Cybersecurity Awareness Campaigns

Cameron Coutu, MSc

Briefing Note
Vol. 1 Iss. 8

RCCP | Research Chair in Cybercrime Prevention

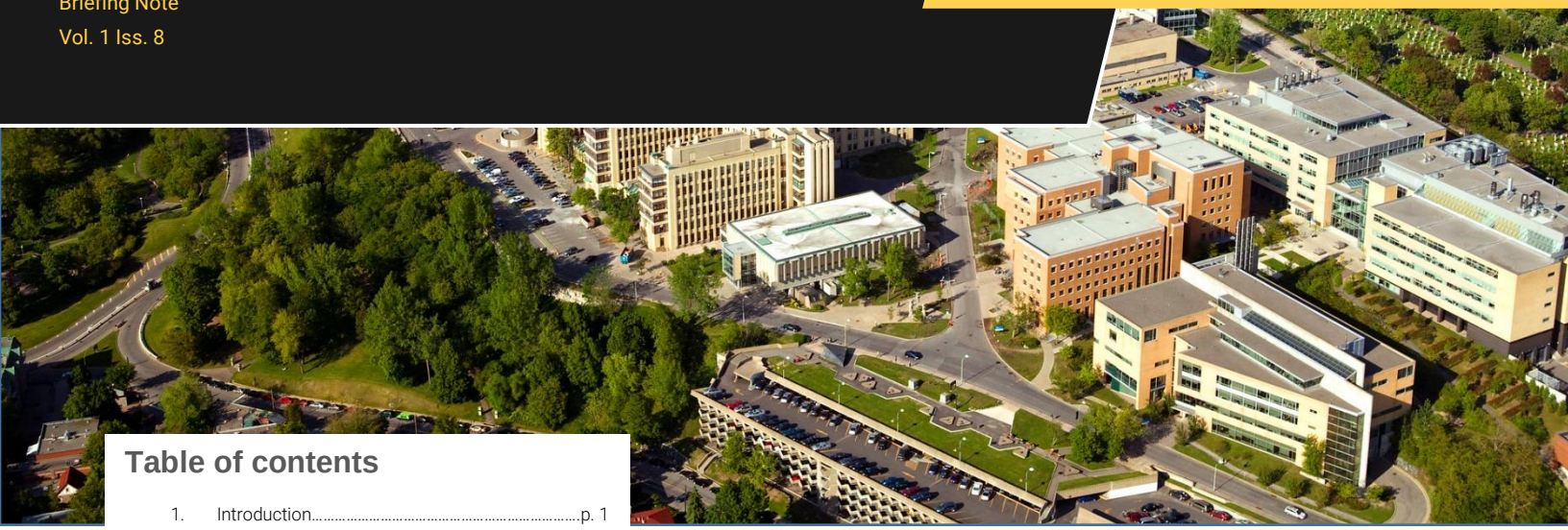

Table of contents

Introduction

Awareness campaigns are often used to promote healthy lifestyle habits in the public health sphere. But they can also be very effective in criminology as a way to inform the public about cyber risks and safe behaviours so individuals can protect themselves online.

Governments and financial institutions alike have developed campaigns over the past few years to help raise awareness about cybercrime.

In this synthesis, we present an overview of the methods and theoretical models used to steer cybersecurity awareness strategies. We have also included a list of recommendations for creating new prevention strategies.

Coutu, C. (2019). La prévention de la cybercriminalité : résultats d'une enquête sur les effets perçus d'une campagne de prévention réalisée par une institution financière [Cybercrime prevention: Survey results of the perceived impacts of a prevention campaign conducted by a financial institution] (Master's thesis, Université de Montréal).

The Research Chair in Cybercrime Prevention was created on the initiative of the University of Montreal, Desjardins and the National Ban k of Canada. Led by Benoît Dupont, researcher at the International Centre for Comparative Criminology at the University of Montreal, its mission is to contribute to the advancement of research on cybercrime phenomena from the perspective of its prevention.

Crime prevention

In criminology, crime prevention refers to any methods and strategies developed to lower the severity and frequency of criminal offences.[1]

Crime prevention is split into 3 categories: primary, secondary and tertiary prevention.[2, 3]

- Primary prevention focuses on changing the physical and social conditions that may lead to crime.
- Secondary prevention uses early detection and intervention methods to steer at-risk groups and individuals away from committing a crime. It also seeks to protect those who are likely to be victimized.
- Tertiary prevention addresses the after-effects of a crime. Its main goal is to reduce the recidivism rate (which is the risk of reoffending). Prevention campaigns at this stage involve detection, conviction, punishment or the correctional treatment of offenders.

Theoretical models adapted for cybercrime prevention

The public health theoretical models can provide a starting point for cybercrime prevention. They use an approach that focuses on helping potential victims protect themselves. They focus on helping them take the necessary precautions before a crime is committed, rather than on the perpetrator or physical environment.

The Protection Motivation Theory and the Health Belief Model are easily adapted to cybercrime prevention.

