A Cognitive Theory-based Approach for the Evaluation and Enhancement of Internet Security Awareness among Children Aged 3-12 Years

Asma Eidhah M. Aloufi
ama9000@rit.edu

Follow this and additional works at: https://scholarworks.rit.edu/theses

Recommended Citation

This Thesis is brought to you for free and open access by RIT Scholar Works. It has been accepted for inclusion in Theses by an authorized administrator of RIT Scholar Works. For more information, please contact ritscholarworks@rit.edu.
A Cognitive Theory-based Approach for the Evaluation and Enhancement of Internet Security Awareness among Children Aged 3-12 Years

By

Asma Eidhah M. Aloufi

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Computing Security

Department of Computing Security

B. Thomas Golisano College of Computing and Information Sciences

Rochester Institute of Technology

Rochester, NY

August 13, 2015
A Cognitive Theory-based Approach for the Evaluation and Enhancement of Internet Security Awareness among Children Aged 3-12 Years

By

Asma Eidhah Aloufi

Submitted August, 2015

Department of Computing Security
Rochester Institute of Technology
Rochester, NY

Approved By:

_____________________________________________ Date: ________________
Dr. Sumita Mishra
Primary Advisor – R.I.T. Dept. of Computing Security

_____________________________________________ Date: ________________
Dr. Yin Pan
Secondary Advisor – R.I.T. Dept. of Computing Security

_____________________________________________ Date: ________________
Dr. Khadeeja M.Amin Khoja
Secondary Advisor – K.A.U. Dept. of Diploma of Education- Female Students
Abstract

In the age of technology, the Internet has spread widely and used for multiple purposes by users of all ages, especially children who start using it frequently to play in their spare time. With the use of the Internet, children must have a sufficient security awareness to avoid security risks found online. This study takes us through the journey of evaluating and enhancing the level of the Internet security awareness among a group of Saudi children aged 3-12 years. The developed evaluation survey shows that there is some awareness among the Saudi Children; however, they still need more concrete ways of ensuring secure practices as they showed a poor knowledge of proper Internet security practices in areas such as interacting with anonymous advertisements as well as understanding some of the Internet Security symbols. The study also presents a suggested Awareness Enhancement solution to raise the security awareness among children. The solution’s design takes into consideration the Piaget’s theory of children’s cognitive development, which states that children in different age groups have different perceptual and learning abilities. The test of the suggested solution shows a significant increase in the sample’s Internet security level. The work of this study emphasizes on the importance of targeting the Saudi children with interactive training sessions to raise their Internet security awareness level.
Dedication

This work is dedicated to my Mother and Father, who believed in their youngest daughter;

To my husband Rashed, who supported me to the infinity and beyond;

And to my son Yazan, who helped by just being there.
Acknowledgement

First of all, I would like to express my utmost thanks to Allah who blessed me with the completion of this thesis.

I would like to sincerely thank my primary advisor Professor Sumita Mishra for all the insightful comments and guidance she gave during my work on this thesis. I also would like to thank the rest of my thesis committee Professor Yin Pan and Professor Khadeeja Khoja for their support and encouragement. A thank you also goes to the Computing Security Department entire faculty and staff.

I wish to express my gratitude to all the Saudi families who enthusiastically participated in this study. To all my friends and family who supported and encouraged me to the very end, thank you.
# Table of Contents

Abstract ................................................................................................................................. iii

Dedication ............................................................................................................................... iv

Acknowledgement ................................................................................................................ ii

Table of Contents .................................................................................................................. iii

List of Figures ......................................................................................................................... v

List of Tables ........................................................................................................................ vii

1. Introduction ...................................................................................................................... 1
   1.1. Study scope .................................................................................................................. 3
   1.2. Purpose of Study ......................................................................................................... 5
   1.3. Hypothesis .................................................................................................................. 6

2. Background ....................................................................................................................... 7
   2.1 Terminology ................................................................................................................ 7
   2.2. Security Threats and Countermeasures in Saudi Arabia: ...................................... 8
      2.2.1. Threats ............................................................................................................... 9
      2.2.2. Countermeasures ............................................................................................. 10
   2.3. The Cognitive Development Theory ........................................................................ 11

3. Literature Review .......................................................................................................... 14

4. Awareness Evaluation ..................................................................................................... 24
   4.1. Evaluation Methodology Design ............................................................................... 24
      4.1.1. Parents’ Survey: ............................................................................................... 25
List of Figures

Figure 1: Perspectives upon Children’s Use of the Internet [6]................................. 2
Figure 2: Percent of Attacked Computers in 2014. [16]............................................. 4
Figure 3: Module categories for computing majors [52]............................................. 15
Figure 4: Module categories for general education. [53]............................................. 16
Figure 5: Four places for personal data. [57]............................................................. 20
Figure 6: Examples of Internet Security Symbols.......................................................... 27
Figure 7: 3-point Visual Analogue Scale...................................................................... 28
Figure 8: Distribution of the parents’ sample according to (Guardianship)...................... 29
Figure 9: Distribution of the parents' sample according to (Age)................................. 29
Figure 10: Distribution of the parents’ sample according to (Residency)......................... 29
Figure 11: Distribution of the parents' sample according to (Region)............................ 29
Figure 12: Distribution of the parents’ sample according to (Education Level)............. 30
Figure 13: Distribution of the parents' sample according to (Work)............................. 30
Figure 14: What type of security problems has your child encountered?....................... 38
Figure 15: Distribution of Children sample according to (Gender)............................... 43
Figure 16: Distribution of Children sample according to (Age).................................... 43
Figure 17: Device Categories Used by Children Sample.............................................. 44
Figure 18: Websites and Applications Most Visited by Children Sample.................... 45
Figure 19: Children who would share personal information on the Internet.................. 45
Figure 20: Proof-of-Concept Awareness Program Flowchart....................................... 53
Figure 21: Distribution of Pre-Assessment sample according to (Gender) .................... 56
Figure 22: Distribution of Pre-Assessment sample according to (Age) ....................... 56
Figure 23: Device Categories Used by the Pre-Assessment Sample ......................... 56
Figure 24: Pre-Assessment Personal Information awareness level. .......................... 57
Figure 25: Post-Assessment Personal Information awareness level .......................... 59
List of Tables

Table 1: Work * parents Cross tabulation................................................................. 31
Table 2: Which age group does your child belong to? ........................................... 31
Table 3: Is your child a male or a female? ............................................................... 31
Table 4: Do you use the Internet? ........................................................................... 32
Table 5: Does your child use Internet-enabled devices? .......................................... 32
Table 6: Does your child use the Internet? ............................................................... 32
Table 7: What type of device does your child use? ................................................. 33
Table 8: What is the main purpose for which your child uses the device? .............. 33
Table 9: Do you consider the device specifications before you buy it for your child? .. 34
Table 10: Do you depend on the specifications or the price when buying a device for your child? ........................................................................................................... 34
Table 11: On average, how many hours a day does your child use the Internet? ....... 34
Table 12: Do you teach your child any kind of device management? ....................... 35
Table 13: Do you check on your child's activities on the device? ............................. 35
Table 14: If the answer is yes, do you do that while or after he/she uses the device? ... 36
Table 15: What is the level of awareness parents have to ensure their children’s safety on the Internet? ........................................................................................................... 37
Table 16: Have these problems once and for all been solved? ................................. 39
Table 17: Who was the individual who solved these problems? ............................... 40
Table 18: What is the top Internet Security risks from which you want to protect your child? .................................................................................................................................................................................. 40

Table 19: In your opinion, who do you think is primarily responsible for securing your child's device? ............................................................................................................................................................................... 41

Table 20: On a scale of 1-5 (1 being "very poor" and 5 being "excellent"), what is your assessment of your child's awareness of the Internet security? ........................................................................................................ 41

Table 21: Would you be interested in introducing Internet security awareness solutions to your child? ........................................................................................................................................................................ 42

Table 22: Tests of Awareness Level of Children Sample ................................................................. 47

Table 23: The relationship between the child's age and his Internet security awareness level .................................................................................................................................................................. 47

Table 24: The relationship between the parents’ use of the Internet and the children’s awareness .......................................................................................................................................................... 48

Table 25: The relationship between the parents’ awareness and the children’s awareness ...................................................................................................................................................................... 48

Table 26: Have you ever heard of the Computer Emergency Response Team, which is a part of the Saudi Communication and Information Technology Commission? .................. 49

Table 27: Have you ever read any awareness publications from the Computer Emergency Response Team? ................................................................................................................................................. 49

Table 28: Have ever read any Information Security Awareness publications from any other sources? .......................................................................................................................................................... 50

Table 29: Do you give your child an overview of the Internet Security Threats? (Such as viruses, spam, and phishing) ........................................................................................................................................ 50

Table 30: Sample's Internet security awareness Level (Pre-Assessment) ........................................ 58

Table 31: Sample's Internet security awareness Level (Post-Assessment) ...................................... 60
1. INTRODUCTION

It is quite clear nowadays that technology and specifically the Internet has become dominant in different fields, such as education and business. People of all ages often use the Internet in order to accomplish different tasks, such as retrieving information by using online search engines, learning new languages through educational websites, or just entertaining themselves in their spare time by playing online games or watching the latest movies. Through the recent years, children, at a young age have started using Internet-enabled devices such as Computers, iPads, and Tablets to play online games, watch cartoons or read electronic books. The younger generation is extremely familiar with the technology mainly because smart devices, such as infant care devices, surround them as soon as they are born [1] [2].

Children are constantly developing their intellectual abilities by interacting with their environment [3]. They are naturally curious learners who tend to learn very fast about the world through observing and playing. With the availability and the advancement of the Internet, children are given the chance to explore more concepts and play more games. There is a noticeable increase of applications and website specialized for children; the increase reflects the interest of top technology providers such as Google and Apple in children’s usage of the Internet and the technology. For instance, Google has launched YouTube for Kids in February 2014 to provide numerous videos for children [4]; Apple, on the other hand, has devoted a special category in their App Store for kids to house different educational applications and games [5].

