Revista de Ciencias Sociales y Humanidades
CHAKIÑAN
ISSN 2550 - 6722

Unach

Número 10 / **ABRIL, 2020** (73-86)

Melissa Valeria Echeverría Joniaux
mecheverriaj@uees.edu.ec

Universidad de Especialidades Espíritu Santo.
Guayaquil, Ecuador

ORCID:
https://orcid.org/0000-0002-5453-8530

Melissa Andrea Garaycoa Walker
mgaraycoa@uees.edu.ec

Universidad de Especialidades Espíritu Santo.
Guayaquil, Ecuador

ORCID:
https://orcid.org/0000-0002-9383-7162

Aleksandar Tusev
atusev@uees.edu.ec

Universidad de Especialidades Espíritu Santo, Escuela de Estudios Internacionales.
Guayaquil, Ecuador

ORCID:
https://orcid.org/0000-0003-3794-9669

ARE ECUADORIAN MILLENNIALS PREPARED AGAINST A CYBERATTACK?

¿ESTÁN PREPARADOS LOS MILLENNIALS ECUATORIANOS CONTRA UN ATAQUE INFORMÁTICO?

DOI:
https://doi.org/10.37135/chk.002.10.05

Recibido:
22/10/2019

Aceptado:
18/02/2020

Revista de Ciencias Sociales y Humanidades
CHAKIÑAN
ISSN 2550 - 6722

Unach

Número 10 / **ABRIL, 2020** (73-86)

ARE ECUADORIAN MILLENNIALS PREPARED AGAINST A CYBERATTACK?

¿ESTÁN PREPARADOS LOS MILLENNIALS ECUATORIANOS CONTRA UN ATAQUE INFORMÁTICO?

Abstract

A cyberattack is an attempt to get unauthorized access, expose, alter, disable, steal or make unauthorized use of information. Over the years, cyberattacks are becoming more frequent, considering that Ecuadorian authorities claimed they had received over 40 million cyberattacks such as denial-of-service (DOS) during a week, in April 2019. The objective of this research work is to assess to what extent Ecuadorians are prepared for a cyberattack focused on Millennials, who attend private universities and maintain a high socioeconomic status, due to they are more likely to be targeted by hackers. This study shows the level of importance that Millennial university students give to their private information. A quantitative study was applied to measure the objective mentioned before and was aimed at 103 university students in Samborondón, Ecuador. The obtained results showed that although the sample population takes some security measures to protect their information, there exist vulnerable aspects that can be used by hackers to obtain unauthorized access.

Keywords: Cyberattack, cyber security, information security, millennials.

Resumen

Un ataque cibernético es un intento de obtener acceso no autorizado, exponer, alterar, deshabilitar, robar o hacer un uso no autorizado de información. En los últimos años, los ataques cibernéticos han sido más frecuentes, considerando que las autoridades ecuatorianas afirmaron que habían recibido más de 40 millones de ciberataques, como DOS, en el lapso de una semana, en abril de 2019. El objetivo de este trabajo de investigación es tener un estudio objetivo sobre hasta qué punto los ecuatorianos están preparados para un ciberataque con un enfoque en los millennials que asisten a universidades privadas y tienen un alto nivel socioeconómico debido a que son más propensos a ser atacados por hackers. Este estudio muestra el nivel de importancia que los estudiantes universitarios Millennials otorgan a la seguridad de su información privada. Se aplicó un estudio cuantitativo para medir el objetivo mencionado, aplicada a 103 estudiantes universitarios en Samborondón, Ecuador. El resultado obtenido evidenció que, si bien la población estudiada, toma algunas medidas de seguridad para proteger sus datos, todavía hay grietas, que pueden ser utilizadas por los piratas informáticos para obtener acceso no autorizado.

Palabras clave: *Ataque informático, seguridad informática, seguridad de la información, millennials.*

INTRODUCTION

How secure do you believe your information is? What would you consider a cyberattack? Cyberattacks first began with the rise of computers in the 1960s, giving rise to the need for cyber security. Today, around 45 million cyber-attacks can occur on a daily basis (Threatcloud 2019). According to the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (2018), a cyberattack is an attempt to gain unauthorized access, expose, alter, disable, steal or make unauthorized use of as asset (ISO/IEC 2018:1). The way to protect your information is with information security or cyber security. Information security includes the preservation of integrity, and availability and confidentiality of information (ISO/IEC 2018:4).

Information security is becoming an essential need for all consumers. Society is constantly advancing, and in order to prevent hackers gaining access to financial and personal data, the implementation of cybersecurity is imperative. Not only will it provide citizens with added safety measures, it will also increase their level of security towards using technology in their everyday lives. For this reason, societies need to address clear boundaries on data sharing, transparency and consent of data privacy, and ethical data usage (Chamorro-Premuzic, Akhtar, Winsborough & Sherman 2017:15).

Considering how widespread the use of technology and the internet has become people need to have the right tools to protect their personal information (Antoun 2015:100). As mentioned (Ablon 2018:15), if internet users do not protect their personal data, they could face considerable risks. Therefore, it is important to research how prepared people are against such attacks, helping reveal the extent of the problem.

