International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cybersecurity Awareness In Saudi Arabia

Sultan Aljabri

Computer Trainer, Technical College Balaas, Saudi Arabia

A B S T R A C T

In recent years, cybercrime has emerged as a top challenge among different sectors, including national security, personal privacy, public safety, among others. One useful measure to deter cybercrime is equipping the potential targets with the right skills to protect themselves. Besides, the rapid growth of cybercrimes has prompted nations such as Saudi Arabia to establish laws to addresses the problem. However, the impact of these legal measure sand their alleged infringement on privacy has been subject to debate. This research aims to investigate the level of cybersecurity awareness among Saudi Arabian residents, focusing on common internet security threats. A well-structured online survey was distributed to analyze cybersecurity awareness among the respondents. The survey, which was the primary research method, was conducted on 600 participants of different backgrounds and gender, to determine their level of awareness, their thoughts on the best techniques to combat cybercrimes, and whether they needed training programs to improve their awareness of cybersecurity. An exhaustive review of qualitative information from secondary sources was also used to determine the impact of the Saudi anti-cyber-crime law in mitigating cybercrime and the current government policy on the privacy of information within the context of the internet's contribution to the development of individual culture in Saudi Arabia.

Keywords: Saudi Arabia, Security Awareness, Cybersecurity, Cybercrime, phishing, Social Media, Risk, Attack

1. Research Questions

1. What is the level of cyber security awareness among the Saudi population?
2. What is the state and impact of the Saudi anti- cyber-crime law in mitigating cybercrime?
3. What is the current government policy on privacy of information within the context of the internet's contribution to the development of individual culture in Saudi Arabia?

2. Research Methodology

The research will use a mixed-methods approach. An exhaustive review of qualitative information from secondary sources will be combined with an analys is of statistical data from a social media-based survey to enable a comprehensive examination of the problem. Since this research aims to collect data from the maximum possible sample size, a survey is the most suitable data-gathering method. Also, the survey also included the option of translating the questions into Arabic to accommodate all the respondents.

The online survey approach will be used to respond to only the first research question. An exhaustive review of qualitative information from secondary sources will be used to provide answers to the other two research questions. Through this approach, findings from qualitative studies will be aggregated, integrated, and interpreted to draw conclusions. This qualitative approach is effective in eliciting in-depth and comprehensive insights in to users 'beliefs, attitudes, emotions, and experiences. Systematic reviews of various primary qualitative sources will present findings from several studies to offer new and more comprehensive conclusions of social phenomena across different cyber security populations and contexts.

* *Corresponding author*
E-mail address: *aljabris@mail.sacredheart.edu*

Inabid to create cybersecurity awareness amongs the Saudi Arabiacitizens,the survey was conducted with 600 participants, with their background. The primary objective of the study was to explore the topic of cybersecurity awareness in Saudi Arabia and summarize the existing data on the matter.Further more,the study was intended to determine what the citizens’think are the best methods to combat cybercrimes and whether they needed training programs to improve their awareness of cybersecurity. A survey was used as the primary method of study. A set of questions was used where the participants of different gender and age groups responded, depending on their level of awareness, experiences, and knowledge on cybersecurity. It was believed that social media would be a significant source of respondents due to its extensive coverage and also the fact that the platforms are the most used form of internet and most vulnerable sites for cybercrimes.

3. Introduction

The unprecedented Internet growth has led to increased cyber-attack incidents that usually result in grievous and disastrous consequences. The modern economy, society, and critical infrastructures have become extensively dependent on digital platforms. This increased dependence on information technology has made online attacks even more attractive to attackers and conceivably more disastrous to society. Besides, asBendovschi(2015)explains, most cybercriminals leverage on the lack of adequate cyber knowledge among their targets.One example of such an attack is social engineering,which involves the psychological manipulation of the targets by convincing them to willingly or unconsciously surrender confidential information that is then used for treacherous intentions (Bendovschi,2015).Another notable method is phishing,where fraudulent emails and links are sent to victims whose login credentials are subsequently mined. As such, there is a need to promote cybersecurity awareness among the community, thereby empowering the citizens to act as the primary line of defense against internet crimes. By introducing cybersecurity awareness and training to the communities, there will be improved prospects of overhauling an attackor as cam before it is successful, thereby reducing damage and lessening the recovery costs. One effective data collection strategy that will beused in this research is surveys,where users will be provided with online questionnaires to fill at their own convenience. This technique will allow the research to target a large population, which guarantees a more accurate sample to make conclusions. The obscurity provided by this approach will also encourage the participants to be as honest as possible while responding to the survey. Also, the surveys will facilitate easier data collection, which tends to utilize simple data sources that can be compiled and analyzed as required for the market research needs.

4. Background Information

The advancements in information technology are essential for economic growth and improved quality of life for modern societies. Hence, the Saudi administration has adopted the long-term vision of ‘‘transformation into an information society and digital economy to increase productivity and provide communications and information technology (IT) services for all sectors of the society in all parts of the country and build a solid information industry that becomes a major source of income’’ (Simsim, 2011, p. 102). However, in the period preceding the late 90s, Internet access in the Gulf nation was limited. The technical difficulties affiliated with the use of Arabic on the Internet and associated devicestended to restrict Internet use to only those who could work in English. Nonetheless, since the commencement of public access to the Internet in 1999, the nation has made notable strides. The figure below shows the number of internet users in Saudi Arabia from 2015 to 2023 (Puri-Mirza, 2019). In 2018, Saudi Arabia had 28.5 million internet users, with the population set to rise to 35 million internet users by 2023 (Puri-Mirza, 2019).

