# Challenges of Virtual Trust

A MATTER OF COOPERATION, EDUCATION, AND CYBERSECURITY


'DAMOLA ADEDIJI
MADDIE ALDRIDGE
MARC OUELLET
ALESSANDRA PUOPOLO
DANIELLE THOMPSON
AND
DR. RICHARD FRANK



Human-Centric Cybersecurity Partnership

## HUMAN-CENTRIC CYBERSECURITY REPORT PROJECT

The 2022 Human-Centric Cybersecurity Report Project brought together postgraduate students from across Canada to work with our partners from both private industry and the public sector to produce reports looking at wicked cybersecurity problems through a transdisciplinary lens. This three volume series comprises the following reports:

- Challenges of Virtual Trust: A Matter of Cooperation, Education, and Cybersecurity
- Digital Twins: Cyber Security Prospects, Pitfalls, and Recommendations
- Cybersecurity Through Human Behavior

## ABOUT HC2P

The Human-Centric Cybersecurity Partnership (HC2P) is a transdisciplinary group of scholars, government, industry and not-for-profit partners that generate research and mobilize knowledge that will help create a safer, more secure, more democratic and more inclusive digital society.

## ACKNOWLEDGMENTS

We would like to thank the Bank of Montreal (BMO), Bell Canada, the Standards Council of Canada (SCC), and Innovation, Science and Economic Development Canada (ISED) for their efforts in supporting this project.

Cover Art - Michael Joyce x Charlesdeluvio@unsplash.com x dream.ai

A Girl learning to be safe in a digital world - Michael Joyce x DALL•E mini by Craiyon.com

A Classroom learning to be safe online - Michael Joyce x dream.ai



Cite as:

Adediji, D., Aldridge, M., Ouellet, M., Puopolo, A., Thompson, D., & Frank, R. (2022) *Challenges of Virtual Trust: A Matter of Cooperation, Education, and Cybersecurity*. Human-Centric Cybersecurity Partnership HC2P.

Dépôt légal, Bibliothèque et Archives nationales du Québec, 2022

ISBN: 978-1-7387249-0-1

The Human-Centric Cybersecurity Partnership is supported in part by funding from the Social Sciences and Humanities Research Council.

Social Sciences and Humanities Research Council of Canada

Conseil de recherches en sciences humaines du Canada

Canada

# Contents

# Challenges of Virtual Trust

A MATTER OF COOPERATION, EDUCATION AND CYBERSECURITY

## Executive Summary

In recent years, the rise of e-commerce has resulted in significant changes to consumer spending habits. Trust between consumers and vendors has been shown to be one of the most important variables that makes e-commerce successful. Increasingly, fraudulent online actors seek to abuse and exploit people's trust for financial gain or to gather personal information, thereby negatively affecting trust-building measures.

Trust is understood to include three primary elements through which individuals evaluate organisations: competence, integrity, and benevolence. Trust enhancing factors, also referred to as "trust antecedents," can be leveraged by organisations to strengthen trust relationships with their users. Trust antecedents depend on the individual characteristics of consumers (e.g., socio-demographics or personality), the design and functioning of a website (e.g., visual design, ease of use, or interactivity), and interactions between individuals and

the organisation (e.g., prior experience of users or perceived reputation of an organisation).

Governments and organisations can take measures to ensure the perceived trustworthiness of legitimate websites, and leverage public awareness campaigns to reduce individuals' risk of falling victim to fraud or other cyber threats.

## Recommendations

- Leverage trust antecedents to establish the three key dimensions of trust for individuals accessing websites (i.e., competence, integrity, and benevolence).
- Promote the use of Canadian 3rd party security certification seals to increase trust in conjunction with educational campaigns simultaneously.
- Create a publicly available register of legitimate organisational URLs gathered as part of the business incorporation process, to provide a trustworthy reference for consumers.
- Increase collaboration between government and private entities and secure coding practices to provide more efficient support and information sharing in the cybersecurity domain.
- Design of awareness and educational campaigns targeting vulnerable populations – particularly Indigenous, youth, and elderly populations.

> ***"the more trust individuals place in an entity, the more vulnerable they become to exploitation"***

# 1 Introduction

Societies rely on ecosystems of trust to function, including trust in financial institutions, food supply chains, energy systems, and more recently cyberspace (Hampson, 2017, pp. xvii). Establishing trust is often difficult to establish, however, it is a valuable tool in reducing people's perception of risk and facilitating exchanges (Gregori et al., 2014). Accordingly, the more trust individuals place in an entity, the more vulnerable they become to exploitation. The Internet's novel platform and services have created more nuanced complexities in trust development (Hampson, 2017). Its trust-building capabilities, including security, privacy, and reliability, have promoted increased user acceptance, while its widespread adoption has also provided more opportunities for fraud and abuse. A lack of regulation and global Internet governance has compounded these issues and fuelled the exploitation of individuals.

In recent years, the rise of e-commerce has resulted in a significant change in consumer spending habits. Globally, e-commerce sales have begun to dominate the retail market and Canadian e-commerce sales are anticipated to continue climbing in years to come. The onset of the COVID-19 pandemic in March of 2020 brought mandatory contactless exchanges and further drove this shift and significantly altered Canadians' purchasing habits. Compared to 2019, e-commerce sales more than doubled in 2020, and experienced a 110.8% increase, reading $64.5 billion (Statistics Canada, 2020). Despite the relaxation of health measures and a return to in-store shopping options in 2021, e-commerce sales

maintained high levels (Statistics Canada, 2022). While online purchasing options provide consumers with increased transactional ease and broad product selections, online retail opens the door to more opportunities for fraudulent behaviour.

Trust has been shown to be one of the most important variables that makes e-commerce successful since it affects people's choice and evaluation of services (Anaya-Sánchez et al., 2019). The simple act of ordering an item online is underpinned by the trust that the individual will get the item they ordered in a safe and timely manner.

The most commonly accepted definition of trust in literature conceptualizes trust as being composed of three primary elements: competence, integrity, and benevolence (Mayer et al., 1995 in Berraies et al., 2015). Competence refers to whether an organisation possesses the required expertise or technical skills to meet its service commitments. Integrity, or reliability, refers to the "sincerity of [organisations] on their intention to honour their commitments and the promises made to the customer" as well as the accuracy of website information (Berraies et al., 2015, p. 913). Benevolence speaks to whether the organisation acts in the interests of its consumers and places their interests above their own (Berraies et al., 2015; Gregori et al., 2014). While different scholars have developed various definitions of trust, there is an agreement on the importance of trust for "fostering successful relationships [and] reducing uncertainty and risk" (Chang & Fang, 2013, p. 149), particularly in online environments.

The economy and public sphere share a common dependency on trust. When individuals lose trust in the Internet, they alter their behaviours, which in turn cripples the adoption of technology and halts innovation (Hampson, 2017). Accordingly, it is important for organisations, in the public and private sectors alike, to better understand how trust operates online, how it is established and abused, and how to address such issues.