The case of Ecuador reveals a particular need for such research. Ecuador is a country where the youth are becoming more involved in technology, and there is little research on their security behaviors. Millennials are known to rely heavily on technology to store their information (Deal, Altman & Rogelberg 2010:192). In Ecuador, as of 2017, Millennials represented 23.2% of the total population (Instituto Nacional de Estadistica y Censos [INEC] 2017). 65% of Millennials own a smartphone (INEC 2017). Also, 68.7% of Ecuadorian Millennials use the internet, and at least 63.8% of them have a social media account.

Due to the fact that most Millennials have an internet presence, it is essential for them to be prepared to protect their information. Late Millennials, or Generation Z are defined as people born between 1996 and 2001 or as late as the mid-2000s (Williams, 2015:2), and older Millennials are defined as people born between 1980 and 1995 (Ng & Johnson 2015:122).

This topic has become even more important after Ecuador released Julian Assange from the Ecuadorian embassy in London. As of April 15, of 2019, Ecuadorian authorities claimed they received over 40 million cyber-attacks (Rivadeneira 2019:1). As reported by El Universo, these attacks came from different parts of the world, and they targeted institutions like the Presidency, the Central Bank and other ministries.

As for developments in Ecuador, starting in 2017, banks started introducing new technology aimed mainly at younger people, who would benefit from the introduction of mobile applications which allowed them control of financial services (Redacción Economía 2017). Considering this new merging of financial services and mobile apps, it is important to investigate how prepared they are against unauthorized access to their personal data. Cyberattacks are a threat for all people and institutions around the world. It is imperative to research how they can affect people and to find out whether people are taking the correct measures to protect their data (Ablon 2018:15).

The aim of this paper is to explore cybersecurity and cyber threats with relation to private university students in Guayaquil, Ecuador. The main focus of the study is to investigate how prepared students are against cyberattacks.

The method for the investigation was a thirteen question online survey. The population of the sur-

vey was university students from the higher socioeconomic level. The main sample population was taken from the prominent coastal university Universidad de Especialidades Espíritu Santo (UEES). The survey responses provide key information about how Millennials in Ecuador handle their personal data. Also, the results indicate the level of cyberattacks this population has experienced.

TECHNOLOGY

The world is increasingly becoming connected via the internet. *The internet of things* has come to symbolize this new reality; according to the International Telecommunication Union (2012), this refers to the infrastructure connecting, either virtually or physically, all things that exist and evolve, where communication technologies and information is interloped.

Computers originate from the abacus in 1,100 BCE (Freiberger, Swaine et al., 2020). However, there were many advances that occurred in order to reach what is considered the modern-day computer. That feat can be attributed to Konrad Zuse who completed the first programmable computer that became fully functional in 1941 (Ceruzzi 1981:249). Theft performed through a computer had been a concern since the 1960s as people were attempting to take information stored inside computers (Warner 2012:784).

CYBERATTACKS

As Warner (2012:781) stated, even people who do not own computers are at risk of suffering a cyberattack or cyber theft. Companies and governments seem to be constantly under attack by hackers that seek to maliciously access private information. Also, there are entities that scam people`s information, while consumers believe they are protected (Rajab, Ballard, Mavrommatis, Provos & Zhao 2010:1).

Advisors and agency officials have been seeking to discern such attacks, with the latest technology available. This creates an increasing security challenge; as the numbers of hackers continue to increase so do the number of potential victims. With the increasing surge of computer viruses, more sophisticated antivirus technology emerged (Bussa 2000:1-2; Rad, Masrom & Ibrahim 2010:115-119). A virus is a program whose main objective is to replicate itself unto as many computers as it can (Hubbard & Forcht 1998:12; Nachenberg 1997:46-47).

Cyberattacks can lead to data breaches, which can be catastrophic. One of the biggest data breach cases was discovered in 2019, after a security researcher found a file online titled Collection 1, which contained 87 gigabytes of data and 773 million email addresses and passwords (Hunt 2019).

After the breach was made public, it was found that more collections (Collection 2 through Collection 5) which contained around 845 gigabytes of data were being sold on the dark web (Greenberg 2019). The dark web is defined as a part of the world wide web, that is only accessible through specific networks and where connections are highly encrypted, so illegal activities can be carried out (Nastiti & Wimmer 2015:3).

CYBERATTACKS IN ECUADOR

Ecuador is not out of reach when it comes to cyberattacks. In 2015, a cyberattack against Banco del Austro (BDA) cost the bank 12 million dollars (Insurance Journal 2016). The attack targeted BDA´s servers and ordered Wells Fargo to make money transfers to a bank account in Hong Kong (Bergin & Layne 2016).

According to Bergin and Layne, Wells Fargo proceeded with making at least 12 transactions over the course of ten days. The authors add that the attack was made through what were previously thought to be secure servers (The Society for Worldwide Interbank Financial Telecommunication [SWIFT] Network), which are used by many banks around the world to transfer billions of dollars.

The country also became vulnerable to cyberattacks due to the revocation of asylum to the foun-

der of Wikileaks, Julian Assange, in early April of 2019 (McKay 2019). According to the minister for information and communication technologies, after Assange was arrested 40 million cyberattacks occurred against Ecuadorian institutions' websites (Fingas 2019). The 40 million attacks refer to the number of requests made to flood website servers and limit access to the internet (McKay 2019). McKay adds that none of the attempts were successful in stealing or destroying data.