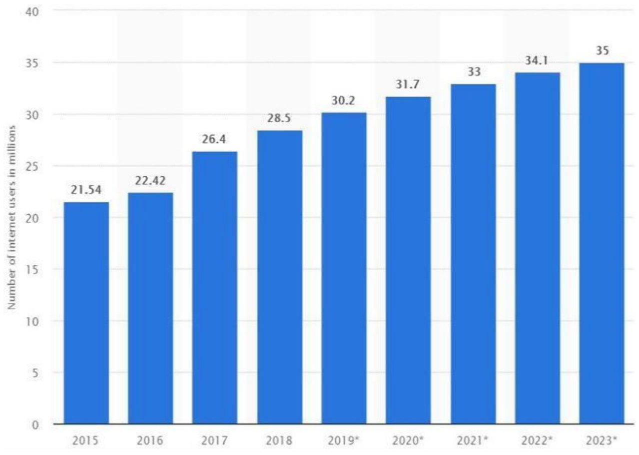


Fig. 1. Internet users in Saudi Arabia from 2015 to 2023 (in millions)

This rising number of Internet users makes the nation a major target for cyber criminals. According to the National Center for Cyber Security at King Abdul Aziz City for Science and Technology, Saudi Arabia faces about 160,000 cyber attacks daily (Alarifi, Tootell, & Hyland, 2012). For instance, in an online survey that featured over 1000 information security professionals from organizations with over 500 staff members, Saudi Arabia emerged as the most affected by ransomware attacks(CyberEdge,2018).As shown in the figure below, 88% of the participants reported being affectedbysuchattackswithinaspanof12monthspriortothe research (Cyber Edge,2018).

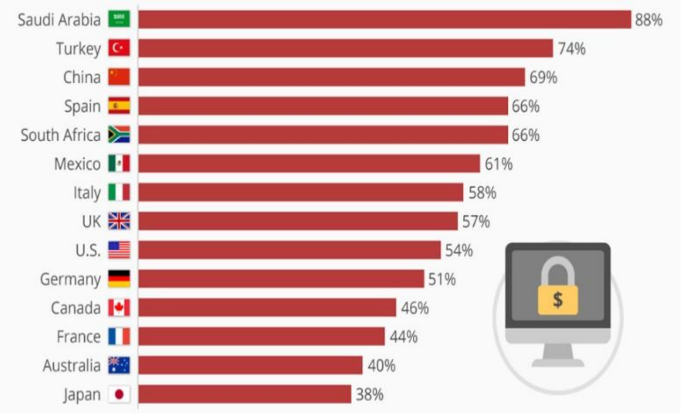


Fig. 2. Countries most affected by ransomware attacks

Besides,the residents of SaudiArabia are ranked among the most active social media individuals in the Gulfregion,making the Internet a vital tool used by activists in raising awareness. Hence,the government is keen on monitoring and containing the freedom of speech. Internet censorship is recognized as one of the most popular techniques used by the state to control the media (Shishkina & Issaev, 2018). Furthermore, Saudi Arabia relies on cybercrime and counterterrorism statutes to prosecute online activists. Other legal instruments criminalizing such activities include the Penal Law for Crimes of Terrorism and its Financing and the Cybercrime Law approved on March 26, 2007.

5. Literature Review

In the recent past,various researchers have sought to explore the topic of cybersecurity awareness among the Saudi population. One such research was performed by Alseadoon, Chan, Foo, & Nieto (2012), who sought to ascertain the critical factors that prompt Internet users in Saudi Arabia to become victims to phishing emails.The results achieved from this study confirmed that users with high levels of submissiveness and limited email experience are more susceptible to phishing (Alseadoonetal.,2012).Among the targets, those with extreme susceptibility levels and are more open are more inclined to expose themselves to email phishing(Alseadoonetal.,2012).

Similarly, Al-Arifi, Tootell, and Hyland (2012) examined the level of cybersecurity awareness among the general public in Saudi Arabia by distributing anonymous online surveys. Findings from the research showed that the high level of attacks is attributed to the low cybersecurity awareness among the Saudi nationals.The inadequate cybersecurity awareness is also due to the patriarchal, highly-censored, and tribal nature of Saudi Arabian culture (Al-Arifi, Tootell, & Hyland, 2012). Poor cultural practices such as the sharing of passwords, and the expectation that the government or other information providers are responsible for security,also contributes to these attacks(Al- Arifi, Tootell, & Hyland,2012).

Similar views were expressed by Alotaibi, Furnell,Stengel, and Papadaki(2016)who examined the cybersecurity awareness among SaudiArabia citizens with in varied contexts.Theauthors used a quantitative online-based survey to assess cybersecurity awareness in SaudiArabia. Findings from this research revealed that, while the respondents had a sound IT knowledge of, their level of awareness, cybersecurity practices, and the role of government and organizations in maintaining information safety across the Internet is very insufficient(Alotaibietal.,2016).The authors concluded that there is an urgent need to develop a model to formulate cybersecurity awareness in the region to combat cybercrime (Alotaibi et al.,2016).

6. Problem Statement

The advent of cybercrime is increasingly affecting Saudi Arabia's economy. With internet activity in the Kingdom increasing by the day, there is a need to determine the current level of cyber security awareness and establish measures on how such efforts can be improved. Underpinning Saudi'sVision
2030. initiative is the increased focus on technology, digital transformation, and the development of digital infrastructure. As such, the state is acutely aware of the cyber security threat it will face as its economy becomes increasingly digitalized. Besides, despite its relentless efforts to curb Internet crimes through anti- cyber-crime law, the state has not sufficiently dealt with this menace. Thus, there is also the need to assess the state's anti- cyber-crime law, as well as the present government policy on the privacy of information within the context of the internet's contribution to the development of individual culture in Saudi Arabia.

