Impact Of Habit On Online Fraud Mitigation

Kevin Kurniawan[1], Bonnie Soeherman[2]

Magister Akuntansi, Pascasarjana, Universitas Surabaya, Surabaya, Indonesia[1,2]

Abstract. *User habits and their use of online mediums can make a bit difference, since the cyberspace is full of opportunities, as well as risks. Carelessness, especially in terms of data storage, information, and financial practices can lead to irreparable damages. The present paper provides a comprehensive overview of how the digital space has changed and how criminals take advantage of the vulnerabilities of internet users. This paper makes use of scholarly and journal articles to establish its arguments as well as crucial information from our informants. The first section outlines the risk behavior and habits of users that invite cybercriminals and increase the threat of intrusion and data leak. The next section is dedicated to the detailed analysis of habits that can help users in prevent the crimes and mitigate their consequences. A set of recipes is provided in the end of our analysis with can help people to mitigate the risk of online fraud. By having habits like professional sceptism, good judgement, and running lean in mind, hopefully people will have better way to mitigate the risk of online fraud than having nothing.*

Keywords. *Habit; Online fraud; Risk Mitigation.*

Abstrak. Kebiasaan dari seseorang dan pemakaian platfom online yang mereka gunakan dapat membuat perbedaan yang cukup signifikan mengingat bahwa dunia online di luar sana memiliki banyak sekali kesempatan (*opportunities*) dan juga risiko-risiko yang dapat timbul. Kelalaian terutama di dalam pengolahan penyimpanan data, informasi, maupun pemakaian data finansial di *online platform* dapat menyebabkan kerusakan yang sangat besar. Penelitian ini memiliki tujuan untuk memberikan sebuah pengamatan berupa analisis komprehensif mengenai bagaimana sebuah dunia digital telah berubah yang mengakibatkan para kriminal mengambil kesempatan dari para pengguna internet yang rentan untuk diserang. Pembahasan akan dimulai dengan bagaimana efek dari *risk behavior* dan *habit* dari seseorang dapat "mengundang" para penjahat *cybercriminal* untuk meretas data mereka maupun menimbulkan adanya kerusakan. Pembahasan selanjutnya akan membahas bagaimana perubahan *habit* dari seseorang dapat membantu untuk mencegah kriminal *online* dan memitigasi konsekuensi yang timbul. Beberapa pola kebiasaan disediakan pada akhir penelitian ini dengan harapan dapat membantu seseorang meminimalisasi risiko penipuan *online*. Dengan memiliki *habit* seperti *professional sceptism*, *good judgement*, dan *running lean*, diharapkan agar para pengguna memiliki cara yang lebih baik untuk menimalisasikan risiko penipuan *online* dibandingkan tidak memiliki apa-apa.

Kata Kunci. *Habit; Online fraud; Risk Mitigation.*

Corresponding author. E-mail: kevinkurniawan35@yahoo.com[1], bee7179@gmail.com[2]

How to cite this article. Kurniawan, K., & Soeherman, B. (2021). Impact Of Habit On Online Fraud Mitigation. *Jurnal Riset Akuntansi dan Keuangan, 9*(3), 435–444.
History of article. Received: Agustus 2021, Revision: Oktober 2021, Published: Desember 2021
Online ISSN: 2541-061X.Print ISSN: 2338-1507. DOI: 10.17509/jrak.v9i3.32182

INTRODUCTION

Internet and digital technology have resulted in a shift of habits, as people have started relying more on online platforms to carry out various operations like data storage, communication, and financial transactions (Varghese et al. 2011). However, this change in online behaviours and habits has given rise to certain risks in which fraudulent activities are the most prevalent (Forsythe ad Shi, 2003). Credit card frauds, identity theft, and virus attacks are among the several forms of fraud that can ruin the online experience of the users and cost them a lot of money. These activities often go undetected and, hence, unprosecuted (Davinson & Sillence, 2010). This is the reason why user privacy and security are two of the major concerns when it comes to internet applications, especially e-commerce (Chen, Su, & Hung, 2011). The present paper presents an analysis of the behaviour of users regarding their use of the internet and other forms of digital technologies (Davinson & Sillence, 2010). The outcomes of this analysis will then be used to identify the role of changed habits in reducing the frequency of online frauds.

