“I Have Only Checked after the Event”: Consumer Approaches to Safe Online Shopping

Jack Mark Whittaker, Matthew Edwards, Cassandra Cross & Mark Button

To cite this article: Jack Mark Whittaker, Matthew Edwards, Cassandra Cross & Mark Button (2022): “I Have Only Checked after the Event”: Consumer Approaches to Safe Online Shopping, Victims & Offenders, DOI: 10.1080/15564886.2022.2130486

To link to this article: https://doi.org/10.1080/15564886.2022.2130486
"I Have Only Checked after the Event": Consumer Approaches to Safe Online Shopping

Jack Mark Whittaker \( ^{a} \), Matthew Edwards \( ^{b} \), Cassandra Cross \( ^{c} \), and Mark Button \( ^{d} \)

\( ^{a} \)Department of Sociology, University of Surrey, Guildford, UK; \( ^{b} \)Department of Computer Science, University of Bristol, Bristol, UK; \( ^{c} \)School of Justice, Queensland University of Technology, Brisbane, Australia; \( ^{d} \)Institute of Criminal Justice Studies, University of Portsmouth, Portsmouth, UK

**ABSTRACT**

Online shopping has now become very common, with consumers increasingly opting to purchase products on the World Wide Web instead of visiting traditional "bricks and mortar" stores, particularly during the COVID-19 pandemic. This has, however, also provided significant opportunities for offenders to abuse the inherent trust-based nature of online shopping, whereby consumers typically do not see the products physically prior to purchasing them. As such, this article sets out to examine the actions and behaviors that individuals take to prevent online shopping fraud and what, if any, discrepancy exists between prevention messaging and consumer behavior. To accomplish this, the study utilizes secondary survey data (n = 3478 respondents) obtained from a private-sector initiative called ScamAdviser. The results find that many respondents do not use appropriate behaviors to reduce their risk when shopping online and that furthermore there is reason to believe that consumers are not served well by the online safety advice that they are given. The paper argues that there is scope to increase guardianship through better prevention advice being communicated to online shoppers.

**KEYWORDS**

Online shopping fraud; shopping scams; retail fraud; consumer safety; e-commerce

**Introduction**

The evolution of technology has radically altered the ways in which society operates. The advancement of technologies, particularly the internet and the World Wide Web, have redefined the ways that individuals are able to conduct both personal and business activities. Nowhere has this been more evident than with the advent of electronic commerce (e-commerce) and the ability to purchase goods and services through the internet, online or other device (Lee, 2021, p. 2).

Online shopping has become a common and convenient means to purchase goods and services. The rise of online retailers such as eBay and Amazon, as well as traditional bricks and mortar retailers setting up online alternatives, has substantially expanded the opportunities to buy online almost anything, from groceries, televisions, cars to even pets. However, the ever-increasing use of the internet for e-commerce and other financial transactions has led to an inevitable increase of Internet-related crimes (Yoshida, 2013, p. 365; Sanddywell, 2009; Yar & Steinmetz, 2022; Button & Cross, 2017; McGuire, 2018). Of specific note is fraud. Given that offenders often use the same
mechanisms used by legitimate businesses such as by creating convincing websites as well as profiles on well-known online retail platforms (for example, eBay, Amazon, and Alibaba), consumers can often be exposed to fraud during these transactions (Holtfreter & Reisig, 2013, p. 326), with some arguing that there is a higher risk of fraud in an online environment compared to face-to-face transactions (Reep-van den Bergh & Junger, 2018, p. 2).

At its core, fraud is characterized by the use of deception for financial gain (Ibrahim, 2016; Lazarus, 2019; Wells, 2017). In the current context, a large amount of fraud occurs using online platforms. There are several ways that fraud can be perpetrated as it relates to the purchase of online goods and services. Online shopping fraud, retail fraud and auction fraud are all terms, which encompass the use of lying and cheating in a retail context. They most often encompass “the online sale of goods that may have been stolen, counterfeit, damaged, or otherwise misrepresented in terms of their quality or features – or simply never delivered to the paying customer.” (Yar, 2016, p. 8). However, they can span all aspects of a transaction to “include delivery, payment, return, and refund fraud committed by both sellers and buyers” (Lee, 2021, p. 2).

The current article examines the issue of online shopping fraud, with a specific focus on consumer behavior and actions taken to prevent online shopping fraud victimization. Using data from a global survey on scam victimization, this article analyzes the self-reported behaviors of individuals to protect against online shopping fraud. This is located within the context of an examination and critique of current prevention messaging related to individual efforts to reduce the likelihood of victimization. This article seeks to answer the following research questions:

1. What actions and behaviors do individuals report undertaking to prevent online shopping fraud?
2. What, if any, discrepancy exists between prevention messaging and consumer behavior?

The article is structured as follows. First, it provides further definitional aspects of online shopping fraud, outlines known prevalence rates of victimization and summarizes existing research targeting this area. Second, it provides an overview and critique of current prevention messaging as related to online shopping fraud. Third, the article outlines the dataset used, with a detailed focus on the process used to clean the data for its current form. Fourth, the article provides the results of the survey, looking at the specific actions taken by individuals to guard against online shopping fraud, and how this contrasts with known victimization. Fifth, the article discusses the implications of these findings on current prevention messaging, and acknowledges the limitations and restrictions of the analysis based on the data in its present form. Finally, the article concludes with a summary of findings as they relate to user behavior, prevention messaging and protecting against online shopping fraud. The central purpose of the article is as follows: consumer fraud is becoming a significant problem, the quality of advice provided by official bodies is of varying quality and utility and consequently many consumers do not pursue appropriate strategies when evaluating shopping websites, putting them at greater risk of fraud victimization.
Online shopping fraud

With online shopping fraud experiencing notable increases in incidents globally, the following section provides greater context on the definitional aspects of this crime category as well as detailing known victimization statistics and summarizing the limited body of existing research to date (Federal Trade Commission, 2022; ONS, 2022).

Defining online shopping fraud

Online shopping fraud (also known as online retail fraud and auction fraud) potentially covers a wide range of fraudulent activities. There have been only a few attempts to define it. The Home Office Counting Rules define online retail and auction fraud:

\[\ldots\text{attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.} (\text{Home Office (UK), 2021, p. 41})\]

In one of the most comprehensive attempts at creating a taxonomy of mass marketing fraud by Beals et al. (2015, pp. 22–26) of the seven broad categories mapped, “Consumer Products and Services Fraud” is one expansive category. They state it “\ldots covers all fraud related to the purchase of tangible goods and services.” They unfold multiple further sub-categories of this type of fraud, which for space constraints can be broadly collapsed into two: \emph{worthless and non-existent products and services} and \emph{unauthorized billing}.

