IJCSN - International Journal of Computer Science and Network, Volume 9, Issue 5, October 2020
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Statistics of Cybercrime from 2016 to the First Half of 2020

Dr. Fatma Abdalla Mabrouk Khiralla

Department of Computer Science, College Of Science and Arts in Unaizah, Qussim University, Buraydah, KSA

Abstract - Expansion of electronic transaction raised the need for more confidentiality and data protection against cybercrime. Cybercrime is defined as a criminal activity that targets internet users. Cybercriminals who commit cybercrime usually aim to make money through this action, but they could also tend to damage computers for reasons other than profit. Cybercriminals could be individuals or organizations. Some cybercriminals are highly technically skilled, well organized, and use advanced techniques. Information technology security specialists have reported a significant increase in cybercrime since early 2001. Cybercrime is expanding because the information technology has become a fundamental part of people's lives. Expansion of cybercrime raised the need to Cybersecurity and information security. Cybersecurity is defined as the practice of protecting information and data from outside sources on the Internet. Information security is defined as the protection of information and information systems from unauthorized use, assess, modification or removal. In this paper, statistics of Cybercrime has been analyzed from 2016 to the First Half of 2020, beside a summarization of cybersecurity and information security, projecting the difference between cybersecurity and knowledge of security.

Keywords - *Cybersecurity-Information Security- Data Science -Cybercrime- Social Engineering- Artificial Intelligence-Internet of Things*

1. Introduction

In the digital age, information became an important economic resource, thus it is considered an essential tool for measurement of success or failure at the individual, organization, and community levels, and at national and international levels, and an essential factor in the concept of development. Therefore, data security has become an important issue and a growing concept, affecting all sectors without exception.

Now, almost everything is displayed online from e-government and e-commerce to social media as every part of life became available on the internet. Hackers can work to access this information and use it for their own purposes. Indeed, everyone needs cybersecurity because everyone has personal information available online. Some events influence cybersecurity like the development of devices, the spread of epidemics, and wars.

2. Cybersecurity and information security

Cybersecurity is defined as the practice of protecting information and data from outside sources on the web. Cybersecurity professionals protect networks, servers, intranets, and computer systems. It also ensures that only authorized people have access to that information [1]. Information security is all about protecting information and knowledge systems from unauthorized use, access, modification, or removal. It is like data security, which should do with protecting data from being hacked or stolen [1].

Data is assessed as information system meaning something, all information is a datum of some kind, but not all data is information. When certain things are stored in an exceedingly automatic data processing system, they are considered data. It is not until it is actually processed that it becomes information. Once it becomes information then it is needs protection from outside sources. These outside sources might not necessarily be in cyberspace.

3. The Important of Cybersecurity

Personal data that might lead to fraud is now posted to the public on our social media accounts. Sensitive information like Social Security numbers, MasterCard information, and checking account details are now stored in cloud storage services. So the rely upon computer systems increase day by day, cloud service security, smartphones, and also the Internet of Things (IoT) make governments around the world bring more attention to cybercrime.

The cybersecurity industry can have good leads to information security. Cybercrime is a crime that involves a computer and a network. The PC (Personal Computer) is the tool used in the commission of a criminal offense, or it should be the target. People rely on technology quite ever than before and there is no sign that this trend will slow. The Coronavirus pandemic has led to the biggest number

of employees globally guaranteed to work remotely. The individuals functioning from domestic required mindfulness and data of phishing tricks, the speediest developing variety of cybercrime, numerous of which are presently playing on fears of the Coronavirus.

Workers from organizations of all sizes and sorts presently have minimal cybersecurity assets, compared to what is ordinarily available to them. Because of the local pandemic work from home gets to be the trendy type.

Criminals are taking advantage of the widespread panic, and in that they succeed, Unused Coronavirus-themed phishing scams are leveraging fear, snaring helpless individuals, and taking advantage of work environment disturbance. Cybercrime costs incorporate harm and devastation of knowledge, cancellation of hacked information and frameworks, stolen cash, misplaced efficiency, robbery of individual and budgetary information and misappropriation [2].

4. The Impact of Social Engineering in The Occurrence of Cybercrimes

With the gigantic development in technology, particularly within the field of the Internet of things and data science, it has to be exceptionally simple to communicate with the client off the web.

Cybercriminals utilize a strategy called social engineering to get private data, and this matter is effectively made less demanding unless the client employments all secure strategies of utilizing the Web. Social engineering is the utilization of human shortcomings to compel work and get a secret [3].

A commonplace case of social engineering is false / spam e-mail as the aggressor sends a misleading mail to an undesirable target or gather with the purpose of getting secret data such as login accreditation, passwords, and security codes. Pranksters regularly construct spam messages with expressions and keywords that create a sense of criticalness and fear, both of which are human weaknesses that encourage social engineering assaults.