The Guardian, a British media outlet, has reported in its latest article about a teenage hacker gang, who earned millions through cyber frauds. The most common means of online frauds committed by these individuals were threating or persuasive text messages. They would pose as tax agencies to convince their victims of their “pending tax” or “debt.” Carlos, a teenager among the gang, was responsible for recruiting and maintaining discipline among the members. According to Carlos, the gang would acquire victim’s phone number to keep it busy with continuous calls so that they could not call their bank to block the account. This would make the transaction easier for the hackers (Mahdhi & Hickey, 2020). The most significant takeaway from this case is how those hackers tapped into their victims’ fears and vulnerabilities to get the job done (Mahdhi & Hickey, 2020).

Growing access to the internet and the availability of various gadgets like smartphones and computers for financial transactions have increased the risk of online fraud. Customers use their credit and debit cards to make online purchases or transfer money to other accounts (Davinson & Sillence, 2010). The information they use to make purchases is often stored in the databases of the company's websites (Yu & Lin, 2013). In the case of unsecured internet connections and events like hacking, data breaches may occur, which ultimately results in credit card fraud (Forsythe ad Shi, 2003).

The younger generation, typically Gen Y and Gen Z, usually rely more on online platforms for both entertainment and other purposes, as compared to other generations (Chen, Su, & Hung, 2011). As a result, they are more likely to expose their personal information on various platforms, especially social media and certain other applications that require access to private data such as photographs and contacts (Atkins & Huang, 2013). However, researchers also believe that the older population is equally, and sometimes more, vulnerable to fraudulent activities since they are unaware of the phishing and scamming techniques of cybercriminals (Castell, 2013). Although the use of the internet for transactions and purchasing is less prevalent in older people, they are more prone to scamming activities due to their trusting nature (Varghese et al. 2011).

Several types of malware are used by cybercriminals to steal from the users; however, most of the time, user activities and habits make the efforts of those criminals successful. Credit card users often neglect to take the necessary precautions due to the zero-liability policy of various credit card issuers and banks (Chen, Su, & Hung, 2011). Here, it is important to note that the zero-liability policy from issuers like MasterCard and Visa is only applicable if the purchase is made using their network. A transaction that is made through any other network is not covered under this policy.

Another common mistake that users make is to use unauthentic websites to purchase items. Well-known websites and retailers like Amazon and eBay have strong network security systems that are capable of keeping the cyber-intruders out. However, less secured and lesser-known retailers and websites are vulnerable to such attacks due to their inadequate security mechanisms (Christin, Yanagihara, & Kamataki, 2010).

Although verified retail platforms reduce the likelihood of cybercrimes and online scams, individual sellers and retail defrauds can also steal from people. These retailers often use attractive coupons and price discounts to target vulnerable and innocent customers and send them counterfeit products and knock-off replicas (Davinson & Sillence, 2010). Through their attractive offers, these sellers can also convince the users to pay them through outside transactions, the ones that are not linked to the website, which are usually untraceable.

The biggest weapon of cybercriminals is their ability to exploit the trust of their targets. Most of these scammers commit fraud by providing “free of cost” offers. For instance, many fake websites offer free credit reports and other services to collect personal information like social security numbers to steal an identity from their targets (Ortlinghaus, Zielke, & Dobbelstein, 2019). Older adults and children are more likely to fall for this bait, usually due to a lack of knowledge of the digital world. The difference in perception about the risk of online fraud among various age groups is the reason why certain groups are more prone to privacy and security breaches as compared to the others (Chen, Su, & Hung, 2011). Vulnerable groups are more likely to perceive scam e-mails and messages as legitimate. Clicking and responding to such e-mails expose their identity and sensitive information to the criminals, which they use to carry out crimes.

Overall, the most common habits of internet users that lead to online fraud and theft include, opening suspicious e-mails and clicking on provided links, downloading malicious attachments and files from insecure sources, connecting to a public hotspot, downloading software from the illegitimate website, visiting certain websites, and accessing internet connections from mobile phones and tablets (Ortlinghaus, Zielke, & Dobbelstein, 2019).