This article uses the definition advocated by Beals et al. (2015) to cover frauds related to the sale of goods and services online. This captures the following categories of incidents:

- Bogus websites offering goods and services which do not exist or products which are significantly different from what is advertised. These are original websites whose purpose is to secure payments/information from victims by luring them to buy products or services. A variation on this are sellers who use legitimate websites such as eBay or Amazon to advertise as sellers on.
- Fake websites offering goods and services which do not exist: a variation on the former, but in this instance, they impersonate legitimate websites.
- Websites selling counterfeit or pirated goods and services. Some criminals do deliver goods and services, but they are counterfeit or pirated, which in some cases might be of equivalent quality, such as some fake football shirts. A more contested area, as some consumers know they are fakes and seek them out (Wall & Large, 2010).

However, our article focuses largely on the first two categories. While counterfeits are problematic and an important category, those sites selling pirated and counterfeit goods where the seller is highly likely to know are beyond the scope of the current dataset and expose a variety of complex issues, such as some people actually seeking counterfeit goods because they are cheaper, beyond the scope of this paper (Wall & Large, 2010). Nevertheless, it is not possible to completely exclude the counterfeit issue as some victims of online shopping fraud might think they are purchasing a genuine Gucci handbag that turns out to be fake.
The prevalence of online shopping fraud

Using data from a collection of European crime victim surveys, Reep-van den Bergh and Junger (2018, p. 8) found that between 0.6% and 3.5% of the population were victims of online fraud each year, with around 90% covering the purchasing of goods or services online (items paid for but not received). Statistics related to online shopping fraud have grown considerably over recent years and have again escalated as a result of the current COVID-19 global pandemic (Buil-Gil, 2021). Reporting on a field trial back in 2015, Levi, 2016, p. 6) notes that “the most common types of fraud experienced were ‘bank and credit card fraud’ followed by ‘non-investment’ fraud – such as fraud related to online shopping or fraudulent computer calls (28% of incidents).” Research has indicated its increase across a variety of countries, including the United Kingdom (UK; Buil-Gil et al., 2021; Kemp et al., 2021), The Netherlands (Levi, 2016), and China (Lee, 2021).

Specifically in the UK, the most recent available statistics provide an indication of the extent and financial losses incurred because of online shopping fraud. Using data obtained from the Office of National Statistics (ONS), Table 1 provides a breakdown of the types of fraud, and it illustrates how growth in consumer and retail fraud is one of the significant drivers of the overall increase: rising from 0.9 million incidents to over 1.5 million during the same period, a 61% increase, with a 50% increase in the number of victims too.


<table>
<thead>
<tr>
<th>Offense group</th>
<th>Jul 2018 to Jun 2019</th>
<th>Jul 2020 to Jun 2021</th>
<th>Number of incidents % change</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Fraud</td>
<td>3,811</td>
<td>5,035</td>
<td>+32</td>
</tr>
<tr>
<td>Bank and credit</td>
<td>2,641</td>
<td>2,868</td>
<td>+9</td>
</tr>
<tr>
<td>account fraud</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consumer and retail</td>
<td>936</td>
<td>1,510</td>
<td>+61</td>
</tr>
<tr>
<td>fraud</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advance fee fraud</td>
<td>47</td>
<td>365</td>
<td>+677</td>
</tr>
<tr>
<td>Other fraud</td>
<td>188</td>
<td>293</td>
<td>+56</td>
</tr>
</tbody>
</table>

ONS (2022)

In the USA the Federal Trade Commission through the Consumer Sentinel Network has published annual statistics relating to consumer complaints, which include fraud since 1997. This data is based upon reports, so is not as accurate as the England Wales data based upon prevalence surveys. The statistics for the last 3 years are presented in Table 2 related to the total complaints received and those specific to online shopping. It shows both a substantial increase in overall complaints and for online shopping complaints have increased by more than double in a short period.

The Federal Trade Commission has also in the past conducted prevalence surveys relating to consumer fraud, offering more accurate insights into the extent of the problem in the USA. Unfortunately, the last published survey was in 2019 using 2017 data. This did, however, find 4% of adult Americans had “Paid for Something That Was Never Received” and a further 3.9% had experienced “Unauthorized Billing for a Product or
Service Other Than Buyers’ Clubs, Cell Phone Products, or Internet Services” (Federal Trade Commission, 2019a).

The COVID-19 pandemic is also a driver of rising online shopping fraud (and various other types) incidents (UK Finance, 2021). Kemp et al. (2021) examined crime trends associated with specific categories of cybercrime and fraud reported to Action Fraud during the period from April 2017 to July 2020. Their analysis indicated an increase in particular categories, which they attributed to COVID-19 and the associated restrictions and lockdowns put into place. In looking specifically at online shopping fraud, their analysis demonstrated that between March and May 2020 there was a significant increase in online shopping and auction fraud (Kemp et al., 2021, p. 12). In a similar vein, another study found big increases in online shopping fraud and hacking after the first lockdown in the UK in the Spring of 2020 (Buil-Gil et al., 2021, p. 4). Culminating in a prediction that “it is plausible that the rising trend seen in cybercrime since March 2020 may not return to levels recorded before the pandemic” (Buil-Gil et al., 2021, p. 4), but may in fact provide the basis for a continued escalation of cybercrime and fraud offenses.

**Existing research targeting online shopping fraud**

In the relatively small body of research on individual fraud victimization (in comparison to other volume crimes), there has been very little scholarship related to online shopping fraud. Some studies have explored vulnerability to consumer fraud at a broader level. In the era before online shopping, Lee and Soberon-Ferrer (1997) investigated consumer fraud using a survey of almost 1000 adults in the USA. They found neither race nor gender as significant in predicting vulnerability, but being older, poor, less educated, and/or living without a spouse were significant factors. Another study of cybercrime in general also noted the perception of seriousness of economic cybercrime (fraud) was not different between men and women, but this changes when psychosociality is considered (bullying, revenge porn etc.), with women being more concerned (Lazarus et al., 2022). In another study of consumer shopping fraud based upon a survey of 2000 American older adults, which also included online, Reisig and Holtfreter (2013), found demographics as not significant predictors of victimization, but that low self-control and that participants who had purchased something after a telemarketing call or an offer through the mail were more likely to be targeted and become victims. Another study by Holtfreter et al. (2008) also found low self-control linked to victimization. Similarly, a study from the Netherlands found low self-control, active online shoppers and those who participated in online forums at greater risk of victimization (Van Wilsem, 2013). Pratt et al. (2010) have also noted how routine activity theory has a place finding increased use of the internet is associated with increased attempts of fraud. A study on consumer fraud in Australia found younger adults were the most likely

| Table 2. Reports to consumer sentinel network USA. |
|-----------------|-----------------|-----------------|
|                 | 2019            | 2020            | 2021            |
| Online shopping and negative reviews¹ | 173,785          | 353,509          | 398,283          |
| Total fraud, identity theft and other | 3,430,000        | 4,870,000        | 5,740,000        |

Consumer Sentinel Network (2022, 2021, 2020)
victims, but that it was one of the crimes older adults were most likely to confront – although at this point not online (the study was in 2002; Muscat et al., 2002). The research also identified active social lives, associated with greater commercial and financial activity as increasing the risk.