This report presents an examination of the issues surrounding the development and application of trust in a digital environment. The first section of this report contains a literature review of the challenges of establishing trust in e-commerce. Then we engage in a critical discussion on the abuse of trust, regulation of fraudulent websites, previous educational campaigns, and strategies for increasing individual trust online. The final section contains recommendations for how organisations can establish strong trust relations with individuals in online environments.

Establishing Trust

# 2 Establishing Trust

A large body of literature has examined the ways in which consumer trust can be established in various online environments such as e-commerce, tourism, and e-banking. Online trust differs from offline trust because consumers interact with websites rather than physical storefronts (Etizioni, 2017). Trust inducing factors, also referred to as "trust antecedents," are connected to various elements of online organisation-user interactions, with certain elements being more easily controlled by organisations to induce trust relationships. Kim (2016) identifies three primary categories of antecedents including individual difference antecedents, website-related antecedents, and consumer-to-website interaction-related antecedents. In the remainder of this section, we will engage in a detailed discussion of these three antecedent types and their impact on the development of consumer trust.

## 2.1 Individual Difference Antecedents

Individual difference antecedents refer to trust-inducing factors that are directly dependent on the individual characteristics of people such as socio-demographics and personality. While this category of antecedents has a significant impact on the development of trust in online environments, organisations have a very limited capacity for manipulating antecedents in this category.

Research has found that socio-demographics such as gender, age, and education influence the development of consumer trust. Younger and more highly educated people have been found to have higher levels of trust in online websites, a finding that may be due to their increased understanding of privacy and security issues when compared to older and less educated individuals (Kim, 2016; Riquelme & Román, 2014). Studies have found contradictory findings on the effects of gender on trust, with one study discovering that males have higher trust in online retailers (Riquelme & Román, 2014) and another finding females to place more trust in online health websites (Kim, 2016). This contradictory evidence may suggest that gendered effects are context-dependent and will therefore vary depending on the type of service offered.

Personality traits such as agreeableness, extraversion, and propensity to trust have also been found to have an impact on levels of user trust. Privacy and security have been found to be stronger antecedents of trust for individuals low in extraversion (i.e., talkative, sociable, etc.) (Riquele & Román, 2014). In a review of the literature on trust antecedents, Kim (2016) found that individuals with higher levels of agreeableness (i.e., "having positive beliefs toward other parties and appreciating their values and convictions") are more likely to be trusting and aware of potential risks (p.363). Propensity to trust (i.e., "general inclination to display faith in humanity and to take a trusting stance toward others") was also found to have a significant effect on increasing user trust (Chang & Fang, 2013). While antecedents in this category cannot be directly controlled by organisations, companies can consider the socio-demographics and personalities of their customer base and cater their services to their individual needs.

## 2.2 Website Related Antecedents

Website-related antecedents encompass trust-inducing factors flowing from the design and functioning of a website. Web-based factors are crucial for trust development, as they are under "direct organisational control" (Anaya-Sánchez et al., 2019) and can therefore be easily manipulated by organisations to increase trust levels. Website-related antecedents can be further divided into two sub-categories which are defined below: functional features and relational features.

### 2.2.1 Functional Features

Functional features can be defined as "the

technical dimensions [of a website] such as visual design, security and privacy, ease of use" and information quality (Kaabachi et al., 2019, p. 504).

The visual aesthetics of a website, including the use of colours, font styles, and pictures, have been found to play an important role in the development of online trust and these features are widely acknowledged as being the online equivalent to the physical appearance of business facilities (Gregori et al., 2014; Beldad, de Jong, and Steehouder 2010; Koufaris and Hampton-Sousa 2004; Etizioni 2017). Research suggests that websites with a "clean, non-cluttered design" are more trustworthy (Bauman, 2014, p.374; see also Qualati et al., 2021), create a friendly virtual environment, and are believed to be more credible (Gregori et al., 2014), competent (López Miguens et al., 2014), and likely to follow through on commitments to their customers (Berraies et al., 2015; Gregori et al., 2014).

Ease of use has been identified as a key quality for establishing consumer trust in a website (Etzioni, 2019). Websites that are user-friendly (Shah et al., 2022), accessible (Bauman, 2014), have a clear structure (Berraies et al., 2015; Gregori et al., 2015), an easily located search box (Bauman, 2014; Berraies et al., 2015), and are overall easy to navigate, are more likely to be viewed as competent (López-Miguens et al., 2014) and credible (Berraies et al., 2015), and are likely to be trusted and continued to be used by people (Kim, 2016; see also Yeh & Li, 2014). Websites with complicated navigation were found to raise concerns about legitimacy (Gregori et al., 2014).

Information quality is crucial for the development of people's trust in a website. Previous research has found that people trust websites that provide useful, relevant, and complete information that is up to date, accurate, and easy to understand (see Amin et al., 2021; Anaya-Sánchez et al., 2019; Berraies et al., 2015; Chang & Fang, 2013; Kaabachi et al., 2019; Kim, 2016). The credibility of website sources is also an important determinant of information quality (Anaya-Sánchez et al., 2019).

Security and privacy are one of the most frequently cited antecedents of online individuals' trust (Riquelme & Román, 2014). While many definitions exist, privacy is generally concerned with the protection of personal and confidential information, while security refers to protective mechanisms employed by a website to safeguard people from fraud (Berraies et al., 2015; López Miguens et al., 2014; Riquelme & Román, 2014). Websites that employ structural security assurances such as encryption, protection, verification (e.g., certificates or seals such as TRUSTe), and authentication (e.g., digital signatures or electronic IDs) mechanisms (see Gregori et al., 2014; Lopéz Miguens et al., 2014; Riquelme & Román, 2014; Sánchez-Torres et al., 2016) are more likely to gain individuals trust and confidence due to assumptions of "guaranteed security" (Sánchez-Torres et al., 2016). Structural privacy assurances (e.g., accessible privacy policies) (Lopéz Miguens et al., 2014) have also been shown to reduce perceptions of risk (Riquelme & Román, 2014) and increase confidence and institution-based trust (Gregori et al., 2014; Sánchez-Torres et al., 2016). However, it is important to note that structural assurances do have limitations and may not always

be successful due to their reliance on individual knowledge and subjective interpretation (Gregori et al., 2014).

### 2.2.2 Relational Features

Relational features can be understood as the "interactive and social aspects of website[s] such as personalization, quality support, virtual community and social presence" (Kaabachi et al., 2019, p. 504). Social presence is defined as "a website's ability to convey a sense of human warmth and sociability" (Amin et al., 2021, p.846) and is often achieved through interactive website features. Interactivity and social presence have been identified in literature as crucial trust antecedents for web-only organisations (e.g., online banks) that lack the direct human interaction available to brick-and-mortar organisations (Kaabachi et al., 2019). Interactive tools such as virtual advisors, video conferencing, online chat, and customer review sections, build individuals' confidence and foster a secure and supportive environment that increases user trust (Kaabachi et al., 2019; see also Bauman, 2014). In addition, a strong social media presence increases the capacity of banks and other organisations to cultivate relationships with people, creates a sense of community, and even gathers information from individuals to improve customer service experiences (Kaabachi et al., 2019; see also Ye et al., 2020). This also helps improve people's knowledge-based trust in a business. Individuals' understanding of an organisation's structure, composition, and background knowledge of a website can be an important factor in establishing trust (Gregori et al., 2014). Some literature also points to personalization as an important interactive feature. Personalization strategies provide people with advice that is tailored to their specific needs, such as personalized financial solutions for banking consumers; such strategies allow banks to demonstrate their reliability and increase consumer trust (Kaabahci et al., 2019).

