A Report
On
Cyber Security- Issues of Privacy and Safety

Prepared for
Jagdish Mahapatra
Specialist-Sales
Asia Pacific Region, McAfee

McAfee Inc.

16th November 2017

A Report
On
Cyber Security- Issues of Privacy and Safety

Prepared for
Jagdish Mahapatra
Specialist Sales - Asia Pacific Region, McAfee Inc.

Prepared by

Aditya Vasudevan-2017A7PS0175P
Tanmay Subodh Moghe-2017A7PS0184P
Paidipelly Hemanth Rao-2017A7PS0159P
Patel Abhishek Bipinkumar-2017A7PS0214P
Anirudh Srinivasan Chakravarthy-2017A7PS1195P

Members, Report Drafting Committee

McAfee Inc.

16th November 2017

Acknowledgments

First, we would like to thank Mr. Tom Fountain, Senior Vice President and Mrs. Allison Cerra, Chief Marketing Officer. Without their guidance, this report would not be possible. Next, we would like to thank our valuable customers who extended their time and support. We also thank them for sharing practical and current insights that helped make this report both authentic and relevant. We would also like to extend our gratitude to our family, friends and colleagues for their unwavering help and support. Finally, we would like to thank Mr. Steve Grobman, Chief Technology Officer and Mr. Akash Jain, Lead Consultant for their extensive support and valuable insights through the entire journey.

Table of Contents

List of Illustrations

Abstract

In an age of heavy dependence on the internet, ensuring secure network access for the users has become increasingly important. First, the report discusses the types of cybercrimes prevalent. Being a cyber security company, the report assesses the trends of various cyber threats in the form of spam, malware and ransomware to help gain insight on how to protect both our customers and the data which they have trusted us with. The next part of the report discusses the financial aspects of cybersecurity, illustrating the costs to the company, consumer and society. Lastly, cyber security awareness among college students was gauged through a survey conducted by us, at BITS Pilani. This data was analysed and used to evaluate opportunities to conduct awareness workshops as a part of the company's outreach program. Overall, this report evaluates the current global and local scenario and suggests strategies the organisation and its consumers should follow to combat cybercrime.

1. Introduction

As the number of users on the internet explode, data is generated on an unfathomable scale daily. A large part of this data contains private and sensitive information, which needs to be protected. The development of new types of ransomware, malware and viruses have made data which was previously thought of as secure, at risk. Criminals are evolving new business models, making it easier to scale cybercrime globally. Motivation of these cyber criminals vary from stealing money or information for commercial gain to disrupting and embarrassing entities. As the frequency and sophistication of these attacks increase, the industry must respond to these threats.

As a company catering to cyber security, Jagdish Mahapatra, Specialist Sales - Asia Pacific at McAfee, has asked the members of the Report Drafting Committee, McAfee Inc. to analyse the risk posed to the organisation and its customers, and make recommendations to ensure security of all the stored data. Although there is no one correct solution, the report aims to identify effective practices for the firm to follow so that we can effectively counter the actions of cyber criminals.

To write this report, records from the McAfee Network were analysed. 100 million attacks were recorded in over 150 countries using McAfee products, technologies and services. Using this and many other publications, we have attempted to analyse the current scenario and postulate prospective suggestions. Also, an online questionnaire survey conducted at BITS-Pilani lent us data on awareness among students in today's social setup. Descriptive and Inferential statistics were used for data analysis. The report does not account for any bugs which may have entered the systems. Moreover, the survey was conducted only at Pilani Campus of BITS Pilani due to time constraints and lack of human and financial resources.

This report will not only help analyse the trends of cybercrime but also help the organisation to guide its future programs and policies to ensure utmost security of our consumers.

The report has been divided into 4 chapters. Chapter 1 introduces the subject of the report, purpose and method. Chapter 2 deals with the types of cybercrime and its trends. Chapter 3 discusses the financial aspects of cybercrime to an organizational entity and an individual. Chapter 4 analyses the results of the survey conducted at BITS Pilani and gauges awareness among them. Chapter 5 has the conclusions of the report.

2.Types of Cybercrime

2.1 Spams

Spam emails account for nearly two-thirds (66-percent) of total email volume exchanged. According to certain threat researchers, 12 to 15 percent of the global spam observed in 2016 could be termed as malicious. The percentage of spam-mails with malicious attachments is increasing rapidly, and hackers appear to be experimenting with a wide range of file types to help their campaigns succeed.

2.1.1 Global Spam Situation

McAfee threat researchers conducted two vast surveys in 2016 using opt-in customer feedbacks to estimate the percentage of total email volume in spam. Our studies also suggest that global spam volume is growing, primarily due to large and thriving spam-sending botnets. One of the major spam-sending botnets used by hackers is Necurs.

From October to December 2016, there was a significant increase in the number of IP connection blocks from which spam was distributed (Figure 1). This trend can be attributed to an overall rise in spam volume, as well as reputation systems adapting to information about spam senders.