METHODOLOGY

The following research paper centers on cyber security and Ecuadorian Millennials. The objective of this research paper is to assess to what extent Ecuadorians are prepared for a cyberattack with a focus on Millennials, who attend university and have a high socioeconomic status, making them more likely to be targeted by hackers.

Ecuadorian university students from the higher socioeconomic level are likely to represent the best prepared segment of Millennials in Ecuador when it comes to cyber-security habits and awareness, compared to less educated and lower socioeconomic Millennials.

Additionally, this segment of the population are at a higher risk for financial cyberattacks as they have greater financial wealth, and likely spend more on online purchases. Also, they are likely to be less reserved when it comes to sharing personal and financial information online (Alton 2017). UEES students were chosen to represent the population, as this university is one of the most expensive in the country, with a reputation for educating some of the wealthier segments of the population.

A quantitative survey instrument was chosen to test the awareness, preparedness and value Millennials have with relation to cybersecurity and cyberattacks. A quantitative study allowed for the gathering of basic information from a larger sample. The instrument was based on a survey published by the Pew Research Center (2017:30-42). The instrument had the purpose of finding out the trust Americans place in cybersecurity and what experiences they have had. The instrument was adjusted for the Ecuadorian population. After conducting a pilot study on the original survey, a number of questions were eliminated, leaving thirteen questions in the final instrument.

In total, there were 103 students that completed the survey. UEES has approximately 5,000 students. By surveying 103 students, the confidence level of 85% was obtained with a margin of error of 7%. The majority of the students surveyed were between the ages of 18 and 21, accounting for 54% of the total respondents. The second largest group surveyed were aged between 22 and 25, with 35% of respondents.

The survey was distributed via the QuestionPro platform. First, it was sent to students via social media. Then, researchers visited classrooms, where, with the permission of the teachers, students were invited to complete the survey online on their devices. The survey was conducted from March 27, 2019 until April 15, 2019.

Some limitations of the instrument were tested before administering it. A pilot study was conducted to test that the questions selected were appropriate for the population and if they had to be altered or removed for reliability and relevance. Originally there were twenty-one questions in the survey (see appendix 1).

After conducting the pilot test, eight of the questions were either unnecessary or had to be merged with another question in order to be more cohesive. The first survey question was regarding the use of the internet, and whether the student used it, at least occasionally. Due to all the answers being yes in the pilot test, we decided it was redundant, and deleted it.

Following that question, there was one about how frequently students used the internet, and another question asking if they owned a smartphone. Since most pilot responses were the same, and the questions did not provide essential information for this study, we removed those questions too. Additionally, we removed questions regarding people's use of social media and questions about how they

handle their passwords across different sites. The purpose of removing these questions was to ensure that the survey was clear and understandable, and that people would feel comfortable and fill it out correctly.

The results of the quantitative test performed were provided by using graphs and tables in order to present the information gathered from the surveys. These were subsequently analyzed in order to address how prepared Ecuadorian Millennials were for a cyberattack.

RESULTS AND DISCUSSION

The objective of conducting this survey was to provide results that will demonstrate the extent that Ecuadorian Millennials protect themselves against cyberattacks, with a focus on private university students with a high socioeconomic status.

Ten yes no questions were asked. Those results are summarized in table 1, and described below.

Question 1 shows the number of people from our sample who currently own a smartphone. Out of the 103 students surveyed, 100 stated yes, or 97.09% of students; 2.91% did not own one.

Question 2 asked if students have ever installed an application to protect their smartphones against viruses that attack phones. Of the 103 responses, 71 said that they had not installed any antivirus application on their phones, or 69%, and 32 of the students answered that they had, or 31% of the surveyed students.

Question 3 asked if they had ever experienced fraudulent charges made to their credit cards. Of

Table 1. Results for yes no questions

Question number	Question	Yes %	No %
1	Is your cell phone a smartphone such as an iPhone, Android, Blackberry or Windows phone?	97	3
2	Have you ever installed an application to protect your smartphone against viruses?	31	69
3	Have you ever experienced any of the following data thefts? Fraudulent charges to credit cards?	24	76
4	Have you ever experienced any of the following data thefts? Have received notice about your personal information being compromised?	51	49
5	Have you ever experienced any of the following data thefts? Someone has had unauthorized access to your email?	33	67
6	Have you ever experienced any of the following data thefts? Someone has had unauthorized access to any of your social media accounts?	12	88
7	Do you have any of the following worries about your passwords? You have difficulty managing all of your passwords?	38	62
8	Do you have any of the following worries about your passwords? Do you worry about the security of your passwords?	69	31
9	Do you have any of the following worries about your passwords? You use less secure passwords because more complicated passwords are harder to remember?	31	69
10	Do you use public Wi-Fi networks in public places such as airports, cafes, hotels or libraries?	89	11

Source: Based on the data obtained in the applied survey

the 103 people surveyed, 76% said no, while 24% said yes.

Question 4 asked if they had ever received a notice stating their personal information had been compromised. Of the 103 people who filled out the survey, 51% said they had, and 49% said they had not.

In question 5, students were asked if they had ever had someone access their email account without their permission. Out of the 103 respondents, 67% said no, and 33% of people said they had experienced it.