## 2.3 Consumer-to-Website Interaction-Related Antecedents

Consumer-to-website interaction-related antecedents refer to those that require an interaction between individuals' perceived experiences and the organisation's website features and as such, are not exclusively controllable by the organisation (as was the case with website-related antecedents). This category of antecedents may include prior experience of individuals, perceived reputation, perceived risk, familiarity with the organisation, perceived reliability, and perceived service quality.

Levels of online expertise have been found to influence individuals' trust in vendor websites. Some research has found people with prior Internet experience to have lower perceptions of risk and view websites more favourably (Kim, 2016) and with higher credibility (Chang & Fang, 2013). However, the level of prior experience is also important, with novice and intermediate individuals having higher levels of trust and highly experienced individuals having low levels of trust due to previous exposure to inaccurate information (Kim, 2016) and an ability to recognize website limitations and informa-

tion credibility (Chang & Fang, 2013).

People's trust in an offline organisation positively influences their perceptions of the same organisation's online transactions (Lee et al., 2007; Hahn and Kim, 2009; Verhagen and van Dolen, 2009). It has been clearly established that the positive effects of an organisation's perceived reputation on user trust. Perceived reputation can be understood as the perceived degree of website popularity and credibility that is determined by the website's "visibility, distinctiveness, authenticity, transparency, and consistency" (Akroush & Al-Debei, 2015, p.1357). A strong website or brand reputation is indicative of organisational integrity, competence (Gregori et al., 2014), quality (Chang & Fang, 2013), low risk (Chang & Fang, 2013; Qualati et al., 2021), and trustworthiness (Kim, 2016; Yeh & Li, 2014). Gregori et al. (2014) found search engine results to be an important indicator of reputation, with high-ranking organisations (i.e., top three to five search engine results) being viewed as more trustworthy by individuals. Trust could also be transferred from in-person to online shopping. Fernandez-Sabiote and Roman (2012) showed that the offline service channel positively impacts peoples' channel evaluations and positively affects online service value. For organisations that operate both online and offline, online trust can also be established and grown from people's interactions with brick-and-mortar stores (Beldad et al., 2010, pp. 866-867).

Previous research has found high perceived risks to negatively impact individuals' trust (Kim, 2016; Qualati et al., 2021). This is a critical finding for online-only organisations which present higher risks to people due to fewer direct individual-organisation interactions (Akroush & Al-Debei, 2015). People often express "uncertainty regarding security, loss of money and time, and social concerns" (Qualati et al., 2015), as well as the protection of personal information. Such concerns can be reduced through security and privacy assurances and strong brand or website reputations. Trust is also enhanced when the advantages of using an online organisation (e.g., convenience) outweigh the associated disadvantages of its use (e.g., risks) (Akroush & Al-Debei, 2015).

A smaller body of literature points to the importance of service quality in the development of online individual trust. Perceived service quality refers to "perceptions about responsiveness, empathy, and assurance" (Agag and El-Mastry in Qualati et al., 2021, p.3) and can be demonstrated by online organisations through interactions with individuals after sales, policies for product returns, and deliveries (Shah et al., 2022). High service quality demonstrates care and develops a strong relationship with individuals which builds trust (Shah et al., 2022). Research also underscores service quality as a crucial factor for preventing a loss of trust following service failures or restoring people's trust after a negative service experience (Ye et al., 2020).

Challenges

# Challenges of Establishing Trust in E-Commerce

In the previous section, we discussed the various factors and dynamics that impact the establishment of trust. We will now turn to a critical discussion of the challenges associated with establishing trust in e-commerce.

## 2.4 The Privacy-Trust Balance

One of the paradoxes or areas of tension of the digital age, and in extension e-commerce, concerns how individuals freely disclose information on the web while also worrying about how such information is used to market or advertise goods to them (Wright et al., 2009). These conflicting actions make it challenging for organisations to construct balanced rules and ensure the right trade-off between privacy and trust in e-commerce. Responsible digital commerce practices should only require the disclosure of relevant personal information and such information should not be used in an unfair or predatory manner. Given that information is often disclosed online for commercial transactions, robust privacy standards, including data transpar-

ency and communication with data subjects, are key to building trust (Wright et al., 2009; Hillman & Neustaedter, 2017, p.18).

## 2.5 Identity Verification

Identity verification is one of the key problems confronting trust-building in e-commerce (Etzioni, 2019). When conducting transactions online, individuals cannot assess an organisation's identity as readily as they can in offline transactions (Hillman & Neustaedter, 2017). To combat this issue, organisations have begun adopting certification seals and deploy review systems wherein individuals can offer public comments regarding purchases for increased transparency (Boulianne & Cho, 2009). Such review systems and trust seals have been linked to increased revenue for vendors (Etzioni, 2019).

## 2.6 Increased Financial Risk

Increased financial risk is another factor that works against building trust in digital transactions (e.g., see Berraies et al., 2015). In a study conducted by Hillman and & Neustaedter (2017, p.14), it was established that individuals' trust during mobile transactions was most frequently negatively impacted by increased prices of the goods and services. These higher prices could be viewed as increased financial risks which raises individuals' hesitancy to complete purchases. This does not mean other factors do not come to play or impact trust, but individuals are more reluctant to trust while transacting digitally if the financial risks are high. In contrast to this position is that individuals who are high-income earners are generally less bothered about trust in the cyber world (Kim & Koo, 2016). The takeaway from this research is that the prices of commodities or services can also hinder the establishment of trust in the e-commerce world.

# Vulnerable Populations

*A Girl Learning to be Safe in a Digital World*

## 3 Vulnerable Populations and the Abuse of Trust in E-Commerce

Online fraudsters may look for particular characteristics to determine who to target - namely, visibility and accessibility (Van Wilsem, 2019). Virtual environments have provided attackers with new tools and opportunities to commit fraud and identify appropriate targets. Physical barriers to committing crimes have been replaced by virtual ones, thereby changing how we should assess threats and define vulnerabilities.

Individuals' trust is abused and manipulated by cybercriminals looking to make a profit. Trust is a

central element to many of the frauds perpetrated online, such as taking advantage of individuals' trust in institutions and pretending to be the Canada Revenue Agency to get access to banking details.

## 3.1 At Risk Demographic Groups

Certain groups of consumers are more vulnerable to becoming victims of cyber-enabled crime. Studies have shown that while race, gender, and location (such as urban and rural) do not have statistically significant impacts on computer crime victimization overall, age does (van Wilselm, 2013). Young individuals (i.e., 35 and under) are more likely to become victims of cybercrime than individuals over the age of 55, who have a very low risk of being victims of web service consumer fraud (van Wilselm, 2013; van de Weijer and Leukfeldt, 2019; Akdemir et al., 2020). However, this difference can be mainly attributed to online behaviours (Choi et al., 2016), since younger individuals tend to purchase more online, and are on the web more frequently. They may also engage in riskier online activities such as browsing risky websites, downloading from peer-to-peer services, and more. Digital natives, having grown up with technology firmly integrated into every aspect of their lives, may overlook the inherent risks of sharing personal and sensitive information online. Although younger computer users are often described as knowledgeable in using devices and online platforms, their lack of comprehension of the importance of developing and maintaining proper cyber habits may lead to a disproportionate increase in threats when visiting websites.