7. Cybersecurity laws

Like other nations, Saudi Arabia has established lawsto govern cybersecurity events, although based on the survey, 53.4% have not seen the cybersecurity laws. In Saudi Arabia, the laws are more compelling, especially with the abidance of the Saria laws. The high use of social media in the nation has resulted in the classification of the laws to create room for media use, which forms one of the primary sites to increase cybercrimes in the country. The laws have been adjusted to accommodate the advent of the individual culture that emanates from social media. Thus, there is a need for the population to learn more about these laws, which according to the survey, only 26.9% have fully benefited from awareness programs.

According to the survey, cybersecurity of Saudi Arabia needs development as indicated in figure 16. Based on the article 2 of the laws governing cybersecurity in Saudi Arabia, cybercrimes should be combated through the identification of the crimes and appropriate punishment applied to initiate an upgrade of data security, protection of the rights in regards to the illegitimate use of information network and to protect the national economy (Abdulaziz, 2009). The article offers regulations that ensure peoples morals, interests and valuesare protected.

Article 3 of the policy illustrates the various forms of punishment that the individuals found guilty of the cybercrimes are exposed to and also possible imprisonment. Based on this article, any individual shall be subjected to imprisonment for less than one year and fined not less than five hundred thousand riyals (Abdulaziz, 2009). In some cases, either of the penalties shall be applied upon beingfound guilty of the crimes. The various criminal cases includespying on or reception of unauthorized data transmitted through an information network or even through a computer with no legitimate authorization (Abdulaziz, 2009). Such an individual will be subject to one of the punishmentslisted.

Moreover, the individuals will be convicted if they are found guilty of the unlawful access to computers, having threatened or blackmail any individual and compelling them into taking or refraining from taking action, whether it is lawful or not. The article also offers protection against unlawful access to websites or hacking sites to change the design without authorization from the owners. Additionally, it protects websites from being destroyed, modified, or occupancy of its URL. The article establishes a law against privacy invasion by misuse of camera-equipped mobile phones and other devices with cameras that can facilitate the attack of privacy.

The severity of the fines can be used in determining the penalties on cybercrimes. The penalties for the crimes committed by the use of social media can be grouped. For instance, group A of the media-based crimes corresponds to a one-year jail term or payment of SAR 500000 fine. The group B crimes correspond to a four-year jail term and a fine of SAR 3000000, while group C of the media crimes subjects one to a fine of SAR 3000000 or a five-year jail term. The different groups represent different seriousness in crime, and this determines their classifications.

Moreover, according to article 4, any individual found guilty of the cybercrimes of procurement of versatile property or bonds for themselves or in any event, signing the bonds through extortion or utilization of illegal identity shall be subject to detainment for a period at the very least three years and a fine not exceeding 2,000,000 riyals or either of the penalties (Abdulaziz, 2009). Additionally, the same punishment would be applied against any person who illegally accesses a bank or credit data with the aim to obtain data, information, funds or services provided. Moreover, committing crimes related to preparation, transmission and production or storage of material impinging on public order, religious values, and privacy through the information network or computers shall results in imprisonment for a period not more than five years and a fine of three million riyals. The penalties are, however, governed by ethical values. The laws do not prejudice the provisions of relevant laws, especially those associated with the intellectual property rights, nor relevant international agreements that involve the kingdom.

8. Saudi Arabia Vs. Usa Cyber Crimes

Certain differences exist between cybercrime between Saudi Arabia and the United States. For instance, the law governing cybercrime in Saudi Arabia is controlled or influenced more by the religious (Islamic) and social mores and local cultural institutions. The laws include the establishment of the penalties for the various offenses regarding cybercrimes, and the fines that the religion considers will be per the values they practice within their communities. On the other hand, the American cybercrime is wider and more complicated due to higher internet access in the nation and broader moral and ethical base. The social mores observed in America are broad, and the values are distinct depending on the different individuals from different ethnic backgrounds. This implies that a single religion cannot establish the rules that will govern the penalties for the individuals found guilty of cybercrime incidences, and this facilitates a complexity in managing the practice.

Moreover, the differences exist in the level of jail term for the same crime in the two nations. For instance, in the United States, accessing a computer with no authorization, and with the belief that the data obtained will have a negative implication on the owner, will be fined not more than $5000 or one-year imprisonment (Al Rees, 2006). On the other hand, the same crime will subject an individual to imprisonment of less than a year, as stated in article 3 of their constitution.

Furthermore, during investigations, Saudi Arabia has its communication and Information Technology Commission, according to its powers, to offer the needed assistance and technical support to the established competent security agency to help with the investigation of the various cybercrime and also during the trials as stated in article 14. However, the body of investigation is different with America that involves the Federal Bureau of Investigation to investigate the offenses under the subsection (a)(1) of the constitution for some random cases including reconnaissance, remote counterintelligence and the protected data against unapproved exposure for the different reasons of national defense.

9. Results and Analysis

The first set of questions sought to determine the respondents' background information, which comprised of their gender, age groups, and education level to determine which categories are more susceptible to cyber-attacks. Below are the results.