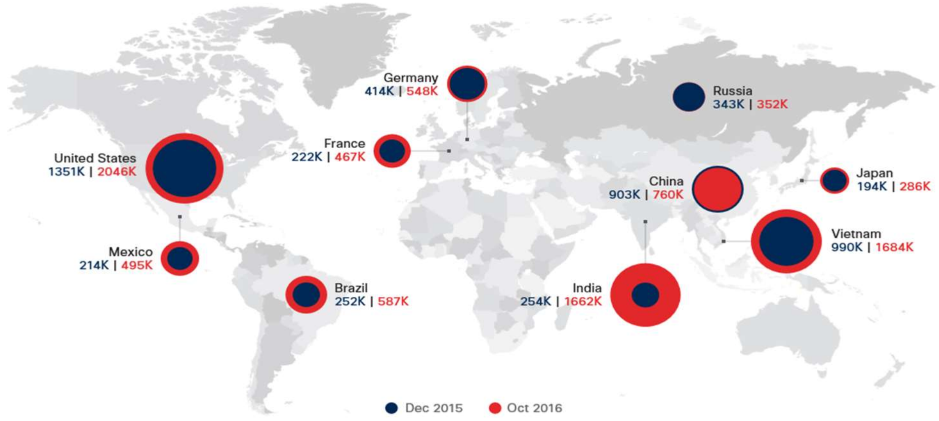


Figure 1 Number of IP connection blocks in October 2016 and December 2016 (Cisco, 2017, pg25)

The five-year graph (Figure 2) shows a dramatic increase in total spam volume during 2016. New anti-spam technologies, and high-profile takedowns of spam-related botnets, have helped to keep spam levels low in recent years. Our threat researchers attribute the recent increase in global spam volume to the Necurs botnet.

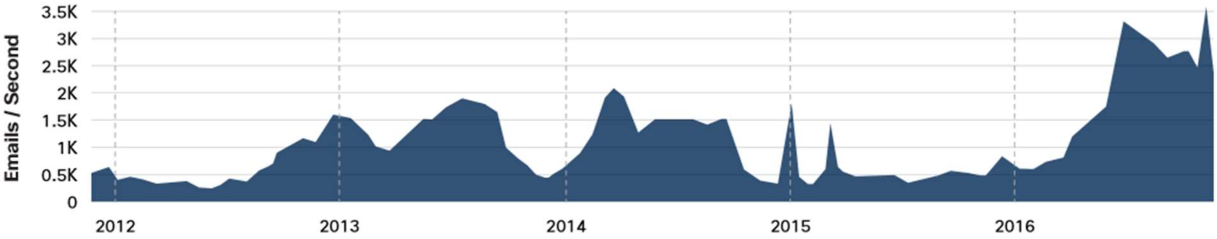


Figure 2 Number of spam emails from 2012 to 2016 (Cisco, 2017, pg26)

Figure 3 is an internal graph that illustrates the change in spam volume observed in 2016. Each row represents a distinct IP address. Between November 2015 and February 2016, it hovered below 200,000 IP addresses. In September and October, it exceeded 400,000 IP addresses before dropping off in October, which our threat researchers attribute to the operators of Necurs simply taking time off. Also note the significant decline in June. At the end of May, there were arrests in Russia related to the banking Trojan. Subsequently, several high-profile threats, including Necurs, went silent. Many of the host IPs sending Necurs spam have been infected for more than 2 years. To help keep the full scope of the botnet hidden, Necurs sends spam only from a subset of infected hosts. This behavior complicates the job of security personnel who respond to spam attacks. They may believe they have found and successfully cleaned

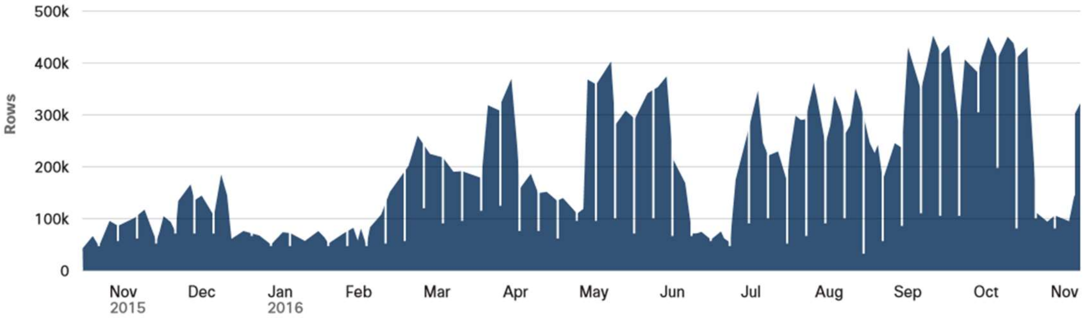


Figure 3 Number of distinct spam distributing IP addresses between Nov 2015 and Nov 2016 (Cisco, 2017, pg26)

an infected host, but the actors behind Necurs are just biding their time until they launch another attack.

2.2 Malware

Malware attacks are used for the retrieval of confidential data. According to the Symantec Internet Threat Security Report (Symantec, 2017, p24), the number of Emails containing malware rose significantly from 2015 (1 in 220) to 2016 (1 in 131). The major reason of this increase was the increase in the use of botnets, which are used in massive spam campaigns.

2.2.1 Emailed Malware Infection Process

Email is received by the target user disguised as a normal notification, most commonly as a receipt or a data-sheet. This Email includes an attachment which is often a JavaScript file or Office file containing malware. On opening the attachment, a pre-written script used to download the malware is executed, thus infecting the device. The aim of most of these malware attacks is the theft of data from the host computer.

2.2.2 Monthly Incidents

The figure 4 shows a steady amount of malware attacks from January 2016 through March 2016. This is followed by a drop in malware attacks in April and June. This may be due to government action against cyber-criminals. However, as soon as some malware are taken down, new ones come in their place. This explains the rise seen in the following months.

