The impact of a Canadian financial cybercrime prevention campaign on clients' sense of security

Cameron Coutu & Benoît Dupont

Coutu, C. & B. Dupont (2021), « The impact of a Canadian financial cybercrime prevention campaign on clients' sense of security », in R. Leukfeldt & M. Weulen Kranenbarg (eds.), *Cybercrime in context: the human factor in victimization, offending, and policing*, Springer, Amsterdam, pp. 157-172.

Abstract: The purpose of this study was to evaluate the impact of a cybercrime prevention campaign that was run by a Canadian financial institution. More specifically, we examined how participants/clients perceived the financial institution's initiative to inform them about cybercrimes. The study also explored whether or not the campaign had the desired effect, which was to reinforce the clients' sense of security. This campaign took place on October 2018 and 1,452 adults (831 males and 621 females) participated in the online web survey. The results indicated that the prevention campaign had been positively perceived by most of the respondents (93.2%). However, only a low percentage of individuals (18%) had seen the poster/campaign prior to the completion of the survey while the majority (82%) accessed the prevention campaign's components during the survey. Further analysis has shown no gender differences in participants' responses. In general, participants felt that the campaign has increased their sense of security, especially among older individuals (55 y/o and over). Most participants have expressed an interest in receiving more information on cybercrime and how to take actions on protecting one's self. Results suggest that it would be advisable to conduct targeted prevention campaigns in order to reach out to as many people as possible. Discussion also includes practical recommendations based on the results and the review of the literature.

Keywords: Cybercrime prevention campaigns, cybersecurity perception, sense of security, financial institution

Financial institutions these days offer a wide variety of online banking services to their clients. These services allow them to access their accounts and make various financial transactions on the Internet. As a consequence, more cyberfrauds are taking place and clients may feel they lack the necessary skills or knowledge to conduct safe transactions online. Recently, a Canadian financial institution launched a prevention campaign effort. This prevention campaign promoted the adoption of safe computer practices (e.g., cyber hygiene) and informed clients about the different types of cybercrimes they might encounter. Prevention campaigns such as these aim at strengthening the clients' sense of security and their motivation to adopt secure online behaviours. To date, very few studies have assessed the effectiveness of security awareness or prevention campaigns (Bada et al., 2015). In fact, little is known about what people think of prevention messages and if campaigns have an impact on their sense of security. This information would prove useful

to develop effective security prevention strategies. The main purpose of the present study is to evaluate, based on a web panel survey, how the clients of the financial institution perceived the prevention campaign.

Cybercrimes are becoming more elaborate as hackers adapt to stay up to date with the technology. Businesses, governmental institutions, and personal users are now at risk of having their identity and information stolen by hackers, which can make them vulnerable to financial losses. As a result, cybercrime prevention has appealed to both businesses and governments to limit the damages. While the initial focus was on securing the technology, attackers quickly diverted to the end users as they are the weakest link, and therefore, an easier target (Gratian et al., 2018; Herley, 2009; Schneier, 2000). As such, users need to acquire the skills to be able to protect themselves from such threats (e.g., by spotting a fake from a legitimate email). This issue came to light over the years due to the ever-increasing number of cybercrimes. The *modus operandi* of attackers has changed: instead of profiling potential victims they send mass emails and wait for the victim to bite the bait (Button, Nicholls, et al., 2014). The general population is also aware of this issue and does not feel adequately equipped to protect themselves online. For instance, according to a survey sponsored by Accenture in 2017, 56% of Canadians do not believe they have the necessary means and knowledge to be secure online. A majority of Canadians (78%) also said that they would like the government and public agencies to inform them of the best methods to protect their personal data online.

Cybercrime prevalence

Over the years, three different generations of cybercrimes have emerged. The first generation includes traditional crimes using a computer and Internet to facilitate the organisation process (e.g., robbery). The second generation is also based on traditional crimes, but technology has increased criminal opportunities and the number of possible victims (e.g., fraud). Then, there is the third generation which is directly connected to Internet use (e.g., computer viruses) (Wall, 2008).

Surprisingly, although cyberincidents are more frequent than in the past, the number of reported cybercrimes has not increased as much as expected (McGuire & Dowling, 2013). Indeed, experts agree that it is hard to know precisely how many cybercrimes are committed each year in a given population, since only a minority of crimes are being reported to the authorities (Cross et al., 2016; Deevy et al., 2012). The police statistics can also vary depending on the country's culture and laws (classification criteria, definitions, counting system) (Van Dijk et al., 1990). Thus, to obtain a more accurate picture victimisation surveys need to be taken into account. For instance, the *Crime Survey of England and Wales* (CSEW, 2019) performed a national survey to assess the victimisation rates in the United Kingdom. Cybercrimes accounted for nearly half of all incidents reported, with one person in ten being a victim of cyberfraud (approximately 3.8 million incidents). Of these, 85% of incidents were not reported to the authorities (CSEW, 2019). In 2011, Statistics Canada conducted a survey (General Social Survey) on Internet victimisation, including questions related to people's experiences and perceptions online.