After the emergence of the Coronavirus pandemic, people started searching for sources of the virus, the number of infected people, and most countries infected, and searching for finding a cure and how to prevent it, so cybercriminals began to take many advanced forms of phishing.
A phishing attack is a kind of used social engineering; it is a customized version of the phishing process where profiles and exact details of the target recipient are intelligently presented in the text of the email to make the correspondence appear authentic.
A classic spear-phishing scam will address the target in his correct official appointment, the salute like dear Dr, and his exact assignment/responsibilities.

Annoying Coronavirus emails will victimize a tone of familiarity while providing a service that claims to contain the most recent information about the disease. Pranksters often build spam messages with expressions and keywords that create a sense of urgency and fear [4].

5. The Beginning of the Era of Cybercrime

Cybercrime started in the 1820s if it is believed the computer did exist since 3500 BC in India, China, and Japan. The crimes continued until this moment [1].

Within the 1960s the attacks on communications frameworks driven to the subversion of the long-distance phone frameworks for entertainment and theft of administrations. Programmers within the 1980s started composing the malevolent program, including self-replicating programs, to meddle with individual computers.

When the 1990s come, monetary crime utilizing infiltration and subversion of computer frameworks increased. The types of malware moved amid the 1990s, taking advantage of unused vulnerabilities and passing on out as working systems were fortified, only to succumb to new attack vectors. Ill-conceived applications of email developed quickly from the mid-1990s forward, creating deluges of unsolicited commercial and false e-mails.

By the mid-2000s, concerns over the physical security of electronic voting systems had risen to public awareness. In 2000s hackers attacked CNN companies in Atlanta and Georgia. The same cybercrime included insidiousness to property in the abundance of $5,000 against Web sites, counting CNN.com, in connection to the February 2000 attacks. The other checks related to unauthorized access to a few other websites, counting those of a few US colleges [5].

A 2013 study by researcher Kelly White, noted that the 1990s was a goals rich decade for the cybercriminals. Fortunately, for Companies and users that enter their sensitive data on the web, hackers firstly made misshape of websites, rather than focusing on the sensitive information stocked in the systems. It took more than years for the criminal exploit to benefit from how to

businesses computer crime financially. [6]. Two events helped to cybercriminals in the 1990s. One of these events was the discovery of the World Wide Web. In 1990, Tim Berners -- Lee ended his build out of three important combinations for his World Wide Web (WWW) project, the three components are a web server, a web browser, a web editor, and the first web pages. In 1991, the project globally available on the Internet as the 'Web'.

Surprisingly, the Web grew and designed over 17 million web sites. The other event was the makeup of globally web access points. In 1994, the National Science base sponsored four business groups to build public Internet access points, the business groups are Pacific Bell Company, WorldCom Company, Sprint Company, and Ameritech Company.

In addition, Kelly White mentioned that in the 2000s, the cybercrimes developed from occasional, from one-person operations to sequential events made with an exceedingly advanced, evenly coordinated criminal industry. Whereas numerous of the crimes had been seen in previous decades, the recurrence and size of the crimes are not happened again [6].

6. Global Cybersecurity Spending Predicted

In Cision, e-news magazine mentioned that 2019 Official Yearly Cybercrime Report Declared by Cybersecurity Ventures Dec 13, 2018, 10:11 ET, Cybercrime is the most prominent risk to every company within the globe [4], and one of the greatest issues with humankind. The effect on society reflected within the Official 2019 Yearly Cybercrime Report, reported nowadays by Cybersecurity Ventures.

The report said that cybercrime is taken a toll the globe $6 trillion each year by 2021, up from $3 trillion in 2015. This speaks to the foremost noteworthy exchange of monetary riches in history, dangers the motivating forces for development and venture.

Steve Morgan, founder, and Editor-In-Chief at Cybersecurity Ventures mentioned the cybercrime costs include damage and destruction of knowledge, stolen money, lost productivity, and theft of belongings [7], theft of private and financial data, embezzlement, fraud, and post-attack disruption to the traditional course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.
Cybercrime is making exceptional harm to both private and public ventures and driving up data and cybersecurity budgets governments also in little businesses and mid-sized businesses.

Cybersecurity Ventures predicts worldwide investment in cybersecurity items and administrations will exceed $1 trillion in total for the five years from 2017 to 2021, also they expect 12%-15% year-over-year cybersecurity market development through 2021.Cybercrime is expected to triple the number of work openings about three million unfilled cybersecurity positions by 2021, which is up from one million in 2014, and the cybersecurity unemployment rate will remain at zero percent [8].

7. What Made Cybercrime Easier

Cybercrime attacks have become a significant increase in the presence of the appropriate environment for them. Computers have become cheap and smartphones have become reasonable for everybody with the use of the Internet and the availability of free applications and deepen on electronic transactions.

Most people use their smartphone to manage budgetary operations or handle sensitive information and most phones are presently utilized for two-factor verification, it is one of the foremost broadly utilized cybersecurity apparatuses. It increases the security risk if the device is lost or stolen.

On the Internet of Things (IoT) innovation, IoT devices are powerless, since significant portions of them do not have a client interface. This may lead to issues understanding what kind of information the device collects or oversees so, it seems to become an entry point for an assailant or device to launch a Distributed Denial-Of-Service (DDOS) attack.