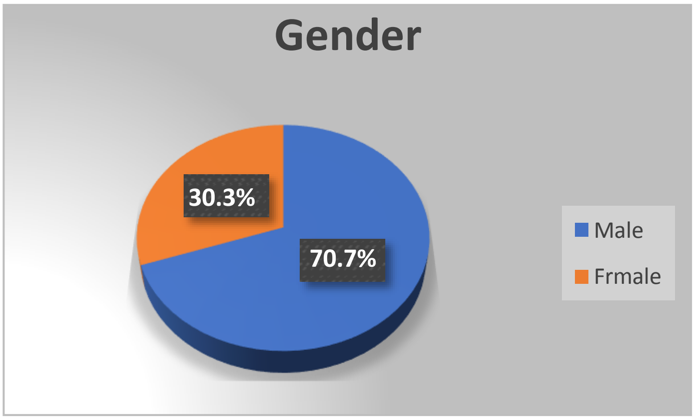


Fig.3. Gender Distribution

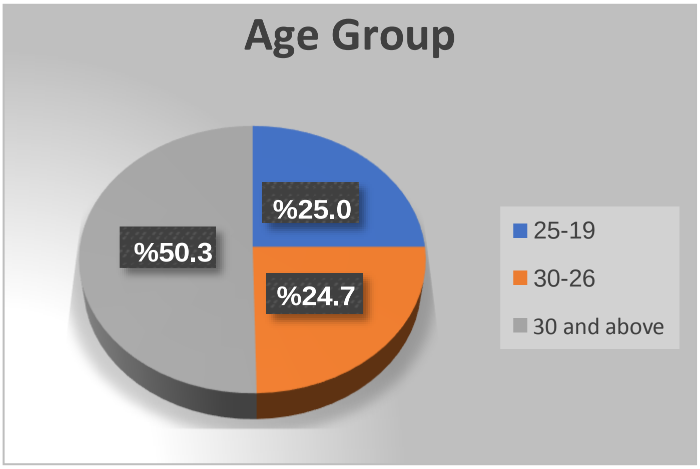


Fig. 4. Age distribution

An individual's education level also plays a crucial role in determining how they respond to internet security incidences. Below is the distribution of the respondent's academic qualifications.

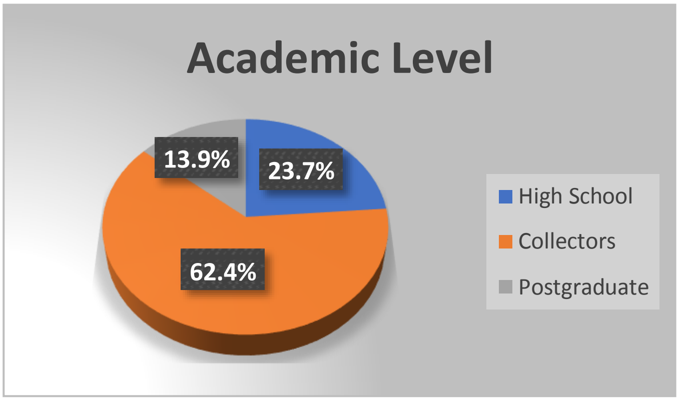


Fig. 5. Education Level

Subsequently, the survey sought to determine which of the most common threats the respondents are informed about

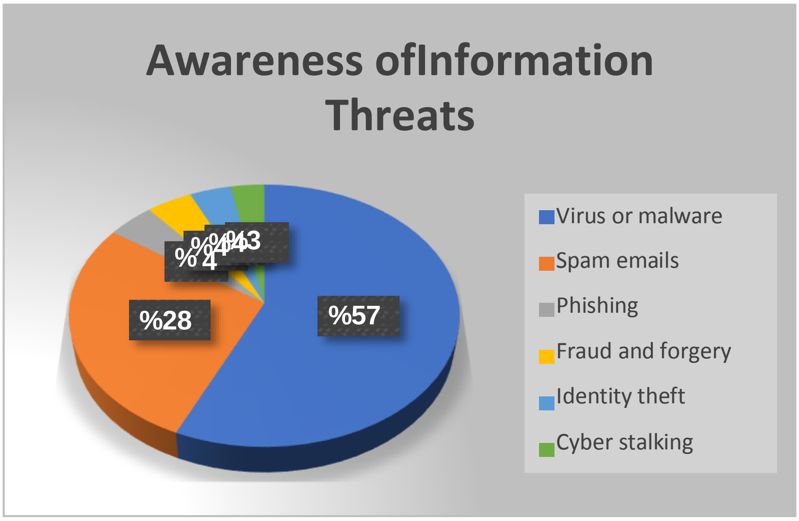
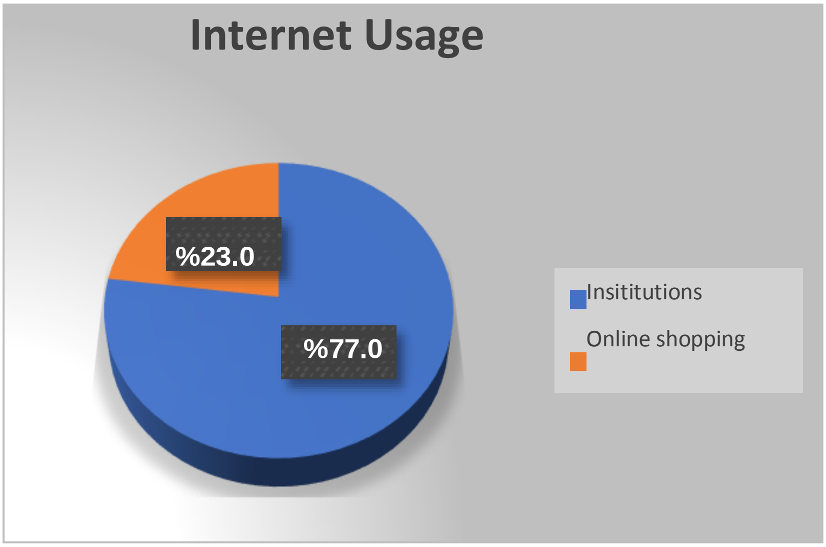


Fig. 6. Awareness of common cyber threats

Indeed, Cybercrime awareness can be enhanced amongst individuals through education and training on the appropriate measures of focus. How users utilize the Internet is important in determining what threats they are likely to face. Hence, the two questions sought to determine how the residents use the Internet, and the frequency of usage. Most individuals visit various websites and shop online from institutions and individuals and do not realize which sites are safe or not, and this should be included in the training programs. According to the survey, 77% deal with institutions, while 23% deal with individuals while shopping online.