Results showed that 7% of users reported having been a victim of cyberbullying in the previous year. Receiving aggressive or threatening messages being the prevailing form of cyberbullying (experienced by 73% of victims). As for banking fraud, 4% of the respondents reported having been victim of this type of cybercrime. Interestingly, the GSS also demonstrated that this latter type of crime is a major source of concern among the Canadian population (64% of respondents). The costs related to cybercrimes are significant and increasing. To illustrate, an estimate of 14 billion CAD was spent by Canadian industries in a year related to cybersecurity incidents (prevention, detection, and recovery) (Statistics Canada, 2018).

Impact of cybercrime

The consequences related to cybercrime can touch upon many different aspects of a person's life (financial, psychological, social, etc.) (Al-Ali et al., 2018; Button, Lewis, et al., 2014). The way victimisation is perceived can also greatly vary depending on the victim's personal characteristics (age, gender, salary) (Keown, 2010; Walklate, 2007). Financial losses will not have the same impact depending on the person's financial situation; in the worst-case scenario people can become homeless (Cross et al., 2016). Victims may be affected psychologically or emotionally; they may experience anger (towards themselves or the hacker) and sadness (Cross, et al., 2016; Henson et al., 2016). Victims are often left to their own devices even when they decide to report the crime. If the perpetrator lives in another country (which is frequent), the authorities will delegate responsibilities to the other country's justice department, which is then free to decide whether or not it will take action.

On a larger scale, cybercrimes can also have economical and institutional consequences. These might affect the end user as well as companies and governments (Choo, 2011). Companies may have their data or intellectual property stolen, which would reduce competitiveness among other companies in the same field. As for institutions (governmental, financial, etc.), consequences can result in loss profit, disruptions of services, and customer disaffection.

Prevention campaigns

As cybercrimes are becoming more frequent, prevention measures need to be implemented to protect the population. Among suitable measures already implemented are the following: Get Cyber Safe in Canada (Public Safety Canada, 2015) and Stop.Think.Connect in the United States (Department of Homeland Security, 2017). These campaigns are nationally spread and aim at raising a sense of awareness regarding cybersecurity. They both promote online security behaviours and security tips to adopt.

To communicate a message to the population, prevention campaigns use different mediums. These include posters in public area, television and radio messages, or online advertisements. Some studies have shown that prevention campaigns are often costly and ineffective (Bertrand et al., 2006). Other studies, however, have demonstrated that this form of prevention initiative can have beneficial effects under certain conditions (Bauman et al.,

2001; Self-Brown et al., 2008). A maintenance phase or a medium- or long-term recall is one of the key elements of a successful campaign prevention (Mitchell et al., 1992). The message needs to be repeated to the population to remind them of the risks and behaviours they need to adopt. The way the message is conveyed is also a key factor that must be taken into account. It has been proven that the content of the message and the strategy used to broadcast it must be adapted to the needs and characteristics of the target population (Schmid et al., 2008).

Sense of security

In the context of online financial transactions, the sense of security stems from the user's perception of the risk possibilities that their data is well managed (Kim et al., 2011). Trust can be defined as the sense of security and the willingness of an individual to rely on another person. It would also be negatively influenced by risk perception, the latter being based on uncertainty about the future (Cheung & Lee, 2000). Thus, if there is trust, the assessed risk is reduced or considered to be negligible. Risk assessment would also be influenced by gender. Women would tend to consider the potential losses associated with the risk as more important than men (Midha, 2012). Tversky and Kahneman (1989) have demonstrated that when losses and gains do not hold the same values for individuals, losses will account for more. This might explain why women are more concerned than men over information security for online shopping (Garbarino & Strahilevitz, 2004). Older individuals also tend to use Internet less; older women being the least knowledgeable about Internet security risks (Grimes et al., 2010). This may suggest that age and gender are two factors that influence how individuals perceive and use the Internet.