IoT tools are not secure by the plan, since putting a center on security would significantly increment manufacturing and supporting expenses [9]. The majority of (Artificial Intelligence) AI qualities serve pernicious purposes. AI systems are cheap, versatile, and anonymous.

8. The growth rate of Cybercrime from 2016 To the First Half of 2020

Presently cybercrime is one of the greatest issues with mankind, because everybody with an e-mail address, a bank account, or any sensitive information. Anyone can become a target, and it has an impact on society that is reflected within numbers.

Cybercrime develops year after year, as criminals adjust their strategies overtime, the changes that occur in the world, the special techniques in the field of the Internet, such as the Internet of things or the emergence of a specific situation in a society like Coronavirus pandemic make the attackers develop Cybercrime. Most Internet users do not understand the crime on the web, how to attack, and how to protect against it. So, it is necessary every user must be study the procedures of cybercrime and they must focused on applications that attacked each year and countries which have a big cybercrime.

To know the prediction on the future, and how to protect from attacks. This paper was study cybercrime in a specific time period.The main point of the study is about the growth rate of cybercrime in specific countries from 2016 to the first half of 2020, and the type of cybercrimes.

8.1 Cybercrime in 2016:

Cyberattack is continually on the rise since more users are connected online. All these connections for business, social media or shopping purposes. By a lot of applications and a difference in devices like smartphone or laptops the variation of ways to attack are big. A cyberattack is an attack that occurs on the web or a crime that includes computers or cyber aspects.

According to the report in April 2017from an American cybersecurity company Symantec shown in figure 1, the United States is the biggest country that has had phishing attacks in 2016. It sits at the top of the Symantec's list. In the final year 2015, it was number two, with 18.89% of dangers recognized universally, but that has risen to 23.96% [10].

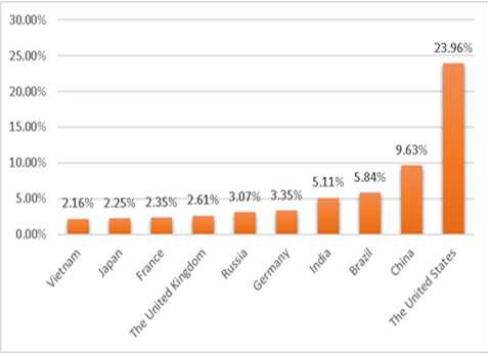

Fig.1: the 10 countries that were the source of the most cybercrime in 2016

The reason for this is that a kind of malware appeared and spread around the world, by the name of Mirai .It began to utilize the Mirai source code to dispatch broad- ranging DDoS attacks (Distributed Denial Of Service) on different targets.

A DDoS is a kind of DoS (Denial of Service) attack which includes various compromised devices, or even a network of them — to perform a particular goal. The DDoS attack employs all of the devices with one another, links to the object, and rise it with passing requests, using a "botnet" from unsecured connected devices, for example, smart devices, and even baby monitors [11].

According to an article published by The Established for Critical Infrastructure Technology, Mirai misused the Internet of Things technology with production line default or hardcoded client names and passwords and utilized them to make and construct a botnet. In October 2016, the Mirai Botnet was sent against the Web infrastructure company Dyn [12].

Dyn is a web application security company, which provides critical innovation administrations for websites all day to give them safe entry to websites like Twitter. Dyn depicted the Mirai botnets as the essential source of pernicious attacks that stopped Web use in 2016 [13].

8.2 Cybercrime in 2017:

The first half of 2017 has seen an inordinate big attack on the internet a level of companies and users. The hundreds of crime cases on the online web, and hacking on an unprecedented level caused new attacks not only in number but also in intensity. This was a busy year for the cybersecurity industry. Concurring to a published report by Symantec Corporation, the world's leading cybersecurity company (2018 Web Security).

In 2017 there was a 600 percent increment in by and large IoT attacks, this implies that cybercriminals might of have exploited the associated nature of those devices [26].The figure2 shows, the 10 countries that were affected by e-crime in 2017. Customers in Brazil experienced cybercrime misfortunes worth 22.5 billion U.S. dollars. Universally, the average cybercrime victim lost 142 U.S. dollars.

According to the investigation report by Alibaba Security Zero Lab statistics, between the fourth to the ninth month of 2017, hundreds of thousands of communications extortion happened within China, this case costed more than 100 million yuan, and tens of thousands of victims were included, Communications have remained a tall and broad case of extortion to date [7].

On the U.S. in 2017, Yahoo hack was as of late re-accounted to affect 3 billion client accounts, and Equifax's hack in 2017 - with 143 million clients affected - was the biggest freely uncovered hack ever. According to the 2017 cyberattacks report [7]. The most common cybercrime in 2017 is WannaCry, NotPetya, and KRACK according to the MailGuard site [15].