Despite individuals being aware of cybercrimes, personal awareness must be reinforced so that people do not only depend on the measures reinforced by agencies or governments but also take it within themselves as a responsibility to protect their data. As a group, we thought that parents or guardians can play a role through parental processes to help reduce the technology use amongst the youth, as the enhanced use of technology impacts high rates of cybercrimes, especially amongst the internet users.

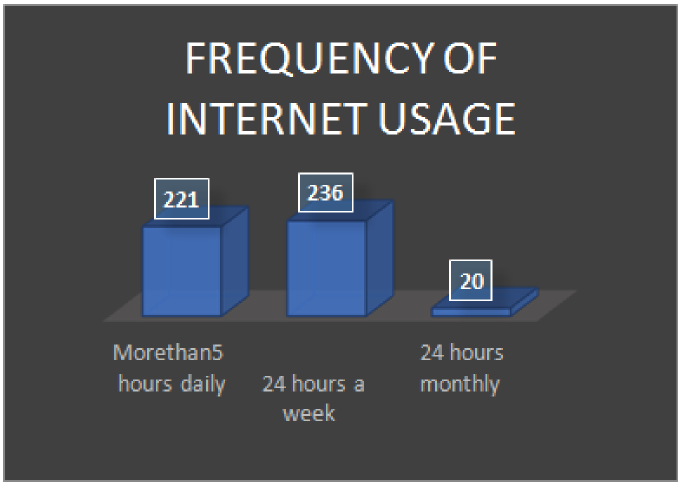


Fig. 8. Frequency of Internet Usage

The research also sought to determine which portion ofthe users have experienced online attacks. Below are the gathered responses.

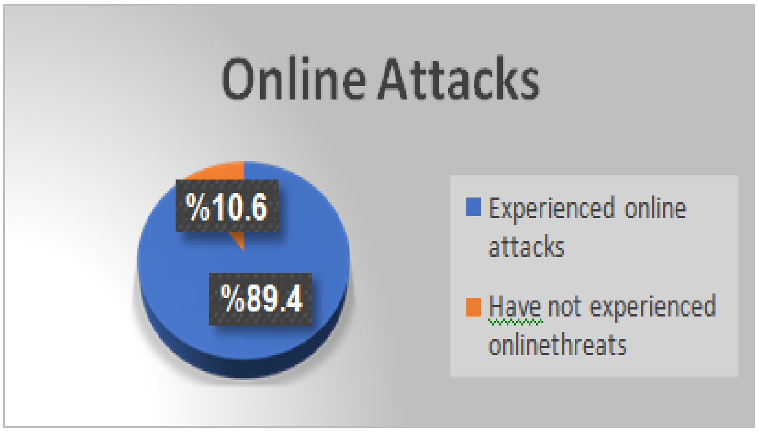


Fig. 9. Online attacks experience

According to the survey, 89.4% of the respondents have reported an online attack. This means that majority of the population in Saudi Arabia faces high levels of cyberattacks. One way to deal with such attacks is having an effective anti- virus software. Thus, this research sough to assess the number of individuals that have installed such applications.

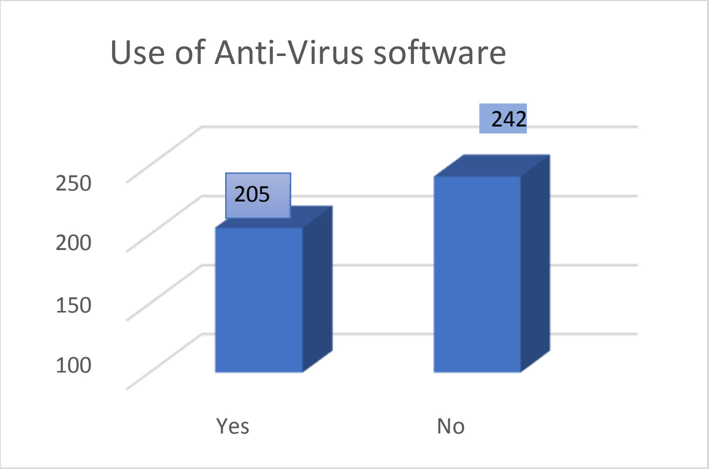


Fig. 10. Anti-virus usage

In the study, when asked about a combination of features that would give the strongest password, 71.8% agreed that a strong password would include letters, numbers, and symbols, while 21.8% of the individuals illustrate that the strongest password was the use of numbers and letters.

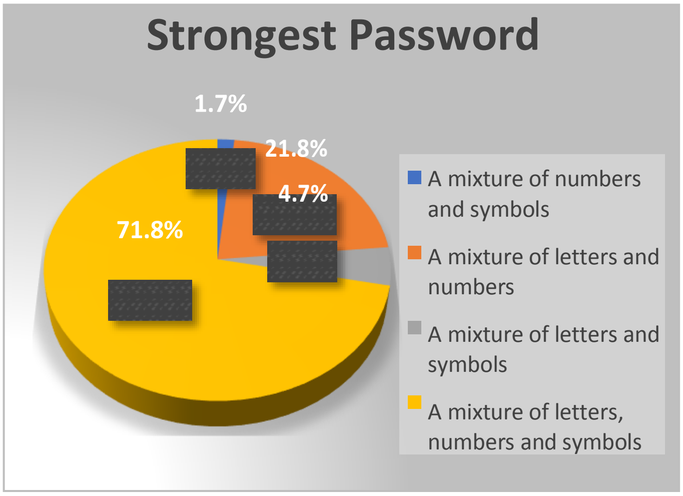


Fig. 11. Strongest Password

Besides, it was established that the best way to authenticate access to a website was to be sending the activation code. This is because the codes are sent to the private emails or numbers for the individuals of which they have personal access through passwords they have created. Thus, they can view them without others having access.