RESEARCH METHODOLOGY

The design of this study, we chose a qualitative research approach and descriptive research to describe the impact of habit on online fraud mitigation. With the help of scholarly, the help of many informants, and journal articles, this research will provide reasonable argument of how to change in habit and risk mitigation on online fraud. Analysis is also provided in the end of this discussion to provide information for user to identify dubious online activities and prevent them before the crimes happens. We provide the list of informants with the information that we got.

Table 1. Informant Table

Informant*	Age	Gender	Use of Internet**	Information
Calvin (C)	20-25	Male	5	1. How often do they access the internet? 2. How do they usually operate the internet? 3. How do they handle the internet? 4. Are there any obstacles from accessing the internet? 5. Have they ever experience the cybercriminal while accessing the internet?
Hendra (H)	40-45	Male	3	
Rosma (R)	25-30	Female	5	
Eni (E)	35-40	Female	2	
Reni (RA)	15-20	Female	4	
Fitri (F)	25-30	Female	4	
Dahmana (D)	15-20	Female	3	
Intan (I)	20-25	Female	5	
Lestari (L)	25-30	Female	3	
Edward (ED)	60-65	Male	2	
Burhan (B)	40-45	Male	1	

**. We mark the initial with () || **. Scale from 1 to 5*

RESULTS AND DISCUSSION

From the standpoint of a cybercriminal, both computers and smartphones/tablets are equally convenient for stealing money through e-mail scams, retail frauds, and website malware. Although numerous antivirus applications are available on the internet, they can only protect the users from a limited range of scams that have been discussed in the paper. User vulnerability against retail and other types of financial fraud can only be reduced through proper education. Knowledge regarding accurate usage of technology can influence positive behaviors and habits among these users, which can reduce the occurrence of unforeseen incidences.

Change in Habits and Risk Mitigation of Online Fraud Mitigation

Poor Judgment

Most of the internet users do not realize the warning signs or choose to ignore security protocols due to lack of awareness (Chen, Beaudoin, & Hong, 2017). They do not realize that the effects of identity theft can be much more deteriorating than a robbery, as they can result in financial loss, threats, damaged reputation, and online harassment (Chen, Su, & Hung, 2011). To avoid such scenarios, it is important to follow cybersecurity practices such as concealing names, number plates, addresses, financial information, ID, and passport number from social sites and other websites (Chen, Beaudoin, & Hong, 2017). Training is necessary to make the individual vigilant about the security of their online networks. According our informants' (ED, F, E, B) point of view, security protocols are not something that they familiar with. In fact, when accessing the internet, they usually ignore the importance of private data like mother's given name, date of birth, address, and any personal or private information because they lack the knowledge of how importance and crucial those data.

It is often difficult to differentiate between legitimate and fraud sites, which is why, it is important to refrain from entering information like e-mails, birthdates, middle names, etc. Most legitimate sites only ask for a little information like an e-mail address for tracking their potential and current visitors (Chen, Beaudoin, & Hong, 2017). On the other hand, the hackers and criminals behind malicious sites prey trick vulnerable visitors into entering information that can be used to exploit them later.

Password Protection

A weak password is among the factors that cause the greatest number of fraud and data breaches. Weak and small passwords are extremely easy to hack, given the recent advancements in technology and hacking software (López et al, 2019). Users often set passwords that can be traced easily through online research such as birthdates, names of loved ones, etc. In fact, 90% of our informants told us that they tend not to change their passwords because it is hard for them to keep remembering one password into another. Some of them are also bragging of how difficult the minimum requirement of password from certain sites that are getting harder and more complex from time to time. This is why; users need to make a habit of using strong and highly randomized passwords with a complex combination of different letters, symbols, and numbers (Davinson & Sillence, 2010).

Similarly, reusing the same password for multiple online accounts can make it extremely easy for criminals to crack them at once. This practice results in severe damage, especially in the case of financial accounts and applications (López et al, 2019). It is important to build a habit of changing the password after a while and keeping them as strong and random as possible. A vigilant mindset is necessary to take all the precautions needed to prevent internet criminals from exploiting sensitive information.