In question 6, students were asked if they had never had someone access any of their social media accounts without their permission. Out of the 103 respondents, 88% said no, and 12% of the sample stated they had had someone breach their accounts.

In question 7**,** students were asked if they had difficulty managing all of their passwords**.** Out of all the people surveyed, 62% said yes, and 38% said no.

Question 8 asked if students had concerns about the security of their passwords**.** Of the 103 people who filled out the survey, 69% said yes, and 31% said they did not.

In question 9, students were asked if they did not use less secure passwords because using more complicated passwords are harder to remember. Out of all the people surveyed, 69% responded no, and 31% said they did use less secure passwords because it was harder to remember more complicated passwords.

Finally, question 10, asked if students used public Wi-Fi networks in public places like airports, cafes, hotels and libraries. 89% said yes, and 11% said they did not make use of these networks.

Seven further questions were asked, where there were at least three options for students to select as a response. The results are described in figures 1 to 7.

Figure 1 is a multiple selection question where students were tasked with selecting what type of security measures they have in place to lock their phone. 34.97% responded that they use a personal identification number (PIN) password to access their phones; the second most used phone lock was the fingerprint scanner with 33.75% of students. The next three responses all have similar results: the use of a pattern received 11.19% of responses; 10.49% of students do not lock their phones; and 9.79% of students stated they used face identification.

Figure 2 looked at how frequently students update their device's operating system (OS) and download applications. The majority of the respondents answered that they updated their devices automatically or as soon as possible, with a 55% of students; 40% of students answered that they updated their OS or applications when it was convenient for them; finally, 5% of students answered that they never updated their OS or applications.

Figure 3 describes whether students have online accounts. For online accounts that involve payments or transactions, 66% stated that they used them, and 32% of the students stated no. 2% of respondents said that the question did not apply to them. With online utility accounts, 69% of students stated they did not have one, while 15.5% said yes and 15.5% said that such online account did not apply to them.

For online accounts related to healthcare providers, 67% of students said they did not have one, 19.4% of students said yes, and 13.6% said it did not apply to them; finally, for online accounts with bank or financial service providers, 77.67% of students said that they had such online accounts, 19.42% said they did not have one and 2.91% said this question did not apply to them.

Figure 4 looked at if students abstained from creating an online service account due to the dubious nature of how their information will be handled. Out of the 103 surveyed, 56% stated that they had abstained from creating such accounts, 23% claimed that they have not stopped themselves from creating online service accounts, and 21% claimed that they do not know if they have done so.

In figure 5, students were asked to rate a number of institutions for how confident they were that

their personal data would be safe from hackers or unauthorized users. Students had the highest confidence in phone manufacturers, scoring an average 3.22 out of 3.5, credit card companies, scoring 3.06 out of 3.5, and email service providers, scoring 2.91 out of 3.5. The lower confidence results were for government, with 1.79 out of 3.5, and companies or retailers they did business with, with 2.15 out of 3.5.

Figure 6 looked at how students felt their personal information had changed over the last five years. 44% of students said they felt that their personal information was as secure as it was five years ago. 37% felt it was less secure, and 19% said they felt as if it was more secure.

Figure 7 asked which types of sites students visited while using a public Wi-Fi network. 52% of students stated they visited social media sites; 29% opened their emails, 10% shopped online; and 9% accessed their online bank accounts.

Source: Based on the data obtained in the questionnaire

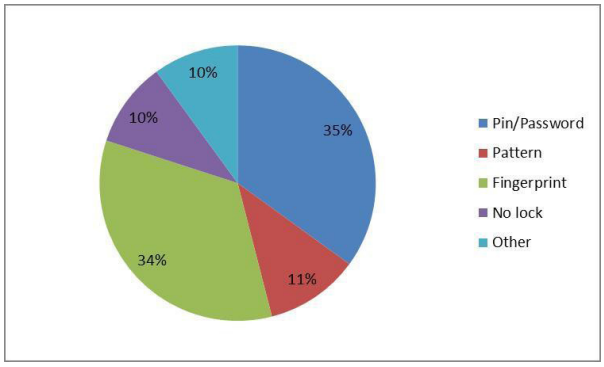

Figure 1: What type of security measures do you have in place to lock your phone?

Source: Based on the data obtained in the questionnaire

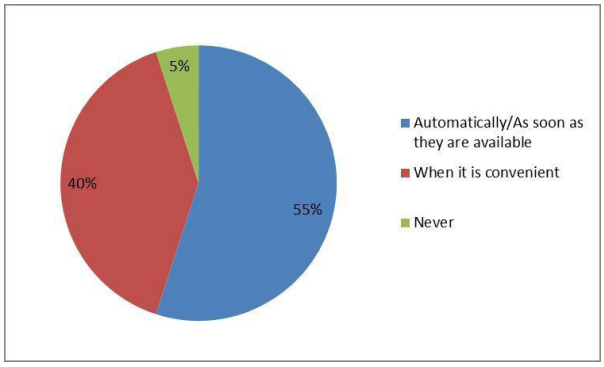

Figure 2: How frequently do you update your device's operating system and applications?