Children's usage of Internet-enabled smart devices is not a frowned-upon matter anymore as indicated by a study carried out by the Mohammed bin Rashid School of Government. The participants were asked when they feel is a good age for a child to start owning a device that connects to the Internet. The results shown in (Figure 1-a) show that approximately 20% of the participants believe that children aged 8-10 years should own and use a smart
device; while 13% think that at age 5-7 year-old is a good start for children to have their own Internet-enabled smart device [6]. On the other hand, another question (Figure 1-b) shows that 22% of the participants have children who own Internet-enabled smart device.

![Graph](image1)

(a)

![Graph](image2)

(b)

*Figure 1: Perspectives upon Children’s Use of the Internet [6].*

With this welcoming wave of children’s Internet usage in the Arab region, it became an obligation to address the obstacles that the little minds could face while using the Internet. Specifically, the Internet Security threats and risks that might be posed to them. There are many threats to the safety and privacy of the Internet user. Kaspersky Lab [7], which is a
distinguished IT security solutions vendor, indicates in a recent report [8] the top security risks that can occur while playing online games on electronic devices. The threats include:

**Phishing**, which is the act of deceiving a user to willingly give sensitive information, such as a password to a website, to the attacker that often poses as a fake authorized representative in the IT team of said website;

**Cyberbullying**, which refers to the act of bullying using electronic devices [9]. A user is cyberbullied by being mistreated or humiliated on the Internet through emails, game’s chatting boards or social networking sites.

**Computer/smartphone compromise** [8], which refers to the device’s exposure to malicious Internet attacks. An example of the compromise is sending malware and virus attacks on the user’s device. Another example is device intrusion, which is the act of gaining access to the device’s system settings and storage.

**Internet Offender**, which is any individual who misuses the Internet to commit crimes. One classification of the Internet offenders are pedophiles, who seek to have inappropriate communication with children online. [10] and [11]

Such threats found in gaming and entertainment websites and applications can present a serious danger to the children who are visiting those websites for playing. Hence, Internet users, including young children, must be aware of these risks to be careful and avoid them; this awareness is accomplished through Internet security awareness (ISA). The term refers to the education and awareness programs that aim to educate users about the best practices to maintain their security and privacy while using the Internet.

### 1.1. Study scope

In this study, the Kingdom of Saudi Arabia was selected as the focus of the study. It is located in the southwest corner of Asia and occupies almost four fifths of the Arabian Peninsula. In 2014, the total population of Saudi Arabia reached 30,770,375 million people [12], spread over five geographic regions: Northern region, Southern region, Eastern region, Western region and Central region.
Saudi Arabia is one of the rapidly developing countries, witnessing a remarkable development on the technological level and Internet usage. Internet access was made available to the public in 1997 [13]. Since then, Saudi Internet users have increased to reach approximately 59% of the total population in 2014 [14].

With this number of Internet penetration, Saudi Arabia has proven to be prone to various security attacks. In 2014, the Symantec Intelligence Report indicates that Saudi Arabia is one of the top five spammed countries, with a spam rate of 66%. One in every 195 Saudi Internet user is targeted by a malware, which puts the country in second place after the United Kingdom [15]. Moreover, about 36% of Saudi Internet users face the risk of online infection, according the latest Kaspersky’s 2014 Security report. Figure 2 shows that Saudi Arabia was one of the most attacked countries while connecting to the Internet [16].

Children are an important part of the Saudi population. Recently, it was recorded that 61% of the children who participated in the study in 2013 were using mobile phones; also, 54% of them use Tablet devices [17]. They also start to use the Internet for education and entertainment purposes such as playing online games, watching videos or using online search engines. As they have access to the Saudi Internet networks, they are prone to the security threats and attacks reported previously. In order to evade those risks, they also

Figure 2: Percent of Attacked Computers in 2014. [16]
have to have a minimum knowledge of Internet Security Best Practices; in other words, what users should and should not do while they are surfing the Internet [18]. In this study, we are developing an approach to measure the current level of Internet awareness of the threats to the Internet among a group of Saudi children aged 3 to 12. Then, we aim to raise awareness through an innovative program designed according to cognitive development theories that accommodates the content to the level of children's understanding and learning abilities.

1.2. Purpose of Study

The study's primary purpose is to spread and raise awareness of Internet security threats among young Saudi children by providing them with awareness content to become aware of the Internet security risks as well as boosting their ability to use the best practices in case they face any threats while using the Internet. This goal is significant since there has been an evident increase in the use of the Internet by young Saudi children who started to prefer using iPads and tablets as a means of entertainment rather than the classical ways of playing outside with friends.

In order to achieve this goal, the researcher is keen to find answers to the following research questions:

1- What is the current level of Internet security awareness among a group of Saudi children?

2- Based on the measured level of Internet security awareness, can we design an awareness solution for children?

Also, the study seeks answers to the following research sub-questions:

1- What is the level of Internet security awareness among the Saudi children's parents?

2- Is there a relationship between the measured parents' level of awareness and the children's measured level of awareness?

3- Is there a relationship between the parents' frequent use of the Internet and the children's level of awareness?
4- Is there a relationship between the age of the children and their level of awareness?

5- Are the parents and children well-informed of Internet security awareness publications?

1.3. Hypothesis

The hypothesis of this study is that measuring and understanding the current Internet security awareness level among a sample of Saudi children from the age 3 to 12 years contributes to designing a specialized training program that implements the children cognitive development theories that fits children’s ages. Subsequently, it will result in children who are capable of not falling a victim to any of the security threats that might be exploiting online games they play.
2. BACKGROUND

2.1. Terminology

In this section, a number of definitions of key terms, which are used in this study, are listed as follows:

The Internet: According to SANS [19], which is a research and training organization with a focus on security, the Internet is a global network that connects millions of users and separate networks together.

Security awareness: NIST Special Publication 800-16 [20] defines the awareness as drawing the attention of users to the security of information and the most important issues related to it as well as the best practices to deal with them through simple and attractive publications and campaigns.

Threat: Any circumstance, capability, action, or event that aims to violate the security or welfare of an individual or an asset is referred to as security threat [19].

Risk: The likelihood of a security breach caused by a security threat that compromises an existing vulnerability in an individual or an asset [21] [19].

Malware (i.e. Malicious Software): Any encoded program that has the intention of harming, exploiting or disturbing system’s or data’s security and specifically its confidentiality, availability and integrity. The malware usually is inserted without the victim’s knowing and can be in the form of a virus, a Trojan horse or a worm [22].

Information Privacy: The term privacy commonly refers to the state of collected and stored data being free from disclosure to unwanted parties or systems. A more professional definition by NIST SP 800-32 states that privacy is “Restricting access to subscriber or Relying Party information in accordance with Federal law and Agency policy” [22].
Password: A combination of letters, numbers or symbols that presents a secret key to authenticate a party’s identity or to confirm access authorization as indicated by FIPS 140-2 [22]

Security Countermeasure: A counter measure is a security control method that could be a specific action, device, procedure or technique that aims to mitigate the risk of exploiting system vulnerabilities. It can be a responsive measure that reacts to detected threats. Examples of countermeasures include Firewalls, Intrusion Detection and Prevention Systems (IDPSs), Access Control Lists (ACLs), Anti-virus software and Malware filters [19] [22].

Computer Emergency Response Team (CERT): A non-profitable organization that is usually run under the supervision of the country’s governmental telecommunication agencies. CERT addresses Information Security issues and aims to find solutions to improve the security awareness of the nation. It also provides incident response services to security attacks’ victims [19].

Smart Device: An electronic device that is connected wirelessly to other devices and networks via Wi-Fi, NFC, Bluetooth, 4G or other wireless protocols. It is usually a transportable device that is operated, to some extent, autonomously. It has the ability of voice and video communication, Internet browsing, and providing geo-location services [23]. Examples of smart devices include smartphones and tablets.

Cognitive Development: Refers to the structure of perception and information processing skills that include learning, remembering, problem solving and other brain developments from childhood to adulthood [24] [25].

2.2. Security Threats and Countermeasures in Saudi Arabia:

The Internet in Saudi Arabia is managed by specialized government agencies, mainly the Communications and Information Technology Commission (CITC) [26] in cooperation with the Internet Services Unit in King Abdulaziz City for Science and Technology (KACST) [27], Saudi Telecommunication Company (STC), and a number of Internet Service Providers (ISPs).
Services provided by these agencies include providing the Internet, connecting the Saudi network to the global network, network domain registration, Internet-content management, and filtering, supervising Internet services providers, protecting Saudi users' rights and spreading Internet awareness.

2.2.1. Threats

One of the Saudi Internet Authorities’ goals is to study, monitor and mitigate security risks that threaten the Saudi network. According to the governmental website for the Communications and Information Technology Commission in Saudi Arabia, the top security threats targeting the Saudi network and its users includes phishing, malware, cyberbullying, (see section 1.1.), as well as the following threats:

**Spam**, which is sending annoying messages randomly to a large number of people without their consent or registration in mailing lists. Spams can be promotional messages for products, services or online websites. It can be delivered via e-mail, telephone or chat rooms [28]. Saudi Arabia is the second most spammed country, as mentioned earlier in section 1.1.

**Online defamation**, which is any intentional action of harming someone’s good reputation. It can be done by spreading false written or spoken statements that might induce hostile opinions or feelings against the person [29]. Most of online defamation cases occur on social media websites, such as Twitter and Facebook, where people can freely write their thoughts.