The way consumers assess consumer websites has been explored rarely. Grazioli (2004) in a study of MBA students who were directed to two websites, one false, one genuine, found those better at detecting the false one noted fewer deceptive cues than those who were not as good, suggesting they had better knowledge that was applied more effectively i.e. as soon as they noted a deceptive cue it confirmed their suspicions, and they did not search any further. The study also noted:

successful individuals rely on assurance cues (e.g., warranties, seals) and tend to discount trust cues (e.g., customer testimonial), arguably because the former offer information from third parties, or because they pose a legal constraint on the future behavior of the site owners. By contrast, unsuccessful individuals rely more on trust cues and less on assurance cues. (p. 165)

Some studies have highlighted how consumers struggle to understand technical security online. Shah et al. (2014) in a study of online consumers in Malaysia found that the perceived technical security of a website was influenced by the technical features and design of website in place to enhance security. The implications of these findings suggest that if increasing consumer use of websites for shopping is linked to feelings of security, the technical and design features related to promoting feelings of security are very important. Research by Emami-Naeini et al. (2019, May) concerning the purchase of Internet of Things (IoT) devices found consumers struggling to find and understand privacy and security-related information. There is also evidence from wider fraud victimization that over-confidence in capability to detect a potential fraud was linked to increased compliance in falling to scammers (Fischer et al., 2013).

In addition to how online retailers can make shoppers feel safer, there is also a body of research directed at how organizations can use analytics to better detect and prevent online shopping fraud (Carta et al., 2019) and how high-ranking fraudulent websites on search engine listings can be detected (Abbasi et al., 2010; Weng et al., 2018; Zahedi et al., 2015) and how online pricing fraud can be detected (Kim et al., 2013). Other research has explored the wider strategies of retailers to detect potential fraudulent customers (Soomro et al., 2019).

There is also a small body of literature that has touched upon offenders involved in consumer fraud. Aleem and Antwi-Boasiako (2011) have explored auction fraud, setting up an account to sell mobile phones and uncovering the extensive means and fraudulent attempts sellers are confronted with, along with weaknesses in the auction site fraud prevention procedures. There has also been a study of criminal entrepreneurs who sell counterfeits on eBay who found substantial opportunities to sell online were leading to changes in the criminality pursued (Treadwell, 2011).

The limited studies above that have been explored provide the main studies of note relating to online shopping fraud and illustrate the gap in research in this area of fraud. Given the continued rise in victimization, this paper with an analysis of consumer approaches to preventing online shopping fraud is a much-needed addition to overall knowledge. In order to contextualize the actions of individual consumers and their actions, the following section provides an overview and critique of the current prevention messages
disseminated by a range of government and non-government agencies, advocating against online shopping fraud.

The review above shows very little research has been conducted evaluating initiatives to prevent consumer fraud, which might seem strange to some criminological scholars not so closely acquainted with fraud prevention research. However, one recent review of literature on the much broader fraud prevention came to the following conclusion:

This paper is the product of an international search for published studies of real-world interventions to prevent fraud, focused on case studies with indicators of success. The results were meagre. Only 19 projects were included, documented in 24 studies. The majority lacked model scientific controls, adequate pre- and post-intervention periods for data, and only four included financial cost-benefit data. (Prenzler, 2019, p. 93)

Of the studies that were noted, they largely related to credit card fraud, insurance fraud, benefits fraud and online fraud in a broader sense. There is virtually no high-quality evidence evaluating initiatives to reduce consumer fraud.

**Consumer advice for safe online shopping**

One of the most significant tools available in fraud prevention, across both broad and consumer-specific areas, are awareness campaigns. These types of initiatives are designed to educate consumers on the potential risks and to instruct consumers to use risk reducing behaviors, in what crime prevention scholars would call “guardianship” (Button & Cross, 2017; Hollis-Peel et al., 2011). It is very important that the messaging in these campaigns and related strategies is clear, easy to understand and, most importantly, conveys behaviors that would actually reduce the risk of victimization. This section will briefly explore some of this messaging. This is not a systematic review, which is beyond the scope of this article, and in itself warrants another analysis to examine the sheer amount of online consumer advice available online. Rather, this section seeks to critique the quality of the security behaviors that were measured in the results section (see, Table 9) and that the respondents claimed to have used when shopping online. Crucially, it will highlight that some of the advice being issued by consumer protection bodies is in fact potentially unhelpful and outdated. These observations are illustrated using sources not only grounded in academia but also the authors’ own observations.

Before embarking on this journey, however, it is important to acknowledge that there is a broad landscape of actors offering advice to consumers. These actors can be conceptualized using a three-tiered approach illustrated in Table 3. The range of actors covered in this framework encompasses those found in the conventional fraud justice network such as official law enforcement initiatives and private-sector actors (Button et al., 2012; Cross, 2018). It also acknowledges the broad range of voluntary initiatives that seek to contribute to these efforts by issuing their own advice (Button & Whittaker, 2021).

A challenge that these actors face when issuing online consumer safety advice can be attributed to an argument laid down by criminologist Paul Ekblom, which in “many kinds of crime offenders contend against crime prevention in a never-ending arms race” (Ekblom, 2001). This statement arguably holds true in the case of online consumer safety advice, which can often quickly become outdated as new technologies develop that assist offenders or when new opportunities arise for offenders to maximize their returns from
victims (Button et al., 2009; Lea et al., 2009). Before critiquing this advice, it is, however, also worth acknowledging that there is in fact a wealth of useful online consumer safety advice. The Antivirus provider Kaspersky, for example, recommends that consumers should get a temporary credit card for online shopping when they make one-time purchases (kaspersky.com, n.d.). In this instance, the temporary new card number is usually linked to the consumer’s normal credit card account and the seller will only see the temporary card’s details, which is a useful strategy in reducing the damage from both theft and fraud from untrustworthy or unsecured websites. If this occurs, the consumer can disable the card immediately after their purchase has been made, thereby reducing the potential for harm to their account if their details are stolen by either a malicious website or a third-party actor.