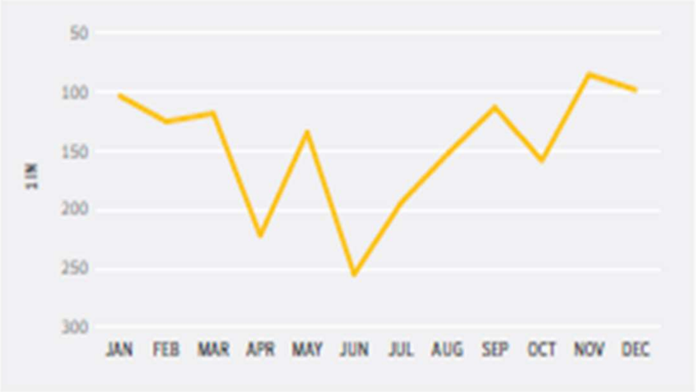
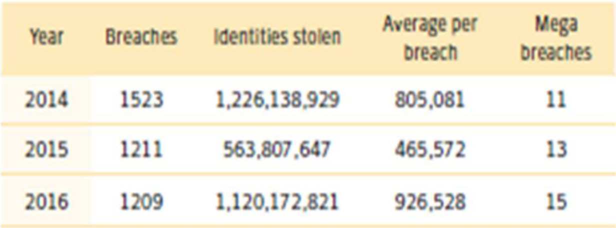


Figure 4 Monthly Instances of Malware (Symantec, 2017, pg 25

2.2.3 Data Breaches

A data breach occurs when sensitive and confidential data is accessed by someone who is not authorized to do so. The number of data breaches and identities stolen decreased drastically from 2014 to 2015. This could be due to increased vigilance amongst the population and law enforcement agencies. However, the number of identities stolen almost doubled in 2016. A possible explanation for this could be the security breach which occurred at Yahoo! Inc.



Year	Breaches	Identities stolen	Average per breach	Mega breaches
2014	1523	1,226,138,929	805,081	11
2015	1211	563,807,647	465,572	13
2016	1209	1,120,172,821	926,528	15

Figure 5 Data breaches and identities stolen between 2014 and 2016

2.3. Ransomware

Ransomware is a type of malicious software. It threatens to publish the data or perpetually block access to it unless some ransom is paid. It is sent to electronic devices through email and download links. The ransomware software gets installed in the device automatically. The access to the data in the device is lost. This section analyzes the modes of detections of ransomware and its effects.

2.3.1 How does it spread?

Among the many ways in which ransomware is spread, the most common method is through email. The email sent to the device contains a downloader hidden in malicious attachment. It will download and install the software.

Another way is by web attacks. Malicious web pages designed to exploit vulnerabilities on the victim's computer install the malware. When the emails containing such malicious attachments come, they are recognised as spam emails by the antivirus. Ransomware is often detected and blocked by generic detection technologies.

Ransomware can also spread via secondary infection, in which malware that has already infected a device can be used to download more malware.

The difficulty in stopping it from spreading comes due to its property of self-propagation, which means that it is spread to all the devices connected to that device.

2.3.2 Analysis of Ransomware detections

Ransomware can be detected by any good antivirus software. The Figure 6 shows the average number of global ransomware detections per day in years 2015 and 2016. Ransomware detections increased by 36% from 2015 to 2016. The huge increase was observed because this is one of the best ways to attack devices, which has made it an extremely popular tool.

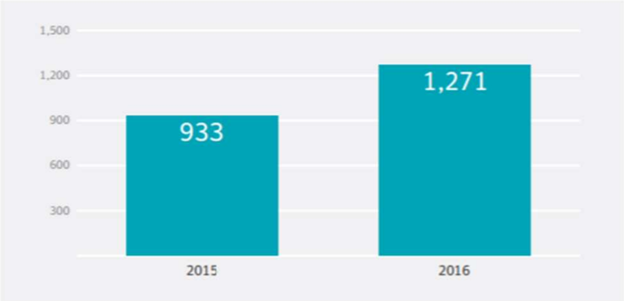


Figure 6 Ransomware detections, 2015-16

The Figure 7 shows percentages of ransomware detections by several countries in the year 2016. One-third of the detections encountered were in the United States of America. Statistics indicate that the attackers are largely concentrating their efforts on developed and stable economies. Since antivirus detection software is more prevalent in such countries, the number of detections also is higher.

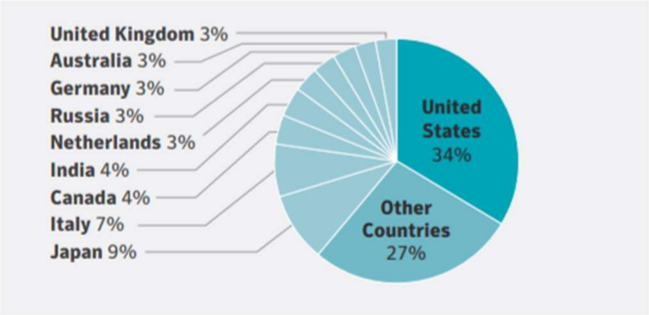


Figure 7 Country-wise Ransomware Detections

2.3.3 Analysis of new ransomware families and variants

Figure 8 gives the number of new ransomware families emerging per year across the globe. It can be observed that in 2014 and 2015 only 30 new families emerged but the number increased significantly in 2016. It indicates that many attackers are now jumping into this field and creating new families.