**Identity theft**, which is the use of other person’s identity, information or account for malicious purposes such as fraud, financial theft or targeting victims on the Internet [30]. This threat is considered a serious danger if the criminal was able to get enough personal information from the user through phishing and use them in cybercrimes; thus, causing the innocent user to face legal charges.

**Internet Fraud**, which it the use the Internet to deceive users by providing them false information that appears legit. Examples of fraud is cyber phishing, in which the
cybercriminal trick victims into believing that they won a prize for instance; thus provide personal information that might cause the victim major losses [31].

2.2.2. Countermeasures

In Saudi Arabia, Internet users rely on several security countermeasures to ensure the security of their information while connecting to the Internet. Some of these countermeasures are already built-in on their devices such as Firewall and Parental Control Settings. On the other hand, some of them are stand-alone software that address one or several security threats. Below are brief descriptions for some of the countermeasures Saudi people use:

**Firewall:** which is a system that regulates the connection between the device and the Internet. For simplification, one can say that the firewall blocks malicious or suspicious data from getting in, and blocks sensitive and important data from going out. Firewalls are usually regulating the data based on specific rules set by the user. Some of the firewall systems are integrated in the devices as a feature. For example, Recent Windows operating systems come with a built-in Windows Firewall that has default settings to protect the system from external threats [32].

**Internet Protection Software:** which is a protection software installed on the device to scan, detect and eliminate malicious threats such as viruses, spyware, worms and Trojan horses. Besides detecting malware, the software may also provide extra services such as Password Management and protection against Email Spam and Phishing. Protection software are either premium products that require users to buy them, such as Kaspersky Internet Security [33] and McAfee Internet Security [34]; or free versions that provide less services compared to the premium ones, such as Microsoft Security Essentials [35] and Avira Free Antivirus [36].

**Parental Control:** which is a set of restrictions applied on the device settings to control some its features. It provides parents the ability to control their children’s use of electronic devices. The parental controls include content filtering, which only allows the access to age-appropriate content; usage control, which addresses device usage concerns such as
setting up a time limits; computer usage management tools, which applies specific software to use; and monitoring, which applies location and activity tracking services while children use the device [37]. Major developers integrate Parental Controls feature with their operating systems settings, such as Apple’s Parental Control on Mac and Restrictions on iPhone, iPad, and iPod touch [38], and Microsoft’s Parental Control on Windows [39].

**Content Filtering:** In Saudi Arabia, a very important countermeasure is used to indirectly prevent Internet threats that occupy websites with inappropriate or adult content. The filtering service is monitored by the permanent security committee as well as the Saudi Communications and Information Technology Commission (CITC). The commission takes responsibility to block any websites with content that doesn’t comply with Islamic religion and national regulations [69]. The filtering service also has other goals, such as blocking piracy websites that commit Plagiarism or steal Intellectual rights.

In addition to the regular defense methods, Saudi governmental agencies, represented in Computer Emergency Response Team (CERT) and Communication and Information Technology Commission (CITC), are using awareness campaigns and publications to spread and increase the Information Awareness among the Saudi nation. A recent nationwide awareness campaign was launched to inform people about Cybercrimes [40]. The campaign activities extend to social websites such as Twitter and Facebook as well as video streaming websites such as YouTube. In addition to campaigns, CERT [41] provides and Awareness Building program that issues awareness publications about spam, Email security and Children protection against Internet dangers; the latter is mainly targeting the parents of the children by providing information and guidelines to protect their children [42].

### 2.3. The Cognitive Development Theory

Childhood is defined in the dictionary as the period of time during which a person is a child [43]. Sociologists define childhood as the early period of human life in which the person is entirely dependable on his/her parents. The childhood period is known to extend from the moment of birth to the age of twelve. During that period, individuals learn and mature
by rapidly developing cognitive skills [44]. Psychology researchers have always been interested in studying and theorizing the cognitive development processes that start from a very young age. A number of distinct theories emerged in this area to define cognitive development as we know it today.

One of the most significant child development theories is Piaget’s theory of cognitive development. Jean Piaget is a Swiss psychologist who became interested in the way children learn after he worked in Alfred Binet Laboratory in Paris. As he evaluated, the children’s responses to a standardized intelligence test, he noted that children had a different way of learning and that their “incorrect” answers are in fact based on how their logic work. He showed a great interest in understanding the relationship between the child’s age and his errors [45].

His major contribution to the field of child psychology is the Cognitive Development Theory, which focuses on the children’s mental development [45] [46]. One of the major concepts discussed in the theory is how the thinking procedure is constructed of two basic processes: Organization and Adaptation. Children develop schemes to adapt to the new objects and behaviors in their environment [46] [47] [49].

According to Piaget, A scheme is “an organized pattern of behavior” [46] and thoughts to list some characteristics of items and activities [47].

Assimilation is a process of applying old schemes to new objects while Accommodation is a process of adjusting old schemes or creating new ones to fit with the new object [46]. For example, a child perceives a new object such as a baseball and tries to adapt it to the soccer ball scheme that he/she already knows; the child might adjust the size of the ball to fit with the baseball characteristics. In contrast, if the child is perceiving a balloon, he/she will more likely to create a new scheme to fit the new object rather than adjusting the soccer ball scheme since the balloon and the soccer ball only share the roundness aspect [48].

Based on the theory, there are four stages that identify the process of cognitive development:
1- The first stage is the Sensorimotor stage, which has six phases and stretches from the child's birth to age 2. The main facet of this period is that the children in this age use their sensory systems, such as touch and taste, to identify and interact with objects in their environment [46]. This stage is not in the study’s scope since the research’s subjects belong to an older age group.

2- The second stage is the Preoperational stage in which the children from age 3 to 7 develop a “symbolic functioning”. This function enables the children to perceive objects as different objects. For instance, they start playing with a wooden stick as if it was a shining sword. The children in this stage can also recognize past and future tenses [46].

3- The third stage is the Concrete Operational stage which starts at age 7 through age 11 and develop significant mental operations for solving problems and interacting with the world. Although the child can solve more problems in this stage, he/she still struggles to solve hypothetical problems and concepts.

4- The fourth stage is the Formal Operational stage that starts in late childhood (specifically at age 11) and continues to age 15 and onwards. The stage remarks the point where a child begins to solve hypothetical problems and abstract concepts smoothly.

Overall, Piaget’s cognitive development theory provides solid background to understand the mental stages of the children targeted in this study. The age scope of the targeted sample are from 3 to 12 years old, which involves three stages of the cognitive theory: Preoperational, Concrete and Formal operational.
3. LITERATURE REVIEW

Information Security is one of the emerging research areas nowadays. It has a limitless number of studies interested in the development of methods to protect the individual's information and privacy. The following studies are mainly focusing on raising the security awareness and customizing the technology for this purpose. A number of them aim to protect the children in particular and educate them when using the Internet.

In general, people with limited Internet experience are classified as new Internet users. Thus, they may not have sufficient expertise and awareness of the security dangers of the Internet. The attitudes and decisions they make when using the Internet depend on their information and background. A study presented by Rader, Wash and Brooks (2012) [51] that aims to verify a hypothesis. The hypothesis states that the non-expert computer users take decisions based on the stories they hear from others such as friends. The study collects information through a survey with close-ended questions. The results of this survey have made it clear that decisions indeed depend on what the individuals know of information and stories reached them by family and friends. The study contributes to the process of enhancing the user's ability to make right decisions when dealing with security issues.

Education is one of the most effective ways to improve the people’s information security background. A study by Howles, Romanowski, Mishra, and Raj (2011) [52] employs this aspect by suggesting that undergraduate students in computing majors such as Computer Science, Computer Engineering, Software Engineering, and Information Technology should be taught topics in Cybersecurity. In this study, the topics are designed into different modules that will provide sufficient knowledge of the latest security developments and concerns in their majors. The modules include several categories about Software, Hardware, Web and E-commerce, Legal/Ethical and Policy/personal topics as shown in Figure 3.
The modules presented in the study are evaluated to verify whether or not they achieve that goal of instilling cybersecurity topics in undergraduate computing majors.

Another study by the same authors (2011) [53] encourages introducing the security concepts to general undergraduate majors as well. This means targeting a bigger audience of undergraduate students in order to receive a comprehensive background about the common information security topics. The study presents different categories (Figure 4) that can be introduced in existing courses. The planned modules include modules that explore areas such as Critical Infrastructure Management and SCADA systems.

Figure 3: Module categories for computing majors [52]
The main purpose of these two studies is to enable students to participate in the development of Information Security and build substantial experience in this field.

Another effective way to improve the information security is to spread awareness among people. We find that many of the studies are interested in developing new awareness programs and study their effects and benefits on various groups of society. A study by Kim and Homan (2012) explores the effectiveness of employing an information security training and awareness program in a middle-sized financial organization since a financial institution is one of the top targets for hackers who steal information. The study is designed to measure the effectiveness of the awareness program with its two modes of delivery: Computer-based Training (CBT) and Instructor-based Training (IBT) in two time periods: within 60 days and within 90 days. The measurement focuses on the participants' levels of knowledge transfer and knowledge retention. The results show that in the first time (within 60 days), the Instructor-based Training (IBT) is more effective than the Computer-based Training (CBT) when it comes to knowledge transfer. On the other hand, Computer-based Training (CBT) gives a higher level of knowledge retention compared to the Instructor-
based Training (IBT). In the second time, which is within 90 days, both trainings provide a similar result in knowledge retention. Overall, the study showed the effectiveness of having different methods of training people in the security field. This study was limited to the employees who work in financial institutions only.

Another study presented by Alhejaili (2013) [55] suggested developing an interactive online program that provides a well-designed information security awareness lessons for the middle school students. The program is best to have a continuously updated and interesting content in different languages in order to be ideal for the students and their families. The study examines the current state of information security through a questionnaire for the middle school students and their families. Also, the study examines the newspapers to search for Technology and Information Security incidents that involve middle school students. The results of this study indicate that middle school students need an interactive awareness program that enriches their knowledge and raise their awareness of the Technology dangers. The study focuses on students in middle school which makes us more interested in shading the light on younger people.