By contrast, there are arguably other pieces of advice currently being issued to consumers that have become increasingly less relevant and even outdated, thereby not protecting online shoppers. One example is the case of Secure Socket Layer (“SSL”) certificates, a technology that encrypts the data files and the information sent between a website and its visitors, which is usually displayed in an internet user’s web browser as a locked padlock icon when a website is “SSL secured.” Whilst the SSL certification of a website is useful in deterring “man in the middle” attacks, whereby an attacker attempts to intercept the communication and information exchanged between two parties on a website, its current usefulness in safeguarding online consumers from fraud is arguably negligible. Offenders, in an effort to camouflage their websites in an effort to appear more legitimate, can obtain with relative ease SSL certificates for their fraudulent websites from a variety of hosting providers (see, for example, Namecheap.com, n.d.; godaddy.com, n.d.) for a fee whilst there are also a number of other websites (see, for example, Zerossl.com, n.d.) that claim to offer SSL certificates for free. The usefulness of SSL certificates is further undermined by research from the Anti-Phishing Working Group (“APWG”) which found in its 2<sup>nd</sup> quarter 2021 report that approximately 82% of phishing websites utilized SSL certificates (APWG, 2022). The FBI’s Internet Crime Complaint Center (IC3) has also identified the problem of fraudulent websites using SSL certificates and in a 2019 press release it issued a warning against using their presence as a useful technique in identifying a website’s level of online safety.

Do not trust a website just because it has a lock icon or “https” in the browser address bar (ic3.gov., 2022).

Yet in-spite of the ease at which offenders can purchase and utilize an SSL certificate in their fraudulent e-commerce websites, some law enforcement initiatives and private sector organizations continue to issue advice suggesting that SSL certificates are a useful indicator of a website’s safety. The European Cybercrime Center (“EC3”), for example, uploaded

---

**Table 3. Sources of online consumer safety advice.**

<table>
<thead>
<tr>
<th>Tier</th>
<th>Type of Initiative</th>
<th>Examples of Initiative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1</td>
<td>Public sector law enforcement and consumer protection initiatives</td>
<td>Action Fraud (UK), Scamwatch (AUS), Internet Crime Complaint Center (USA)</td>
</tr>
<tr>
<td>Tier 2</td>
<td>The private sector</td>
<td>ScamAdviser, AVG Technologies, McAfee</td>
</tr>
<tr>
<td>Tier 3</td>
<td>Voluntary Initiatives</td>
<td>Scam Warners, Scam Survivors, Global Cyber Alliance</td>
</tr>
</tbody>
</table>

(Button, Lewis, & Tapley, 2009; Button & Whittaker, 2021; Cross, 2018)
consumer advice on its Twitter account in 2021 entitled “How can I tell if a website is safe for me to shop at?” They recommend that the presence of an SSL certificate serves as a useful “clue” as to what an internet user should look for when identifying a legitimate online shopping website.

The presence of a padlock & HTTPS and SSL protocols (EC3, 2021).

The same statement from the EC3, however, does state that “the padlock symbol alone does not make a website legitimate,” yet it provides no elaboration about what other safety features that readers could look for to help them in identifying whether a website is safe or not (EC3, 2021). In a similar vein, the UK-based internet service provider Plusnet displays similarly unclear advice on its website. On the company’s website, a web page entitled “How to shop safely online” describes some ad-hoc broad online shopping risks ranging from counterfeiting to the issue of making purchases when connected to a public Wi-Fi. A later section on the same web page states its own iteration of online consumer safety advice, which echoes that of the European Cybercrime Center, that the presence of an SSL certificate is “a good indicator of trust and legitimacy on a website” (Plus.net, n.d.). The advice subsequently describes how SSL encryption can be useful in preventing man-in-the-middle attacks; however, it provides no acknowledgment that offenders may now be using SSL certificates on their fraudulent e-commerce websites as a means of assisting in their deception.

A similar problem exists for consumer advice regarding the checking of reviews of websites. Trustpilot, for example, is a well-known website that provides customers with the opportunity to review their online shopping experiences. However, if taking this advice prima facie, there is no acknowledgment that fraudsters can seek to produce fake online reviews to deceive consumers. As Wu et al. (2020) discuss in their literature review of research into online fake reviews, the estimated proportion of deceptive reviews ranges from 16% (Luca & Zervas, 2013), 20% (Shuckert et al., 2015), 25% (Munzel, 2016), to 33.3% (Salehi-Esfahani & Ozturk, 2018). Lawsuits can also provide a useful snapshot into this problem. In 2015, for example, Amazon filed a lawsuit in the US against 1114 unidentified individuals that it claimed were producing fake reviews on the website Fiverr (Gani, 2015). However, in spite of this problem, many organizations continue to advise that consumers should check the reviews pertaining to e-commerce websites, often with little or no acknowledgment that these reviews could also be fake, which is also exemplified in the Australian context. Scambyst (hosted by the Australian Competition and Consumer Commission), states on its web page entitled “Online Shopping Scams” that “the best way to detect a fake trader or social media online shopping scam is to search for reviews before purchasing” (scambyst.gov.au, n.d.). Again, this does not flag the potential for fraudulent reviews. However, some organizations have started to acknowledge this problem. The UK’s Trading Standards has warned consumers in a 2021 press release that trust in online reviews is contributing to the problem of consumer fraud and that approximately one in five people attempt to spot fake online reviews by checking their timing and spacing (nationaltrading-standards.uk, 2021).

The above summary highlights the challenges faced in providing consumers with relevant and effective advice to reduce the likelihood of online shopping fraud victimization. This demonstrates examples where current advice is unlikely to effectively reduce the potential for victimization. Further, many of the current prevention messages and suggested
actions for consumers are somewhat outdated and may not reflect the current techniques used by offenders to deceive consumers. Offenders are constantly evolving in their methods of deception, and the continuing advancement of technology often works in the favor of offenders. Fraud continues to target human vulnerabilities of individuals but is able to use increasing levels of technological sophistication to facilitate its deception. Prevention messaging that focuses on the specifics of technology rather than the higher-level actions of human behavior is always going to struggle to retain its timeliness and relevance.

With this as a foundation, the remainder of the article seeks to assess the types of actions reportedly taken by consumers in an attempt to prevent online shopping fraud, and contrasts these against current prevention advice, and its perceived efficacy based on the above analysis. To do this, the following section provides an overview of the data underpinning this article and the methodological approach taken.

**Method**

To answer the research questions targeting consumer behaviors to prevent online shopping fraud, this article uses secondary data obtained from an initiative called ScamAdviser, operated by the Dutch company Ecommerce Foundation BV. ScamAdviser describes itself as an initiative that “helps consumers making their online shopping decisions by rating websites” (scamadviser.com, n.d) from over 40 data sources. It applies an algorithmic trust score to each website in its database according to the “IP address of the web server, the availability of contact details on the website, the age of the URL, ratings on review sites and much much more” (scamadviser.com, 2022). As well as providing these trust scores, ScamAdviser also invites those using its website to participate in a range of surveys on topics related to scams.

The current article uses the results of one of these surveys, entitled “Why do consumers get scammed or not.” The online survey was disseminated through the ScamAdviser website and was live for the four-week period from the 7th August 2021 until the 7th September 2021. The survey link was available on the ScamAdviser website and those who were visiting the site were invited to complete it. The deidentified results of this survey were requested by one of the authors (Whittaker) and subsequently approved and received by the research team. An ethics exemption was granted by the University of Portsmouth (#ETHICS-10364) for the use of the current dataset.