In addition to age considerations, Plosker and Srivastava (2021) have highlighted the stark digital divide facing rural populations and Indigenous populations, who are often underequipped and lack the technological skills to securely interact in online environments. As the transition to online business is growing, organisations need to consider the range in individuals' expertise, which can be accounted for through cooperation between regulators, governments, and industries (Georges et al., 2015).

## 3.2 Online Behaviours and Risk

According to Felson and Clarke (1998, in Van Wilsem, 2019, p. 170), the general suitability of a crime target is determined by visibility and accessibility. This provides an explanation as to why higher-educated individuals and high-income households are more vulnerable to fraud victimization (Van Wilselm, 2013), and why individuals who are online more frequently are more likely to become targets of other cyber threats. Certain activities carry different risk factors as well: buying goods or services online enhances the risk of cybercrime victimization or e-commerce fraud while engaging in online activities such as peer-to-peer sharing, watching free adult content and free streaming is linked with higher malware infection and cyber threats (Akdemir and Lawless, 2020).

Opportunity is a root cause of victimization – greater online exposure to motivated cyber criminals corresponds with increased risks for online victimization (Reyns, 2015). People may expose themselves to cyber criminals simply by being more present online. However, this threat can be mitigated by the practice of good cyber hygiene and awareness to protect one's security while using the web (Reyns, 2015), as long as one does not get lulled into a false sense of security (Akdemir and Lawless, 2020). Avoiding risky online behaviours is crucial (Reyns, 2015, p.408; Van Wilsem, 2013).

Those who perceive a higher risk to themselves may do more to protect their activities online (Reisig et al., 2009). Accordingly, education programs are vital to helping people establish better cyber hygiene and remain aware of existing risks. Implementing efficient cybersecurity awareness, training, and educational programs is critical to increasing individuals' sense of risk and critical engagement online.

# Regulating Fraudulent Websites

## 4 Difficulties in Addressing Fraudulent Websites Through Regulation

The following sections discuss potential solutions and best practices for governments and organisations to consider when seeking to reduce fraud and strengthen individuals' trust online.

Criminal activities can sometimes be managed via regulation, however robust strategies including civilian engagement and cultural change are often required. In this case, addressing the issues posed by fraudulent websites through regulations will likely prove difficult due to jurisdictional reach, technical constraints, and the high cost of using various dispute resolution mechanisms. For Canadian regulators, lessons in legislative attempts to govern domain name disputes can be drawn from jurisdictions with similar legal systems and values, including international bodies and the United States.

## 4.1 Case Studies from Other Jurisdictions

Internationally, the Internet Corporation for Assigned Names and Numbers (ICANN) has established a Uniform Domain Name Dispute Resolution Policy to govern disputes regarding the registration of domain names related to top-level domains (e.g. .com, .net, .org, etc.) (ICANN, 1999). While this process has resulted in successful outcomes for large corporate entities, it has its pitfalls. Filing a complaint requires a minimum $1,500 USD filing fee, plus all of the legal fees incurred during the dispute process. Additionally, the tribunal's rulings are non-binding, and the tribunal is not required to use a specific set of national laws, resulting in inconsistent decisions (Plotkin, 2015). Finally, due to the proliferation of new generic top-level domains (known as gTLDs), fraudulent registrants can register any of a seemly endless array of other domain names (e.g. .biz, .info, .computer, etc. ) which often exist beyond the jurisdictional reach of ICANN. Currently, the United States (US) is the only country to have attempted to regulate fraudulent domain names via national legislation and introduced its ***Anticybersquatting Consumer Protection Act*** (ACPA) (Plotkin, 2015). While the ACPA has enjoyed some success in protecting trademark holders' rights, like ICANN, it cannot protect nor regulate all fraudulent domain registrations due to its limited reach (Plotkin, 2015).

## 4.2 Regulation in the Canadian Context

Websites using top-level domain names (such as .ca, .com, .org) can be registered from anywhere in the world and accessed by individuals globally. Canadian legislators can take steps to formally regulate domains registered in Canada, i.e. using the .ca domain name, through existing trademark legislation. Indeed, the Canadian Internet Registration Authority's (CIRA) Dispute Resolution Panel (2017) has recently affirmed that cybersquatting or bad faith registrations of .ca domain names will not be upheld against legitimate trademark owners. Similarly, the British Columbia International Commercial Arbitration Centre (2017) ordered the return of whatsapp.ca to the registered trademark holder from an unaffiliated third party who was found to have registered the domain in bad faith.

While opportunities exist to formally codify these trademark protection standards via amendments to the ***Trademarks Act***, enforcing Canadian legal standards upon entities that are not registered nor are incorporated in Canada comes with additional challenges. Firstly, it will be difficult to impose penalties on an entity not registered or operating within Canada. Moreover, the high costs of commencing arbitration or litigation proceedings will pose a barrier for many small and medium businesses with limited resources seeking

***“legislative solutions alone to regulate fraudulent websites may prove difficult to achieve their desired outcomes.***

to defend their trademark rights. Finally, the process to obtain a .ca domain name is generally simple, providing ample opportunity for fraudulent registrations and disputes. A registrant typically has to pay a nominal fee and demonstrate that they have a Canadian “presence,” primarily by providing proof of citizenship, permanent residency, or incorporation in Canada. Accordingly, legislative solutions alone to regulate fraudulent websites may prove difficult to achieve their desired outcomes.

Educational Campaigns

*A Classroom Learning to be Safe Online*

# 5 Previous Educational Campaigns & Best Practices

Most organisations maintain an online presence by using websites as a point of entry to reach as wide of an audience as possible. While people access resources on a webpage for information, to purchase commodities, or to share experiences, browsing safely has become a significant issue for both individuals and organisations. In this context, governments, businesses, and individuals must possess an awareness of cybersecurity principles that were previously delegated to specialists and IT professionals. Accordingly, countries have begun funding and supporting various campaigns targeted at educating, informing and raising awareness

with the aim of mitigating cyber attacks and online fraud.

## 5.1 Overview of Previous Educational Campaigns

Our review of cybersecurity campaigns from around the world revealed marked similarities in practices between initiatives, particularly in terms of targeted audiences, cooperation between the public and private sectors, and the importance of interacting with individuals through online platforms and public events.

Since the mid-2000s, most governments have directed resources towards developing a wide range of informational campaigns to raise cybersecurity awareness. Examples include the United Kingdom's National Cyber Strategy (2022), Canada's Get Cyber Safe (2021), the National Cyber Security Masterplan 2018 (2014) from Singapore, and Africa's Internet Safety Campaign that recently began deploying additional initiatives in parallel. Many governments, including those of Canada, France and the US, have declared October to be cybersecurity awareness month, and each year select a thematic topic to focus their messaging. In the UK, the government runs a program called "Get Safe Online" to disseminate easy-to-understand information on online safety. The initiative offers the public multiple free security tools such as a website authenticator and subscription to a neighbourhood alert for recent fraud. Moreover, many nations including the US and the UK have begun targeting youth populations by deploying special cybersecurity curricula and activities in schools.