- Protection Motivation Theory (PMT): This theory suggests that a person's response to a threat depends on two factors: Their perception of a threat, which includes the perceived severity of the threat and their perceived vulnerability to it; and their coping ability, referred to as response efficacy and self-efficacy. Both cognitive processes manifest when a person is faced with a threatening situation and a protective behavioural response is triggered to reduce the threat.[4]

- Health Belief Model (HBM): This model explains the cognitive processes (beliefs, biases and perceptions) involved in safety-related behaviours. The HBM theorizes that there are two determining factors that shape a person's beliefs: The perception of threats and the expectations of the efficacy of the recommended actions to the threat.[5, 6]

This suggests that by monitoring users' attitudes and perceptions, we can glean a better understanding of their beliefs regarding information security and the safeguards they can use to protect themselves.

Effective awareness campaigns

Research has shown that cybercrime awareness campaigns need to be better targeted. There are too few of them, and, of those that do exist, most have not been reviewed. What's more, the results of the few that have been reviewed were inconclusive.[3, 7]

Most prevention measures don't consider people's realities, or how well they understand cybercrime and its risks. Awareness campaigns around internet piracy (the illegal download of online content such as movies, video games, etc.) did help slow down piracy, but only for a short period of time.[8]

Evaluation research on awareness campaigns in the fields of criminology and public health has shown that prevention measures are more effective when they send a clear, direct message to its target audience. But very few preventative measures are designed based on the user's perspective, perceptions and beliefs, or on their

knowledge of the tools they can use to protect themselves.

Some studies suggest that certain factors are key to successful awareness campaigns in any field, such as follow-ups and reminders over the medium or long term.

One of the biggest issues is that the creators of these campaigns are trying to reach as many people as possible. As a result, the message becomes diluted and too broad, which reduces the campaign's effectiveness. Awareness campaigns need to be better targeted and focused on achievable goals by promoting specific attitudes and behaviours.[9]

National awareness campaigns

Over the past decade, governments have begun to introduce cybersecurity awareness campaigns.

- As part of the National Cyber Security Strategy, the Canadian government introduced **Get Cyber Safe** in 2010.[10] The campaign has addressed a variety of topics including cyberbullying, wireless network security, the importance of backups, personal information security protection and fraud prevention.[11]
- The US developed its own campaign, **Stop. Think. Connect**.[12] Its goal is to raise awareness about the risks of the internet. Like its Canadian equivalent, the campaign teaches the public about safe online behaviours and the tools available to help protect themselves.
- The Australian Competition and Consumer Commission (ACCC) runs **Scamwatch**. It provides information on the different types of scams, such as fake charities and fraudulent investment schemes. The website also provides resources and a reporting form.[13]

Tips for effective awareness campaigns:

- Increase visibility and effectiveness of awareness campaigns by promoting them on different multiple media platforms.
- Extend the length of campaigns for better visibility (but be careful you don't run it for too long, otherwise you run the risk of overexposure, referred to by the experts as security fatigue).[14]
- Use interactive online games and training to raise your public's interest.[15, 16] (See Synthesis Vol. 1, No. 1.)
- Adapt the message for each group in your target audience.
- Limit the number of topics presented to keep the message accessible (e.g., campaign raising awareness about identity theft).
- Present the risks explicitly and in a concrete way (without inducing fear and anxiety) to raise awareness (e.g., real-life stories).

References

[1] Cusson, M., Dupont, B. & Lemieux, F. (2007). *Traité de sécurité intérieure.* Montreal: HMH.

[2] Monchalin, L. (2009). Pourquoi pas la prévention du crime ? Une perspective canadienne. *Criminologie*, *42*(1), 115-142.

[3] Brewer, R., De Val-Palumbo, M., Hutchings, A., Holt, T. J., Goldsmith, A. & Maimon, D. (2019). *Cybercrime Prevention: Theory and Applications.* Cham, Switzerland: Palgrave.

[4] Doane, A. N., Boothe, L. G., Pearson, M. R. & Kelley, M. L. (2016). Risky Electronic Communication Behaviors and Cyberbullying Victimization: An Application of Protection Motivation Theory. *Computers in Human Behavior*, *60*, 508-513.

[5] Rosenstock, I. M. (1974). Historical Origins of the Health Belief Model. *Health Education Monographs*, *2*(4), 328-335.

[6] Rosenstock, I. M., Strecher, V. J. & Becker, M. H. (1994). *The Health Belief Model and HIV Risk Behavior Change.* Preventing AIDS. Springer.

[7] Bada, M., Sasse, A. et Nurse, J. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 118-131.

[8] Bachmann, M. (2007). Lesson Spurned? Reactions of Online Music Pirates to Legal Prosecutions by the RIAA. *International Journal of Cyber Criminology*, *2*, 213-227.

[9] Sacco, V. F. & Trotman, M. (1990). Public Information Programming and Family Violence: Lessons from the Mass Media Crime Prevention Experience. *Canadian J. Criminology*, *32*(1), 91-105.

[10] Public Safety Canada. (2015). Canada's Cyber Security Awareness Initiative, Get Cyber Safe.

[11] Get Cyber Safe. (2017). Campaigns.

[12] United States Department of Homeland Security. (2017). About Stop. Think. Connect.

[13] Scamwatch. (2019). Scam statistics.

[14] O'Donnell, A. (2019). Create an Effective Security Awareness Training Program. *Lifewire*.

[15] Chung, H. & Zhao, X. (2004). Effects of Perceived Interactivity on Web Site Preference and Memory: Role of Personal Motivation. *Journal of Computer-Mediated Communication,* 10(1).

[16] Song, J. H. & Zinkhan, G. M. (2008). Determinants of Perceived Web Site Interactivity. *Journal of Marketing*, *72*, 99-113.