The sense of security is closely linked to trust. An individual is more likely to trust if they feel secure. The opposite is true as well. Generally, women feel less secure than men in most situations (Delbosc & Currie, 2012; Quine & Morrell, 2008; Grohe, 2011). They would perceive a bigger risk in many fields (financial, medical, and environmental) (Garbarino & Strahilevitz, 2004). This could also apply to online browsing. For instance, a study has shown that women are less likely to buy online without the recommendation of someone they know and trust than men (Garbarino & Strahilevitz, 2004). An influencing factor could be past victimisations (Keown, 2010). According to Button and colleagues (2009), 74.5% of victims reported that they changed their behaviours following an online incident related to fraud. This would have prompted them to be more careful and would also have had an impact on their trust ability. However, it appears that victims of cybercrime are more likely to be re-victimised. For example, Reyns and Henson (2016) have suggested several ways to reduce the risk of online identity theft victimisation (e.g., change password, installation of an antivirus software, deletion of emails from unknown senders). The proposed suggestions were not successful in preventing re-victimisation. This may be due to the illegal (or risky) behaviours of the victims (e.g., if they download pirated content, putting themselves at risk).

With clients increasingly concerned about their security, it has become important for governments and larger institutions to develop and implement prevention measures. As stated earlier, this study focuses more specifically on a prevention campaign launched by a

Canadian financial institution. This campaign had two objectives: (1) to provide information to clients about the risks of being victimised by cyberattacks and how to protect themselves, and, (2) to increase clients' sense of security towards their financial institution.

This research is in the context of a survey (sample survey) conducted by a financial institution immediately after the end of a cybercrime prevention campaign. The paper focuses on some of the data collected from clients in the province of Quebec through an opt-in online panel.

The purpose of this study was as follows:

1) Examine how clients perceived the prevention campaign. More specifically, we tried to answer these questions: What is the general perception of the prevention campaign? How many respondents remember seeing the campaign posters? How many clients remember having visited the website? How useful were the tips in the campaign? What is the level of interest of the respondents for the different themes of the campaign?

2) The second research question relates to the perceived effects of the campaign on respondents. The goal was to examine the campaign's impact on the clients' sense of security and their perception of the financial institution (FI). As a secondary goal we also investigated whether the perceived effects on sense of security vary according to the respondents' characteristics. Based on results of previous studies, four individual variables were considered: gender, age, savings, and level of interest in the targeted topics. Indeed, studies have shown that the aforementioned variables can explain individual differences in one's sense of security (Hoy & Milne, 2010; Reyns, 2013; Williams et al., 2000)

Methods

Participants in this study were adult clients of a Canadian financial institution who were recruited throughout the province of Quebec, Canada. These respondents have agreed to be part of a list of clients (online panel) that the institution consult frequently to collect data, gather opinions, etc. These online consultations aim at improving the quality of service to better meet the client's expectations. Thus, an invitation to fill out the online survey was sent to 3,218 clients who had agreed to be part of this online panel one-month post-campaign. The campaign was two-fold: a poster (displayed in branches and on social media) and a website with articles on how to stay secure online. The questions in the survey were composed of three parts: 1) questions collecting the demographics of the respondents (age, gender, savings); 2) questions relating to their perceptions of the campaign, and 3) questions addressing their interests in security tips. Participants were grouped into 5 different age-groups: 18-34 (13.7%), 35-44 (16.6%), 45-54 (14.3%), 55-64 (27.3%), and 65 and older (28.1%). The savings variable (in CDN) included four groups: 0-999 (8.3%), 1,000-9,999 (16.7%), 10,000-49,999 (23.3%), and 50,000 and more (51.7%).

Respondents had to answer the following questions (Table 1): 1) Do you remember seeing the posters? (Yes/No); 2) Have you ever accessed the (security tips) section of the website? (Yes/No); 3) I appreciate that the FI informs its clients about security (Agree/Disagree/Don't know); 4) How useful are the security tips? (Useful/Useless/Don't

know); 5) How interested are you in receiving tips on the following topics? a) Protection of your devices (A lot/A little-Not interested/Don't know); b) Protection of your bank account (A lot/A little-Not interested/Don't know); c) Protection of your identity (A lot/A little-Not interested/Don't know); 6) Did the campaign poster impact your sense of security towards the FI? (Yes/No/Don't know); 7) How did the campaign website impact your sense of security towards the FI? (Increased/Decreased/Neither increased nor decreased/Don't know).

The survey was completed by 1,468 participants, with a response rate of 45.6%. Of this number, 16 were excluded either because they did not reside in Quebec (n=14) or because a significant amount of data was missing (n=2). The final sample consisted of 1,452 adults (age range= 18-94; mean age= 53.7); 831 of which were males (57.2%) and 621 females (42.8%). To be eligible respondents had to: be clients of the financial institution, be able to read French, and be resident of the province of Quebec, Canada. Having seen the prevention campaign beforehand was not mandatory because participants were shown the campaign components during the survey. Eighteen percent had seen the campaign (poster, website) before the survey while the majority (82%) were exposed to the poster/website for the first time during the survey completion.