Two-factor authentication provides an extra level of security to user accounts (López et al, 2019). This security protocol requires a password as well as the second type of authentication, mainly in the form of a one-time password (OTP) or code, to allow access to the account (Chen, Beaudoin, & Hong, 2017). The one-time code is usually generated by the user's device, which makes their account safer and less likely to be intruded (Milne, Rohm, Bahl, 2004). It makes it impossible for other users to access a particular account on a new device without the code.

Staying up-to-date

The best way to avoid online frauds is to stay aware of the types of current and prevalent scams. Knowing the intentions of scammers and their ways to trap the victims can significantly lessen the chances of financial and reputational loss or identity theft (Chen, Su, & Hung, 2011). For instance, scammers often pose as government agents, bankers, computer experts, and social volunteers to retrieve information like credit card or social security numbers (Chen, Beaudoin, & Hong, 2017). As a result, people, who are generally unaware of these techniques, easily give in and reveal sensitive information, which leads them towards several consequences (Yazdanifard et al. 2011).

Another frequent habit of many users is that they often forget or choose to ignore the software update messages that pop-up on their screens (Chen, Su, & Hung, 2011). Although some of our informants usually access the internet all the time, they tend not to update their software because they see “updates” as a pointless job and makes them uncomfortable to imagine the future changes like user interface, the location of icons, terms, etc. These software updates play a huge role in making the device secure from any cyber intrusions, as they often contain revisions for security mechanisms and tend to remove the loopholes in the outdated version of the software (Davinson & Sillence, 2010). Hackers and cybercriminals consider the security flaws in outdated software, also termed as “security vulnerabilities”, as an opportunity to attack the system of their victim. They can easily target the vulnerability by writing a code packaged with malware, which steals data or encrypts the files to take control of the computing system (Chen, Su, & Hung, 2011). These software and security updates also provide security against hackers who tend to steal valuable and personally identified information and use it to commit several crimes. Moreover, a device infected with malware is likely to transfer it to other systems as well, hence, exposing everyone in contact with cyber threats.

Doing Research

Before making a purchase online, it is important to research to identify the credibility of the source/seller and the quality of their products. The easiest way to do so is to use search engines research with keywords like "reviews", "scams", and "complaints" (Buttons et al. 2014). These keywords along with the product and brand's name can help the first-time shoppers to see if there have been many reports of fraud against the website or phone number provided by the seller (Buttons et al. 2014). Consulting an expert or a friend before making a purchase is also a good approach to avoid such scams. From our informants’ point of view, they often doubt many online store with less cridibility. One of informants, C provide us that he tends to view any review, searchs for online information about the store, and tends to buy things from official or verified store with high credibility. Even though some stores with high credibility often makes the price of the good more expensive, C told us that he does not bother with the slighly price change about it and consider it as the price of “genuine” of things.

Public Wi-Fi

Free or public Wi-Fi poses a higher risk of security breaches as compared to password-protected internet connections. Lack of authentication mechanisms in these connections makes them desirable for both the users and the hackers (Maimon et al, 2017). Cybercriminals can easily get access to unsecured devices connected with free Wi-Fi by placing themselves between the connection point and the user (Gupta & Mundra, 2015). As a result, any information that is communicated over the network is sent through the hacker, who can then access important messages and sensitive credentials that can even lead them to user’s personal or business networks (Watts, 2016).

Cybercriminals often provide free Wi-Fi facilities to users to distribute malware, especially when a connected device shares a file over the unsecured network (Watts, 2016). These hackers often trick vulnerable and unaware users into clicking pop-up messages with a software update or download offers, which is another way to introduce malware into the device (Gupta & Mundra, 2015)

For the aforementioned reasons, users must be careful while connecting their devices to public internet connections (Watts, 2016). Users must make a habit of using a virtual private network (VPN) if they use public Wi-Fi, as it encrypts the data and makes it secure from the hackers who tend to go after an easy target (Maimon et al, 2017). A better approach is to turn off the sharing option when the device is connected to open networks and to keep the Wi-Fi off when it is not needed to avoid automatic connections and data transmission with the networks in range.