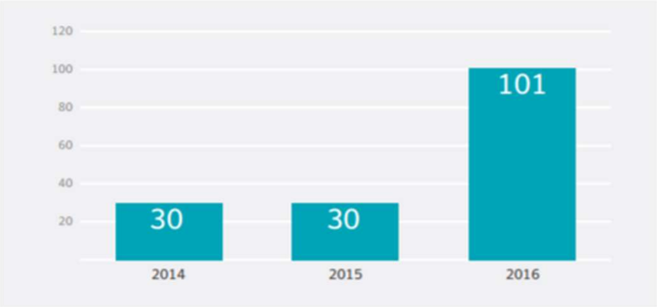


Figure 8 New Ransomware Families, 2014-16

2.3.4 Analysis of Consumer vs Enterprise infections

Although, ransomware threats affect devices indiscriminately, some groups specifically target businesses, as they can give greater amounts of ransom, as they are confidential and more valuable. Figure 9, which shows the number of blocked infections since 2015, indicates that the attackers are shifting focus from consumers to enterprises. 70% of the affected corporations have paid the ransom, whereas only 50% of the consumers paid ransom.

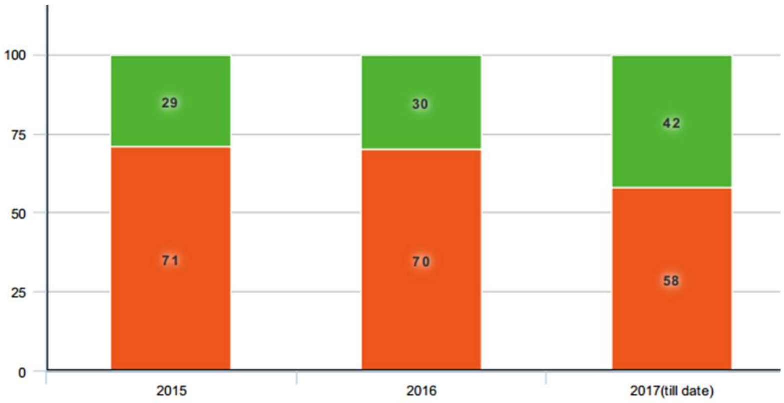


Figure 9 Ransomware: Consumer vs Enterprise

3. Financial Aspects

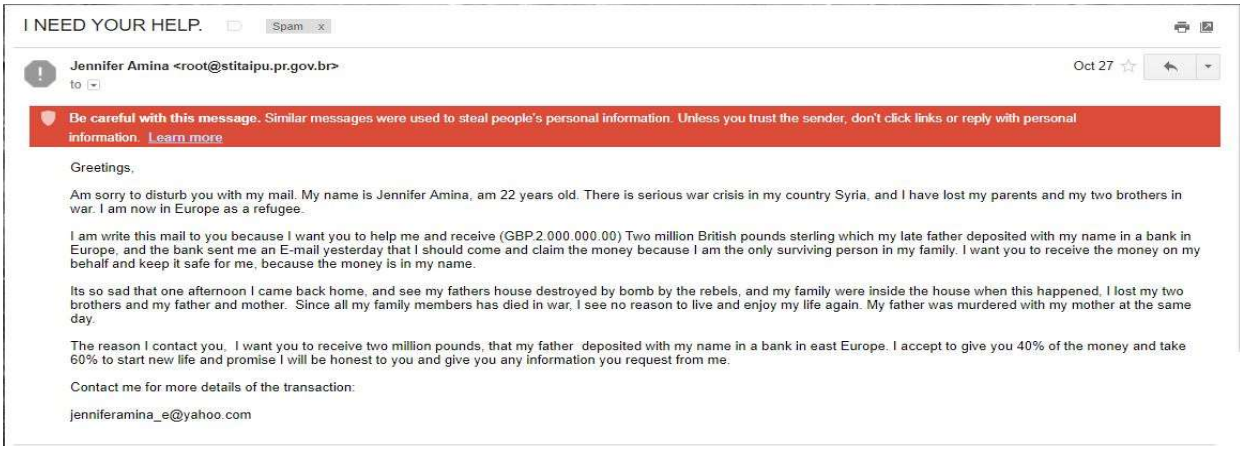
Over the past decade, the increase in the number of internet users and the advent of the Internet of Things (IoT) has led to the financial aspects of cyber security gaining importance. Cyberattacks and the related security measures have two primary financial aspects: the losses due to attacks and the cost incurred while implementing countermeasures.

3.1 The Losses

This section discusses the financial losses suffered by individuals, business outfits and companies through cybercrimes. The section will describe the Types and Quantity of scams in individual sections.

3.1.1 Types

Most forms of modern cybercrimes involve stealing data, mainly personal account details, from both consumers and the institutions which store them, like banks and IT companies. Many scams are targeted towards individuals who are unaware which include not only children and the elderly, but also CEOs of companies and important government officials. The most common form is phishing in which the attacker tries to obtain sensitive information like usernames and passwords by posing as a trusted individual over electronic communication software, usually email. An example is given in Figure 10.



I NEED YOUR HELP.