Results

The first research question sought to describe how the posters / website was perceived by respondents (visibility, appreciation, usefulness and topics of interest). For the second research question, descriptive analyses were also conducted to assess the perceived effects of the posters and website (on their opinion of the institution and sense of security). The number and percentage of respondents who provided the answers to each question are reported (Table 1). Chi-squared (Chi-2) analyses were performed to determine to what extent individual characteristics (age group, gender, savings, and interest level) were related to participants' responses. This statistic hypothesis test is valid to determine whether there is a statistically significant difference between the expected frequencies and the observed frequencies in one or more categories of a contingency table (nominal variables).

Table 1 about here

Descriptive analyses

As shown in Table 1, of all participants 18.4% said that they had seen the prevention campaign's poster and 15.5% said that they had accessed the prevention campaign's website. However, when presented with the poster during the survey, only 6% recalled that they had previously seen it. However, a large majority of respondents found the campaign useful and appreciated the initiative. In fact, more than 80% of respondents answered that the campaign's security tips were useful (81.1%) and that the FI's initiative of

informing its clients was very much appreciated (93.2%). Two topics were of particular interests: the protection of the bank account (78.8%) and the protection of personal identity (79.2%).

As stated above, the prevention campaign consisted of informative posters and a website including useful articles about Internet security. We analysed the data related to the posters and website separately to determine if one campaign component had more impact than the other. Overall, the informative posters were better perceived than the website part of the prevention campaign. Two-thirds (66.5%) of the respondents declared that the poster messages had improved their sense of security and their opinion towards the financial institution (FI). As for the website, the impact was moderate. It increased the sense of security of only half (48.9%) the respondents. Thus, these results suggest that the informative posters were more efficient than the website at increasing clients' sense of security. Of the 717 people who said that the prevention campaign had an effect on their perception (positive or negative), almost all (99%) perceived it as positive. Only seven people responded that their sense of security had decreased as a result of the prevention campaign.

The relation between gender and sense of security. A chi-square analysis was performed to examine the relation between gender and sense of security. The relation between these variables was not significant, for the posters $\chi 2$ (1) = .01, p = .99, n.s. and for the website $\chi 2$ (1) = 1.88, p = .17 n.s. Males and females responded similarly as both stated that the prevention campaign had a positive impact on their sense of security.

The relation between age and sense of security. A chi-square analysis was performed to examine the relation between age and sense of security. The relation between these variables was significant, for the posters $\chi 2$ (4) = 14.8, $p < .05$. and for the website $\chi 2$ (4) = 62.76, $p < .0001$. Older respondents (over 55-year-old) were more likely to have responded that their sense of security was affected by the prevention campaign than younger respondents.

The relation between savings and sense of security. A chi-square analysis was performed to examine the relation between savings and sense of security. The relation between these variables was not significant, for the posters $\chi 2$ (3) = 3.84, p = .28. but was significant for the website $\chi 2$ (3) = 10.28, $p < .05$. Seventy five percent of those surveyed reported that the posters had a positive effect on their sense of security. The responses were similar in all categories of savings. Thus, the amounts of savings did not have a significant effect. For the website, the effect was smaller and varied depending on the categories of savings. Wealthier respondents (over $55,000) were more likely to have responded that their sense of security was affected by the website than the other subgroups.

The relation between respondents' interest in device protection and sense of security. A chi-square analysis was performed to examine the relation between respondents' interest in protecting their device and sense of security. The relation between these variables was significant, for the posters $\chi 2$ (1) = 83.31, $p < .001$. and for the website $\chi 2$ (1) = 186.13, $p < .0001$. These results indicate that respondents with a higher interest in device

protection also perceived both the posters (82.9%) and the website (64.8%) more positively than those with a lower interest (59.8% for the posters and 27.2% for the website).

The relation between respondents' interest in bank account protection and sense of security. A chi-square analysis was performed to examine the relation between respondents' interest in protecting their bank account and sense of security. The relation between these variables was significant, for the posters $\chi 2$ (1) = 68.1, $p < .001$. and for the website $\chi 2$ (1) = 118.55, $p < .0001$. These results indicate that respondents with a higher interest in bank account protection also perceived both the posters (79.8%) and the website (58%) more positively than those with a lower interest (54.9% for the posters and 22.1% for the website).

The relation between respondents' interest in identity protection and sense of security. A chi-square analysis was performed to examine the relation between respondents' interest in protecting their identity and sense of security. The relation between these variables was significant, for the posters $\chi 2$ (1) = 82.01, $p < .001$. and for the website $\chi 2$ (1) = 109.4, $p < .0001$. These results indicate that respondents with a higher interest in identity protection also perceived both the posters (80.2%) and the website (57.6%) more positively than those with a lower interest (52.6% for the posters and 23% for the website).