Source: Based on the data obtained in the questionnaire

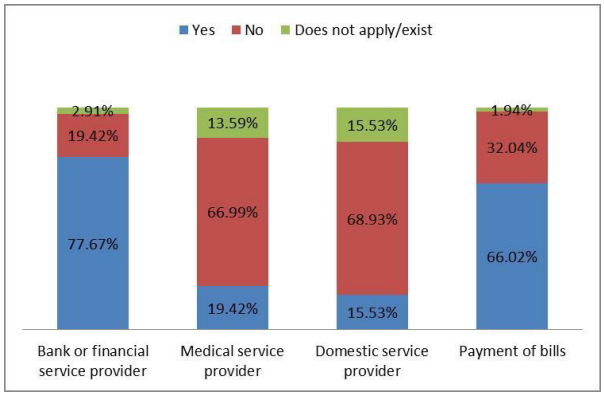

Figure 3: Do you have any internet accounts of this nature?

Source: Based on the data obtained in the questionnaire

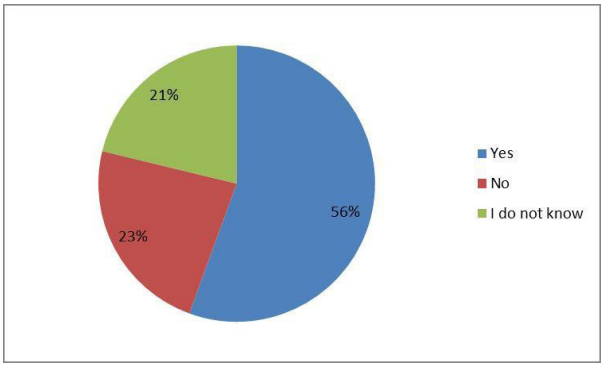

Figure 4: Have you ever decided not to use or not to create an account with an online service provider due to concerns for how your personal information would be handled?

Source: Based on the data obtained in the questionnaire

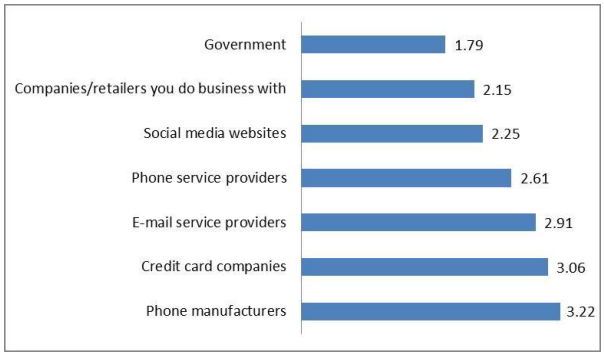

Figure 5: Regarding the following institutions, how confident are you that your personal data will be safe from hackers or unauthorized users?

Source: Based on the data obtained in the questionnaire

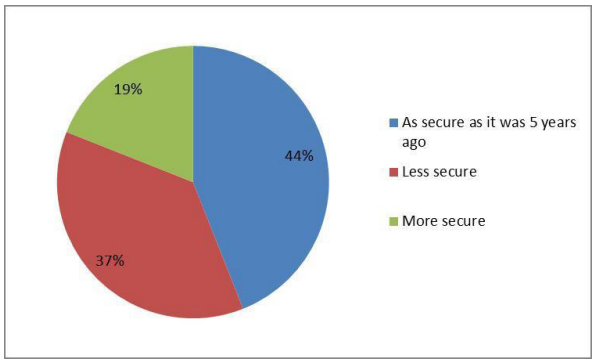

Figure 6: How do you feel your personal information has changed over the last five years?

Source: Based on the data obtained in the applied survey

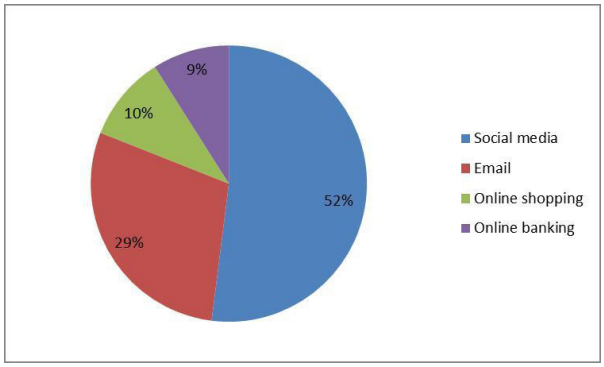

Figure 7: Which websites do you visit while connected to a public Wi-Fi network?

DEVICE SECURITY

The results show that most students have not had their bank accounts targeted. Also, the great majority of the sample has not had a situation where their credit card information was stolen. Furthermore, most students stated that they had not had their emails or social media account compromised or hacked. However, students did have issues with notifications that their information had been compromised, at some point in their lives.

Overall, it can be said that the respondents have been victims of some type of hack, by phishing or other types of information theft, which allowed hackers to access their personal information and send messages to them. Even though the majority of students stated that they had not suffered from a cyber-attack, there were still many students who had been affected by such attacks.

Millennials tend to have more trust in cell phone manufacturers; companies such as Apple advertise that they refuse to give out information of customers, even if a government agency seeks it (Nakashima 2016:1). Also, students have a higher level of trust in in credit card companies, cell phone service providers and email providers.