Speaking of younger people and their security introduces us to a more concerned field. People usually put a great care in ensuring their children’s safety and privacy. There are several studies that propose methods to accomplish that. For example, a study by Ervasti, Isomursu and Kinnula (2009) [56] employs technology in the school in order to ensure the safety of the young students. The main objective of the study is the keep track of the children's attendance at an elementary school in Finland. Near Field Communication Technology (NFC) is used to log the attendance of 23 students between the ages of 6 and eight years. Each student has his/her smart cards with a unique code that can be read by teachers' NFC-enabled devices. The end users categories benefited from the technology are the Teachers, the Children as well as the Parents who track their children in a real-time manner. The results were measured by phone interviews and feedback questionnaires targeting the three user categories about their experience of the proposed method. After analysis, the result shows that the children did not face any difficulties in understanding and using the method. Also, teachers and parents both were happy to keep track of the
students’ whereabouts accurately and log their activities. This method contributes to 
harming the safety of children and reduces the level of anxiety that may accompany 
raising children.

The previous study focused on the importance of ensuring the safety of children. Likewise, 
the safety of children’s digital identities and information must be ensured as well. A 
number of studies recognized this aspect and developed methodologies to accomplish it.
Read and Beale (2009) [57] conducted a study that aims to develop a new design for the 
security of a children application. The development of such a design comes from answering 
the research question: Where and how do children keep their special things safe? The study 
emphasizes that knowing the answer will provide a lot of understanding to the security 
methods appropriate for children as well as designing new methods that will protect and 
teach them how to maintain the confidentiality of their digital properties such as passwords 
and personal data as they would protect their own special things.

The researchers in this study adopted the use of pictures rather than words since children 
understand better with pictures. Another reason is to entertain the children while 
completing the tasks. The study targeted 43 children between the ages of 8 and 9 from two 
different schools in the United Kingdom. The methodology is a 20-minute session with the 
children divided into four stages:

- **Stage 1**: Introducing and explaining the task to the children by distributing a "My 
  Special Things" booklet to each child.
- **Stage 2**: Asking the children to write down their names and ages on the booklet; 
  then proceed to draw five things they consider special to them.
- **Stage 3**: Instructing each child individually to choose the most special thing to them 
  by circling it.
- **Stage 4**: Conducting one-on-one interview with each child to ask them about how 
  they would keep their chosen special thing safe. The answers are written by the 
  researcher on each child's booklet.
After collecting the data from the children's booklets, the analysis process started and focused on two key information that are the selected most special things and the method of keeping them safe. The researchers found that most of the children chose either experiential items such as Game Consoles or emotional items such as parents. The protection methods provided by children include keeping the items very close in a safe environment such as bedroom, or hiding the items in a safe place; for example, inside boxes or under the bed. The researchers were able to conclude and design a number of solutions in the light of the analysis information. The suggested solutions include the following:

1. Linking major security concepts such as password and personal data (which are the focus of this study) with the special items selected by the children in the study; thus, using the provided safe places for each item to protect the password and personal data. For instance, passwords can be created in the form of pictures or numbers. The protection method can have passwords clues hidden in boxes to help the children retrieve their passwords. The researchers find this solution subject for further study.

2. Personal data can be protected by designing a security solution in a form of alerts and warning messages illustrated for the children in graphics to show them the current place of their entered personal data such as name and age. Furthermore, these alerts represent the personal data as a teddy bear to imply for children how special personal data are. Figure 5 below shows the design's four comical places of the personal data: Person, Room, Home, and Outside (North Pole).
The study collected data from the children to develop a security design that will be implemented in a mobile application for children. The study finds that designing a solution based on children's understanding of safety methods will help to improve the security of their data.

Moreover, people have established special agencies and websites for developing awareness programs. Halpert proposed a study in the InfoSecCD’10 conference (2010) [2] that encourages educating children before they use the computers and the Internet. In the recent generations, children of young age are more familiar with technology and demand to use it. Nowadays, we find the children are surrounded by manufactured devices specialized for them [58]. The study suggests a development of a specialized curriculum that educate preschool children about the technology dangers that can threaten the safety and behavior of the child. The study's motives came from the increased risks and bad behaviors indirectly seen in the online games. For example, teaching children gambling and video recording others for the purpose of abuse and Cyber Bullying. The solution presented by the researcher is to create a non-profit organization called "Savvy Cyber Kids." The organization uses traditional education methods for children such as picture books. The proposed method of education is to issue an illustrated picture book featuring a three-year-old girl and a five-year-old boy who are taking their first steps into the technology world.
The book employs a Child-to-Child learning that is based on the constructivist educational theory. The organization's publications are planned to be distributed to preschool teachers. There is no result yet for this solution; however, we can see the importance of using educational methods suitable for children to ensure their understanding of the technology risks that may pose a threat to their safety.

This thesis study is particularly interested in the Saudi society; therefore, taking an overview of the existing studies about the information security in the Middle East region including Saudi Arabia is significant. Aloul presented a study in 2012 [59] that explores the need for effective Information Security Awareness program for a broader group of people in the Middle East and the UAE specifically. The study discusses the current situation of the Information Security by presenting a number of published studies' results about the topic. The first study is about the Phishing Attacks in UAE that steals sensitive information such as personal and bank information. The second study explores the wireless security vulnerabilities in Dubai and Sharjah. The last study shows the Radio Frequency Identification (RFID) security in UAE. After that, the researcher encourages the governments, schools and universities to implement an effective information security awareness programs that take into consideration a number of key factors such as developing cybercrime teams and laws. Finally, the study presents a list of recommendation for each sector of the country in order to participate in raising awareness among people.

In the same area, in Saudi Arabia, a number of researchers proceeded to study and understand how Saudi people use the Internet. A study by Sait, Ali Al-Tawil and Sanaullah [60] aims to understand the trends in Internet Usage in Saudi Arabia and its Social Effects on the Saudi people. The study was conducted through an online questionnaire that asks questions like ‘who is using Internet in Saudi Arabia?’ and ‘what users do online’? As well as studying the social effects of the Internet, privacy and security concerns. The results derived from 4,400 respondents' answers made it clear that there are various patterns of Internet usage along with different users who are either new to the Internet or long-term users. The top two usages for the Internet are work-related and for fun. The study also
shows that 64% of participants are concerned about their privacy and would strongly want to protect their information while using the Internet.

Another study was conducted in the Kingdom of Saudi Arabia in 2012 by Alarifi, Tootell and Hyland [18]. This study examined the level of Information Security Awareness and practices among Saudi people. The researchers indicate that the level of Information Security Awareness in Saudi Arabia is still low compared to levels in the developed Western countries. The reasons of this indication are believed to be related to the strict tribal customs and high-level of censorship practiced in Saudi Arabia. The study measures the level of Information Security Awareness through an anonymous online questionnaire which was designed based on the Cyber Security Organization in Malaysia and the Klynveld Peat Marwick Goerdeler (KPMG) surveys. The questionnaire included a collection of questions about Information Security issues and preferences for information dissemination. The total number of the online survey's participants is 462. The results of the study show that there is a significant weakness in the Information Security Awareness among Saudis. This statement is reinforced after comparing some of the study's results with results of a similar study conducted in South Africa. Moreover, the results shows that the most weaknesses are found in the Password area where people are not following proper security practices such as changing passwords periodically and avoiding easy passwords. The Saudi people are found to be more aware of virus attacks compared to their knowledge about other security attacks associated with passwords such as phishing, Identity theft and Denial of Service (DOS). Thus, that results in them use anti-viruses software more than other security solutions such as anti-spyware and anti-spam. The study surveyed the most preferred mean to spread Information Security Awareness; the results shows that web portals is the most voted one along with the newspapers. Overall, the study focuses on measuring the level of ISA among the public of Saudi Arabia and finding the most appropriate and widespread methods to spread awareness.
The collection of studies reviewed in this section are unanimous on the importance of developing awareness programs on the Information Security threats and study their benefits and effects. The studies targeted a varying groups of society with different ages, ethnics, and occupations. However, due to the lack of a specialized study targeting children from age 3 to 12 years in Saudi Arabia, who might have never taken an Information Security Awareness program before using the Internet, this thesis study focuses on developing a methodology to measure their current awareness level and design an awareness program for them.
4. AWARENESS EVALUATION

The methodology used in this study to achieve its goals and prove or disapprove the hypothesis is divided into two stages. The first stage is evaluating the Internet security awareness of a sample of Saudi children. This section of the report shows the design of the evaluation tool as well as the results of the evaluation process.

4.1. Evaluation Methodology Design

As a component of this study that aims to measure the Internet security awareness level among the Saudi children, the study sample were identified as two categories of population: the first category is a group of Saudi children who fall in the age between 3 to 12 year-old and use Internet-enabled devices, and the second category is the parents or guardians of the children selected in the first category. These two sample categories qualify the researcher’s specification which is for each participating Saudi child, his/her parent or guardian is required to participate.

After the selection of the study sample, it becomes essential to conduct a field study. The term "Field Study" refers to any study that is being conducted outside the lab environment and settings [61]. Instead, it is studying and interacting with the research's samples in their natural environment by many methods of collecting data such as Observation or Surveys. In observation methods, the researcher does not interact directly with the research sample and collect the data by observing the subjects in their natural settings [62]. On the other hand, surveys are used to collect data from subjects themselves through a constructed sequence of questions that are delivered to them either via phone interviews, paper-based questionnaires or electronic surveys [63].