**The data**

The results of the survey were provided to the research team in the form of an Excel spreadsheet. A total of 4,304 deidentified responses were received. Each survey response included the following information: participant background information (four questions), questions that broadly correspond to their experiences of consumer fraud in the last year (eight questions), as well as questions that broadly asked the respondents about the reporting of scams and their perception of law enforcement efforts in tackling online consumer fraud (four questions).

Survey data was examined to understand the relationship between self-reported loss of money in online fraud and various demographic factors and other items. The original ScamAdviser survey data (n = 4,304) was first checked, and a number of responses were
selected for exclusion on the basis that either (1) the respondent indicated that they were under the age of 18 or (2) the answers provided within a response were contradictory. Most identified contradictions occurred because responses to multiple-answer questions were contradictory, leaving an unclear picture of the respondent’s behavior. Three multiple-answer questions containing contradictory results were:

- “In the last year, what types of scams were you confronted with? (Select all that apply)”
- “If you were targeted by scams in the last year – As a consequence, which of the following happened?”
- “Which methods do you use to check if a website is legitimate or a scam?”

In all cases, a result was considered contradictory only if they both claimed they had not met the requirement for the question (had not encountered a scam, had not suffered a loss from a scam, or never checked a website’s legitimacy) and provided another answer for the same question. Other responses were considered contradictory for answering under one question that they lost money as a result of a scam, and then under a follow-up question asking how this occurred answering that they had not fallen for a scam. In total, 826 responses were excluded, leaving a revised sample of 3,478 survey responses. It is on this sample that the following analysis is conducted.

An overview of the sample

Table 4 shows a demographic overview of our sample. Respondents were drawn from 154 different countries in total. The most common origins were the United States (931, 27%), India (260, 7%), the United Kingdom (188, 5%), Australia (183, 5%), South Africa (164, 5%), Canada (121, 3%), the Philippines (82, 2%), Pakistan (73, 2%), Indonesia (71, 2%), and Nigeria (53, 2%), with other nationalities each accounting for 1% or less of the total response. Of the total 3,478 survey results used for the current analysis, a total of 2,004 respondents (58%) were men, with 1,258 (36%) being women. There were 32 “Other” responses, and 184 (5%) either did not answer the question (78) or answered that they would prefer not to say (106). The survey originally included age ranges from under 18, but these responses were excluded from the analysis as described above.

Results

The survey results can be grouped around two main themes, one being previous victimization to online fraud, and the second being actions taken to prevent online fraud. Each of these is presented in turn.

Online fraud victimization

Of the total 3,478 survey responses, 1,317 participants (38%) indicated that they had lost money as a result of an encounter with online fraud. A total of 1,529 (44%) indicated that they had suffered no harm, while 337 (10%) indicated that they had suffered harm through data loss, 146 (4%) reported an experience of extortion, and a further 90 (3%) indicated they had been forced to take part in illegal activities. Sampling bias is particularly relevant when
considering these victimization rates – our sample is drawn from visitors to an anti-fraud website and so might be expected to substantially overestimate fraud victimization relative to a general population survey.

Regarding the form of fraud encountered, participants reported a variety of common scams, as broken down in Table 5. Participants were able to report encountering multiple fraud formats, and where they reported losing money it is not possible to be certain which of the encountered formats were responsible for this loss. However, certain results are suggestive: the category with the highest proportion of respondents also reporting losing money was that of non-delivery fraud, a form of fraud particularly targeted at online shoppers. The receipt of inferior products is a category also targeted at shoppers and also had high rates of loss. Overall, 36% of the participants encountered these fraud formats targeted at online shoppers.

Demographics of gender, age and education may be expected to have some relationship with reported loss. Table 6 shows the breakdown of the relationship between gender and monetary loss. Respondents answering “Prefer not to say” (or not answering) appear significantly less likely to report a monetary loss, though the interpretation of this result is not straightforward: respondents so identified may be in general less willing to provide information within the survey, including about losses. Once accounting for multiple comparisons, no age group and no education level was found to be significantly more or less likely to report monetary loss because of online fraud.

In seeking to ascertain possible explanations for victimization, one survey item asked participants “If you were involved in a scam, what was the main reason this happened? Please select the single most appropriate answer.” Table 7’s tabulation of the responses from the participants who reported losing money reveals that the dominant explanation (44%) was that the realization came “too late” in the scam. The second-most-common answer (20%) was that they lacked the knowledge to identify the form of fraud they encountered. These

---

**Table 4. Demographics of respondents to the survey.**

<table>
<thead>
<tr>
<th>Demographic</th>
<th>Responses</th>
<th>% of sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>3,400</td>
<td>98%</td>
</tr>
<tr>
<td>Man</td>
<td>2,004</td>
<td>58%</td>
</tr>
<tr>
<td>Woman</td>
<td>1,258</td>
<td>36%</td>
</tr>
<tr>
<td>Other</td>
<td>32</td>
<td>1%</td>
</tr>
<tr>
<td>Prefer not to say</td>
<td>106</td>
<td>3%</td>
</tr>
<tr>
<td><strong>Age Group</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18–24 years old</td>
<td>340</td>
<td>98%</td>
</tr>
<tr>
<td>25–34 years old</td>
<td>593</td>
<td>17%</td>
</tr>
<tr>
<td>35–44 years old</td>
<td>625</td>
<td>18%</td>
</tr>
<tr>
<td>45–54 years old</td>
<td>618</td>
<td>18%</td>
</tr>
<tr>
<td>55–64 years old</td>
<td>555</td>
<td>16%</td>
</tr>
<tr>
<td>65–74 years old</td>
<td>516</td>
<td>15%</td>
</tr>
<tr>
<td>75 years or older</td>
<td>105</td>
<td>3%</td>
</tr>
<tr>
<td><strong>Education Level</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefer not to say</td>
<td>273</td>
<td>8%</td>
</tr>
<tr>
<td>No schooling</td>
<td>94</td>
<td>3%</td>
</tr>
<tr>
<td>completed to 8th grade</td>
<td>36</td>
<td>1%</td>
</tr>
<tr>
<td>High school</td>
<td>927</td>
<td>27%</td>
</tr>
<tr>
<td>Vocational training</td>
<td>590</td>
<td>17%</td>
</tr>
<tr>
<td>Bachelor’s degree</td>
<td>1,014</td>
<td>30%</td>
</tr>
<tr>
<td>Master’s degree</td>
<td>382</td>
<td>11%</td>
</tr>
<tr>
<td>Doctorate degree</td>
<td>71</td>
<td>2%</td>
</tr>
</tbody>
</table>
Table 5. Respondents’ experience of different types of scams (n = 3283).