On the other hand, students do not have a high level of trust in companies or retailers they conduct business with, possibly due to the fact that they do not know who oversees the regulations of these companies, including social media sites. The least trusted institution was government agencies. This lack of trust in government agencies can lead to an overbearing obstacle for such agencies to implement and enforce cyber security measures and regulations. Students are more inclined to perform such security through private actors. It is clear that the age of users and their personal experiences with the internet have an impact on their perceptions towards trust in different institutions (Alzahrani, Al-Karaghouli & Weerakkody 2018:143).

SAFETY MEASURES

The majority of Millennials have a smartphone. They mostly keep their information safe by keeping their smartphones under lock by using measures such as PIN passwords. Out of all the options to choose from, using a PIN or a password is not the most secure choice, when compared to biometric locks, such as fingerprint scanners or facial recognition (Cherapau, Muslukhov, Asanka & Beznosov 2015). PINs are combinations of four numbers, which can be more convenient, but less secure (Cherapau *et al*. 2015).

Although the sample population is known for being more reliant on technology, most students do not own an application on their phones in order to protect them against an attack or virus. This could have a negative effect on the security of personal data. Antivirus applications serve to protect computers or mobile devices from threats like malware, which could include spyware (Williams 2014:1).

However, the results show that the majority of students surveyed did download updates when available or automatically. This is a sign that they are aware of cybersecurity threats because "running out-of-date software can provide an open door for hackers to take advantage of holes left in programs that haven't had critical security updates applied" (Palmer 2019:5).

Most Millennials have online accounts with banking institutions and have accounts that involve online bill payments or transactions. As stated by Choo (2011:722), in recent years, banking institutions have offered the service of mobile banking or payment services. With that, there is a new gateway to cyberattacks, with malware created to purposely target phones to give information to hackers about banking login credentials and other personal information.

INFORMATION SAFETY

Most Millennials believe that the safety of their information, in the last five years, has either remained the same or gotten worse. This may be amplified as cyberattacks continue to increase in frequency and severity, such as the Sony Pictures attack in 2014, the Anthem healthcare attack in 2015 or the Panama papers incident that occurred in 2016 (Middleton 2017).

In addition, the majority of Millennials use public Wi-Fi networks in order to access the internet. This can put their data at risk. Information can be taken; for example, in 2016 a test was conducted where a hack was attempted on mobile and tablet devices through a public Wi-Fi hotspot. The purpose was to test whether data can be gathered from devices connected through the public Wi-Fi network by recording the keystrokes performed on devices. The results were worrying: they recovered keystrokes with a high success rate, without victims noticing.

When entering a public Wi-Fi source, students enter sites such as social media and their email, yet they generally refrain from accessing their bank accounts or online shopping. This may be a sign that they are aware of the risks of public Wi-Fi networks and cyber-attacks.

MANAGEMENT OF PASSWORDS AND ACCOUNTS

Most Millennials do not have difficulty handling their passwords, and they do not use less secure passwords. This shows that they are worried about security. Their concerns are valid; attacks such as clickjacking are becoming more common. Clickjacking is a term that describes a technique where embedded links hijack users to make moves that they did not intend to take. Embedded browsing has become more popular these days, making it common for a normal viewer to click on sites that were not the ones they were intended for. By using these types of frameworks, a malicious website can open on an unsuspecting person's computer (Selim, Tayeb, Kim, Zhan & Pirouz 2016:2-3).

Overall, Millennials have both positive and negative habits when it comes to cybersecurity. Most of them do not use antivirus software on their phones and they access sites using public Wi-Fi, making their information vulnerable. However, they do

take some measures to protect their information. They use secure passwords and lock their devices, and they avoid open Wi-Fi networks when making financial transactions.

RECOMMENDATIONS

There are some basic things that Millennials can do to increase the safety of their online data and reduce their risk of cyberattacks. Students should consider using password managers in order to encrypt their devices. Furthermore, they should download reputable anti-virus software to their devices, and if possible use a Virtual Private Network (VPN) to encrypt their data when accessing the web through public Wi-Fi networks.

CONCLUSIONS

This study set out to explore cyber security with relation to university students from Ecuador. The aim was to gauge students' awareness to such threats, the value they place on cybersecurity and their general level of preparedness against such hacks.

The results found that they were aware of the potential threats that they face, yet do not seem to take the required measures against such threats, suggesting that they do not have a high enough value for such measures. Also, while the majority of Millennials had not been victims of cyberattacks, their information is not completely secure against potential unauthorized access, suggesting they are not as prepared as they could be. The measures they take to protect their data are not the best available, seeing as most still use a PIN or password and do not download antivirus applications to ensure no one will gain access to their devices.

To sum up, anyone can be a victim of cyberattacks. Millennials in Ecuador, at least those in our sample, whilst being aware of the dangers of cyberhacking, do not take them as seriously as they should. They take some measures to protect themselves, but not enough. Students should use password managers to encrypt their devices, download reputable anti-virus software, and use a VPN to encrypt their data when accessing public Wi-Fi networks. Seeing as the sample in this study was limited, further research is encouraged to test the results. Furthermore, expanding the populations to older generations as well as non-university students would be valuable for comparative studies.