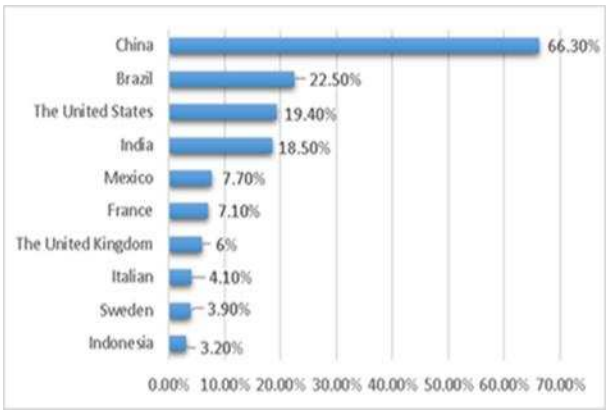

Fig.2: the 10 countries that were affected by e-crime in 2017

8.2.1 WannaCry worm

When the WannaCry appeared has infected about 200,000 computers in 150 countries. It was assaulted security in older versions of Windows operating systems known as the EternalBlue exploit. Once it infected a PC it would then duplicate itself over systems, spreading rapidly and invisibly [15].

Unfortunately, WannaCry affected huge businesses and fundamental frameworks in a big number of countries. The largest Spanish telecommunications Telefonica firm was the first one that reports a WannaCry ransomware attack , Largest Russian telecommunications MegaFon was infected ,Hungarian telecommunications provider affected the name Telenor.

The firm's manufacturing plant Nissan in Sunderland, northeast England was influenced and car manufacturing plants owned by Renault ,German train operator Deutsche Bahn was influenced , also infected Russian Railways' IT systems , and Sberbank the Russia's largest lender ,Bank Of China,Singapore malls and Sandvik the Swedish IT, and FedEx distribution centers, etc.

Some institutions were able to successfully thwart the attack. The governmental entities and offices in many countries was infected for example Hundreds of Health centres in the UK which ran by older computers ,Russian Interior Ministry around 1,000 computers had been affected , Indian police on the state of Andhra Pradesh said being out of their systems in as a lot of as 18 different police units, and Chinese police station, immigration and public security bureaus were influenced by a WannaCry ransomware attack, also Brazil Foreign Ministry, social security systems, and court systems and Russia Central Bank[16] . Estimates of the monetary hurt caused by WannaCry are still a point of debate, the harm in an overabundance of US$4 billion.

8.2.2 NotPetya virus

After a few weeks when the WannaCry attack occurred around the world, the NotPetya virus appeared in Ukraine, France, Germany, Italy, Poland, UK, US, and Russia.

The big impact to NotPetya virus in Ukraine where 80 companies and organizations were attacked by the virus, including the National Bank. Both FedEx and Maersk publicly said that the NotPetya various hit cost them about $300 million each [17].

8.2.3 KRACK

By the end of 2017, security researchers at the College of Leuven in Belgium found the critical weak point in all standard WiFi devices. The weak point within the WiFi protocols makes it possible for the attacker to read encrypted data on WiFi devices and utilize them to break into a network, Breakout point was named KRACK (Key Reinstallation AttaCKs). Quickly notified manufacturers of WiFi gadgets, who began executing patches to shut the gap within the security of their frameworks [15].

8.3 Cybercrime in 2018:

According to writer John Pescatore on the Identity Theft Resource Center (ITRC), USA, April 2019, in 2018, there were more than 300 cases of data breaches in the world. It affected medical and healthcare organizations. Noted that the medical patient registers are seen as easy targets for an attack because security often lags due to the focus on the case in healthcare, and patient care over the information and technology [17].

Also, the Phishing email detections increased globally by 250% from January to December 2018. Phishing attack methods have evolved, as attackers are forced to bypass increasingly efficient anti-phishing tools and techniques [18].

Globally, China was the foremost extremely attacked country shown on figure 3, seeing 36% of total around the

world attacks, the second was the USA at a percentage of (32%) [19].

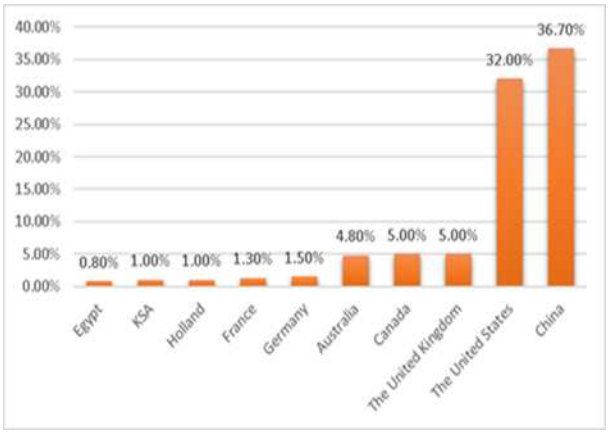

Fig.3: The growth rate for global distribution of attacked IP addresses in 2018

In 2018, KSA notified that over 160,000-cybercrime hit its servers each day, Saudi Arabia telecom authority alerted before to make all organizations ready for a new variation called Shamoon 2, this attack making the KSA the biggest country attacked in the Middle East in 2018 [20].