The data collection method used in this study is a survey that asks study subjects to answer a number of questions carefully designed to acquire accurate data. The questions are closed-ended which means that the questions have a set of predetermined answers and the participant has to choose one of these answer rather than developing an answer themselves.
as in the case of open-ended questionnaires. The predetermined answers in this survey facilitate the process of designing complicated questions about information security concepts which the participants may not have a knowledge of.

The survey in this study is taking the form of an online questionnaire, which is a questionnaire that is delivered to the participants via E-mail or links to websites. The online questionnaire is commonly published through a third party survey websites. The used website in this study is called KwikSurveys.com, which is a free survey builder specifically designed for researchers to publish their surveys and distribute them to the participants across the Internet [64].

There are two sets of online surveys. Each one of these surveys is directed to one of the two categories of study population. In other words, one survey is directed to the parents, and the other survey is directed to the children. The methodology followed in this study is designed so that parent answers the first set of survey (which we will refer to as the parent’s survey from now on), then the child answers the second set of survey, which will be referred to as the children’s survey. Each one of these surveys is designed based on social and cognitive development theories such as Piaget’s cognitive development theory. Moreover, there are several specifications for the survey that include using a simplified language for the children to be able to comprehend the survey questions [63].

4.1.1. Parents’ Survey:

Based on the study’s aims and requirements, it is a necessity for the parents to participate in this study since it will provide more information about the children’s background and Internet usage. In terms of the parent’s survey, it is divided into three main sections:

1- **Demographic Information:** which are basic information such as gender, age and occupation. These questions are used to understand the background of the participants and help in the analysis process by providing a sort of categorization to the answers [49]. A number of the survey’s demographic questions were assembled from a previous online survey built by Alshamrani and Furnell in 2010 to target the Internet users [50].
2- **General information about the Internet usage**: This section aims to provide information about the children usage of the devices and Internet as well as their parent’s role in monitoring devices.

3- **Security practices and Awareness information**: This section is specialized in providing information about the current security measures the parents are taking in order to secure their child’s Internet usage. Moreover, a number of questions about security risks are included in the parent’s survey. According to Piaget’s theory of Cognitive development (see section 2.3.), some of the theoretical concepts such as Security and Risks are difficult for children to comprehend at a young age [57], which leads to requiring an adult answering some of the questions the child might not grasp their meaning.

Other sets of questions were added to the survey after the design of the children’s survey whereas these questions were deemed to be challenging for the children by the researcher. However, it was important for the research to obtain the answer to these questions to enhance the process of evaluating the child’s awareness level.

**4.1.2. Children’s Survey**

Children are the main target of this study, therefore, the children's survey is carefully designed based on specific theories and guidelines. A major number of the guidelines were retrieved from a study by Read and Fine in 2005, which provides tips and strategies to design children surveys. The top design tips include using simple language structures and vocabulary instead of ambiguous words and meanings; moreover, simplifying answers with the aid of pictures and Visual Analogue Scales (VAS) to prompt children’s opinion [63]. Piaget's theory of cognitive development also helped in forming basic conceptual questions that consider the mental and cognitive abilities of children aged 3-12 years, which are the targeted study subjects. The theory addresses the cognitive development of children from birth to adulthood and divides the process to four stages based on the child’s age. Based on the children’s age scope, we are especially interested in three stages: Preoperational stage (from 3-7 years), Concrete stage (from 7-11) and Formal operational stage (from 11-adulthood).
In addition, a number of questions and answer choices are inspired by existing Internet Security quizzes designed by governmental agencies in countries such as Australia [65], United States of America [66], and Sudan [67]. Overall, the survey contains 14 multiple-choice questions written in Arabic and divided into three sections as follows:

1- **General Information:** This section aims to obtain some of the child’s general information, such as gender, age, type of the Internet-enabled device used by the child and the top visited websites and applications.

2- **Internet Security:** This section includes direct questions about the common security concepts and scenarios that children can be exposed to while they are using the Internet. Examples of these scenarios are providing personal information to online websites, adware and malicious advertisements, anonymous friendship requests and password protection. The questions in this sections are designed to prompt the children to choose which action they would take if put in the situation. These scenarios were specifically since they most likely are common to occur while using the Internet.

3- **Symbol Recognition:** This section aims to measure the child’s ability to recognize the symbols commonly used to indicate Internet security concepts. Examples of these symbols are shown in figure (6). Figure (6-a) is the warning icon that often appears in alert messages when there is a security problem. Figures (6-b) and (6-c) show the locked and unlocked padlock icons that illustrate websites’ deployment, or non-deployment, of the Secure Socket Layer (SSL) protocol, which is an encryption

![Figure 6: Examples of Internet Security Symbols.](image-url)
technology to secure the connection between the browser and the web server [68]. The measurement process for the symbol questions is using a 3-point Visual Analogue Scale shown in figure (7). The choice “Good” indicates a state of security, choice “Bad” indicates a state of insecurity or a security problem and choice “I don’t know” indicates the child’s unfamiliarity with the symbol. In addition to the symbols questions, the children are asked to choose the correct action to take for every symbol that might appear to them. These questions are created to measure the awareness regarding taking correct actions when encountering such symbols.

![3-point Visual Analogue Scale](image)

*Figure 7: 3-point Visual Analogue Scale*

Overall, the survey addresses simple and familiar security concepts children can comprehend since the concepts are presented in relatively concrete scenarios. Unlike the complex conceptual questions in the parents’ survey, which require adults to answer them accurately.

4.2. Evaluation Results

4.2.1. Parents’ Survey

The initial number of recorded parents’ surveys is 230. The filtering process decreased the number to 136 eligible surveys. The rest of the surveys were eliminated since they were incomplete. The surveys were analyzed as follows:

A. Demographic Information

The collected demographic information have been analysed to understand the background of the survey participants. The analysis focused on a number of factors such as Guardianship (*Figure 8*), Age (*Figure 9*), Residency (*Figure 10*), Region (*Figure 11*), Education (*Figure 12*) and Work (*Figure 13*):
Figure 8: Distribution of the parents' sample according to (Guardianship)

Guardianship

- Mother: 67%
- Father: 23%
- Guardian: 10%

Figure 9: Distribution of the parents' sample according to (Age)

Age

- Under 20: 4%
- 20 to 29: 37%
- 30 to 39: 41%
- 40 to 49: 16%
- Over 50: 2%

Figure 10: Distribution of the parents' sample according to (Residency).

Residency

- Inside KSA: 92%
- Outside KSA: 8%

Figure 11: Distribution of the parents' sample according to (Region)

Region

- Western: 56%
- Central: 21%
- Eastern: 5%
- Southern: 16%
- Northern: 2%
It is notable from the demographic analysis that most of the survey participants are mothers, with a percentage of 67%. Also, the majority of the participants are aged between 20 to 39 years old as can be seen in figure 9. Giving the residency factor in figure 10, it is clear that about 92% of participants live inside Saudi Arabia. Moreover, a large percent of participants are originally from the Western region.

The demographic information also shows the level of education that participants have received. About 51% of participants have bachelor’s degree. The percentage indicates that most of Saudi parents have a reasonable level of education. However, according to figure 13, the working participants are slightly fewer that the non-working individuals. To get more details, table 1 below shows the cross tabulation between the parents and work:
From table 1, we can see that most of the participants who are also non-workers are Mothers. This might indicate a high percentage of unemployment among Saudi females.

From the participants’ answers about their children’s age and gender in tables (2) and (3), we can see that preschoolers are in the first rank with a percentage of 41.2%. The other 59% of children are distributed from the middle and late childhood. Also, we can see that male children are slightly more than female children with percentages of 52.9% and 47.1% respectively.
B. General Information about Internet usage

Table 4: Do you use the Internet?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>107</td>
<td>78.7</td>
</tr>
<tr>
<td>Sometimes</td>
<td>26</td>
<td>19.1</td>
</tr>
<tr>
<td>Rarely</td>
<td>1</td>
<td>.7</td>
</tr>
<tr>
<td>Never</td>
<td>2</td>
<td>1.5</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

The table above shows how often the parents use the Internet in Saudi Arabia. About 79% of them declared that they always use the Internet. This makes us assume these participants are experts to some extent with Internet applications and online websites. On the other hand, only 3% of the participating parents rarely or never use the Internet.

Table 5: Does your child use Internet-enabled devices?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>117</td>
<td>86.0</td>
</tr>
<tr>
<td>No</td>
<td>19</td>
<td>14.0</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Table 6: Does your child use the Internet?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>46</td>
<td>33.8</td>
</tr>
<tr>
<td>Sometimes</td>
<td>62</td>
<td>45.6</td>
</tr>
<tr>
<td>Rarely</td>
<td>19</td>
<td>14.0</td>
</tr>
<tr>
<td>Never</td>
<td>9</td>
<td>6.6</td>
</tr>
</tbody>
</table>

Tables (5) and (6) illustrate the number of responders who allow their children to use an Internet-enabled device as well as grant them access to the Internet. About 86% of responders have their children using an Internet-enabled device. Only 14% do not allow that which means that they also don’t allow their children to use the Internet. On the other hand, the results of allowing the children to actually use the Internet vary. About 79% of
the parents confirms that their children always or sometimes use the Internet. In contrast, only 20.6% declare that their children rarely use the Internet.

Table 7: What type of device does your child use?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktops/Laptops</td>
<td>14</td>
<td>10.3</td>
</tr>
<tr>
<td>IPad/iPod/Android</td>
<td>96</td>
<td>70.6</td>
</tr>
<tr>
<td>Tablets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Phones</td>
<td>26</td>
<td>19.1</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

It can be seen from the table (7) that IPad/iPod/Android Tablets occupy the first rank with percentage of 70.6%. The high percentage could be related to the easiness of using screen-touch devices with medium sizes that children can hold easily. Also, it could be because of the richness of children’s applications found on these devices. Compared to tablet devices, smartphones and desktops gained low percentages which is 19% and 10% respectively.