Unfortunately, tracking changes in a population's cyber hygiene after exposure to informational campaigns remains a challenge since it cannot be easily measured by economic or financial metrics. Moreover, little research has been conducted into quantifying the short or long-term effects of cyber awareness campaigns and prevention campaigns worldwide.

We observed several constant trends in a few key aspects when delivering education, awareness, and prevention campaigns. For governments, simultaneously targeting diverse segments of society like CISA's Cybersecurity Awareness Program (e.g., students, educators, small businesses, etc.), the RCMP's National Cybercrime Coordination Unit (law enforcement bodies and government private partners) and educating the public from an early age appears to be beneficial, in addition to encouraging people to actively participate in cybersecurity through interactive events (Lemos, 2016). These events, including competitions through simulations (e.g., the Collegiate Cyber Defense Competition in the United States), gamified content (Giannakas et al., 2019), and community-based forums show promise as methods for improving people's knowledge of online safety.

## 5.2 Lessons Learned from Previous Campaigns & Practices

Generally, measurements of the success of a cybersecurity campaign have been limited. The results obtained demonstrated the number of individuals contacted, without an indication

of the amount of information absorbed (Bertrand et al., 2006). Measuring the success of awareness campaigns more comprehensively will likely continue to be difficult because the outcome is difficult to measure and requires long periods of observation (Bada et al., 2015).

In terms of content, previous campaign strategies have often problematically focused on the use of fear of consequences (Arthur & Quester, 2004). Leveraging fear requires carefully segmenting the population concerned, since it may only stimulate people's intentions to eliminate a perceived threat or emotional discomfort without considering possible adverse outcomes instead of developing and maintaining safer cyber hygiene such as performing device updates, encrypting private data and using protection softwares. Other campaigns were found to be too information dense and lacked the engaging qualities necessary for knowledge retention (Bada et al., 2015). Moreover, oftentimes such campaigns failed to identify distinct targets with the effect that people were not able to interpret if the information presented related to them (van Steen et al., 2020).

Aspects of how information is presented have been shown to decrease people's awareness when interacting online. Security fatigue (Stanton et al., 2016) or warning fatigue occurs when individuals are overexposed to repeated visual messages (Akhawe et al., 2013). This fatigue has been shown to limit the effectiveness of previous cyber awareness campaigns (Coutu, 2019). Moreover, when individuals undervalue visual cues indicating possible security threats such as Secure Sockets Layer (SSL) certificates, phishing icons, or malware alerts, such behaviour increases opportunities for attackers. These real-time security alerts presume prior knowledge of the risk associated with selecting a dangerous option and often do not prevent people from accessing the resource (Coutu, 2019).

Community-based platforms from private and government initiatives (e.g., ScamDoc.com, scamwatch.gov.au, fraude-alerte.ca) stimulate cybersecurity education, awareness, and cybercrime reporting. Through competition, challenges, or sharing of experiences, these websites attract groups based on similar focus, interest, and other relevancies. Additionally, such collaborative platforms allow moderators to monitor information relevance, promote participation, assess the efficiency of a campaign through metrics, and contribute to human-like interaction that reinforces learning and promotes sharing.

## 5.3 Designing Awareness Campaigns and Leveraging Psychological Tools

Providing individuals with cybersecurity information and best practices alone will not guarantee secure behaviour (Carpenter, 2019). While awareness campaigns can be effective, and indeed even transformational, policy makers must connect security messaging to "topics, situations, and outcomes" that the audience will find relevant and meaningful, often through emotion and story (Carpenter, 2019). Informational videos, simulation events,

> ***"policy makers must connect security messaging to "topics, situations, and outcomes" that the audience will find relevant and meaningful"***

games, and learning modules deployed via micro-learning (i.e., short content delivered on a frequent basis) can be useful tools to deliver awareness messaging (Carpenter, 2019). Moreover, in partnership with educational campaigns, targeted psychological tools can be instrumental in promoting best practices and safe behaviour in online settings.

One of the most widely deployed psychological online instruments is nudges. Nudge theory seeks to structure choice architecture so as to influence or alter individual choices to induce predictable behaviour (Thaler & Sunstein, 2008). In the domain of human-centred cybersecurity, digital nudges have proven to be effective when deployed correctly, however, their use raises issues of liberal paternalism and control (Zimmerman & Renaud, 2020). Nudges exert influence by activating individuals' automatic cognitive processes, to encourage them to act in a particular way. Responsible nudge implementation seeks to ensure individuals' freedom of choice so not as to exert undue control and influence over the decision makers. Moreover, to produce effective results when deploying nudges, close attention must be paid to the "decision context, the nudge design, and their interaction" with their audience (Zimmerman & Renaud, 2020, p.2). An example of a commonly used digital nudge is password assessments - when a person creates a new password often a message appears rating the security strength of the password with "strong", "good", "too short", or "weak", to prompt the person to consider the complexity of their choice.

Recommedations

# 6 Recommendations

The previous sections of this report discussed the factors affecting trust in virtual relationships and previous campaigns and strategies that have been deployed to increase online security. The following section details various recommendations that can be harnessed by organisations to build trust between individuals and strategies to increase our population's understanding of security standards.

## 6.1 Leveraging Trust Antecedents

Trust antecedents can be leveraged by organisations to establish the three key dimensions of trust: competence, integrity, and benevolence (López Miguens et al., 2014). Competence can be demonstrated by organisations to individuals through website experience design, such as by in-

cluding a clean and professional visual design and an easily navigable interface. This can be built upon through functional features that ensure the provision of accurate, credible, and up-to-date information. Relational website features, such as interactivity and personalization strategies, are also beneficial in demonstrating organisational integrity to people. Finally, organisations must demonstrate benevolence by prioritizing people's interests over their own. Organisations can begin to demonstrate this by cultivating relationships with individuals through interactive website features (e.g., virtual chat), a strong online social presence, and high service quality.

Organisational security posture and responses to security and privacy breaches are also key in establishing virtual trust (López Miguens et al., 2014). Organisations can inform people of security and privacy protections through structural assurances (i.e., functional website features) such as browser encryption symbols and verification seals (i.e., CyberSecure Canada), as well as publicly accessible privacy policies. Riquelme and Román (2014) also recommend that organisations expand their educational campaigns and promotional materials to explain their privacy and security policies in a way that can be easily understood by all individuals regardless of their experience or education level. Organisations can also consider individual difference antecedents, such as socio-demographics and personality traits, when creating online content and tailor it to individual needs.

## 6.2 Technical Solutions

From innovative web application technologies will appear new and undiscovered security implications. Ensuring a harmonious implementation of technology in online activities is now a matter of cooperation between organisations and governments regardless of industry and size. Moreover, people increasingly play an essential role in shaping website content and contributions. Since trust is manifested in cooperation between the display of information perceived by individuals and their previous experiences, the continuum of this relation also lies in how a website is created, published, and maintained by content creators and third-party businesses involved.