The attack in 2018 connected with cybercrime in 2012, where cybercrime increased on KSA since 2012 when shammon attack Saudi Aramco Company amid which information was crushed on tens of thousands of computers. After a long time another version of it appeared with more modern highlights it was given the name Shamoon 2.0. Shamoon 2.0 attacked the KSA. On 17 November 2016, the attacks continued until January 2017 and then 2018 [21].

8.4 Cybercrime in 2019:

2019 saw the greatest cyberattack targeted ransomware on health care and public sectors. the attack in a network layer DDoS in the first and second quarter of the year reached 580 million packets per second (PPS). Within the second quarter of the year, DDoS attacked China by 63.8 percent and attacked the U.S. by DDoS attacks with 17.5 percent of the attacks. So, China and the U.S. was positioned as the greatest two targets for DDoS attacks within the second quarter of the year [11].
In 2019 saw the high number of network layer attacks against businesses in the East Asia locale, making the area exceptionally dangerous by the number of attacks and the probability of being attacked. India topping the list, seen in figure 4 it was the greatest attacked country. East Asia had 77.7 percent of all network layer DDOS attacks [22].

In addition, there are other industries attacked with DDoS like the media information services and insurance industries. Mirai and Mirai botnet variants also have been the most common malware to target enterprise IoT devices in 2019 [11].

Some countries started to protect themselves before the attack in 2019, including the Kingdom of Saudi Arabia, which witnessed an increase in the attempted attacks in Aramco Company in the last quarter of 2019, and it succeeded in responding to this attack [23].

Internet of Things (IoT) technology opens the door for the greatest distributed dissent of service (DDoS) botnet attacks in 2019. Because IoT device producers proceeded to ship items that could not be legitimately secured.

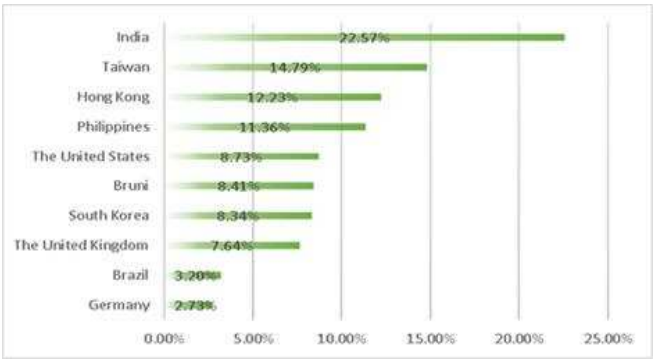

Fig.4: Top 10 attacked countries, by number of network layer attacks in 2019

According to CPO magazine report, the last quarter of 2019 showed the connection between IoT devises and DDoS attack in a few characteristics some new patterns, including joint powerlessness in the WD-Discovery protocol that's being broadly misused and the utilize of Autonomous Number Systems (ANS) to track assaults back to their source. The report also investigates how the rollout of 5G will affect DDoS attacks [24].

8.5 Cybercrime on 1rst half in 2020:

The effect of social engineering was apparent from the start of 2020 when the looks of the corona pandemic because the criminals utilize this procedure to induce private data from defenceless victims and utilize such data to launch other assaults. Social engineering utilized human shortcomings to induce secret data [3].

People needed to remain on the house and make electronic transactions, and the look for information on the Coronavirus, so cybercrime trusted the requirement for the network. The reflected was later DDoS attacks, the

foremost-targeted resources within the first quarter in 2020 were websites of health care and medical systems, transport administrations, and gaming and academic stages.

In January 2020, The Greece government especially the websites of the government offices and emergency administrations were attacked. In February, a DDoS attack fails on the registration, and the knowledge website for the US presidential election was attacked.

In March 2020, the cyberattack was starting on the positioning of the US Department of Health and Human Services (HHS) with none impact. Moreover, some attackers spread deception in social systems and this through text and e-mail.

In Paris, a group of healing centers was attacked with DDoS Cyberattack attempted to disable on the infrastructure of medical institutions. Also DDoS attacks on food delivery services Lieferando in Germany and Thuisbezorgd in Netherlands, all of these attacks were successful [25]. In Germany, the distance-learning platform Mebis was attacked on the primary e.learning school day.

In Arabic countries figure 5, the researchers saw between January – June 2020, the cybercrime on mobile users reached the following, UAE 68,063, Egypt is 220,000, and Saudi Arabia saw 160,000 attacks in 5 months, followed by Kuwait (20,000) and Oman (15,000) [26].