Discussion

This study had two main purposes. The first was to evaluate, based on the results of a web panel survey, how the clients of a financial institution (FI) perceived the safety tips suggested during a prevention campaign. More specifically, we evaluated the extent to which the information conveyed was perceived as useful by respondents. The appreciation level of clients regarding the prevention initiative led by their institution and the message they have learned from the posters have also been studied. The second objective was to evaluate the perceived effects of the campaign on the sense of security of the respondents. We also assessed whether or not clients perceived that the prevention campaign had an effect on their FI's image. Finally, analyses were performed to determine whether the perceived effects were related to certain individual characteristics (gender, age group, level of savings, and their interest in cybercrime protection).

The first results suggest that the prevention campaign only partially achieved its target in terms of visibility and getting the client interested (to learn more about the subject). In fact, fewer than one in five (18.4%) remembered having seen preventive messages (before the survey), and even fewer reported having consulted the articles informing them of the security measures at their disposal (15.5%), which is lower than the FI marketing team's expected visibility goal. As the consultation began shortly after the end of the campaign, it is unlikely that clients would have forgotten it. A more likely explanation is that the posters did not draw the clients' attention (lack of visibility). The public is flooded with information of all kinds (on the Internet but also in the media and in the many displays installed in public and commercial places) and it is possible that the messages of the campaign have gone unnoticed or was not visible enough for a large number of clients to remember. As pointed out by Bada, Sasse, and Nurse (2015), “simple

transfer of knowledge about good practices in security is far from enough" (p.9). Awareness campaigns need to be implemented in conjunction with other influencing strategies, such as targeted actions providing feedback (Bada et al., 2015). A one-off campaign will not be as effective as a campaign with multiple reminders highlighting the importance of the issue (Casswell & Duignan, 1989).

A second hypothesis would be that the clients consulted did not relate to the messages. If so, it would not be a lack of visibility but rather a lack of interest. It is possible that a large proportion of respondents did not pay attention to the campaign messages because they did not feel concerned or were under the impression that they were meant for other people. Indeed, research has shown that prevention campaigns are more effective when they focus on "specific local" issues (Bowers & Johnson, 2003). Additionally, a study by Verril and Bentley (cited by Bowers & Johnson, 2005) indicated that more than two-thirds of respondents reported that they did not pay attention to the preventive message when it was too general - our results suggest that this may have been the case here. Interestingly, the analyses reveal that it is the respondents in the older age groups (55 years and older) who remembered more the posters and read the articles intended for them (2/3 of the people who answered positively to the first questions belong to these age groups). It can thus be reasonably assumed that older people were more interested in the preventive message than younger participants. Younger people are generally more familiar with technology and may be more careless about protecting themselves. Older people, however, may be more aware of the risks and limitations of their ability to ensure their safety. A review conducted by Gourbesville (2007) on the dangers of the Internet confirms that younger people are more confident than their elders and therefore more vulnerable to the risks of using the Internet. In the context of the campaign, it is not surprising that younger respondents have little recollection of preventive messages.

On a more positive note, many respondents answered that the campaign's security tips were useful (81.1%) and that the FI's initiative of informing its clients was very much appreciated (93.2%). Such results support the relevance of the prevention campaign. However, the possibility that a social desirability bias has influenced participants' responses cannot be ignored. This type of bias is often present in satisfaction surveys and it is common for respondents to overstate the positive elements of consultation (their level of appreciation, the usefulness of the proposed measures) to "convey a positive message" (Steenkamp et al., 2010).

Other positive responses are obtained in relation to respondents' interest in three specific topics (or themes) related to cybersecurity: device protection, bank account protection and identity protection; all three topics are perceived to be of interest to a majority of them. However, respondents were more likely to show interest in the last two types of protection (78.8% and 79.2% respectively) compared to device protection (61.7%). Such results suggest that providing more information or advice on how to protect banking data and identity may be more relevant to the needs of most clients. These topics are arguably more important and interesting because lack of protection (identity and data) is more likely to have serious consequences. In comparison, device protection is considered

somewhat less important, possibly because people feel they are better able to protect themselves. Consequences associated with a lack of protection for the devices are perceived as more negligible. The answers provided on the questions relating to the clients' interest seem to be contradictory. We would have expected that if the interest is present among the clients, they would pay more attention to the messages and remember the gist of it. In this case, either the messages were not visible enough or the interest is not as high as reported.