### 6.2.1 3rd Party Security Certifications

To overcome issues of trust, the concept of transference via a 3rd party seal seeks to promote people's confidence in an unfamiliar website through a known 3rd party. Strategic awareness campaigns can increase individuals' privacy empowerment and inspire trust when a third-party seal is displayed (Kim & Kim, 2010). In Canada, Innovation, Science and Economic Development's certification body allows accredited businesses to display various certification marks easily added to a webpage. However, the effectiveness of such a program requires increased public awareness of its purpose.

One of the potential issues that arise with this strategy is that electronic verification symbols

can often be used to promote fraud. In the past, such symbols have been easily copied and used unlawfully (van der Toorn et al., 2022). A possible solution for this issue is to publicly allow list verified Uniform Resource Locators (URL) for legitimate businesses via a government website or trusted organisation. Accordingly, individuals would be able to cross-reference the URL of the vendor from whom they are seeking to make a purchase, with an updated list provided by federal or provincial authorities. Moreover, nudging techniques could be deployed by the payment processor to invite people to cross reference the website with the government's list. The European Union has implemented a similar system for due diligence regulations and maintains an online central register for company registrations.

To implement this solution, companies seeking to incorporate at the federal level in Canada (or in provincial jurisdictions) could be required to provide their URLs to the Canadian or provincial governments to be included on the central list. Legitimate online sellers who are not incorporated in Canada could also have the option to be included in the website list via an additional verification process. Although the implementation and maintenance of this initiative will raise organisations' administrative workload and government expenditure, individuals and organisations will likely welcome such transparency resulting in improved trust in websites.

### 6.2.2 Cyber Threats Monitoring and Collaboration

While most organisations in Canada are strongly advised to develop and maintain secure websites, increased cooperation between government and private entities can bolster online security (Oriola et al., 2021). Sharing new findings on website vulnerabilities and mitigation techniques between organisations and governments allows all parties to stay up to date with new developments and keep up with evolving technologies, similar to the Open Web Application Security Project Foundation (OWASP) international contribution. Given smaller organisations' limited resources and potential lack of cybersecurity expertise, such information sharing offers an affordable and accessible method for maintaining cybersecurity best practices. Cybereco is an example of such initiatives that seek to bring together security experts to facilitate information sharing across multiple sectors within Canada and includes partners such as the National Bank of Canada, IBM, Fasken, and Concordia University. Expanding such programs and others not mentioned, such as the Canadian Cybersecurity Threat Exchange (CCTX), to include smaller to medium-sized businesses can promote the increased dissemination and adoption of security standards.

In addition to information sharing, collaboration between levels of government and the private sector can lead to the development of resources for individuals, resulting in a more robust security ecosystem and enhanced trust relationships. For example, the Government of Quebec through its ***Ministère***

***de la Cybersécurité et du Numérique,*** is currently developing a digital identity initiative to increase citizen online safety when accessing government platforms and documents, in addition to non-government resources such as automobile insurance. Similar partnerships could be useful in deploying and maintaining the previously mentioned public ledger of verified URLs for people to use as a certification method.

### 6.2.3 Promoting Secure Coding Practices

Insecure coding of websites leads to many cyber security incidents on both the individuals' and organisation sides. Historically, website development only considered cybersecurity later in the development process. The integration of security into all stages of the development lifecycle and the training of developers on cybersecurity principles is considered to be fundamental in embedding security in all layers of website architecture. Ensuring websites' security features are turned on by default instead of proposing them as an alternative will facilitate the creation of trust in websites.

## 6.3 Educational Initiatives

Educational initiatives are vital in transmitting information about new initiatives and emerging cyber threats. Moreover, governments should promote community-based websites to disseminate information on cyber hygiene and cybercrime. Extra consideration should be taken to reach Indigenous, youth, and elderly populations. Such forums provide a participatory experience for the individuals (Furnell et al., 2007) and can help combat security fatigue. Additionally, simulation events can also inspire public awareness, as evidenced in the UK and US, where governments have hosted contests between cybersecurity experts to stimulate increased visibility and innovation in awareness training.

As interactive activities and simulations have proven to be effective in educating people, we suggest governments and private sector organisations (such as financial institutions) integrate short anti-fraud learning modules and questionnaires into their services and frame these as benevolent and caring. For example, to access the Government of Ontario's student loan program or OSAP, individuals must complete a brief survey to demonstrate their understanding of financial products. Similarly, prior to creating a Canada Revenue Agency account or making a first purchase online, individuals could be required to engage with educational materials designed to test their knowledge of fraudulent vendor recognition and identity verification. As previously discussed, such techniques are most effective when deployed incrementally and continuously.

Ultimately, best practices and case studies demonstrate that no single approach will be entirely effective on its own. Instead, deploying multiple strategies in tandem to combat online fraud will build user trust between legitimate organisations, and bolster public awareness of security threats.

# 7 Conclusion

This report addressed the main factors of online virtual trust and how to foster and maintain it. Organisations must contribute to website trust using the three key dimensions leveraged by the concept of trust antecedents (competence, integrity, benevolence). Our work illustrates the effectiveness of educational initiatives in establishing and combating ill-founded trust when deployed strategically and in parallel with other strategies. When designing awareness and educational campaigns, organisations must prioritize vulnerable populations, particularly Indigenous, youth, and elderly populations. Moreover, collaboration at all levels of governments and organisations improves the quality of information sharing, the dissemination of best practices, such as secure coding, to provide more efficient support and information sharing in the cybersecurity domain, and the establishment of robust solutions. Promoting the use of Canadian 3rd party security certification seals increases trust in conjunction with educational campaigns. Finally, we strongly suggest the creation of a public register of legitimate organisational URLs as part of the incorporation process to provide a trustworthy reference for consumers. Our report is a starting point for improving Canadians' cybersecurity knowledge and inspiring fraud prevention practices. Further research is required to comprehensively understand how to enhance individuals' skills with the evolution of website technologies.

# 8 References


Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. ***Internet Research***, ***30***(6), 1665–1687. https://doi.org/10.1108/INTR-10-2019-0400

Akhawe, D., & Felt, A. P. (n.d.). ***Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness***. 17.

Akroush, M. N., & Al-Debei, M. M. (2015). An integrated model of factors affecting consumer attitudes towards online shopping. ***Business Process Management Journal***, ***21***(6), 1353–1376. https://doi.org/10.1108/BPMJ-02-2015-0022

Amin, M., Ryu, K., Cobanoglu, C., & Nizam, A. (2021). Determinants of online hotel booking intentions: Website quality, social presence, affective commitment, and e-trust. ***Journal of Hospitality Marketing & Management***, ***30***(7), 845–870. https://doi.org/10.1080/19368623.2021.1899095

Anaya-Sánchez, R., Molinillo, S., Aguilar-Illescas, R., & Liébana-Cabanillas, F. (2019). Improving travellers' trust in restaurant review sites. ***Tourism Review***, ***74***(4), 830–840. https://doi.org/10.1108/TR-02-2019-0065

Signal Arnaques. (n.d.). ***Arnaques en ligne: Signalements, Informations et Assistance aux victimes***. SignalArnaques. Retrieved August 10, 2022, from https://www.signal-arnaques.com/

Arthur, D., & Quester, P. (2004). Who's afraid of that ad? Applying segmentation to the protection motivation model. ***Psychology and Marketing***, ***21***(9), 671–696. https://doi.org/10.1002/mar.20024

Aston, Jason, et al. "Retail E-Commerce and COVID-19: How Online Shopping Opened Doors While Many Were Closing." Statistics Canada, 24 July 2020, https://www150.statcan.gc.ca/n1/pub/45-28-0001/2020001/article/00064-eng.htm.