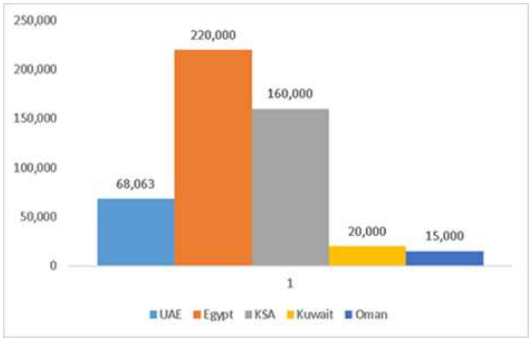

Fig.5: The cybercrime attack on mobile users in Arabic countries between Januarys – June 2020

According to Saudi Gazette Journal newspaper of the Kingdom of Saudi Arabia the statistic of cybercrimes in 2020 on smartphone clients, the analysts saw that in the period of January-June 2020, the amount of malware on the phone about 157,475. So, the clearly it appeared that isolate failed to have a chosen impact on the risk scene, the sum of attacks has expanded up to 35,000 on the average [27].

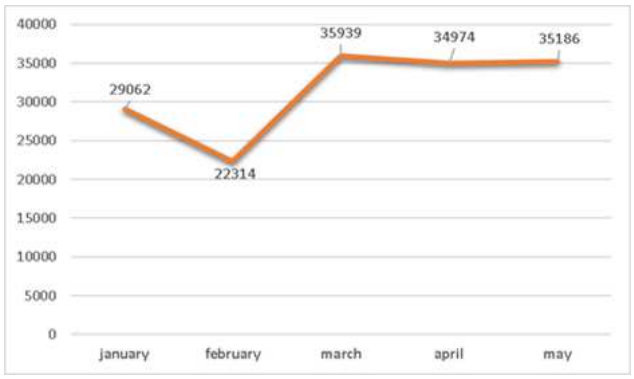

Fig. 6: Cybercrimes on smartphones in KSA in 2020

Smartphones in commerce forms are developing quickly, and cybercriminals are paying more consideration to how they are conveying malware conjointly the assault vectors utilized, expanding their movement in times of crisis.

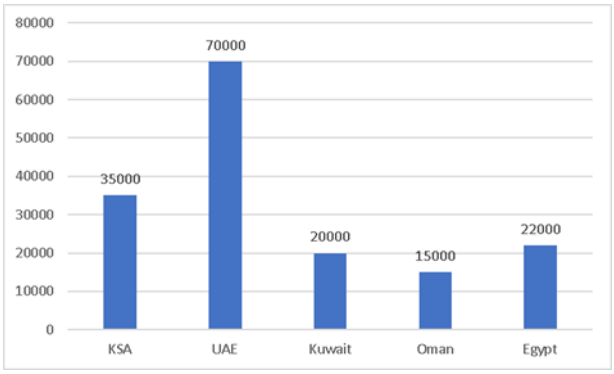

Fig. 7: Cybercrimes on smartphones in Middle Eastern countries in 2020

9. Challenges for Safety cybersecurity system

The Internet has gotten to be one of the foremost important things in life. It is used for several purposes, for example, governmental transactions, education, and business, etc.

Nearly 80 percent of transactions are via the Internet, especially when the COVID-19 pandemic arose. The attackers began to hit on the internet, they develop the ways year after year their attacks, they used a variety of methods to put malware on the network, and rely on social engineering in their attacks and the methods of phishing were developed.

Social engineering makes hackers devising ever-more clever methods for fooling users and individuals into handing over sensitive data, so it was obligatory to protect information from electronic attack and know the gaps

through which the attackers take opportunities to access sensitive information.

First and foremost, it is necessary to know the methods that the cybercriminals used in recent years. When referring to the attacks between 2016 and the starting of 2020, it was found that the attack were carried out with mistakes and gaps that must be paid consideration.

When managing with the Web, the client must have full awareness and consideration to managing with any e-mail, clients must be alert from random emails and each mail with an interesting sender's address or unknown, should be taken care because this emails can be a potential cybersecurity risk masked as an honest to goodness resource.When searching for specific information, you should pay attention to the source of the information and the trusted sites and Avoid questionable web addresses.

It is important for users to be clever and with vigilance when searching for any data on the web because social engineers usually take advantage of human weaknesses to obtain confidential information. For example, at the beginning of 2020, coronavirus pandemic was a big reason to attack the web, the user behaviors have the negative influence impact of the internet. The effect of social engineering was apparent from the start of 2020 when the looks of the corona pandemic.

The criminals utilize this procedure to get private data from defenseless victims and utilize such data to launch other assaults. Complete care during commercial transactions from buying and managing account transactions. The client must be a consideration to commercial websites before making payments or any e-transaction.

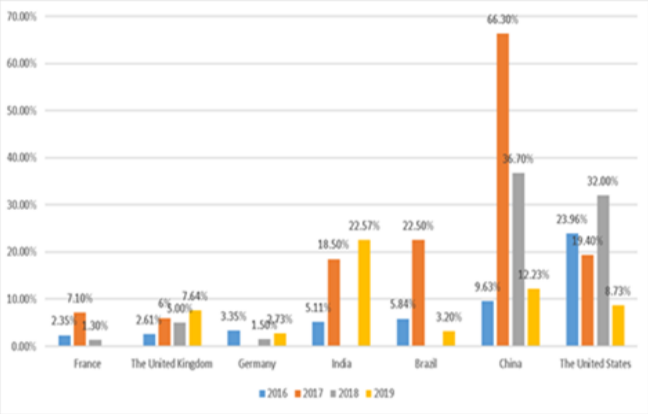

Fig.8: The growth rate of Cybercrime in specific countries from 2016 to 2019

- Users must be sure to protect the device and use original antivirus software, and periodically updating antivirus and malware protection programs. Today's cybercrime incorporates huge of viruses and malware. There are numerous different sorts of online threats that can infect devices and allow cybercriminals access to client data. So the user must download an anti-virus program designed to recognize substances that is possibly hurtful to the computer. For example Norton antivirus and Kaspersky virus protection software.