Jennifer Amina <root@stitaipu.pr.gov.br>

to

Oct 27

Be careful with this message. Similar messages were used to steal people's personal information. Unless you trust the sender, don't click links or reply with personal information. Learn more

Greetings,

Am sorry to disturb you with my mail. My name is Jennifer Amina, am 22 years old. There is serious war crisis in my country Syria, and I have lost my parents and my two brothers in war. I am now in Europe as a refugee.

I am write this mail to you because I want you to help me and receive (GBP.2.000.000.00) Two million British pounds sterling which my late father deposited with my name in a bank in Europe, and the bank sent me an E-mail yesterday that I should come and claim the money because I am the only surviving person in my family. I want you to receive the money on my behalf and keep it safe for me, because the money is in my name.

Its so sad that one afternoon I came back home, and see my fathers house destroyed by bomb by the rebels, and my family were inside the house when this happened, I lost my two brothers and my father and mother. Since all my family members has died in war, I see no reason to live and enjoy my life again. My father was murdered with my mother at the same day.

The reason I contact you, I want you to receive two million pounds, that my father deposited with my name in a bank in east Europe. I accept to give you 40% of the money and take 60% to start new life and promise I will be honest to you and give you any information you request from me.

Contact me for more details of the transaction:

jenniferamina_e@yahoo.com

Figure 10 An example of a phishing email.

Using the information obtained, the attacker is quite easily able to raid accounts and exploit credit cards. Recently, these attackers have become bolder and have tried to attack not only individuals with bank accounts, but also the banks themselves.

Another scam is termed as Business Email Compromise (BEC), involves scammers emailing employees, posing as the boss of the company and demanding transfers of large sums of money.

Ransomware is also a widely used scamming software which was in the news recently for affecting many people across the globe. The software locks down the affected server and does not release the information until a ransom has been paid. According to Internet Security Threat Report (Symantec, 2017, p8) the average ransom amount increased from $294 in 2015 to $1077 in 2016, an increase of 266%. And, with 4,63,841 detections in 2016, that brings the total losses to nearly $500 million.

3.1.2 Quantity

The average global annual cost of cybercrimes, acquired from Cost of Cyber Crime Study, is given in Figure 11:

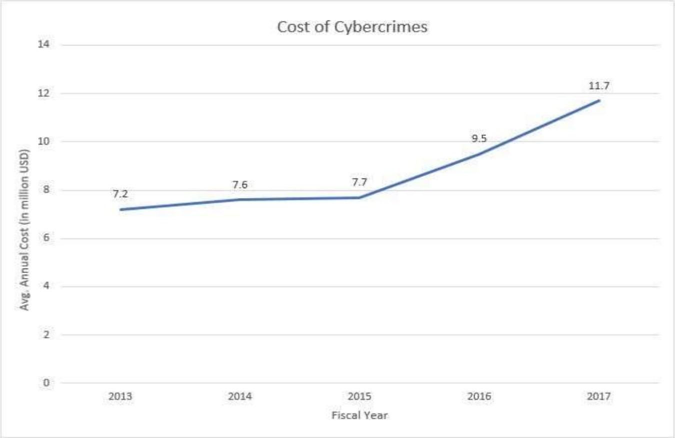


Figure 11 Cost of Cybercrimes

From Figure 11, it can be observed that in the recent years, the average annual expenditure has seen a significant increase. While the cost of cybercrimes had been relatively stagnant in the period 2013-15, the sudden increase in internet accessibility and the shift of developing countries like India towards online, cashless transactions could be the reason for the sudden change in 2015-16. Crimes of a larger magnitude, like attempting to steal money directly from banks, through forged online transactions can also be a reason for the observed rise, especially in 2017.

The loss to an individual, can vary widely, depending on the type of scam, access granted to scammers, vigilance and pre-existing security measures. While implementing security software like antiviruses is a solution, they are not always easily accessible, cheap or effective.

3.2 Costs Incurred

Many users consider a paid antivirus software as an unnecessary investment. Most people owning an antivirus software have the free or trial version, which does not include all features. Figure 12 shows the undiscounted prices of five popular antivirus software used in India. The prices have been obtained from the respective websites and have been scaled down (when required) to the cost of buying the software for one device for a year-long license.

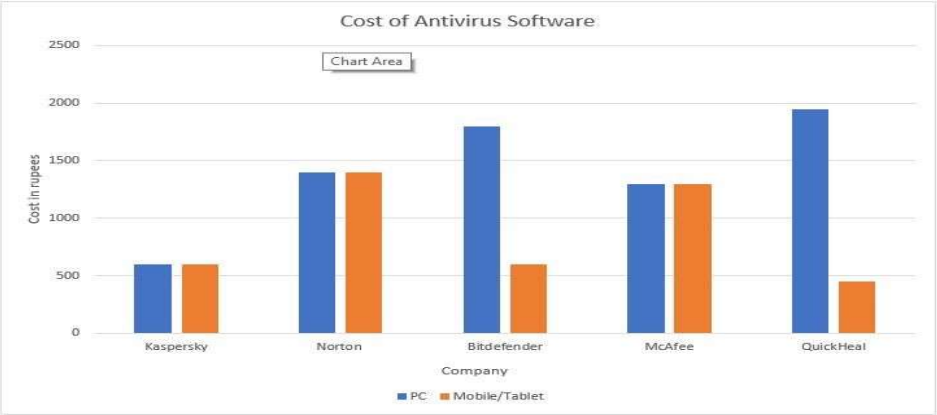


Figure 12 Cost of Antivirus Software

From Figure 12, we can see that Kaspersky, Norton and McAfee market the same software for both PCs and mobile devices. This can be an advantage for those requiring protection for a large number device as it is more convenient to buy a single software for all devices. However, Bitdefender and Quick Heal market separate software and are thus able to reduce the price of their antivirus for mobile phones. Apart from Kaspersky, who have lower prices for both interfaces, when a company markets a single software, the price is between that of the two-separate software.