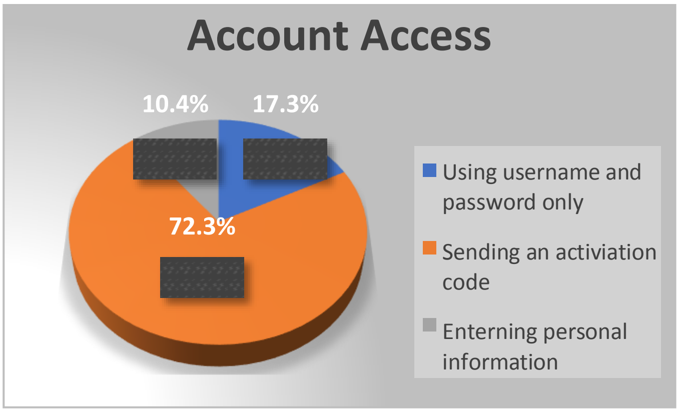


Fig.12. Account access

Most people reported using the same passwords for both work and personal accounts (54.2%), while a high number of respondents reported using a parenting process to protect the children from accessing inappropriate websites. Indeed, this was a significant measure to regulate the use of technology, subject to attacks, and we believe this is a measure to control technology use and hence, cybercrimes amongst the future generation.

Moreover, according to the survey results, the increased cybersecurity incidences in the nation are a result of the lack of human factors. For instance, 88.7% of respondents believe they is a need for urgent training on cybersecurity awareness, 84.6% have not lost money due to cybercrimes, and only 24.8% read privacy policies before accessing a site. When asked about whether the private policies should be included in the government websites, 86.5% of the participants illustrated the importance of privacy policies as it will help reduce inappropriate or unauthorized access to the websites.

Moreover, the research established that only a few people follow electronic platforms of the cybersecurity to see what is new, with 65.3% of the participants admitting not to follow the latest developments on the issues associated with cybersecurity. Moreover, of the participants, most people explained they have partially benefited from the awareness campaigns by the government, with 20.1% reporting that they have entirely not benefited from the same. Still, most people (45.8%) of the participants accepted that they werecompatible with all the age groups. Moreover, most people have not seen the cybercrime laws in Saudi Arabia (53.4%) and this illustrates that awareness of this practice should be a priority to the government and other associatedagencies.

Moreover, social media poses a significant threat to cybersecurity. Users engage in different activities that expose them to these attacks. Hence, user's engagement to some of the most common dangers was assessed.

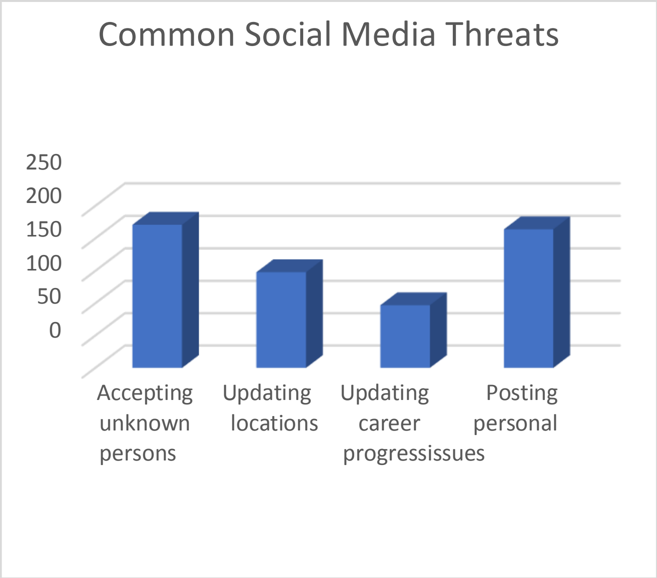


Fig. 13. Social Media Threats

These results give a true reflection of why Saudi Arabia continues to be among the top targets for cyber-criminals. Indeed, the level of awareness and preparedness among the citizens is very low. The demographics show that a majority of the Internet users are between the ages of 18-30 and above, with the male users being slightly more that their female counterparts. A large section of those aged between 18-30 are students. Thus, most of the Internet users are students, followed by educators and other professionals. Figure 8 provides the distribution of Internet usage, thus outlining which channels are likely to be targeted more by assailants. Survey results indicate that 38% of the respondents use the Internet for communication, which entails channels such as Email and social media platforms like Facebook and Snapchat. Indeed this data explains why attackers have increasingly targeted social media platforms. Other key uses of the Internet include work purposes, entertainment reasons (social media is also included here), health research, among others. Given the importance of social media, users should be more cautious of their activities while on these channels.

Nevertheless, as shown in Figure 13, a troubling number of users are still endangering themselves by accepting requests from unknown people/sources, as well as continuously update their physical location, personal issues, and career progress. Also, emphasizes the poor password management practices among Saudi Arabia Internet users. Most of the users do not update their passwords regularly and use phrases with weak combinations. As expected, Figure 6 shows that a large majority of the Internet users (57%) of malware and email spamming attacks. However, worrying statistics indicate that these users are not aware of other threats such as phishing, identity theft, and cyber stalking. Nonetheless, despite being aware of the danger, most of Internet users do not use Anti- Virus software.