Considering the cost of internet and the challenge to get signal in the certain urban area, many of our informants provide us that free Wi-

Fi is the only way of them to easily access the internet. In fact, Free Wi-Fi is considered as a "savior" rather than a future threat. From our informants' (C, R, & I) point of view, as an active internet user, they tend not to think the risk of free Wi-Fi and considering free Wi-Fi as the freeway for them for keep accessing the internet. Futhermore, **I** provides us that the benefit from using free Wi-Fi is higher than the unimagine risk from using it. Nevertheless, **I** told us to remind older generation while accessing free Wi-Fi with the risk of cybercriminal in mind.

Taking precautions might decrease the chances of security breaches in open networks; however, public interconnectedness can still be risky (Frantsiyants, 2019). Therefore, users must follow robust security techniques and update their security mechanisms and antiviruses from time to time to avoid new kinds of malware and stealing methods.

Personal E-mail Accounts

It is a common practice to use a single e-mail address to create different accounts on social media, websites, bank accounts, and shopping sites. However, this habit can cause significant damage regarding finances and information breaches in case a criminal successfully hacks the e-mail address (Buttons et al. 2014). Therefore, it is important to secure the e-mail address with strong passwords and two-factor authentication. Considering our informants have more adults than teenagers, some of our informants tend to have one or two e-mail addresses when accessing the internet. From our informants' point of view, we can concluded that using more than two e-mail accounts were rare to have. As the researcher, Kevin and Bonnie also have separate e-mail accounts while one e-mail address for job and the other is for other businesses like shopping, personal e-mail, and other purposes. An even better approach is to create multiple e-mail accounts and assign them for separate purposes (Buttons et al. 2014). Different e-mail addresses for shopping, personal e-mails, work, subscription, and social media accounts can save a user from getting multiple linked accounts hacked all at once (Frantsiyants, 2019).

Recognizing Phishing

Recognizing phishing scams is often difficult since cybercriminals often pose as legitimate and trustworthy institutions and often use logos and headers of legitimate brands to lure the users into giving money and confidential information (Huie et al, 2013). Therefore, users must make a habit of looking for small details in the e-mails or text messages they receive. For instance, phishing e-mails and messages often contain generic information and greetings instead of user-specific information (Harrison, Vishwanath, & Rao, 2016). In such cases, users must contact the company and validate the information they have received through a dubious e-mail (Harrison, Vishwanath, & Rao, 2016). A good practice is to double-check the source every time before entering credit card and banking information online.

Changing Habit Mitigating Risk

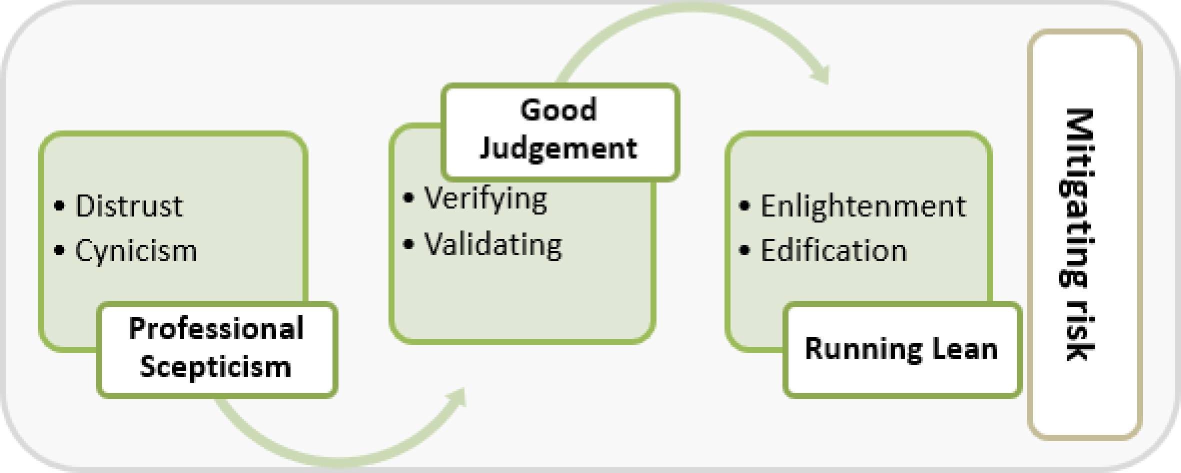

Figure 1. Changing Habit Mitigating Risk

As we discussed it before, the internet is full of uncertainty and unpredictability things. To make up things easily, a set of recipes of how to change habit to mitigate risk is provided in this last discussion. The chart above explained of how a set of habit can be used to mitigate the risk in the internet that will be explained. Following by the first set of recipes, the professional scepticism; a tool to have a scepticism mind when doing things; will resulting a "good judgment behaviour" in the way of thinking and doing every action we do in the internet. With the result of having the two recipes, people is expected to have a new habit that is called "running lean".