Table 8: What is the main purpose for which your child uses the device?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entertainment (To play)</td>
<td>128</td>
<td>94.1</td>
</tr>
<tr>
<td>Education (To do Homework)</td>
<td>8</td>
<td>5.9</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

The table above shows the main purpose for which the child uses the device. About 94.1% of children use the Internet for entertainment or to play, which makes them more prone to Internet attacks and threats commonly found on entertainment websites and centers. Some of the attacks are Phishing, Malware and Adware. Also, some of the entertainment websites promotes inappropriate concepts such as Gambling.
Table 9: Do you consider the device specifications before you buy it for your child?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>106</td>
<td>77.9</td>
</tr>
<tr>
<td>No</td>
<td>30</td>
<td>22.1</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

In table (9), it can be seen that parents have a high awareness level when they choose a device for their children. Nearly 78% of them consider the device specifications before buying it. On the other hand, only 22% are ignorant to this step of choosing a device.

Table 10: Do you depend on the specifications or the price when buying a device for your child?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device’s specifications</td>
<td>99</td>
<td>72.8</td>
</tr>
<tr>
<td>Device’s Price</td>
<td>37</td>
<td>27.2</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

From another point of view, table (10) shows that 72% of parents choose the specifications over the price when buying a device for their children. The other 27.2%, which is not a small percentage of people, favor the price when buying devices.

Table 11: On average, how many hours a day does your child use the Internet?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 1 hour a day</td>
<td>39</td>
<td>28.7</td>
</tr>
<tr>
<td>1 to 3 hours a day</td>
<td>56</td>
<td>41.2</td>
</tr>
<tr>
<td>4 to 7 hours a day</td>
<td>34</td>
<td>25.0</td>
</tr>
<tr>
<td>More than 7 hours a day</td>
<td>7</td>
<td>5.1</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

From table (11), we conclude that about 41% of children use the Internet 1-3 hours a day. This is a reasonable proportion. More significantly, about 30% of children spend 4-7 hours or longer on their devices. The proportion is not very small which suggests that parents should reduce those hours. The disadvantages of spending long time on the Internet include game addiction, health issues and possible long exposure to Internet threats.
Table 12: Do you teach your child any kind of device management?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, a minimum knowledge (such as adjusting device’s volume)</td>
<td>20</td>
<td>14.7</td>
</tr>
<tr>
<td>Yes, a limited knowledge (such as visiting websites, opening applications and powering the device on or off)</td>
<td>73</td>
<td>53.7</td>
</tr>
<tr>
<td>Yes, my child knows how to set up a password or connect to new networks</td>
<td>29</td>
<td>21.3</td>
</tr>
<tr>
<td>No, my child depends on me to manage the device</td>
<td>14</td>
<td>10.3</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>136</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

We can note from table (12) that most of responders with a percentage of 53.7% give their children a limited knowledge, while 10.3% of them never teach their children or let them manage the device without any assistance. In the same concept, only 14.7% of responders give their children a minimum knowledge and no more. Finally, 21.3% of responders give their children a good background of controlling their devices, such as setting up a password or connecting to new networks.

Table 13: Do you check on your child’s activities on the device?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>124</td>
<td>91.2</td>
</tr>
<tr>
<td>No</td>
<td>12</td>
<td>8.8</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>136</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

Table (13) shows that about 91.2% of responders check on their children’s online activities. This is a reasonable proportion that suggests a great awareness level towards children. A very small proportion, which is about 8.8% of the responders, does not check on the activities of their children.
Table 14: If the answer is yes, do you do that while or after he/she uses the device?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>While using the device</td>
<td>73</td>
<td>53.7</td>
</tr>
<tr>
<td>After using the device</td>
<td>51</td>
<td>37.5</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>124</strong></td>
<td><strong>91.2</strong></td>
</tr>
<tr>
<td>Not included</td>
<td>12</td>
<td>8.8</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>136</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

Table (14) indicates that nearly half of the responders check on the activities while their children are using the devices; Once more, this proves how these responders are well aware towards their children. On the other hand, 37% of the parents check on the activities of their children after using the device.
C. Information about Security Practices and Awareness:

*Table 15: What is the level of awareness parents have to ensure their children’s safety on the Internet?*

<table>
<thead>
<tr>
<th>no.</th>
<th>Question</th>
<th>Mean</th>
<th>Std. Deviation</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>q24</td>
<td>Have ever read any Information Security Awareness publications from any other sources?</td>
<td>0.838</td>
<td>0.370</td>
<td>1</td>
</tr>
<tr>
<td>q25</td>
<td>Is there any Internet Security software installed on your child’s device?</td>
<td>0.684</td>
<td>0.467</td>
<td>2</td>
</tr>
<tr>
<td>q26</td>
<td>If the answer is yes, do you regularly update the software?</td>
<td>0.672</td>
<td>0.471</td>
<td>3</td>
</tr>
<tr>
<td>q27</td>
<td>Do you verify the credibility and safety of the sites and applications your child visits and uses?</td>
<td>0.515</td>
<td>0.502</td>
<td>4</td>
</tr>
<tr>
<td>q30</td>
<td>Does your child have the privilege to download applications or games on the device?</td>
<td>0.478</td>
<td>0.501</td>
<td>5</td>
</tr>
<tr>
<td>q28</td>
<td>Do you give your child an overview of the Internet Security Threats? (Such as viruses, spam, phishing)</td>
<td>0.441</td>
<td>0.498</td>
<td>6</td>
</tr>
<tr>
<td>q29</td>
<td>Do you use Parental Control settings on your child’s device</td>
<td>0.427</td>
<td>0.496</td>
<td>7</td>
</tr>
<tr>
<td>q31</td>
<td>Does your child know the password used to download programs and games?</td>
<td>0.382</td>
<td>0.488</td>
<td>8</td>
</tr>
<tr>
<td>q22</td>
<td>Have you ever heard of the Computer Emergency Response Team, which is a part of the Saudi Communication and Information Technology Commission?</td>
<td>0.118</td>
<td>0.323</td>
<td>9</td>
</tr>
<tr>
<td>q23</td>
<td>Have you ever read any awareness publications from the Computer Emergency Response Team?</td>
<td>0.066</td>
<td>0.250</td>
<td>10</td>
</tr>
</tbody>
</table>

|       |                                                                                                                                           | 0.437 | 0.462          |      |
To get a vivid view of the participating parents’ awareness towards ensuring their children’s safety on the Internet, a simple 2-point Likert scale was used. The questions have two choices; the right answer, which indicates a high awareness level, is coded as 1 and the wrong one, which indicates a low awareness level, as 0. The results, shown in table 15, show the mean of every question as well as the overall average for all questions. The overall average is 0.437, which indicates a low level of awareness among parents since it is less than 0.5. The results comply with the research done by Alarifi et al [18] that indicates that the level of information Security Awareness in Saudi Arabia is still low compared to the other countries’ Awareness level. On the other hand, it can be seen from the table that the top four questions with high mean results are “Reading Information Security Awareness Publications from Any Sources” with an average of 0.838, “Installing any Internet Security Software on the Child's Device” with an average of 0.684, “Updating the Internet Security Software” with an average of 0.672 and “Verifying the Credibility and Safety of the Sites and Applications that Children Visit and Use” with an average of 0.502. These average results refer to a satisfying awareness level among most of the parents about some critical concepts of the Internet security. Hence, the first research sub-question of this study is answered.

*Figure 14: What type of security problems has your child encountered?*

*Type of Security Problems has Your Child Encountered*

- Spyware: 3%
- Viruses: 43%
- Spam: 4%
- Trojan horse: 7%
- Adware: 7%
- Phishing: 4%
- Intrusions: 4%
- Masquerade: 14%
- Cyberbullying: 14%
The parents were asked if their children have ever encountered any problems related to the information security; only 16% of them said yes. Their answers were analysed, and the Pie Chart in figure 14 represents the types of security problems that the children encountered. The Viruses occupied the first rank with a percentage of 43%. This large percentage might be because Saudi people are more aware of virus attacks compared to the other types of security attacks as assumed in the research done by Alarifi et al [18]. The other types earned modest percentages such as 14% for cyberbullying and masquerade, 4% for intrusions, phishing and spam and the lowest proportion allotted for spyware with a percentage of 3%. It is noteworthy that the spam’s result does not fit with Symantec Intelligence Report that puts Saudi Arabia as the one of the most spammed countries by a rate of 66%. Once more, the contrast of the results could be related to the Saudi people’s lack of knowledge of different security threats.

Table 16: Have these problems once and for all been solved?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>14</td>
<td>10.3</td>
</tr>
<tr>
<td>No</td>
<td>8</td>
<td>5.9</td>
</tr>
<tr>
<td>Total</td>
<td>22</td>
<td>16.2</td>
</tr>
<tr>
<td>Not include</td>
<td>114</td>
<td>83.8</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Table 16 shows that about 10% of the study population who encountered security problems have been able to solve them, while the rest of the problems, which is only 5.9% of parents had, have not been solved. The rest of responders did not give an answer to this question with a percentage of 83.8%.
Table 17: Who was the individual who solved these problems?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parents (or other adults)</td>
<td>14</td>
<td>10.3</td>
</tr>
<tr>
<td>The Child</td>
<td>3</td>
<td>2.2</td>
</tr>
<tr>
<td>A professional at a</td>
<td>5</td>
<td>3.7</td>
</tr>
<tr>
<td>maintenance store</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>22</td>
<td>16.2</td>
</tr>
<tr>
<td>Not include</td>
<td>114</td>
<td>83.8</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

The table above illustrates that 10% of security problems were solved by parents or other adults; while computer maintenance professionals were able to solve 3.7% of the problems. The lowest percentage goes to the children who were able to solve only 2.2%.