Moreover, most people agreed that they make updates required to close vulnerabilities, with over 72.8% of the participants responding to the effect. Perhaps the most significant question was how the individuals would identify a safe website. According to the answers, only 8.5% lacked an idea, on how to identify a safe website, while the rest were a bit informed. Therefore, most of the respondents agreed that it was important to include a combination of the web address, which starts with https://, as well as the golden lock that appears at the bottom of the screen.

The survey also gathered the residents' opinions regarding the current cyber security laws. The first question on Saudi laws sought to determine the portion of the population are aware of the cybersecurity laws in the country. Indeed, results show that there is need for further awareness programs, as 53.4% have not seen the cybersecurity laws.

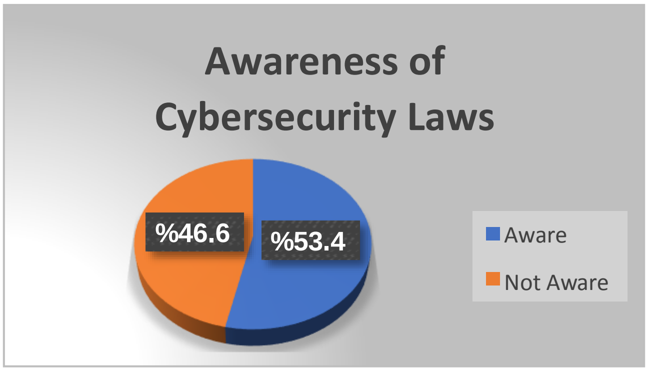


Fig. 14. Awareness of cyber security laws

The second question asked if the respondents have benefited from these laws. The survey revealed that there is a need to improve these legislations, as only 26.9% have fully benefited from awareness programs.

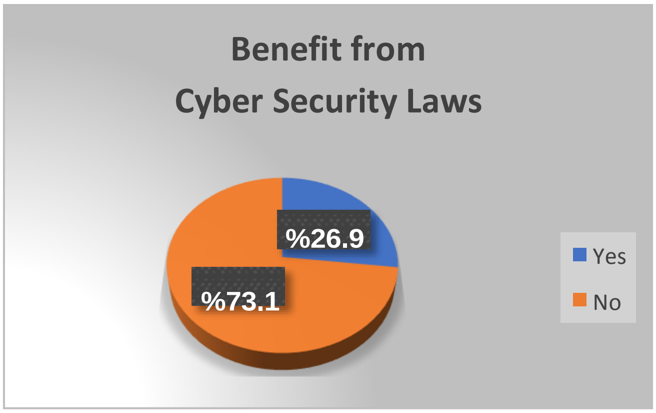


Fig. 15. Benefit from cybersecurity laws

A majority of the participants (37.8%) believe that Saudi Arabia needs to develop its cybersecurity preparedness

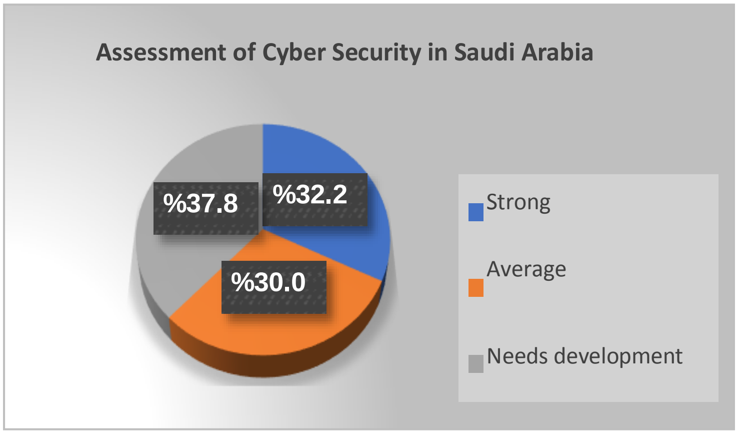


Fig. 16. Assessment of cyber security laws

• Exhaustive Review of Qualitative Information

Securing cyberspace is a fundamental element for Saudi Arabia's 2030 Vision. In a bid to fight cyber-attacks, the Saudi Arabian government has also developed several web portals that help citizens combat these threats in various ways. One such platform is The Bug Bounty Platform (https://bugbounty.sa/#/), which is a crowdsourced security platform promoted by the Saudi Federation for Cyber Security andProgramming(SAFCSP)tooffercybersecurityresearchers and enterprises a place where they can connect to identify and combat vulnerabilities in a cost-efficient way, while reserving the rights of both parties (The Bug Bounty, 2019). The administration also manifested its commitment by establishing the SAFCSP, which is a national agency under the Saudi Arabian Olympic Committee aiming to develop national and professional abilities in the cybersecurity and programming sectors (SAFCSP, 2019). Another national security agency is the National Cybersecurity Authority, also known as the National Cyber Security Authority or the Saudi National Cybersecurity Authority, which was formed after orders from King Salman in October 31, 2017 (Taher, 2019). NCA mainly concentrates on the Kingdom's computer security and is directly associated with the King's office (Taher, 2019). Besides, the National Information Security Strategy (NISS)for the Kingdom of Saudi Arabia represents another cybersecurity plan formed is in response to a Request for Proposal issued by the Ministry of Communications and Information Technology (MCIT) (MCIT, 2011). The main objectives of this document include facilitating free and secure information sharing, increasing the security, safety, and integrity of online information, building more resilient information systems, increasing awareness and education of cybersecurity, and creating a set of national guidelines for Information Security Management, Risk Management, and Business Continuity based on international standards and best practices (MCIT, 2011).