BIBLIOGRAPHIC REFERENCES

Ablon, L. (2018). Data thieves: the motivations of cyber threat actors and their Use and monetization of stolen data. *Rand Corporation*, 1-16. doi:10.7249/ct490

Alton, L. (2017, December 1). How Millennials Think Differently About Online Security. *Forbes*. Retrieved from https://www.forbes.com/sites/larryalton/2017/12/01/how-millennials-think-differently-about-online-security/#51fba8da705f

Alzahrani, L., Al-Karaghouli, W. & Weerakkody, V. (2018). Investigating the impact of citizens' trust toward the successful adoption of e-government: A multigroup analysis of gender, age, and internet experience. *Information Systems Management*, *35*(2), 124-146. doi:10.1080/10580530.2018.1440730

Antoun, C. (2015). Who are the internet users, mobile internet users, and mobile-mostly internet users?: demographic differences across internet-use subgroups in the U.S. *Mobile Research Methods: Opportunities and challenges of mobile research methodologies*, 99-117. doi:10.5334/bar.g

Bergin, T. & Layne, N. (2016, May 20). Special Report: Cyber thieves exploit banks' faith in SWIFT transfer network. *Reuters*. Retrieved from https://www.reuters.com/article/us-cyber-heist-swift-special-report/special-report-cyber-thieves-exploit-banks-faith-in-swift-transfer-ne-

twork-idUSKCN0YB0DD

Bussa, T. (2000). *The Future of Fighting Viruses: A History and Analysis of the Digital Immune System*. Bethesda: SANS Institute. Retrieved from http://ivanlef0u.fr/repo/madchat/vxdevl/papers/avers/toby_bussa_gsec.pdf

Ceruzzi, P. E. (1981). The Early Computers of Konrad Zuse, 1935 to 1945. *IEEE Annals of the History of Computing*, *3*(3), 241-262. doi:10.1109/mahc.1981.10034

Chamorro-Premuzic, T., Akhtar, R., Winsborough, D., & Sherman, R. A. (2017). The datafication of talent: how technology is advancing the science of human potential at work. *Current Opinion in Behavioral Sciences*, *18*, 13-16. doi:10.1016/j.cobeha.2017.04.007

Cherapau, I., Muslukhov, I., Asanka, N. & Beznosov, K. (2015). On the Impact of Touch ID on iPhone Passcodes. *Symposium on Usable Privacy and Security (SOUPS)*, 1-20. Retrieved from https://pdfs.semanticscholar.org/e021/f57012562610e8a997963995d00f5cde9b7d.pdf

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

Deal, J. J., Altman, D. G. & Rogelberg, S. G. (2010). Millennials at Work: What We Know and What We Need to Do (If Anything). *Journal of Business and Psychology*, *25*(1), 191-199. doi:10.1007/s10869-010-9177-2

Fingas, J. (2019). Ecuador says it faced 40 million cyberattacks after giving up Assange. *Engadget*. Retrieved from https://www.engadget.com/2019/04/16/ecuador-cyberattacks-after-assange-arrest/

Freiberger, P. A., Swaine, M. R. et al. (2020). Computer - History of computing. *Encyclopaedia Britannica* [electronic version]. New York, EU: Encyclopaedia Britannica Inc. Retrieved from https://www.britannica.com/technology/computer/History-of-computing

Greenberg, A. (2019). Hackers are passing around a megaleak of 2.2 billion records. *Wired*. Retrieved from https://www.wired.com/story/collection-leak-usernames-passwords-billions/

Hubbard, J. C. & Forcht, K. A. (1998). Computer viruses: how companies can protect their systems. *Industrial Management & Data Systems*, *98*(1), 12-16. doi:10.1108/02635579810199708

Hunt, T. (2019). The 773 million record "Collection #1" data breach. *Troy Hunt*. Retrieved from https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

INEC. (2017). *Hablando de Millennials*. Quito: INEC. Retrieved from http://www.ecuadorencifras.gob.ec/documentos/web-inec/Inforgrafias-INEC/2017/millenials.pdf

Insurance Journal. (2016). Cyber Bank Thieves Stole $12M from Ecuador Bank in 2015, Using SWIFT System. *Insurance Journal*. Retrieved from https://www.insurancejournal.com/news/international/2016/05/24/409577.htm

International Telecommunication Union. (2012). Internet of Things Global Standards Initiative. *ITU*. Retrieved from https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

ISO/IEC 27000. (2018). *ISO/IEC 27000:2018(E): Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary*. USA: ISO/IEC. Retrieved from https://www.sis.se/api/document/preview/80001198/

McKay, T. (2019). Ecuador Claims It's Been Hit with 40 Million Cyberattacks Since Giving Up Julian Assange. *Gizmodo*. Retrieved from https://gizmodo.com/ecuador-claims-its-been-hit-with-40-million-cyberattack-1834070219

Middleton, B. (2017). *A History of Cyber Security Attacks: 1980 to Present*. Boca Raton, FL: CRC Press.