- A security arrangement includes antivirus as one of the establishments of how it helps protect against malware, web security regularly alludes to a computer program suite that has extra types of innovation in expansion to antivirus.

- Computer program security innovation incorporates multiple layers of defense to assist capture and block all kinds of online dangers that attempt to infect devices. Antivirus checks and makes a difference evacuate malware records that enter a computer, tablet, or smartphone [28].

- Be careful with downloading files, especially large ones. Awareness when dealing with smart devices and pay attention to dealing with the Internet means opening all sensitive information. Deal with caution with the Internet of Things technology. In 2016, Mirai misused the Internet of Things technology with production line default or hardcoded client names and passwords and utilized them to make and construct a botnet [3].

A backup on the PC or web is exceptionally helpful to decrease the effect of an information loss. For the protection of data, it is fitting to perform periodically customary information backup to prevent the plausibility of gigantic information loss in case of attack.

10. The Result of Study

The statistics report of this paper indicated the increasing number of cybercrime when the number of Web users is high. The more attacks and its advancement are observed yearly. In addition, making distinctive shapes of cyberattacks.

Unfortunately, it is incomprehensible to record and classify cybercrime in official measurements making, moreover it is inconceivable to know the degree to which computers were included within the commission of a crime or were the base target, and cannot to decide precisely how numerous people have been effectively arraigned around the world.

According to the study the growth rate of Cybercrime in specific countries from 2016 to the first half of 2020, that most of the countries that were vulnerable to cyberattacks are China, followed by the U.S. The most common years where cyberattacks happened were in 2017, these happened globally.

11. Conclusion

This paper recommends that awareness of cybersecurity and information security is very important when using the web. When analyzing the attacks between 2016 and the beginning of 2020, it was found that the attacks were carried out through mistakes and holes that could have been solved if there were more consideration and knowledge about these holes and mistakes.

It is essential to be careful when using sensitive information, and it is obligatory to secure data from electronic attacks and identify the holes through which the attackers get through to get to sensitive data. It is necessary to be aware of the strategies utilized by cybercriminals during cyberattack.It was clearly found that social engineering was clear within the 2020 cyberattack.

There must be more awareness of how to search appropriately, download programs, and more attention when employing a smart device, especially internet of thing techniques, because it was found the internet of thing techniques was the most important device to expand cybercrime in the last few years.

References

[1] Edephonce Ngemera Nfuka .el al.,2014,The Rapid Growth of Cybercrimes Affecting Information Sys, INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE ,M. Mshangi et al., Vol. 3, No. 2,pp.182-199.

[2] Tabrez Ahmad , Corona Virus (COVID-19) Pandemic and Work from Home:Challenges of Cybercrimes and Cybersecurity, 2020,Available at SSRN: Available at :http://dx.doi.org/10.2139/ssrn.3568830

[3] Kenneth Okereafor , Olajide Adebola,2020 ,Tackling The Cybersecurity Impacts Of The Coronavirus Outbreak As A Challenge To Internet Safety Article , international jornal In IT February & Engineering ,pp.1-11.

[4] Hussain Aldawood ,Geoffrey Skinner,2019,Social Engineering: Hacking a Human Being through Technology , International Journal of Security (IJS), Volume (10) : Issue (1) ,pp.1-15.

[5] M. E. Kabay ,A Brief History of Computer Crime:An Introduction, Copyright © 2008 M. E. Kabay.

[6] Kelly White (2013),The Rise of Cybercrime 1970 through 2010 ,Available at https://drive.google.com/file/d/0B_GoF8uQ95lGWU1RMXZ0WmV2YnM/edit, Accessed on 12/6/2020.

[7] Steve Morgan (2017),2017 Cybercrime Report Steve Morgan, Editor-in-Chief Cybersecurity Ventures , Available at : https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf , Accessed on 14/6/2020.

[8] Cybersecurity Ventures (Dec 13, 2018), Cyberattacks are the fastest growing crime and predicted to cost the world $6 trillion annually by 2021 , Available at :https://www.prnewswire.com/news-releases/cyberattacks-are-the-fastest-growing-crime-and-predicted-to-cost-the-world-6-trillion-annually-by-2021-300765090.html , Accessed on 8/6/2002.

[9] Einaras von Gravrock (04 Mar 2019) ,Here are the biggest cybercrime trends of 2019,Available at :https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/, Accessed on 11/6/2020.