Table 18: What is the top Internet Security risks from which you want to protect your child?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Game Addiction and using the device for a long time</td>
<td>69</td>
<td>50.7</td>
</tr>
<tr>
<td>Cyberbullying (such as exposure to blackmail, intimidation and verbal abuse)</td>
<td>8</td>
<td>5.9</td>
</tr>
<tr>
<td>Personal and Financial information theft</td>
<td>2</td>
<td>1.5</td>
</tr>
<tr>
<td>Access to inappropriate content such as gambling and pornography</td>
<td>44</td>
<td>32.4</td>
</tr>
<tr>
<td>Exposure to malware and penetration attacks</td>
<td>2</td>
<td>1.5</td>
</tr>
<tr>
<td>Communicating with strangers</td>
<td>11</td>
<td>8.1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>136</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

Table 18 shows the top Internet security risks which the responders want to protect their children from. The most voted risk, with a percentage of 50%, is the game addiction and using the device for a long time. This could be controlled by setting specific time length for children to use the devices. Next, 32.4% goes to the Access to inappropriate content such as gambling and pornography. The risk can be controlled by activating parental...
controls options on the child’s device; also, it can be controlled by the filtering services the Saudi Communications and Information Technology Commission (CITC) provides. The rest of ranks go as the following: 8.1% for communicating with strangers, 5.9% for Cyberbullying such as exposure to blackmail, intimidation and verbal abuse and 1.5% for Exposure to malware and penetration attacks together with Personal and Financial Information theft. It can be noted that Saudi parents place great concern on their children physical and moral safety compared to their information safety.

Table 19: In your opinion, who do you think is primarily responsible for securing your child’s device?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>I am the one responsible for securing it by using security software</td>
<td>110</td>
<td>80.9</td>
</tr>
<tr>
<td>The ISP (Internet Service Provider)</td>
<td>9</td>
<td>6.6</td>
</tr>
<tr>
<td>The Operating System that I’m using (e.g. Windows, MacOS, Linux....)</td>
<td>7</td>
<td>5.1</td>
</tr>
<tr>
<td>The government</td>
<td>10</td>
<td>7.4</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

From table (19), it can be seen that the Saudi parents have a high sense of responsibility for securing their children’s devices since 80.9% of them think that they are primarily responsible for that. On the other hand, the remaining 19% of them think that it is the prime responsibility of the government, the ISP and the Operating System.

Table 20: On a scale of 1-5 (1 being "very poor" and 5 being "excellent"), what is your assessment of your child’s awareness of the Internet security?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very poor</td>
<td>44</td>
<td>32.4</td>
</tr>
<tr>
<td>poor</td>
<td>26</td>
<td>19.1</td>
</tr>
<tr>
<td>good</td>
<td>48</td>
<td>35.3</td>
</tr>
<tr>
<td>Very good</td>
<td>11</td>
<td>8.1</td>
</tr>
<tr>
<td>Excellent</td>
<td>7</td>
<td>5.1</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Table 20 above shows the Internet security awareness assessment of the participated Saudi children through the parents' opinions. 35% of the parents think their children have
a good awareness. While 32% of them think that their children have a very poor awareness. 19.1% of the children have a poor awareness. Finally, A very few children have a very good or excellent awareness with percentages of 8.1% and 5.1% respectively. The assessment indicates that according to the Saudi parents, their children have an insufficient level of awareness ranging from Very Poor to Good.

Table 21: Would you be interested in introducing Internet security awareness solutions to your child?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>135</td>
<td>99.3</td>
</tr>
<tr>
<td>No</td>
<td>1</td>
<td>.7</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

The table (21) shows the parents dominantly agree on introducing an Internet security awareness Solutions to their children. Only one participant seems to be not interested. This result confirms the study done by Sait et al [60] that expresses the Saudi people’s concern about their security and information privacy when using the Internet.

4.2.2. Children’s Survey:

The initial number of the children survey participants is 92 children. After the filtering process, only 87 surveys were determined to be eligible for analysis after eliminating incomplete surveys. The demographic information of the participants, obtained from participants in the General Information section, shows the distribution of children sample according to Age (Figure 16) and Gender (Figure 15).
The first figure above shows the age of the children who participated in the study. Nearly 36% of the participating children are in the late childhood stage, which is from 9-12 years old. The rest of participants are divided into children aged 3-5 with percentage of 33.3%, and children aged 6-8 with percentage of 31%. The second figure shows that only 46% of the total participants are boys and more than half of the – the participants - are girls.
Also, the general information section of the survey shows that the Tablet, such as Apple iPad and Android tablets, is the dominant device used by children in Saudi Arabia with percentage of 75%. The other two categories did not get such popularity. The categories of used devices are shown in figure 17 above.

When analyzing the most visited websites and applications by participating children, every option was set to be independent since the participant can select more than one answer. This makes any option represents 100%. The results in figure 18 below shows that YouTube, the video streaming website, is occupying the first rank in websites that are visited by a percentage of 71.3%. The reason probably is because children use it to watch cartoons. Apple’s App Store comes in the second rank with percentage of 29.9%, followed by Instagram with percentage of 26.4%. Which makes them the top three visited websites and applications by the children’s sample in Saudi Arabia.
Figure 18: Websites and Applications Most Visited by Children Sample

Figure 19: Children who would share personal information on the Internet.
Figure 19 above explains the information which the children think they can share with websites on the Internet. The question addresses the children’s ability to recognize personal information that has to be protected. As can be seen, 51 children agreed that it is correct to give their nickname. While 42 of children think that the full name is shareable. Finally, a few children are ready to give their surname or school address or home address with percentages of 8.04%, 4.59% and 3.44% respectively. None of the children think that sharing the financial information, such as Credit Card Information, with websites is right. The numbers shown in the figure lead us to assume that the children’s level of awareness regarding Sharing Personal Information is in need of more enhancement.

To answer the study’s question “What is the current level of Internet security awareness among a group of Saudi children?,” the questions in the Internet Security and Symbol Recognition sections were grouped and formulated to become a 3-point Likert scale test. The answer that indicates high security awareness was given 3 points, the answer that indicates moderate security awareness was given 2 points, and the answer that indicates low security awareness was given 1. Table 22 below shows the mean scores for each question. The overall average of these scores indicates the level of awareness of the participating children. Thus, we find that the awareness average is 2.25, which means that the children have a slightly insufficient level of awareness. Moreover, when looking to the average scores of each question, we can note that averages of “Password Protection” and “Warning Message Symbol” questions are 2.7 and 2.45 respectively, and that indicates a high awareness level that children have about these specific risks. On the contrast, the questions about determining secure and insecure websites are occupying the bottom of the list which indicates that the children may not be familiar with these concepts.
Table 22: Tests of Awareness Level of Children Sample

<table>
<thead>
<tr>
<th>Question</th>
<th>Rank</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q8: Password Protection</td>
<td>1</td>
<td>2.70</td>
<td>.717</td>
</tr>
<tr>
<td>Q9: Warning Message Symbol</td>
<td>2</td>
<td>2.45</td>
<td>.606</td>
</tr>
<tr>
<td>Q10: Warning Message Action</td>
<td>3</td>
<td>2.33</td>
<td>.676</td>
</tr>
<tr>
<td>Q6: Anonymous Advertisements</td>
<td>4</td>
<td>2.29</td>
<td>.850</td>
</tr>
<tr>
<td>Q12: Secure Website Action</td>
<td>5</td>
<td>2.26</td>
<td>.769</td>
</tr>
<tr>
<td>Q7: Anonymous Friend Request</td>
<td>6</td>
<td>2.17</td>
<td>.809</td>
</tr>
<tr>
<td>Q13: Insecure Website Symbol</td>
<td>7</td>
<td>2.10</td>
<td>.506</td>
</tr>
<tr>
<td>Q11: Secure Website Symbol</td>
<td>8</td>
<td>2.06</td>
<td>.566</td>
</tr>
<tr>
<td>Q14: Insecure Website Action</td>
<td>9</td>
<td>1.90</td>
<td>.741</td>
</tr>
</tbody>
</table>

Analyzing both children's and parents' surveys provided the ability to identify whether or not there are relationships between Information Security Awareness levels among both samples; thus, answering the research sub-questions which include the following:

1- Is there relationship between the child's age and his Internet security awareness level?

Table 23: The relationship between the child's age and his Internet security awareness level

<table>
<thead>
<tr>
<th></th>
<th>Sum of Squares</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Between Groups</td>
<td>.155</td>
<td>2</td>
<td>.077</td>
<td>1.161</td>
<td>.318</td>
</tr>
<tr>
<td>Within Groups</td>
<td>5.606</td>
<td>84</td>
<td>.067</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>5.761</td>
<td>86</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To measure the relationship between the child's age and his awareness level about the risks of Internet, we use One Way ANOVA.
From ANOVA table, it can be seen that there is no a significant difference between the age of child and his awareness level, where (sig=0.318). Hence, we can conclude that there is no relationship between them.

2- Is there a relationship between the degree of the Internet use by parents and children's awareness of information security and the risks of the Internet?

Table 24: The relationship between the parents' use of the Internet and the children's awareness

<table>
<thead>
<tr>
<th>Do you use the Internet?</th>
<th>N</th>
<th>Mean Rank</th>
<th>Sum of Ranks</th>
<th>Mann-Whitney U</th>
<th>Z</th>
<th>Asymp. Sig. (2-tailed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>76</td>
<td>42.59</td>
<td>3236.50</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sometimes</td>
<td>11</td>
<td>53.77</td>
<td>591.50</td>
<td>310.500</td>
<td>1.387</td>
<td>0.165</td>
</tr>
<tr>
<td>Total</td>
<td>87</td>
<td>53.77</td>
<td>591.50</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To test the relationship between the degree of the Internet use by parents and children's awareness of information security and the risks of the Internet, we use Mann-Whitney test. It can be seen from the table that there are no significant differences between the awareness of parents in terms of the degree of the Internet use, where (sig=0.165). Consequently, we find that there is no relationship between the degree of the Internet use by parents and children's awareness of information security and the risks of the Internet.