Statistical analyses were used to determine if there was a link between respondent characteristics and perceived effects on sense of security, which yielded some interesting results. In short, significant relations were obtained for three of the four variables taken into account: the age group, the level of savings, and the interest in protection (device, bank fraud and identity theft). Only the gender variable was not significantly related to the participants' responses. Female respondents could have been expected to report that the campaign had a bigger effect on their sense of security since studies show that they are more likely than men to be concerned about their protection. Our findings do not confirm this hypothesis, but rather show that a similar proportion of respondents of both genders report that the poster and the website have contributed to increasing their sense of security.

Statistical tests demonstrate that older people in the sample with a higher level of savings and a high interest in protection topics predominate significantly from the other respondent groups in terms of the perceived positive effect of the poster and website on their perception towards the FI. The variable that appears most important is the age group; indeed, the oldest respondents are those who have the highest level of savings and it is also older people who show a higher level of interest towards protection means. These three characteristics are not independent of one another. It seems logical that the older subgroup is different from the others by reporting more positive effect of the campaign on the sense of security: they are more likely to remember the campaign, to have retained an accurate and specific preventive message, and to have consulted the website. Such results suggest that the campaign has better met a need in this subset of clients (more than for the other groups of respondents).

Strengths

This study has several strengths. First, the consultation was conducted with a fairly representative sample of the general population. The number of participants is high (more than 1,400), which adds to the sample validity of the results. The survey was designed by a team of marketing experts and was conducted by a firm with expertise consulting the public. Clients were surveyed shortly after the end of the campaign. The data were rigorously verified and analysed.

Limitations and future directions

It is plausible that a number of limitations may have influenced the results obtained. The number of questions related to the sense of security was quite limited (questions only related to feelings about the FI). It would have been relevant to include questions about the sense of personal safety, self-efficacy, and perceived threats. Moreover, as in any survey, there is a probability of error arising from different possible biases: social desirability, indifference, random responses, etc. These results thus need to be interpreted with caution.

Another limit was that participants who had not seen the prevention campaign beforehand completed the survey. Due to the small number of individuals who remembered the campaign, it was not possible to determine whether the two groups of participants (those who remembered having seen the campaign before the survey and those who accessed the campaign components during the survey) were inclined to provide different answers – statistical test requires a minimum of 5 participants per category (cells) of answers. Also, it would have been interesting to document in the survey if participants had previous victimisation experience. This information would have been useful to investigate whether this variable is related to the impact of the campaign. Moreover, pre- and post-campaign measurements assessing the sense of security would have been a more appropriate design to evaluate prevention campaigns' effects.
An important contribution to this area of research would be to conduct effectiveness studies with more sophisticated research designs (longitudinal, experimental studies, etc.). Future studies could explore this further.

Conclusion

Cybercrime is a growing phenomenon. Due to the increased use of the Internet in all areas of activity and the expansion of online services, there are new opportunities for fraudsters and scammers to commit cybercrimes by targeting all types of users. The consequences and costs of cybercrime are substantial and justify all means being used to prevent them. This study has gone some way towards enhancing our understanding of the effectiveness of cybercrime prevention campaigns. It has shown that the prevention of cybercrime is a major challenge, both in terms of complexity and difficulty in providing effective, responsive ways to reduce cybercrimes. Prevention campaigns (governmental or from private organisations) are becoming more frequent, but their effectiveness is still relatively limited to this day. This study has shown that although the prevention campaign was perceived positively by the majority of respondents, the impact appears to be rather limited. In fact, less than a quarter of respondents had seen the poster and / or the website before completing the survey and very few of them remembered the message. The campaign seems to have been successful primarily with one group of clients: older and wealthier people. Thus, it is still necessary to improve prevention campaigns to make them more effective. A promising approach in this area is not to focus solely on educating people about information technology protection, but rather to adopt a conceptualisation of prevention using a multidisciplinary perspective that integrates knowledge from criminology, computer science, psychology, and public health. Future prevention campaigns should have fewer general messages and focus more on specific issues. By using a general message, the impact is likely to be lower as a smaller number of individuals feel concerned. By combining preventive strategies from different disciplines, the efficiency of prevention campaigns could potentially improve because it would make it possible to reach and better target vulnerable populations. Further work needs to be done involving multidisciplinary teams to design and evaluate the effects of new cybercrime prevention strategies.

References

Accenture (2017). Canada Cybercrime Survey 2017. Retrieved from https://www.accenture.com/ca-en/company-news-release-canada-cybercrime-survey-2017

Al-Ali, A. A., Nimrat, A., & Benzaid, C. (2018). Combating cyber victimisation: Cybercrime prevention. In H. Jahankhani (Ed.), *Cybercriminology* (pp. 324-340). Switzerland: Springer Nature Switzerland AG.

Bada, M., Sasse, A., & Nurse, J. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 118-131.