Bada, M., Sasse, A.M., & Nurse, J.R. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? ***ArXiv, abs/1901.02672***.

Bauman, A. (2015). The use of the repertory grid technique in online trust research. ***Qualitative Market Research: An International Journal***, ***18***(3), 362–382. https://doi.org/10.1108/QMR-08-2014-0080

Berraies, S., Chtioui, R., & Yahia, K. B. (2015). Functional characteristics of banking websites and customer loyalty: The mediating role of online

trust. *The Journal of Applied Business Research*, *31*(3), 911–923.

Bertrand, J. T. (2005). 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

Canadian Cybersecurity Threat Exchange. (n.d.). *Home*. Canadian Cyber Threat Exchange – CCTX – Informing Canadian Business. Retrieved August 10, 2022, from https://cctx.ca/

Canada's Centre for Digital and Media Literacy. (n.d.). *MediaSmarts*. Retrieved August 10, 2022, from https://mediasmarts.ca/

Carpenter, Perry. Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors. John Wiley & Sons, 2019.

Chang, Y.-S., & Fang, S.-R. (2013). Antecedents and distinctions between online trust and distrust: Predicting high- and low-risk internet behaviours. *Journal of Electronic Commerce Research*, *14*(2), 149–166.

Choi, K., Choo, K., & Sung, Y. (2016). Demographic variables and risk factors in computer-crime: An empirical assessment. *Cluster Computing*, *19*(1), 369–377. https://doi.org/10.1007/s10586-015-0519-8

Canadian Internet Registration Authority. (n.d.). *CIRA Cybersecurity Awareness Training*. CIRA Cybersecurity Awareness Training Platform. Retrieved August 10, 2022, from https://www.cira.ca/cybersecurity-services/cybersecurity-awareness-training

Clinique de cyber-criminologie. (n.d.). *Fraude-Alerte | Plateforme de partage de la Clinique de cyber-criminologie*. Fraude Alerte. Retrieved August 10, 2022, from https://www.fraude-alerte.ca/

Coutu, C. (2020). *La prévention de la cybercriminalité: Résultats d'une enquête sur les effets perçus d'une campagne de prévention réalisée par une institution financière.* [Master's thesis, Université de Montréal]. https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/23715/Coutu_Cameron_2019_Memoire.pdf

Cybereco. (n.d.). *Projects*. Cybereco. Retrieved August 15, 2022, from https://cybereco.ca/en/projects/

Cybersecurity & Infrastructure Security Agency. (n.d.). *CISA Cybersecurity*

***Awareness Program Toolkit***. CISA Cybersecurity Awareness Program Toolkit. Retrieved August 10, 2022, from https://www.cisa.gov/publication/cisa-cybersecurity-awareness-program-toolkit

Etzioni, A. (2019). Cyber Trust. ***Journal of Business Ethics***, ***156***(1), 1–13. https://doi.org/10.1007/s10551-017-3627-y

Fernández-Sabiote, E., & Román, S. (2012). Adding clicks to bricks: A study of the consequences on customer loyalty in a service context. ***Electronic Commerce Research and Applications***, ***11***(1), 36–48. https://doi.org/10.1016/j.elerap.2011.07.007

National Institute of Standards and Technology. (2021, April 9). ***FISSEA***. NIST | FISSEA Cybersecurity | Innovation . Awareness . Training. https://www.nist.gov/itl/applied-cybersecurity/fissea

Fryer, H., Stalla-Bourdillon, S., & Chown, T. (2015). Malicious web pages: What if hosting providers could actually do something.... ***Computer Law & Security Review***, ***31***(4), 490–505. https://doi.org/10.1016/j.clsr.2015.05.011

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. ***Computers & Security***, ***26***(5), 410–417. https://doi.org/10.1016/j.cose.2007.03.001

***Get Safe Online | The UK's leading Internet Safety Website***. (n.d.). Get Safe Online. Retrieved August 10, 2022, from https://www.getsafeonline.org/

Giannakas, F., Papasalouros, A., Kambourakis, G., & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. ***Information Security Journal: A Global Perspective***, ***28***(3), 81–106. https://doi.org/10.1080/19393555.2019.1657527

Gouvernement du Québec. (2022, June 28). ***Programme Service québécois d'identité numérique***. Programme Service québécois d'identité numérique. https://www.quebec.ca/gouvernement/identite-numerique/programme-service-quebecois-identite-numerique

Government of Canada. (n.d.). ***Get Cyber Safe***. Get Cyber Safe. Retrieved August 10, 2022, from https://www.getcybersafe.gc.ca/en

Government of Canada, R. C. M. P. (2020, February 11). ***The National Cybercrime Coordination Unit (NC3) | Royal Canadian Mounted Police***. https://www.rcmp-grc.gc.ca/en/nc3

Government of Canada, S. C. (2020, October 14). ***The Daily—Canadians spend more money and time online during pandemic and over two-fifths report a cyber incident***. https://www150.statcan.gc.ca/n1/daily-quotidien/201014/dq201014a-eng.htm

Gregori, N., Daniele, R., & Altinay, L. (2014). Affiliate marketing in tourism: Determinants of Consumer Trust. ***Journal of Travel Research***, ***53***(2), 196–210. https://doi.org/10.1177/0047287513491333

Hampson, F. O. (2017). ***Look who's watching: Surveillance, treachery, and trust online*** (Revised edition.). Centre for International Governance Innovation.

Hongyoun Hahn, K., & Kim, J. (2009). The effect of offline brand trust and perceived internet confidence on online shopping intention in the integrated multi-channel context. ***International Journal of Retail & Distribution Management***, ***37***(2), 126–141. https://doi.org/10.1108/09590550910934272

Hopkins, N. (2013, January 3). Cybersecurity drive to target schoolchildren and "risky men." ***The Guardian***. https://www.theguardian.com/technology/2013/jan/03/cybersecurity-drive-schoolchildren-risky-men

Internet Corporation for Assigned Names and Numbers (ICANN). Uniform Domain Name Dispute Resolution Policy. 24 Oct. 1999, https://www.icann.org/resources/pages/policy-2012-02-25-en.

