." *Information & Management* 53: 787–802. doi:10.1016/j.im.2016.03.003.

Ou, C. X. J., and R. M. Davison. 2011. "Interactive or Interruptive? Instant Messaging at Work." *Decision Support Systems* 52: 61–72.

Ou, C. X., C. Ling Sia, and C. K. Hui. 2013. "Computer-Mediated Communication and Social Networking Tools at Work." *Information Technology & People* 26: 172–190.

Peterson, A. P. 1992. "Counteracting Viruses in an MS-DOS Environment." *Information Systems Security* 1: 58–65.

Plumlee, R. D. 2002. "Discussion of Impression Management with Graphs: Effects on Choices." *Journal of Information Systems* 16: 203–206.

Posey, C., T. L. Roberts, and P. B. Lowry. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets." *Journal of Management Information Systems* 32: 179–214.

Posey, C., T. L. Roberts, P. B. Lowry, and R. T. Hightower. 2014. "Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns Between Information Security Professionals and Ordinary Organizational Insiders." *Information & Management* 51: 551–567.

Post, G., and A. Kagan. 1998. "The Use and Effectiveness of Anti-Virus Software." *Computers & Security* 17: 589–599.

Ramachandran, S., C. Rao, T. Goles, and G. Dhillon. 2013. "Variations in Information Security Cultures Across Professions: A Qualitative Study." *Communications of the Association for Information Systems* 33 (11): 163–204.

Rennecker, J., and L. Godwin. 2005. "Delays and Interruptions: A Self-Perpetuating Paradox of Communication Technology Use." *Information and Organization* 15: 247–266.

Richardson, J. T. E. 2011. "Eta Squared and Partial Eta Squared as Measures of Effect Size in Educational Research." *Educational Research Review* 6: 135–147.

Robertson, T. J., S. Prabhakararao, M. Burnett, C. Cook, J. R. Ruthruff, L. Beckwith, and A. Phalgune. 2004. "*Impact of Interruption Style on End-User Debugging.*" In *Proceedings of the 2004 Conference on Human Factors in Computing Systems*, edited by Elizabeth Dykstra-Erickson and Manfred Tscheligi, 287–294. Vienna, Austria: Association for Computing Machinery.

Russell, M. D., J. A. Clark, and S. Stepney. 2003. "*Making the Most of Two Heuristics: Breaking Transposition Ciphers with Ants.*" In *CEC 2003: International Conference on Evolutionary Computation IEEE*, edited by Rahul Sarker, Robert Reynolds, Hussein Abbass, Kay Chen Tan, Bob McKay, Daryl Essam, and Tom Gedeon, 2653–2658. Canberra, Australia: IEEE Press.

Russell, E., L. M. Purvis, and A. Banks. 2007. "Describing the Strategies Used for Dealing With Email Interruptions According to Different Situational Parameters." *Computers in Human Behavior* 23: 1820–1837.

Safa, N. S., M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan. 2015. "Information Security Conscious Care Behaviour Formation in Organizations." *Computers & Security* 53: 65–78.

Safa, N. S., R. Von Solms, and S. Furnell. 2016. "Information Security Policy Compliance Model in Organizations." *Computers & Security* 56: 70–82.

Salvucci, D. D., and P. Bogunovich. 2010. "*Multitasking and Monotasking: The Effects of Mental Workload on Deferred Task Interruptions.*" In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10*, edited by Elizabeth Mynatt, Geraldine Fitzpatrick, Scott Hudson, Keith Edwards, and Tom Rodden, 85–88. New York, NY: Association for Computing Machinery.

Seitz, K., and R. Schumann-Hengsteler. 2000. "Mental Multiplication and Working Memory." *European Journal of Cognitive Psychology* 12: 552–570.

Shropshire, J. D., M. Warkentin, and A. C. Johnston. 2010. "Impact of Negative Message Framing on Security Adoption." *Journal of Computer Information Systems* 51: 41–51.

Solingen, R., E. Berghout, and F. Latum. 1998. "Interrupts: Just a Minute Never Is." *IEEE Software* 15: 97–103.

Sophos. 2019. *Sophos Labs 2019 Threat Report*. Abingdon: Sophos, Ltd.

Speier, C., I. Vessey, and J. S. Valacich. 2003. "The Effects of Interruptions, Task Complexity, and Information Presentation on Computer-Supported Decision-Making Performance." *Decision Sciences* 34: 771–797.