Bauman, A. E., Bellew, B., Owen, N., & Vita, P. (2001). Impact of an Australian mass media campaign targeting physical activity in 1998. *American Journal of Preventive Medicine, 21*(1), 41-47. https://doi.org/10.1016/S0749-3797(01)00313-0

Bertrand, J. T., O'Reilly, K., Denison, J., Anhang, R., & Sweat, M. (2006). Systematic review of the effectiveness of mass communication programs to change HIV/AIDS-related behaviors in developing countries. *Health Education Research, 21*(4), 567-597. https://doi.org/10.1093/her/cyl036

Bowers, K., & Johnson, S. (2003). *Reducing burglary initiative: The role of publicity in crime prevention* (Home Office Research Study 272). London, UK: Home Office.

Bowers, K., & Johnson, S. (2005). Using publicity for preventive purposes. In N. Tilley (Ed.), *Handbook of crime prevention and community safety* (pp. 329-354). Devon, UK: Willan Publishing.

Button, M., Lewis, C., & Tapley, J. (2009). A better deal for fraud victims: Research into victims' needs and experiences. *National Fraud Authority*. Retrieved from https://researchportal.port.ac.uk/portal/files/1924328/NFA_Report_1_15.12.09.pdf

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36-54. https://doi.org/10.1057/sj.2012.11

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391–408. https://doi.org/10.1177/0004865814521224

Casswell, S., & Duignan, P. (1989). Evaluating Health Promotion: A Guide for Health Promoters and Health Managers. 28pp, November. Auckland: Department of Community Health.

Cheung, C., & Lee, M. K. O. (2000). Trust in Internet Shopping: A Proposed Model and Measurement Instrument, *AMCIS 2000 Proceedings,* 681-689.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731. https://doi.org/10.1016/j.cose.2011.08.004

Crime Survey of England and Wales (CSEW). (2019). Crime in England and Wales: year ending March 2019. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2019

Cross, C., Richards, K., & Smith, R. (2016). Improving responses to online fraud victims: An examination of reporting and support. *Final Report, Criminology Research Council, Australian Institute of Criminology*. Retrieved from http://www.crg.aic.gov.au/reports/1617/29-1314-FinalReport.pdf

Deevy, M., Lucich, S., & Beals, M. (2012). Scams, schemes and swindles: A review of consumer financial fraud research. *Financial Fraud Research Centre.* Retrieved from: http://longevity.stanford.edu/wp-content/uploads/2017/01/Scams-Schemes-Swindles-FINAL-On-Website.pdf

Delbosc, A., & Currie, G. (2012). Modelling the causes and impacts of personal safety perceptions on public transport ridership. *Transport Policy*, *24*, 302–309. https://doi.org/10.1016/j.tranpol.2012.09.009

Garbarino, E., & Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *Journal of Business Research*, *57*(7), 768–775. https://doi.org/10.1016/S0148-2963(02)00363-6

Gourbesville, O. (2007). Faut-il avoir peur d'Internet ? *Pour, 3*(195), 21-26.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358. https://doi.org/10.1016/j.cose.2017.11.015

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of Internet hazards. *Educational Gerontology, 36*(3), 173-192. https://doi.org/10.1080/03601270903183065

Grohe, B. (2011). Measuring residents' perceptions of defensible space compared to incidence of crime. *Risk Management, 13*(1/2), 43-61.

Henson, B., Reyns, B. W., & Fisher, B. S. (2016). Cybercrime victimization. In C. A. Cuevas & C. M. Rennison (Eds.), *The Wiley handbook on the psychology of violence* (pp. 555-570). Chichester, UK: Wiley Blackwell.

Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *NSPW '09 Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, 133-144.

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10*(2), 28-45. https://doi.org/10.1080/15252019.2010.10722168

Keown, L-A. (2010). Les precautions prises pour éviter la victimisation : Une perspective selon le sexe. *Tendances Sociales Canadiennes*, *89*.

Kim, M.-J., Chung, N., & Lee, C.-K. (2011). The effect of perceived trust on electronic commerce: Shopping online for tourism products and services in South Korea. *Tourism Management*, *32*(2), 256–265. https://doi.org/10.1016/j.tourman.2010.01.011

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Research Report 75. Retrieved from https://www.publicsafety.gc.ca/lbrr/archives/cnmcs-plcng/cn36762-eng.pdf

Midha, V. (2012). Impact of consumer empowerment on online trust: An examination across genders. *Decision Support Systems*, *54*(1), 198–205. https://doi.org/10.1016/j.dss.2012.05.005

Mitchell, E. A., Aley, P., & Eastwood. J. (1992). The national cot death prevention program in New Zealand. *Australian Journal of Public Health, 16*(2), 158-161. https://doi.org/10.1111/j.1753-6405.1992.tb00045.x