McAfee provides a single software for all types of devices. It is cheaper than most of the comparable PC antivirus software available in the market. Although the software is costlier than most mobile protection software, it is a widely trusted software in India due to its easy to user interface, consumer-friendly offers and large vulnerability coverage.

4. Survey Analysis

While it is important for everyone to be aware of how to safely protect themselves online, some groups are markedly more vulnerable than others. School and college going students also fall under this category as they are one of the major users of the internet and related services. Thus, as part of our outreach program, we decided to gauge the levels of awareness about issues pertaining to cybersecurity among the students of BITS-Pilani, a technical university in Pilani, Rajasthan.

4.1 Methodology

An online questionnaire survey (Appendix A-1) was designed by the team using Google Forms. This was then circulated among the engineering students in their first year, via WhatsApp Messenger and through e-mail. In the span of two days, 200 responses were logged by the server, following which we stopped accepting responses. The data obtained has been presented and analysed in subsequent sections.

4.2 Type of Attack Experienced

Through the survey we found that only 19% of the respondents had never faced any form of online attack. This population could be the ones who are safe, however it is more likely that they are not well-informed about the different categories of cyberattacks.

Nearly 60% of the respondents were victims of spamming (Figure 13). Since most of students end up giving their email-ids on various websites, they become more vulnerable to spam. A reassuring fact however is that only 12% of respondents, were victims of phishing. This could be an indication of increased awareness among students. Around one-third of the respondents had encountered fake accounts. This could be because most students in that age group (18-21

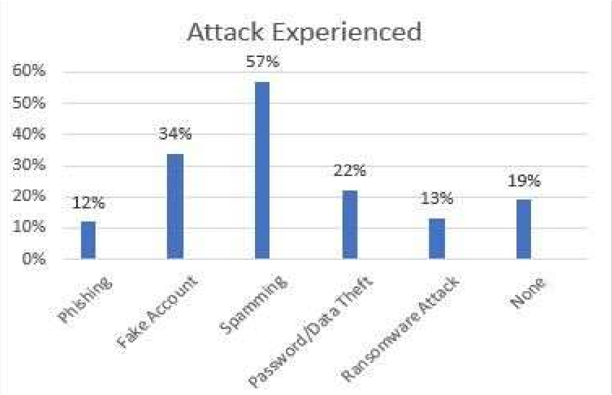


Figure 13 Types of Attacks Experienced

years) have accounts on social networking sites, like Facebook, Instagram and Snapchat, were creation of fake accounts is rampant. Password and Data theft is caused usually due to negligence of the user or systemic failure at the server end. It seems that the rather large fraction of respondents (22%) who have experienced this recently could be due to the recent security breach in Yahoo! Inc. Similarly, the recent rise of the ransomware malware, WannaCry, could be the reason for 13% of respondents to have experienced this usually corporate cyberattack.

4.3 Passwords

All forms of accounts online have at least a single-step authentication method, which is usually a password. While many websites force users to use a certain type or composition of passwords, others allow for variations, which may lead to easily decodable passwords.

4.3.1 Type

It is often advised that we use a password composed of Uppercase alphabet, Lowercase alphabet, Numbers, Symbols in a random order of a significant length, so that it cannot be decoded by brute-force cracking software. It is also advised not to use simple known strings, like birthdates, anniversaries, '1234' and 'qwerty'.

From our survey, it was found that 92% of our respondents choose to keep alphanumeric passwords (Figure 14). This is a good sign and shows awareness among the students about keeping a strong password.

Also, using similar passwords for all accounts is a common error among students. While it makes it easy for one to remember all their passwords it also puts all their data at a higher risk. From our survey, we have gathered that 54% of respondents use similar passwords for all accounts. This is not a very good practice and students must be made aware of the same.

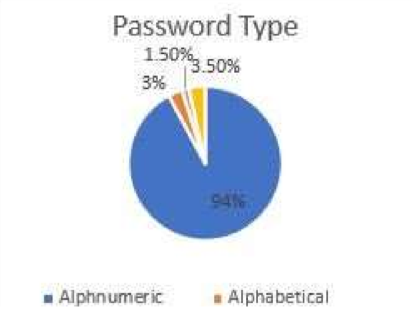


Figure 14 Type of Password Used

4.3.2 Frequency of Changing

Another guideline for a secure password, is to keep changing it frequently. While there is no ideal length of time that one should keep a password for, it is advised that passwords for accounts containing sensitive information, like online banking accounts should be changed monthly. Many websites also prompt users to change their passwords periodically.