[10] James Cook (May 14, 2017,), The world's 10 biggest cybercrime hotspots in 2016, ranked, Available at : https://amp.insider.com/worlds-10-cybercrime-hotspots-in-2016-ranked-symantec-2017-5 , Accessed on 1/6/2020.

[11] St. Petersburg, Fla (2020).,The 15 Top DDoS Statistics You Should Know In 2020,Available at:https://cybersecurityventures.com/the-15-top-ddos-statistics-you-should-know-in-2020/,Sybercrime magazine ,Accessed on 19/6/2020.

[12] CEA •, The Council of Economic Advisers 9February 2018), The Cost of Malicious Cyber Activity to the U.S. Economy ,Available at:https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf,Accessed on 13/6/2020 .

[13] Krebs on Security (2016), “Hacked Cameras, DVRs Powered Today’s Massive Internet Outage.”, Available at:https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/#:~:text=A%20massive%20and%20sustained%20Internet,video%20recorders%2C%20new%20data%20suggests, Accessed on 16/6/2020 .

[14] Symantec (March 2018), 2018 Internet Security Threat Report,Available at:https://docs.broadcom.com/doc/istr-23-2018-executive-summary-en-aa , Accessed on 16/6/2020.

[15] Emmanuel Marshall (29 December 2017) , Cybercrime 2017: This Year's Big Stories, Available at :https://www.mailguard.com.au/blog/cybercrime-2017-headlines , Accessed on 16/6/2020.

[16] Norton Rose Fulbright (May 17, 2017),WannaCry Ransomware Attack Summary, Available at :https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/ Accessed on 20/6/2020.

[17] John Pescatore, Available at : https://www.infoblox.com, Accessed on 15/6/2020.

[18] Filip Truta (March 8, 2019), Microsoft: Phishing Attacks Increased 250% from January to December 2018, Available at :https://securityboulevard.com , Accessed on 15/6/2020.

[19] Mina Hao (May 29 2019), 2018 DDOS ATTACK LANDSCAPE-8,Available at:https://nsfocusglobal.com/2018-ddos-attack-landscape-8/, Accessed on 15/6/2020.

[20] Oxford Business Group (2020), Saudi Arabia works to enhance cybersecurity,Availableat:https://oxfordbusinessgroup.com/analysis/secure-access-authorities-work-enhance-cybersecurity-and-resilience-face-evolving-online-threats, Accessed on 18/6/2020.

[21] Salem Alelyani, Harish Kumar G R (June 2018) , Overview of Cyberattack on Saudi Organizations, JOURNAL OF INFORMATION SECURITY AND CYBERCRIMES RESEARCH (JISCR) Vol. 1, Issue 1 ,pp.42-50.

[22] Nadav. et al.(Feb 4), 2019 Global DDoS Threat Landscape Report,Available at:https://www.imperva.com/blog/2019-global-ddos-threat-landscape-report/ , Accessed on 15/6/2020.

[23] Marwa Rashad, February (6, 2020) , Saudi Aramco sees increase in attempted cyber attacks , Accessed on 20/6/2020.

[24] A10 Networks (2019),Report The State of DDoS Weapons,Available at:http://presse.hbi.de/pub/A10_Networks/5G_Pressetour/A10_Networks-The_State_of_DDoS_Weapons.pdf , Accessed on 20/6/2020.

[25] DDoS attacks in Q1 2020– 10 minute mail(may,2020), Available at:https://disposableemail.org/index.php/tag/ddos-attacks/ ,Accessed on 22/6/2020.

[26] ZEWYA (14 JUNE, 2020),UAE saw almost 70,000 cyberattacks on smartphones in 2020, Available at :https://www.zawya.com/mena/en/press-releases/story/UAE_saw_almost_70000_cyberattacks_on_smartphones_in_2020-ZAWYA20200614092408/ , Accessed on 22/6/2020.

[27] Saudi Gazette (June 16, 2020),Saudi Arabia saw almost 160,000 cyberattacks on smartphones ,Available at :https://saudigazette.com.sa/article/594321/BUSINESS/Saudi-Arabia-saw-almost-160000-cyberattacks-on-smartphones , AccessED on 20/6/2020 .

[28] Antivirus & Security Technology,Available at:https://us.norton.com/antivirus ,Accessed on 29/6/2020.

Author Biographies

Dr. Fatma Abdalla Mabrouk Khiralla. She worked Lecturer in the Faculty of Computer Science and Information Technology - Shaqra University, working now as Assistant Professor on Faculty of Science and Arts Unizah, Department of Computer Science Qassim. She has obtained Doctor of Philosophy (Ph.D.) from Computer Science National University of Rabat Sudan in 2017. She has obtained also Master of Computer Science and Information from Faculty of Engineering and Technology - University of Gezira in 2003. Moreover, she has obtained Bachelor Computer Science from College of Computer Sudan University College for Girls. She has published Book is Database Hiding On Tag Web Using Steganography by Genetic Algorithm , LAP LAMBERT Academic Publishing,15 July 2019.she has 4 Published Papers in the International Journal of Innovations & Advance in Computer Science IJIACS.