<table>
<thead>
<tr>
<th>Scam Format</th>
<th>Responses (% of sample)</th>
<th>Lost Money (% of category)</th>
<th>% of those who lost money overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Attempts to gain your personal information (phishing)”</td>
<td>1314 (37%)</td>
<td>373 (28%)</td>
<td>28%</td>
</tr>
<tr>
<td>“(Cryptocurrency) Investments”</td>
<td>937 (26%)</td>
<td>503 (54%)</td>
<td>38%</td>
</tr>
<tr>
<td>“I was promised money (inheritance, lottery, etc.)”</td>
<td>884 (25%)</td>
<td>303 (34%)</td>
<td>23%</td>
</tr>
<tr>
<td>“I ordered a product that did not arrive”</td>
<td>799 (23%)</td>
<td>481 (60%)</td>
<td>35%</td>
</tr>
<tr>
<td>“I received a fake or inferior product/service”</td>
<td>753 (22%)</td>
<td>344 (46%)</td>
<td>26%</td>
</tr>
<tr>
<td>“I was involved in a dating or romance scam”</td>
<td>341 (10%)</td>
<td>161 (47%)</td>
<td>12%</td>
</tr>
<tr>
<td>“Fake charities”</td>
<td>435 (13%)</td>
<td>145 (33%)</td>
<td>11%</td>
</tr>
<tr>
<td>“I have received threats or been extorted”</td>
<td>325 (9%)</td>
<td>123 (38%)</td>
<td>9%</td>
</tr>
</tbody>
</table>

results, taken together, indicate that by their own diagnosis victims could in many cases benefit from being better informed about online fraud, either in general or as situated prompts early in the online fraud encounter.

One possible explanation for self-reported financial loss may be self-reported confidence, assessed by the item “To what extent are you confident that you would be able to identify a scam if you came across one?.” Table 8 shows the relationship of confidence with monetary loss. The items are negatively correlated (Spearman’s $\rho = -0.21$), with more confident participants being less likely to report having lost money to a scam. As individual levels, “Not at all,” “Not very” and “Very” confidence levels significantly differed from the overall sample population in terms of victimization rate. Despite this, the pervasively high levels of confidence in self-report mean that 59% of all loss reports come from users who are either “Fairly” or “Very” confident they could identify a scam.

**Consumer actions to prevent online shopping fraud**

Participants were also asked about the methods they use to identify a website as legitimate or a scam, selecting all methods they used. The results are presented in Table 9 and represent our most direct measure of respondents’ understanding of fraud. Nearly half of the respondents who lost money (and a similar proportion of all respondents) will check the reviews hosted on a website itself to determine whether or not the same website is a scam – this is the most common verification method reported, more common than the use of

Table 6. Gender and monetary loss (n = 3400). Uncorrected P-values from the exact binomial test with significance determined by $p < .05$ after Bonferroni correction for multiple comparison.

<table>
<thead>
<tr>
<th>Gender</th>
<th>Responses</th>
<th>Lost Money(% of category)</th>
<th>% of those who lost money overall</th>
<th>Uncorrected p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA/Prefer not</td>
<td>184</td>
<td>39 (21%)</td>
<td>3%</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>Other</td>
<td>32</td>
<td>6 (19%)</td>
<td>&lt; 1%</td>
<td>0.027</td>
</tr>
<tr>
<td>Man</td>
<td>2004</td>
<td>754 (38%)</td>
<td>57%</td>
<td>0.836</td>
</tr>
<tr>
<td>Woman</td>
<td>1258</td>
<td>518 (41%)</td>
<td>39%</td>
<td>0.016</td>
</tr>
</tbody>
</table>
external reviews (32%), and seems to expose a widespread lack of understanding about the ease with which fraudsters can generate falsified social proof. Many subgroups differed significantly from the overall victimization rate of 38%, the majority of these differences being associated with lower victimization rates. The only subgroup of respondents that were significantly more likely than the sample average to lose money to online fraud were those who reported that they never check if a website is legitimate (73% of this group lost money). The subgroup least likely to lose money (26% lost money) were those who reported using the rule “if it looks too good to be true . . .” Some methods associated with lower victimization rates are surprising: checking for an SSL certificate, for example, rarely provides any information about whether a site is a scam. It is possible that reports of using such methods reflect a greater familiarity with security advice in general, rather than a direct relationship to preventing victimization.

The top two most common self-protective methods both involve checking reviews, suggesting that participants place trust in crowdsourced opinion. Unlike checking reviews on a site itself, checking external sources of reviews was associated with a significantly lower rate of self-reported loss. While these can also be faked by fraudsters, external reviews are at least more difficult to fabricate than reviews on a platform controlled by the fraudsters, and checking external sites may expose real reviews raising alarm. The methods used least often were those which involved moderately effortful online search queries – reverse image searches, checking company registries, searching for duplicated text, or identifying a VOIP number. These require additional skills or patience, and their modest uptake even in this sample of anti-fraud site visitors suggests that the role of such services is necessarily limited. Interestingly, however, a company’s visibility on social media was checked more often, suggesting that web users find this form of background check more approachable, and social media companies may have a role to play in preventing fraud even when this takes place outside of their platform.

### Table 7. Self-diagnosis for victimization among those who lost money (n = 1,223).

<table>
<thead>
<tr>
<th>Self-diagnosis</th>
<th>Responses</th>
<th>% of lost</th>
</tr>
</thead>
<tbody>
<tr>
<td>“I did not identify the scam until it was too late”</td>
<td>579</td>
<td>44%</td>
</tr>
<tr>
<td>“I lacked the knowledge to identify the scam”</td>
<td>260</td>
<td>20%</td>
</tr>
<tr>
<td>“I was attracted by the lure of money”</td>
<td>161</td>
<td>12%</td>
</tr>
<tr>
<td>“I suspected it was a scam, but I chose to risk it”</td>
<td>149</td>
<td>11%</td>
</tr>
<tr>
<td>“The scammer forced me to send them money”</td>
<td>74</td>
<td>6%</td>
</tr>
</tbody>
</table>

### Table 8. Respondents’ confidence in scam detection (n = 3,316).

<table>
<thead>
<tr>
<th>Confidence in scam detection</th>
<th>Responses(% of sample)</th>
<th>Lost Money(% of category)</th>
<th>% of those who lost money over all</th>
<th>Uncorrected p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all</td>
<td>127 (4%)</td>
<td>70 (53%)</td>
<td>5%</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>Not very</td>
<td>575 (17%)</td>
<td>342 (59%)</td>
<td>26%</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>Don’t know</td>
<td>257 (7%)</td>
<td>114 (44%)</td>
<td>9%</td>
<td>0.034</td>
</tr>
<tr>
<td>Fairly</td>
<td>1539 (44%)</td>
<td>558 (36%)</td>
<td>42%</td>
<td>0.198</td>
</tr>
<tr>
<td>Very</td>
<td>818 (24%)</td>
<td>224 (27%)</td>
<td>17%</td>
<td>&lt; 0.001</td>
</tr>
</tbody>
</table>
Table 9. Respondents’ scam detection methods (n = 3250). Uncorrected P-values from the exact binomial test with significance determined by p < .05 after Bonferroni correction for multiple comparisons.