10. Future Recommendations

This research sought to determine the level of cybersecurity awareness among the Saudi population. However, technology was addressed in general, rather than focusing on specific aspects. However, emerging technologies, including Cloud, IoT, and BYOD, each possess different threat levels. Hence, future researchers should evaluate each of these concepts individually. Besides, future researchers should assess and compare the cybersecurity awareness between individual residents and organizations.

11. Conclusion

In conclusion, Saudi Arabia is currently rightfully ranked among the most vulnerable nations regarding falling victim to cybercrimes. The advent of the Internet has posed new challenges to individuals and bodies tasked with ensuring cybersecurity. As a wider population, from different age groups and professions, are using the Internet for different reasons, there is need to increase awarenesss of common risks pertaining to cybercrime and how to protect/recover from such attacks. The youth, in particular, are more susceptible to these attacks due to their higher usage and riskier behavior while on online platforms. Hence, cybercrime sensitization programs should be introduced in educational institutions to equip future generations venturing into different fields, on how to be safe while on online platforms. Furthermore, Firewall procedures should be used in Saudi Arabia as a measure to prevent cybercrimes and illegal access to personal information when individuals are using the internet. Moreover, we recommend that parents should consider the parental guidance process to deter or reduce the level of internet usage by the children as the increased use of internet forms one of the primary ways in which cybercrimes have increased. Due to the dynamic nature of cyber attacks , the Saudi Arabian Anti-Cybercrime law should be continuously updated to address the emerging legal loopholes. Awareness of the existing laws among the Saudi Society should also be improved, as more victims will be motivated to report such crimes. Moreover, a clear regulation about publicly publishing incident reports and cases is a good step toward a better, more secure digital environment. Upon adhering to all of the mention arguments, Saudi Arabia, and other nations across the globe will witness minimal cases of cybersecurity in the future.

References

1) Abdulaziz, A. B. (2009). Anti-Cyber Crime Law: Royal Decree No. M/17. pp.1-6.

2) Al Rees. (2006). Cybercrime Laws of the United States. Computer Crime and Intellectual Property Section, U.S. Department of Justice , pp.1-76.

3) Al-Tawil, K. M. (2001). The Internet in Saudi Arabia. Telecommunications Policy, 8(25),625-632.

4) Alabdulatif,A.(2018).Cybercrimeandanalysisoflawsin Kingdom of Saudi Arabia (Doctoraldissertation).

5) ALArifi,A.,Tootell,H.,&Hyland,P.(2012).Information securityawarenessinSaudiArabia.CONF-IRM,57.

6) Alarifi,A.,Tootell,H.,&Hyland,P.(2012,June).Astudy of information security awareness and practices in Saudi Arabia.InternationalConferenceonCommunicationsand Information Technology (ICCIT), 6-12.

7) Alotaibi,F.,Furnell,S.,Stengel,I.,&Papadaki,M.(2016,December).Asurveyofcyber-securityawarenessinSaudi Arabia.InternationalConferenceforInternetTechnology and Secured Transactions, 154-158.

8) Alseadoon,I.,Chan,T.,Foo,E.,&GonzalesNieto,J. (2012,January).Whoismoresusceptibletophishing emails? A Saudi Arabian study. In ACIS 2012: Location, location, location: Proceedings of the 23rd Australasian Conference on Information Systems, 1-11.

9) Bendovschi,A.(2015).Cyber-attacks–trends,patternsand security countermeasures. Procedia Economicsand Finance, 28, 24-31.

10) CyberEdge(2018).SaudiArabiahardesthitby ransomware. Statista. Retrievedfrom https://www.statista.com/chart/18028/ransomware-attacks-by-country/

11) Duffy,M.J.(2014).Arabmediaregulations:Identifying restraintsonfreedomofthepressinthelawsofsix Arabian Peninsula countries. Berkeley Law Journal of Middle Eastern and Islamic Law, 6, 1.

12) Elnaim,B.M.E.(2013,December).Cyber-crimein KingdomofSaudiArabia:Thethreattodayandthe expected future. In Information and Knowledge Management, 3, 12, 14-19.

13) Fatani,R.(2011).SecuringinternetrightsinSaudiArabia. Global Information Society Watch. Retrieved from https://www.giswatch.org/en/country-report/internet- rights/securing-internet-rights-saudi-arabia

14) MinistryofCommunicationsandInformationTechnology, MCIT (2019). Developing National Information Security StrategyfortheKingdomofSaudiArabia.Retrievedfrom https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Reposit ory/SaudiArabia_NISS_Draft_7_EN.pdf

15) Saudi Federation for Cyber Security andProgramming, SAFCSP (2019). About. Retrieved from https://safcsp.org.sa/en.html

16) Shishkina,A.,&Issaev,L.(2018).Internetcensorshipin Arabcountries:Religiousandmoralaspects.Religions, 9(11), 358

17) Simsim,M.T.(2011).Internetusageanduserpreferences in Saudi Arabia. Journal of King SaudUniversity- Engineering Sciences, 23(2), 101-107.

18) Taher,A.(2019).SaudiArabia'seffortstoensurecyber security. Retrieved from https://eng.majalla.com/node/65466/saudi-arabia%E2%80%99s-efforts-to-ensure-cyber- security%C2%A0

19) TheBugBounty(2019).WelcometotheBugBounty Platform. Retrieved fromhttps://bugbounty.sa/#/

Puri-Mirza, A. (2019). Number of internet users in Saudi Arabia from 2015 to 2023 (in millions). Statista. Retrieved from https://www.statista.com/statistics/462959/internet-users-saudi-arabia/