Nachenberg, C. (1997). Computer virus-antivirus coevolution. *Communications of the ACM*, *40*(1), 46-51. doi:10.1145/242857.242869

Nakashima, E. (2016, February 17). Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html

Nastiti, A. & Wimmer, A. (2015). Darknet, Social Media and Extremism: Addressing Indonesian Counterterrorism on the Internet. *Deutsches Asienforschungszentrum Asian Series Commentaries*, *30*, 1-13. Retrieved from https://www.academia.edu/20813843/Darknet_Social_Media_nad_Extremism_Addressing_Indonesian_Counterterrorism_on_the_Internet

Ng, E. S. & Johnson, J. M. (2015). Millennials: who are they, how are they different, and why should we care? *The Multi-generational and Aging Workforce*, 121-137. doi:10.4337/9781783476589.00014

Palmer, D. (2019). PC security warning: That out-of-date software is putting you at risk. *ZDnet*. Retrieved from https://www.zdnet.com/article/pc-security-warning-that-out-of-date-software-is-putting-you-at-risk/

Rad, B. B., Masrom, M. & Ibrahim, S. (2010). Evolution of computer virus concealment and anti-virus techniques: a short survey. *IJCSI International Journal of Computer Science Issues*, *7*(6), 113-121.

Rajab, M. A., Ballard, L., Mavrommatis, P., Provos, N. & Zhao, X. (2010). The nocebo effect on the web: an analysis of fake anti-virus distribution. *Login*, *35*(6), 18-25. Retrieved from https://www.usenix.org/system/files/login/articles/rajab.pdf

Redacción Economía. (2017, May 17). Cuentas virtuales y servicios digitales son las nuevas tendencias que impulsa la banca. *El Telégrafo*, pp. 1-2. Retrieved from https://www.eltelegrafo.com.ec/noticias/economia/4/cuentas-virtuales-y-servicios-digitales-son-las-nuevas-tendencias-que-impulsa-la-banca

Rivadeneira, G. (2019, April 15). Ecuador ha recibido 40 millones de ataques cibernéticos, revela viceministro de Telecomunicaciones. *El Universo*, pp. 1-2. Retrieved from https://www.eluniverso.com/noticias/2019/04/15/nota/7287215/ecuador-ha-recibido-40-millones-ataques-ciberneticos-revela

Selim, H., Tayeb, S., Kim, Y., Zhan, J. & Pirouz, M. (2016). Vulnerability Analysis of Iframe Attacks on Websites. *Proceedings of the The 3rd Multidisciplinary International Social Networks Conference on SocialInformatics 2016, Data Science 2016 - MISNC, SI, DS 2016*. doi:10.1145/2955129.2955180

Smith, A. (2017). *Americans and Cybersecurity*. USA: Pew Research Center. Retrieved from https://www.pewinternet.org/2017/01/26/methodology-183/

Threatcloud. (2019). Live Cyber Attack Threat Map. *Check Point*. Retrieved from https://threatmap.checkpoint.com/ThreatPortal/livemap.html

Warner, M. (2012). Cybersecurity: A Pre-history. *Intelligence and National Security*, *27*(5), 781-799. doi:10.1080/02684527.2012.708530

Williams, A. (2015, September 18). Move Over, Millennials, Here Comes Generation Z. *The New York Times*, pp. 1-7. https://www.nytimes.com/2015/09/20/fashion/move-over-millennials-here-comes-generation-z.html

Williams, J. (2014). What is anti-virus? *OUCH!* Retrieved from https://www.rwu.edu/sites/default/files/downloads/it/what_is_anti_virus.pdf

APPENDIX

Appendix 1. Pilot study and final survey

Question #	Question:	Question Status
1	Age	In the survey
2	Do you use the internet or email, at least occasionally?	Deleted. Almost everyone uses it. Would not provide new information.
3	How often do you use the internet?	Deleted. Wouldn't provide new information.
4	Do you have a cell phone?	Deleted. Felt too obvious.
5	Is your cell phone a smartphone such as an iPhone, Android, Blackberry or Windows phone?	In the survey
6	What types of security measures do you have in place to lock your phone?	In the survey
7	How frequently do you update your device's operating system and downloaded applications?	In the survey
8	Do you ever use a social networking site or an application such as Facebook, Twitter or LinkedIn?	Deleted. Almost everyone uses at least one of them.
9	Have you ever used your social media account information to log in to another website or have you ever done so?	Deleted, felt too personal.
10	Have you ever installed an application to protect your smartphone against viruses?	In the survey
11	Do you have online accounts of the following nature?	In the survey
12	Have you ever decided not to use or not to create an account with an online service provider due to worries of how your personal information would be handled?	In the survey
13	Thinking about the following institutions, how confident are you that your personal data will be safe from hackers or unauthorized users?	In the survey
14	How do you keep a record of your passwords?	Deleted
15	Have you ever experienced any of the following data thefts?	In the survey
16	How do you keep your passwords safe?	Deleted.
17	Do you use the same or similar passwords in your different accounts?	Deleted, felt too invasive
18	Do you share your password with your friends or family?	Deleted, people would not have answered with honesty.
19	Do you use two factor authentication?	Deleted, felt too invasive
20	Do you have any of the following worries about your passwords?	In the survey
21	How do you feel your personal information has become in the last five years?	In the survey
22	Do you use public Wi-Fi networks in public places such as airports, cafés, hotels or libraries?	In the survey
23	If you do, what websites do you visit while connected?	In the survey
24	In the next 5 years, do you think a cyber-attack will occur?	Deleted

Source: Pew Research Center (2017:30-42)