The first recipe is to change your habit to become a professional scepticism habit. As the name suggested, professional scepticism is a normal term usually used by auditor to questioning and have a critical assessment of the appropriateness and sufficiency of audit evidence. It's a great habit that can be implemented to our daily activity with the internet. When we are surfing the internet with professional scepticism in mind, we allowed ourselves to have a thoughtful and sceptic mind. All the site we access and all unknown people we met across the internet, will instantly labelled by "suspicious" by us. This "suspicious" label will eventually will be lifted if we find out that is enough evidence to trust this site or people.

Professional scepticism comes with two handy tools, distrust and cynicism. As the word suggest, distrust habit is good when you come across a suspicious thing. The first thing in mind is to distrust anyone you are not familiar with in the internet. Following with distrust, the second tool that come in handy is "cynicism". Although, cynicism term is used to express a disbelief to people because people always hide something in their back; it's a great tool to make ourselves "guarded" with a cynicism habit. For example, when we surfs around in the internet and find an offer from stranger; with these two sets of tool, we immediately will become "on guard". Not to trust and believing that people has bad motivation in their back will make ourselves more and more secure than having a free bird mind.

Having professional sceptic in mind will resulting having a good judgement habit. Basically, with a high amount scepticism, people tend to perceive things more thoughtful and resulting to have a good judgement habit. Like the old people said, "you never know who behind those screens"; when surfing internet or purchasing things, it is better to verifying it first who is the people who we talk to. A good judgement will make people to accept thing when they are already verifying and validating it first. After verifying that the people is a good and secure one, it is time to validating it with other people judgement. Just like perception, judgement tends to have a subjective variable. Therefore, confirming and validating our judgement will resulting a "valid" judgement about things. When purchasing thing on internet, people who has a good judgment will tend to see review first, to see other people comment, and making sure the seller is trusted. Finally, having a good judgement will resulting a secure tag when we are surfing the internet.

Combining these two new habits will resulting a new habit called "running lean". The term running lean is used by Maurya (2012) in his book with the same name. Basically, running lean tell us how to do thing while adjust it with changes. For example, having a good judgement and professional sceptic habit will make us become more caution of how to surf the internet; and little be little we know how to do surf the internet securely. Corresponding with good judgement, people will tend to adjust how the way the surf the internet. Little by little, people will already have enlightenment of how internet works. With that, people will edification themselves of how things should be done in the internet. Therefore, with running lean, good judgement, and professional sceptic in mind; hopefully we have better way to handle internet than having nothing.

CONCLUSION

The availability of better technology and digital spaces has made life easier for many. However, increased dependence on the internet and online activities is also giving rise to increased security risks (Tsang et al. 2014). Cyberspace has become extremely vulnerable to security attacks, data breaches, malware attacks, information leak, and identity and financial theft. While many of these crimes are unable to track and it is virtually impossible to reverse its consequences, users can adopt certain habits to avoid these scams before they happen (Yazdanifard et al. 2011). The present paper outlines the risk behaviours and habits of people that increase the risk of hacking and provide an opportunity for criminals to steal their information, followed by a detailed analysis of the red flags to look for regarding suspicious online activities. The paper also explains various ways and techniques to secure personal and business cyberspaces along with the set of analysis to mitigate risk with the help of habit changing. Professional sceptic, good judgement, and running lean habit will help people to mitigate online fraud for having a good way to surf the internet securely.

REFERENCES

Atkins, B., & Huang, W. (2013). *A study of social engineering in online frauds*. Open Journal of Social Sciences, 1(03), 23.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). *Online frauds: Learning from victims why they fall for these scams*. Australian & New Zealand journal of criminology, 47(3), 391-408.