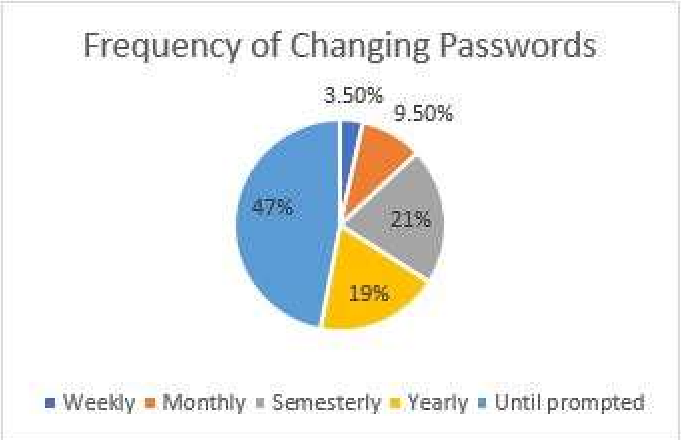


Figure 15 Frequency of changing Passwords

Nearly half of the respondents said that they changed their passwords only when prompted. As these accounts are likely to be primarily social media accounts, this frequency although not recommended, is relatively harmless. The remaining half change their passwords quite frequently with around 42% changing every semester and approximately 38% changing their passwords annually.

4.3.3 Saving Passwords Online

Many browsers, like Google Chrome, Mozilla Firefox and Microsoft Edge allow the users to save passwords. While this is usually a very secure practice, it is not advisable to do so on public computers, or for accounts containing sensitive information. Even on home computers, it is possible for someone to misuse this access, hence, it is better to be safe.

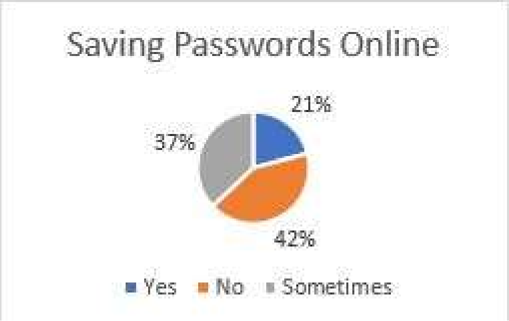


Figure 16 Saving Passwords Online

4.4 Logging in on Public Networks

Many times, students are often forced to login to their accounts in public places, like cyber cafes, libraries, airports. In such cases, it is advisable to be very vigilant as public networks have minimal protection and can leave your data susceptible to theft. Using an incognito browser is effective for some threats, however, if the computer you are using, or the network you are connected to have been tampered with, using it will be of no use. Unless absolutely required, it is not advisable to use public computers at all, however, in case it is necessary, prefer one with a reliable antivirus software in a reliable place.

From Figure 17, nearly two-thirds of the respondents log in to their personal accounts on public networks, around half of them on incognito mode. While this is not a very safe practice, circumstances may mandate the situation.

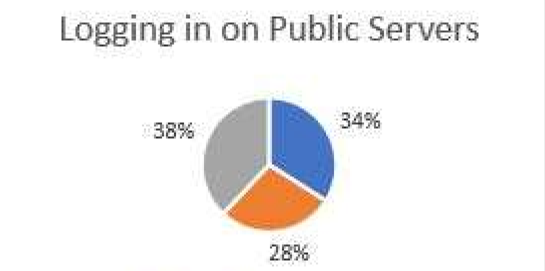


Figure 17 Logging in on Public Servers

4.5 Use of Antivirus Software

As mentioned in chapter, many students will be reluctant to download paid antivirus software, especially on mobile phones and tablets.

As expected, nearly 75% of the respondents have antivirus on their laptops, while only 35% have it installed on their phones. Similarly, around one-third of those who use tablets, have antivirus software installed on it. The reason why a large percentage of smartphone users do not use antivirus applications could be that very few of the applications are free and it is rare for students to spend money on mobile applications. The large percentage of laptop users owning antivirus software could be attributed to the fact that many trial versions are available for free online.

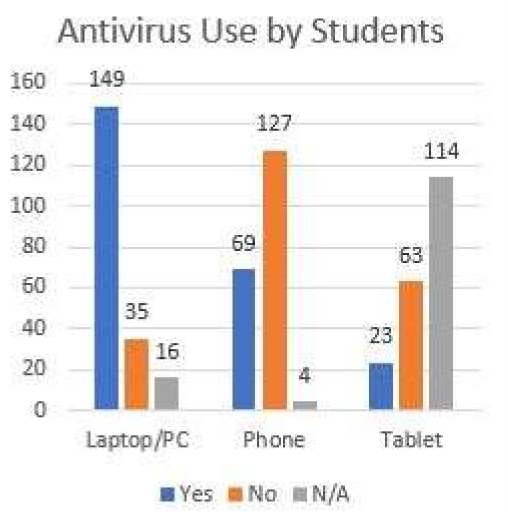


Figure 18 Antivirus Usage

4.6 Frequency of updating antivirus

As technology gets more sophisticated, more serious threats emerge. To combat these, companies like ours frequently update our software so that they are better suited to protect the device. Always having an updated version of the software is a safe practice.

Around 60% of the respondents who use antivirus software, update it as soon as an update is available. A possible reason could be that most software have an auto-update feature. A significant percentage, 18.7% update only when it is absolutely required. This could be because software updates often take up disk space, which is undesirable for many.