<table>
<thead>
<tr>
<th>Method</th>
<th>Responses (% of sample)</th>
<th>Lost Money (% of category)</th>
<th>% of those who lost money overall</th>
<th>Uncorrected p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>“I check for reviews on the website itself”</td>
<td>1661 (48%)</td>
<td>639 (38%)</td>
<td>49%</td>
<td>0.613</td>
</tr>
<tr>
<td>“I check for reviews on other websites”</td>
<td>1434 (41%)</td>
<td>420 (29%)</td>
<td>32%</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>“I use the rule ‘if it is too good to be true’”</td>
<td>1214 (35%)</td>
<td>314 (26%)</td>
<td>24%</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>“I check for spelling/grammar errors”</td>
<td>1161 (33%)</td>
<td>316 (27%)</td>
<td>24%</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>“I check whether you can pay with Credit Card/Paypal”</td>
<td>778 (22%)</td>
<td>255 (33%)</td>
<td>19%</td>
<td>0.003</td>
</tr>
<tr>
<td>“I check if there is a phone number”</td>
<td>750 (22%)</td>
<td>249 (33%)</td>
<td>19%</td>
<td>0.008</td>
</tr>
<tr>
<td>“I check if the company is also active on social media”</td>
<td>662 (19%)</td>
<td>206 (31%)</td>
<td>16%</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>“I verified if there is a valid SSL certificate”</td>
<td>583 (17%)</td>
<td>162 (28%)</td>
<td>12%</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>“I check if the email address is free”</td>
<td>559 (16%)</td>
<td>144 (26%)</td>
<td>11%</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>“I ask friends/family”</td>
<td>536 (15%)</td>
<td>214 (40%)</td>
<td>16%</td>
<td>0.328</td>
</tr>
<tr>
<td>“I check company registries”</td>
<td>481 (14%)</td>
<td>162 (34%)</td>
<td>12%</td>
<td>0.060</td>
</tr>
<tr>
<td>“I do a reverse image search”</td>
<td>457 (13%)</td>
<td>127 (28%)</td>
<td>10%</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>“I check for copied text on the website”</td>
<td>387 (11%)</td>
<td>111 (29%)</td>
<td>8%</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>“I never check if a website is legitimate or a scam”</td>
<td>235 (7%)</td>
<td>171 (72%)</td>
<td>13%</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>“I check if the phone number is a VOIP number”</td>
<td>226 (6%)</td>
<td>74 (33%)</td>
<td>6%</td>
<td>0.115</td>
</tr>
</tbody>
</table>

Respondents were also given the opportunity to provide a qualitative “comment” for how they check the legitimacy of a website. A small number of respondents elected to leave comments, and after excluding those which were either ineligible or too vague and incomplete to interpret, a total of 21 comments were selected for further consideration as they provided some additional insight into how the study’s participants sought to conduct their due diligence on websites. One account, provided by a woman aged 65–74 years from Australia, who in a previous response indicated “she did not identify the scam until it was too late” stated that she had previously only sought to check websites on two occasions, which was in both cases after making the purchases. The respondent’s justification was that she had never experienced online shopping fraud before, which she claimed had subsequently resulted in her becoming complacent. The reported loss in this instance was “about $200 AUD,” described in a previous response on the survey.

On both these occasions I have only checked after the event. Most of the time things I have ordered have not had a problem so I guess I was lulled into a false sense of security!

Another female respondent, also aged 65–74 and from the United States, claimed to have lost $133 USD. Her response indicated that a perceived desperation was the main factor in why she was defrauded, that her hair was thinning, and she needed a product, which meant she did not undertake any checking of the website’s legitimacy.

I didn’t check because it looked real. My hair is thinning and I was desperate.
Among the responses were two respondents who appeared to rely on warnings from antivirus software providers as a means of determining the legitimacy of websites. One of the respondents, a male aged between 45 and 54 years old from Germany, claimed to use Norton Web Secure to check whether websites are legitimate before electing to sign up to them.

I check websites with Norton Secure Web before I register.

Finally, one female respondent aged 45–54 years old from Australia, who claimed to have received products that did not arrive and received inferior products, as well as having donated to a fake charity, stated that as a result of her victimization she no longer makes payments for products and services that advertise offers on Facebook.

I’m done clicking on the groovy offers on Facebook for things like pet products and fake charities.

In combination, the above results present an overview of known victimization statistics, as well as individual perceptions of what contributed to victimization. It also highlights the actions taken by respondents to protect against fraud victimization. With this as a foundation, the following section aims to locate these results in the wider context of fraud and consumer awareness messaging.

Discussion

The COVID-19 pandemic has provided the foundations for increased consumer shopping online and, accompanying that, substantial increases in fraud (Federal Trade Commission, 2022). Given the significant proportion of fraud that occurs in a consumer context, it is surprising how little academic research has been conducted on this problem (Van Wilsem, 2013). This article has sought to initiate what should be an ongoing research program to further explore and understand the complexities of online shopping fraud. The data available is by no means comprehensive, but it does allow for an outline of the problem. Our key finding is that in a sample with a high overall victimization rate (38%), many participants have a poor understanding of the efficacy of preventative measures. Of the participants in this survey, some 36% have encountered a form of fraud related to online shopping, and of those over half lost money to some form of fraud – though due to the survey design we cannot be sure they lost money to the online shopping fraud specifically. Victimization is for the most part not affected by sociodemographic characteristics, and in contrast to prior work we find that confidence in scam detection is negatively correlated with losses. Responses indicate that, despite the sample being drawn from visitors to an anti-fraud website, many participants make use of ineffective (or even no) methods to protect themselves from online fraud of all forms, and by their own diagnosis those who lost money suffer from a lack of knowledge about fraud, either in general or in the moment, with the identification of fraud coming “too late.” The literature reviewed earlier in this paper noted several studies that have highlighted the relevance of routine activities theory, which naturally leads to a situational crime prevention solution (Holfreter et al., 2008; Mears et al., 2016; Pratt et al., 2010). Increasing guardianship, assisting compliance posting instructions that are achieved through campaigns and education among others, are significant strategies in the 25 techniques of situational crime prevention that have been
commonly advocated by crime prevention scholars and practitioners (Smith & Clarke, 2012). Such frameworks of prevention applied to fraud have been under-developed and utilized (Button & Cross, 2017). The current summary of consumer protection advice as it relates to online shopping fraud highlights the inadequate guidance provided to consumers in some contexts to reduce their risk of consumer fraud victimization. While the current analysis does not allow for a determination of how this advice influences the actions of individuals, it is argued that there is a need to better promote effective and relevant messaging to consumers, which takes into account current offending practices. There is also a need to acknowledge that the presence of certain indicators does not guarantee the legitimacy of a site and promotes the use of critical thinking to assess situations on a case-by-case basis. This should be a clear priority for policy makers to develop clear, concise and up to date guidance that is then used as the norm by any legitimate website offering advice.