Castell, M. (2013). Mitigating online account takeovers: The case for education. In Retail Payments Risk Forum Survey Paper (Vol. 27, p. 2015).

Chen, C. S., Su, S. A., & Hung, Y. C. (2011). *Protecting Computer Users from Online Frauds U.S. Patent No. 7,958,555*. Washington, DC: U.S. Patent and Trademark Office.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). *Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors*. Computers in Human Behavior, 70, 291-302.

Christin, N., Yanagihara, S. S., & Kamataki, K. (2010). *Dissecting one click frauds*. ACM conference on Computer and communications security (pp. 15-26).

Davinson, N., & Sillence, E. (2010). *It won't happen to me: Promoting secure behavior among internet users*. Computers in Human Behavior, 26(6), 1739-1747. (Davinson & Sillence, 2010)

Forsythe, S. M., & Shi, B. (2003). *Consumer patronage and risk perceptions of Internet shopping*. Journal of Business Research, 56(11), 867-875.

Frantsiyants, K. (2019). *Online Shopping: The Influence of the Internet on the Transformation of Consumers' Buying Habits and Experiences* (Doctoral dissertation, Empire State College).

Gupta, P., & Mundra, A. (2015). *Online in-auction fraud detection using online hybrid model*. In International Conference on Computing, Communication & Automation (pp. 901-907). IEEE.

Harrison, B., Vishwanath, A., & Rao, R. (2016). *A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing*. In 2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 5628-5634). IEEE.

Huie, S. C., Maguire, L. C., Malo, J. A., Inskeep, T. K., King, D. C., & Shroyer, D. C. (2013). *Phishing redirect for consumer education: fraud detection*. U.S. Patent No. 8,608,487. Washington, DC: U.S. Patent and Trademark Office.

López, A. U., Mateo, F., Navío-Marco, J., Martínez-Martínez, J. M., Gómez-Sanchís, J., Vila-Francés, J., & Serrano-López, A. J. (2019). *Analysis of computer user behavior, security incidents and fraud using Self-Organizing Maps*. Computers & Security, 83, 38-51.

Mahdhi, M., & Hickey, S. (2020). *Six grand and a Rolex: lure of riches sucked me into online fraud*. Retrieved 7 October 2020, from https://www.theguardian.com/technology/2020/feb/29/how-teenage-money-mules-funnel-millions-from-online-fraud

Maimon, D., Becker, M., Patil, S., & Katz, J. (2017). *Self-protective behaviors over public WiFi networks*. In The {LASER} workshop: Learning from authoritative security experiment results ({LASER} 2017) (pp. 69-76).

Maurya, A. (2012). *Running Lean: Iterate from Plan A to a Plan That Works, Science of Aging Knowledge Environment*. doi: 10.1126/sageke.2002.20.nw68.

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). *Consumers' protection of online privacy and identity*. Journal of Consumer Affairs, 38(2), 217-232.

Ortlinghaus, A., Zielke, S., & Dobbelstein, T. (2019). *The impact of risk perceptions on the attitude toward multi-channel technologies*. The International Review of Retail, Distribution and Consumer Research, 29(3), 262-284.

Tsang, S., Koh, Y. S., Dobbie, G., & Alam, S. (2014). *Detecting online auction shilling frauds using supervised learning*. Expert systems with applications, 41(6), 3027-3040.

Varghese, T. E., Fisher, J. B., Harris, S. L., & Durai, D. B. (2011). U.S. Patent No. 7,908,645. Washington, DC: U.S. Patent and Trademark Office.

Watts, S. (2016). Secure authentication is the only solution for vulnerable public wifi. Computer Fraud & Security, 2016(1), 18-20.

Yazdanifard, R., WanYusoff, W. F., Behora, A. C., & Sade, A. B. (2011). Electronic banking fraud: The need to enhance security and customer trust in online banking. Advances in Information Sciences and Service Sciences, 3(10), 505-509.

Yu, C. H., & Lin, S. J. (2013). Fuzzy rule optimization for online auction frauds detection based on genetic algorithm. Electronic Commerce Research, 13(2), 169-182.