Innovation, Science and Economic Development Canada. (n.d.). ***CyberSecure Canada***. CyberSecure Canada. Retrieved August 10, 2022, from https://ised-isde.canada.ca/site/cybersecure-canada/en

***Internet Safety Campaign | ISC AFRICA***. (n.d.). Internet Safety Campaign. Retrieved August 10, 2022, from https://iscafrica.net/#home

Kaabachi, S., Mrad, S. B., & Fiedler, A. (2020). The moderating effect of e-bank structure on French consumers' trust. ***International Journal of Bank Marketing***, ***38***(2), 501–528. https://doi.org/10.1108/IJBM-04-2019-0119

Kaloudi, N., & Li, J. (2021). The AI-Based Cyber Threat Landscape: A Survey. ***ACM Computing Surveys***, ***53***(1), 1–34. https://doi.org/10.1145/3372823

Kim, Y. (2016). Trust in health information websites: A systematic literature review on the antecedents of trust. ***Health Informatics Journal***, ***22***(2), 355–369. https://doi.org/10.1177/1460458214559432

Koufaris, M & Hampton-Sosa, W. (2004). The Development of Initial Trust in an

Online Company by New Customers. *Information and Management*, *41*, 377–397. http://dx.doi.org/10.1016/j.im.2003.08.004

Lee, K. C., Kang, I., & McKnight, D. H. (2007). Transfer From Offline Trust to Key Online Perceptions: An Empirical Study. *IEEE Transactions on Engineering Management*, *54*(4), 729–741. https://doi.org/10.1109/TEM.2007.906851

Lemos, R. (2006, June). Cybersecurity Contests Go National. *The Register*. https://www.theregister.com/2006/06/05/security_contests

López Miguens, M. J., Vázquez, E. G., & Turnes, P. B. (2013). Multilevel and multidimensional scale for online trust. *Revista de Administração de Empresas*, *54*(2), 187–200. https://doi.org/10.1590/S0034-75902014206

*MediaSmarts |*. (n.d.). Retrieved August 10, 2022, from https://mediasmarts.ca/

National Cyber Security Centre. (n.d.). *What we do*. About the NCSC. Retrieved August 10, 2022, from https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

*National Cyber Security Masterplan 2018: What you need to know*. (2014, December 19). https://www.tech.gov.sg/media/technews/national-cyber-security-masterplan-2018-what-you-need-to-know

*National Cyber Strategy 2022 (HTML)—GOV.UK*. (n.d.). Retrieved August 10, 2022, from https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

OWASP Foundation. (n.d.). *OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation*. Retrieved August 17, 2022, from https://owasp.org/

Plosker, S., & Srivastava, G. (2021). Cybersecurity Education in Rural Indigenous Canada. *2021 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 1–6. https://doi.org/10.1109/CCECE53047.2021.9569147

Plotkin, James. "The Model for a Path Forward: A Proposal for a Model Law Dealing with Cyber-Squatting and Other Abusive Domain Name Practices." The Denning Law Journal, vol. 27, 2015, https://ssrn.com/abstract=2975507.

Qualati, S. A., Vela, E. G., Li, W., Dakhan, S. A., Thuy, T. T. H., & Merani, S. H. (2021). Effects of perceived service quality, website quality, and reputation on purchase intention: The mediating

and moderating roles of trust and perceived risk in online shopping. *Cogent Business & Management*, *8*(1), 1–20. https://doi.org/10.1080/23311975.2020.1869363

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived Risk of Internet Theft Victimization: Examining the Effects of Social Vulnerability and Financial Impulsivity. *Criminal Justice and Behavior*, *36*(4), 369–384. https://doi.org/10.1177/0093854808329405

Reyns, B. W. (2015). A routine activity perspective on online victimisation. *Journal of Financial Crime*, *22*(4), 396–411. https://doi.org/10.1108/JFC-06-2014-0030

Riquelme, I. P., & Román, S. (2014). Is the influence of privacy and security on online trust the same for all type of consumers? *Electron Markets*, *24*, 135–149. https://doi.org/10.1007/s12525-013-0145-3

Sánchez-Torres, J. A., Canada, F.-J. A., Sandoval, A. V., & Alzate, J.-A. S. (2016). E-banking in Columbia: Factors favouring its acceptance, online trust and government support. *International Journal of Bank Marketing*, *36*(1), 170–183. https://doi.org/10.1108/IJBM-10-2016-0145

Shah, R., Jan, B., & Jabarkhail, I. M. (2022). Factors influencing online trust and repeat purchase intention: A study of Afghan consumers. *International Journal of Information, Business and Management*, *14*(1), 17–37.

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security Fatigue. *IT Professional*, *18*(5), 26–32. https://doi.org/10.1109/MITP.2016.84

"Table 20-10-0072-01 Retail e-Commerce Sales (x 1,000)." Statistics Canada, 15 Aug. 2022, https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2010007201.

Thaler, Richard, and Cass R. Sunstein. Nudge: Improving Decisions about Health, Wealth, and Happiness. Penguin Books, 2009.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big Five Personality Traits of

Cybercrime Victims. ***Cyberpsychology, Behavior, and Social Networking***, ***20***(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. ***European Journal of Criminology***, ***16***(4), 486–508. https://doi.org/10.1177/1477370818773610

van der Toorn, O., Müller, M., Dickinson, S., Hesselman, C., Sperotto, A., & van Rijswijk-Deij, R. (2022). Addressing the challenges of modern DNS a comprehensive tutorial. Computer Science Review, 45, 100469. https://doi.org/10.1016/j.cosrev.2022.100469

van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? ***Journal of Cybersecurity***, ***6***(1), tyaa019. https://doi.org/10.1093/cybsec/tyaa019

van Wilsem, J. (2013). "Bought it, but Never Got it" Assessing Risk Factors for Online Consumer Fraud Victimization. ***European Sociological Review***, ***29***(2), 168–178. https://doi.org/10.1093/esr/jcr053

Verhagen, T., & van Dolen, W. (2009). Online purchase intentions: A multi-channel store image perspective. ***Information & Management***, ***46***(2), 77–82. https://doi.org/10.1016/j.im.2008.12.001

***Virox Technologies Inc. v Nameshield Inc***. 344, 3 Oct. 2017, https://static.cira.ca/cdrp/virox.ca%20decision.pdf?VersionId=JYGgIEG.ymtaCv8sMli13avo0FomdQJj.

Ye, C., Hofacker, C. F., Peloza, J., & Allen, A. (2020). How online trust evolves over time: The role of social perception. ***Psychology and Marketing***, ***37***, 1539–1553. https://doi.org/10.1002/mar.21400

Yeh, Y.-S., & Li, Y.-M. (2014). Design-to-lure in the e-shopping environment: A landscape preference approach. ***Information & Management***, ***51***(8), 995–1004. https://doi.org/10.1016/j.im.2014.06.005

Zimmermann, Verena, and Karen Renaud. "The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions." ACM Transactions on Computer-Human Interaction, vol. 28, no. 1, Feb. 2021, https://strathprints.strath.ac.uk/75237/1/Zimmermann_Renaud_ACM_TCHI_2021_The_nudge_puzzle_matching_nudge_interventions_to_cybersecurity.pdf

"Governments and organisations can take measures to ensure the perceived trustworthiness of legitimate websites, and leverage public awareness campaigns to reduce individuals' risk of falling victim to fraud or other cyber threats."