In terms of the current analysis, the article set out to answer two research questions.

(1) What actions and behaviors do individuals report undertaking to prevent online shopping fraud?

The data presented clearly show that many respondents used inadequate strategies to reduce their risks of becoming victims of online shopping fraud, which may be linked for some to the low self-control noted as a risk factor in several studies (Holtfreter et al., 2008; Reisig & Holtfreter, 2013). The common use of inadequate strategies arises despite our sample being drawn from visitors to an anti-fraud website, who as a population might be expected to be more engaged in protective behaviors than the general public. Most importantly, those who never check whether a website is legitimate were also most likely to lose money to fraud. That a substantial number of respondents reported an utter lack of self-protective behavior illustrates that not only must good advice be articulated, but campaigns need to be developed to change the behavior of consumers, so they actually do more to reduce their risk. Such a campaign requires the active engagement of consumers, and this arguably poses an even bigger challenge. It is one thing to get the right advice in places where consumers might read it, it is another to get them to act on it. A key hurdle is that individuals often do not believe they could be victims and believe they are not susceptible to these types of incidents (Button and Cross, 2017; Cross, 2015). Messaging that punctures this belief could be an important priority for future interventions.

(2) What, if any, disconnect exists between prevention messaging and effective self-protective consumer behavior?

For those who did employ the use of protective measures, several were of questionable relevance in their ability to prevent victimization. For example, checking for product reviews hosted on the website in question – the most commonly reported protective behavior – is not likely to be an effective means of identifying a fraudulent site. Offenders are able to create sophisticated websites, which imitate the look and feel of genuine online retailers, which includes the creation of fake reviews to support their overall guise and promote the appearance of legitimacy. However, online shoppers are faced with a variety of purchasing situations that imply potentially different levels of (deserved or undeserved) trust in the manufacturer, vendor, online retail platform and payment processor involved in
their purchase. Future research should aim to disentangle the differing targets of self-protective behaviors in online shopping and identify mismatches between the targets and the practical effects of protective behavior. Prevention messaging could also benefit from this disentanglement – clearer communication about which parties in an online transaction can pose risk to consumers may help consumers more easily identify whether advice is likely to be effective or ineffective.

Limitations

It is worth acknowledging that the current dataset is not without limitations, particularly given the extensive and rigorous cleaning process outlined previously. As with many surveys, the current sample comprises a group of individuals who self-selected its completion and who self-reported that they were victims. In this way, the survey is not representative of any country or any particular population nor have the victims (as would be the case in an official report) been subjected to any scrutiny as to whether the facts of their case warrant victim status. Being drawn from visitors to an anti-fraud website, the sample may be expected to have an unusually high victimization rate and awareness of fraud-related topics. The sample is also comparatively young and well-educated, with 84% under the age of 65 and 42% having a Bachelor’s or higher degree, tending to increase our expectation of awareness.

Second, no steps were taken to verify any of the details provided in the survey. While steps were taken (as outlined above) to remove responses that were obviously contradictory in nature, the data received was taken at face value. It is therefore reliant upon the ability of individual consumers to accurately report their actions and any victimization experienced.

Third, limited direction was given in the completion of the survey, particularly as it relates to the definition of concepts used in the survey. In this way, those who completed the survey may have interpreted the survey differently to what was intended, and again differently to how we have analyzed the results.

Fourth, the level of data varied in terms of its detail and quantity. Not all questions were mandatory, meaning that respondents chose whether they were comfortable to respond. Further, for the open-ended questions, respondents chose the level and type of detail they wished to disclose.

While the above is important to note, the data is still argued to provide an important initial insight into online shopping fraud and associated protective behaviors used by consumers in their attempts to prevent this, at a global level. Given the limited research to date, which has explored online shopping fraud and associated consumer behavior and victimization, the current dataset provides key insights that enable a future program of work to be initiated.

**Conclusion**

Consumer behavior has been changing over the last 20 years, and the associated increased risks of fraud with the movement online, amplified by the pandemic, do not look likely to decline in the short or medium-term. Consumers well versed in the risks to themselves of entering shops, answering the telephone, and responding to paper-mail are having to learn – often the hard way – how to protect themselves online when shopping. This article has shown that some consumers may not be served well by the advice they are given, and many do not use appropriate behaviors to reduce their risk. The scale of the problem
illustrates the need for more research on this problem, more prevention schemes to be implemented and for those to also be properly evaluated to determine if they actually work. Overall, the analysis suggests the need to focus on prevention messaging as it relates to online shopping fraud. Existing research provides for limited examples of current programs to target fraud (Prenzler, 2019). As part of this, there is evidence of initiatives to change the behavior of persons to reduce their risk exposure to fraud and related crimes, but it is rare and an area in need of further evaluative research (Mears et al., 2016). Cross (2016) has illustrated how targeting probable victims sending monies to West Africa using financial intelligence can yield results in fraud reduction. Kumaraguru et al. (2007) has shown how targeted training can reduce people falling for phishing attempts. Ultimately, more initiatives need to be tried and evaluated using rigorous research approaches and consumer fraud would seem to be a priority area (Sherman et al., 1997).

Notes

1. This includes undisclosed costs, failure to deliver on time, non-delivery, and refusal to honor a guarantee on purchases made online (not including auction sales); businesses trying to prevent people from giving honest reviews about products or services they purchased.
2. The responses in Table 9 are limited in that they do not cover all of the security behaviors that a consumer can take when shopping online. Therefore, the discussion in this section is confined to the survey’s design.
3. The categories of scams used by ScamAdvisor in the survey were not ideal from the researchers’ perspective, but the important categories of “I ordered a product that did not arrive” and “I received a fake or inferior product/service” were appropriate for consumer fraud, which is the focus of this paper.

Acknowledgments

The authors would like to thank Jorij Abraham, CEO of ScamAdviser, for providing access to the initiative’s data.

Disclosure statement

The authors report there are no competing interests to declare.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID

Jack Mark Whittaker http://orcid.org/0000-0002-3669-9066
Matthew Edwards http://orcid.org/0000-0001-8099-0646
Cassandra Cross http://orcid.org/0000-0003-0827-3567
Mark Button http://orcid.org/0000-0002-4169-2619
References


EC3. (2021). How can I tell if a website is safe for me to shop on? Retrieved 22 June 2022, from https://twitter.com/EC3Europol/status/1463447306317877248


doi.org/10.1016/j.ijinfomgt.2013.10.001 Evidence 1080/10941665.2015.1029954