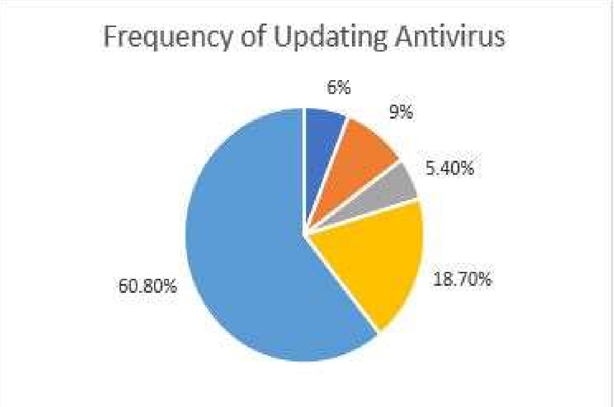


Figure 19 Frequency of Updating Antivirus

4.7 Sharing Card Details Online

With the growing success of e-commerce, nearly every store online allows for multiple methods of payment including credit and debit cards. Thus, browsers and websites, both allow for their users to save card details online, thus saving the task of typing it in at every instance.

Although most students among the sample space own either a debit card or a credit card, online purchases are not always made using them. Thus, not many people would feel the need to save card details online. This is supplemented by the fact that people are even otherwise, reluctant to save card details online, due to qualms about security.

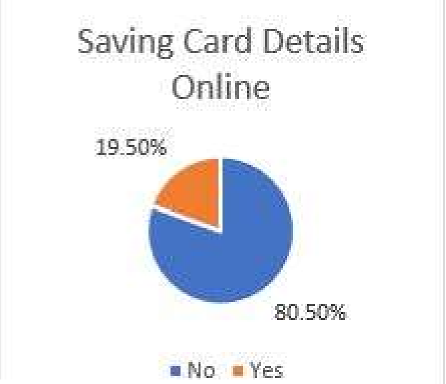


Figure 20 Saving Card Details Online

5. Conclusions

The following conclusions can be drawn from the reasoned analysis carried out in Chapter 2 through Chapter 4:

1. A low-cost and user-friendly security system equipped with ground-breaking technology has a positive effect on market value of the organisation.
2. Weak network and data security may lead to major losses, be it for an individual or an organisation.
3. Spam mail may often contain malware, infecting the computer and retrieving confidential information.
4. A free or trial version of an antivirus is not very effective. Investing a small amount in an antivirus software may prevent major losses, be it in confidential information or in financial resources.
5. Awareness among youth generation, although encouraging, is incomplete. While many students are aware of the threats they face, complete awareness of the various secure practices is required.

6. Recommendations

The following recommendations can be made based on the conclusions drawn in the previous chapter:

1. The rise is the number of cyberattacks implies a greater need for secure software. The Research and Development Division, should direct their future path accordingly and produce mass-distributable, consumer friendly software.
2. The marketing division, using the conclusions drawn from this report is advised to market our new products by emphasizing on the importance of using secure software.
3. The company through its outreach program, should conduct workshops, to enlighten students about:
    - To prevent ourselves from such kind of malware attacks, we must regularly back up our data. The security software of our devices should be kept up-to-date.
    - Operating systems and apps must be updated as soon as a new update is available.
    - Be wary of any attachments in your Emails especially those of Office and JavaScript.
    - Delete any Email which looks suspicious.
    - Passwords should be strong and unique.

7.Appendix

Appendix 1- Questionnaire Survey conducted at BITS Pilani

1. Which of the following cyber security issues have you faced?
- Phishing
- Fake Account
- Spamming
- Password/Data Theft
- Ransomware Attack
- None
- Other:______

2. How do you frame your password?
- Alphanumeric
- Only alphabets
- Only numeric
- General codes (e.g.- 123456, password, qwerty, *mobile number* etc.)

3. How often do you change your password?
- Once a week
- Once a month
- Once in 6 months
- Once a year
- Unless prompted by admin

4. Do you use similar passwords for all your accounts?
- Yes
- No

5. Do you use the "save password for this site" option while logging in to your online account?
- Yes
- No
- Sometimes

6. Do you login to your personal accounts while using public networks?
- Yes, using incognito mode
- Yes, without using incognito mode
- No, I do not login

7. Do you use antivirus on the following devices?

	Yes	No	I don't use this device
Laptop/PC			
Smartphones			
Tablets			

7.1 If you answered yes to any of the above options, how often do you update it?

- Whenever a new update is available
- Once a month
- Once in 6 months
- Once a year
- Until version stops working

8. Do you save your credit/debit card details online?

- Yes
- No

8. List of References

1. Finra Report on Cybersecurity Practices. (n.d.). Retrieved from https://goo.gl/H7IPYA
2. Accenture Cost of Cyber Crime Security. (n.d.). Retrieved from https://goo.gl/jQ2bgg
3. Symantec Internet Security Threat Report 2017. (n.d.). Retrieved from https://goo.gl/FPjSgC
4. Cisco Annual Cybersecurity Report 2017. (n.d.). Retrieved from https://goo.gl/JW8DTW
5. George, J. Wipro State of Cybersecurity Report 2017. (n.d.). Retrieved from https://goo.gl/mcFfaF
6. The Best Antivirus Protection of 2017. (n.d.). Retrieved from https://goo.gl/ezvoxv
7. India's Top 10 Best Antivirus Software 2017. (n.d.). Retrieved from https://goo.gl/sHqABm
8. Phishing. (n.d.). In Wikipedia. Retrieved on November 8, 2017 from https://en.wikipedia.org/wiki/Phishing
9. Singer, P.W., Friedman, A. (2013). Cybersecurity and Cyberwar: What Everyone Needs to Know?. New York, NY: Oxford University Press.