Steinbart, P. J., M. J. Keith, and J. Babb. 2016. "Examining the Continuance of Secure Behavior: A Longitudinal Field Study of Mobile Device Authentication." *Information Systems Research* 27: 219–239.

Stich, J.-F., M. Tarafdar, and C. L. Cooper. 2018. "Electronic Communication in the Workplace: Boon or Bane?" *Journal of Organizational Effectiveness: People and Performance* 5: 98–106.

Stich, J.-F., M. Tarafdar, C. L. Cooper, and P. Stacey. 2017. "Workplace Stress from Actual and Desired Computer-Mediated Communication Use: A Multi-Method Study." *New Technology, Work and Employment* 32: 84–100.

Sukwong, O., H. S. Kim, and J. C. Hoe. 2011. "Commercial Antivirus Software Effectiveness: An Empirical Study." *IEEE Computer* 44: 63–70.

Sykes, E. R. 2011. "Interruptions in the Workplace: A Case Study to Reduce Their Effects." *International Journal of Information Management* 31: 385–394.

Symantec Labs. 2017. *Internet Security Threat Report – Ransomware 2017*. Mountain View, CA: Symantec Corporation.

Teer, F. P., S. E. Kruck, and G. P. Kruck. 2007. "Empirical Study of Students' Computer Security Practices/Perceptions." *Journal of Computer Information Systems* 47: 105–110.

Tsai, H. S., M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon, and S. R. Cotten. 2016. "Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective." *Computers & Security* 59: 138–150.

Visinescu, L. L., O. Azogu, S. D. Ryan, Y. "Andy" Wu, and D. J. Kim. 2016. "Better Safe Than Sorry: A Study of Investigating Individuals' Protection of Privacy in the Use of Storage as a Cloud Computing Service." *International Journal of Human–Computer Interaction* 32: 885–900.

Wachyudy, D., and S. Sumiyana. 2018. "Could Affectivity Compete Better Than Efficacy in Describing and Explaining Individuals' Coping Behavior: An Empirical Investigation." *The Journal of High Technology Management Research* 29: 57–70.

Wang, Z., P. David, J. Srivastava, S. Powers, C. Brady, J. D'Angelo, and J. Moreland. 2012. "Behavioral Performance and Visual Attention in Communication Multitasking: A Comparison Between Instant Messaging and Online Voice Chat." *Computers in Human Behavior* 28: 968–975.

Warkentin, M., A. C. Johnston, and J. Shropshire. 2011. "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention." *European Journal of Information Systems* 20: 267–284.

White, G., T. Ekin, and L. Visinescu. 2017. “Analysis of Protective Behavior and Security Incidents for Home Computers.” *Journal of Computer Information Systems* 57: 353–363.

Williams, C. K., D. Wynn, R. Madupalli, E. Karahanna, and B. K. Duncan. 2014. “Explaining Users’ Security Behaviors With the Security Belief Model.” *Journal of Organizational and End User Computing* 26: 23–46.

Xia, L., and D. Sudharshan. 2002. “Effects of Interruptions on Consumer Online Decision Processes.” *Journal of Consumer Psychology* 12: 265–280.

Ye, Y., T. Li, D. Adjeroh, and S. S. Iyengar. 2017. “A Survey on Malware Detection Using Data Mining Techniques.” *ACM Computing Surveys* 50: 41.

Yoo, C. W., G. L. Sanders, and R. P. Cerveny. 2018. “Exploring the Influence of Flow and Psychological Ownership on Security Education, Training and Awareness Effectiveness and Security Compliance.” *Decision Support Systems* 108: 107–118.

Yoon, C., J.-W. Hwang, and R. Kim. 2012. “Exploring Factors That Influence Students’ Behaviors in Information Security.” *Journal of Information Systems Education* 23: 407–415.

Yoon, C., and H. Kim. 2013. “Understanding Computer Security Behavioral Intention in the Workplace: An Empirical Study of Korean Firms.” *Information Technology & People* 26: 401–419.

Zenkin, D. 2001. “Fighting Against the Invisible Enemy: Methods for Detecting an Unknown Virus.” *Computers & Security* 20: 316–321.

Zhang, L., and W. C. McDowell. 2009. “Am I Really at Risk? Determinants of Online Users’ Intentions to Use Strong Passwords.” *Journal of Internet Commerce* 8: 180–197.