Public Safety Canada. (2015). Canada's Cyber Security Awareness Initiative, "Get Cyber Safe". Retrieved from https://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2011/20111003-1-en.aspx

Quine, S., & Morrell, S. (2008). Research: Perceptions of personal safety among older Australians: Perceptions of personal safety. *Australasian Journal on Ageing*, *27*(2), 72–77. https://doi.org/10.1111/j.1741-6612.2008.00289.x

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216-238. https://doi.org/10.1177/0022427811425539

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology, 60*(10), 1119-1139. https://doi.org/10.1177/0306624X15572861

Schmid, K. L., Rivers, S. E., Latimer, A. E., & Salovey, P. (2008). Targeting or tailoring? Maximizing resources to create effective health communications. *Mark Health Serv, 28*(1), 32-37.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world.* New York: John Wiley.

Self-Brown, S., Rheingold, A. A., Campbell, C., & de Arellano, M. A. (2008). A Media Campaign Prevention Program for Child Sexual Abuse: Community Members' Perspectives. *Journal of Interpersonal Violence*, *23*(6), 728–743. https://doi.org/10.1177/0886260507313946

Statistics Canada. (2011). Self-reported Internet victimization in Canada, 2009. Retrieved from http://www.statcan.gc.ca/pub/85-002-x/2011001/article/11530-eng.htm

Statistics Canada. (2018). Impact of cybercrime on Canadian businesses, 2017. Retrieved from: https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-fra.htm

Steenkamp, J.-B. E. M., De Jong, M. G., & Baumgartner, H. (2010). Socially desirable response tendencies in survey research. *Journal of Marketing Research, 47*(2), 199-214. https://doi.org/10.1509/jmkr.47.2.199

Tversky, A., & Kahneman, D. (1989). Rational choice and the framing of decisions. In B. Karpak & S. Zionts (Eds.), *Multiple criteria decision making and risk analysis using microcomputers* (pp. 81-126). Berlin, Germany: Springer-Verlag Berlin Heidelberg.

United States Department of Homeland Security. (2017). About Stop. Think. Connect. Retrieved from https://www.dhs.gov/about-stopthinkconnect

van Dijk, J. J. M., Mayhew, P., & Killias, M. (1990). *Experiences of crime across the world: Key findings of the 1989 from the International Crime Survey*. Deventer, The Netherlands: Kluwer Law and Taxation Publishers.

Walklate, S. (2007). *Imagining the victim of crime.* Berkshire, UK: Open University Press.

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime1. *International Review of Law, Computers & Technology*, *22*(1–2), 45–63. https://doi.org/10.1080/13600860801924907

Williams, F. P., McShane, M. D., & Akers, R. L. (2000). Worry About Victimization: An Alternative and Reliable Measure for Fear of Crime. *Western Criminology Review 2*(2). Retrieved from http://www.westerncriminology.org/documents/WCR/v02n2/williams/ williams.html

Table 1.

Number and percentage of participants who answered the main survey questions (visibility, appreciation, usefulness and interest)

Main questions - Perception of the posters/website	Number (n) and percentage of participants (%)
Do you remember seeing the posters?	
Yes	267 (18.4%)
No	1185 (81.6%)
Total	1,452 (100%)
Have you ever accessed the (security tips) section of the website?	
Yes	225 (15.5%)
No	1227 (84.5%)
Total	1,452 (100%)
I appreciate that the FI informs its clients about security	
Agree	1353 (93.2%)
Disagree	45 (3.1%)
Don't know	54 (3.7%)
Total	1,452 (100%)
How useful are the security tips?	
Useful	1177 (81.1%)
Useless	198 (13.6%)
Don't know	77 (5.3%)
Total	1,452 (100%)
How interested are you in receiving tips on the following topics?	

a) Protection of your devices:	
A lot	896 (61.7%)
A little/Not interested	536 (36.9%)
Don't know	20 (1.4%)
Total	1,452 (100%)
b) Protection of your bank account:	
A lot	1144 (78.8%)
A little/Not interested	295 (20.4%)
Don't know	13 (0.9%)
Total	1,452 (100%)
c) Protection of your identity:	
A lot	1150 (79.2%)
A little/Not interested	292 (20.1%)
Don't know	10 (0.7%)
Total	1,452 (100%)
Did the campaign poster impact your sense of security towards the FI?	
Yes	966 (66.5%)
No	327 (22.5%)
Don't know	159 (11%)
Total	1,452 (100%)
How did the campaign website impact your sense of security towards the FI?	
Increased	710 (48.9%)
Decreased	7 (0.5%)
Neither increased nor decreased	704 (48.5%)
Don't know	31 (2.1%)
Total	1,452 (100%)