3- Is there a relationship between the parents’ awareness level and the children’s awareness level?

Table 25: The relationship between the parents’ awareness and the children’s awareness

<table>
<thead>
<tr>
<th>Pearson Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>awareness of parents</td>
</tr>
<tr>
<td>awareness of parents</td>
</tr>
<tr>
<td>awareness of children</td>
</tr>
</tbody>
</table>

*. Correlation is significant at the 0.05 level (2-tailed).
From the table above, it can be seen that the correlation coefficient equal 0.285, which shows that there is a relationship between the parents’ awareness level and the children’s awareness level but it is very weak.

4- Are the parents and children well-informed of Internet security awareness publications?

Table 26: Have you ever heard of the Computer Emergency Response Team, which is a part of the Saudi Communication and Information Technology Commission?

<table>
<thead>
<tr>
<th>q22</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>120</td>
<td>88.2</td>
</tr>
<tr>
<td>Yes</td>
<td>16</td>
<td>11.8</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

The previous table explains that there are 120 responders who did not hear of the Computer Emergency Response Team with percentage of 88.2%, a small number of them did hear of the Computer Emergency Response Team with percentage of 11.8%.

Table 27: Have you ever read any awareness publications from the Computer Emergency Response Team?

<table>
<thead>
<tr>
<th>q23</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>127</td>
<td>93.4</td>
</tr>
<tr>
<td>Yes</td>
<td>9</td>
<td>6.6</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

The table above, shows that a very small numbers of parents – only about 9 responders – read about awareness publications from the Computer Emergency Response Team with percentage of 6.6%. A large number of them did not read such publications with percentage of 93.4%.
Table 28: Have ever read any Information Security Awareness publications from any other sources?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>22</td>
<td>16.2</td>
</tr>
<tr>
<td>Yes</td>
<td>114</td>
<td>83.8</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

The table above, shows that there are 114 of parents read the Information Security Awareness publications from other sources rather than the Computer Emergency Response Team with percentage of 83.8%. Only 22 of responders were not with percentage of 16.2%.

We conclude that the level of parent’s attention about awareness materials of information security and the risks of the Internet is good especially from other sources rather than the Computer Emergency Response Team. As a suggestion, the Computer Emergency Response Team should distribute the awareness materials to people through seminars, conferences and more campaigns.

Table 29: Do you give your child an overview of the Internet Security Threats? (Such as viruses, spam, and phishing)

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>76</td>
<td>55.9</td>
</tr>
<tr>
<td>Yes</td>
<td>60</td>
<td>44.1</td>
</tr>
<tr>
<td>Total</td>
<td>136</td>
<td>100.0</td>
</tr>
</tbody>
</table>

The table, at hand, illustrates the level parents’ efforts in providing their children awareness overview about information security and the risks of the Internet. There are 60 children who are provided overview of Internet security with percentage of 44.1%, which is not a bad proportion. On the other hand, there are 76 children were not aware about such versions with a percentage of 55.9%. That indicates that we need to increase the level of awareness of children.
5. AWARENESS ENHANCEMENT

Over the course of the previous section, a survey tool was developed to measure the current level of Internet security awareness among the sample of Saudi children in order to understand and determine the areas where children needed to be educated. The suggested awareness solution in this study is an application that aims to raise the children’s awareness level. The proof-of-concept solution is designed based on the results of the evaluation survey discussed in the previous chapter. The most notable observations elicited from the evaluation results include:

1- The parents are taking sufficient precautions to ensure their children’s safety online by intently studying device’s specifications before buying them, applying parental controls, keeping track of children’s activities and maintaining security programs on the devices. However, it is highly notable that children themselves do not receive sufficient awareness training as expected.

2- The parents unanimously agree that their children need to be educated through Awareness programs and solutions. This agreement is supported by the parents’ own assessment of their children's current Internet security awareness level. The assessment ranged between Averages to Poor levels.

3- The children are believed to have less than the average knowledge about Internet Security Threats. The result that appears in table 15 suggests that the parents are putting less effort in giving their children an overview about Internet Security threats such as Viruses, Spam and Phishing. This suggestion calls for a focus on developing an awareness solution that provides children with such information.

4- Nearly half of the children sample are using electronic devices -mostly Tablets- in a semi-independent manner. In other words, they have enough experience to power on the device, navigate through the system to open applications and websites. This is remarkable since it suggests that children are most likely will be able to handle awareness solutions targeting them.
5- Children showed interest in many online websites listed in the survey. The top ranked website is YouTube which suggests that streaming videos are more appealing to children. This observation is used to include external link list of existing Internet security awareness clips found on YouTube as additional learning sources in the designed awareness solution.

6- The top Internet Security concepts in which children’s awareness recorded to be low include: Security symbol recognition and interpreting; Dealing with anonymous messages and advertisements; Knowledge of Internet security threats such as viruses, malware and adware; and Personal information protection; although their ability to determine most of the personal information is significantly better than the aforementioned concepts. On the other hand, children showed high level of awareness about Password protection and Warning messages concepts.

These observations are taken in consideration when designing the awareness solution and selecting the appropriate concepts to be included in the awareness material.

5.1. Proof-of-Concept Solution Design:

In the second stage of the study, an awareness solution is designed as a proof-of-concept training application for the children. The top specification taken in consideration is applying Piaget’s cognitive development theory on the design. According to the theory, children are continually developing their perception and cognitive abilities. Piaget divides children’s cognitive development into four stages based on their ages. The study’s sample of children fall into the preoperational stage (from 3-7 year old) and Concrete Operational stage (from 7-11 year old) as well as Formal operational stage (12 year old). Children aged 3-7 year old are preschoolers who have limited abilities compared to the older children. Therefore, the suggested design of the solution is to divide the awareness materials into two stages based on the age: Preschool (3-6 year old) and Elementary School (7-12 year old). The other important specification is applying Piaget’s theory regarding children and playing. The theory believes that playing is important in children cognitive learning. They learn more effectively through playing since they apply the learned skills, concepts and schemes.
The Internet security awareness concepts are selected as shown in figure 20 below which shows the application flowchart and processes.

Figure 20: Proof-of-Concept Awareness Program Flowchart.
The current version of the awareness program is developed in Visual Basic language as a stand-alone Windows Form application. The application consists of four main forms, or windows, designed as the following:

1- **Welcome Screen:** This is the main page of the application. It contains a welcoming message for the children and prompts them to select their age. The age selection is displayed as a question for the children to select which age group they belong to: (3-7 years old) or (8-12 years old). The question is designed to determine the age group the children belong to so they can be directed to the training session suitable for their age.

2- **(3-7 years old) Children Screen:** This section consists of different tabs that have different simple activities for younger children. The concepts covered for younger children are teaching them new security terms and their meanings as well as teaching them what are some of the personal information they must not share online. These two concepts are displayed to give children a basic overview of Internet security. Activities also include learning games where children can apply what they learned in playing.

3- **(8-12 years old) Children Screen:** This section has two main concepts that are deemed to be slightly complicated for young preschoolers (3-7 years old). The concepts are Symbol Recognition and Checking messages and Advertisements resources. The awareness content is displayed as simplified texts aided with graphics and followed by interactive games. The first game is a matching game to help the child recognize the symbols and their differences, such as locked and unlocked padlock. The second game is a multiple choice game where the child is provided a sample of a message or an advertisement and asked to decide if the source is trusted or not.

4- **Other Resources Screen:** Since the children are interested in YouTube, several Internet security awareness videos are included in this window to provide the children access to already existing resources that aim to increase their Internet Awareness Security.

Note that the application is directed to the children from 3-12 years old; thus, the terms and sentences used in the content are simplified to accommodate their comprehensive abilities. The current application has two versions designed in two different languages:
Arabic and English. The Arabic version is the one used in the testing stage since all the participating children are Saudis whose native language is Arabic.

5.2. **Proof-of-Concept Solution Testing:**

To test the Awareness Enhancement Solution and its effectiveness in raising the children’s level of Internet Security Awareness, we have to test it on the targeted population, which are the Saudi children. The strategy of the solution testing includes the following procedures:

1- Selecting a subgroup from the total study sample.
2- Recording their initial Evaluation Survey data (Pre-Assessment).
3- Testing the Awareness Solution and recording new test data (Post-Assessment).
4- Comparing the Test data (Post-Assessment) with the initial data (Pre-Assessment).
5- Concluding the results and observations.

As stated in testing strategy, we will start with randomly selecting children from the total sample to participate in the second stage of this study, which is to test the suggested solution. The subset sample is assigned to have 25 children selected based on the easiest to reach from the total 87 children who participated in the Evaluation Survey in the first stage.

Upon selecting the children sample, their initial awareness level data, determined by the Evaluation survey’s answers, are recorded and labeled as the “Pre-Assessment Data”. The data indicate the children’s level of Internet security awareness before using the Awareness Enhancement Solution. The Pre-Assessment data of the selected subgroup are shown in the following figures and table. The first three figures show the demographic information of the selected sample. As can be seen, figure (21) show the distribution of the Pre-Assessment sample according to the Gender factor. Female children are slightly more of the Male children with a percentage of 52%. Figure (22) represents the Age distribution of the sample. More than half of the sample are children in their late childhood. The rest are from the early childhood and middle childhood with percentage of 36%. Finally, figure (23) shows that 56% of the children are using tablets comparing to the other half who use smartphones (32%) or laptops (12%).
Figure 21: Distribution of Pre-Assessment sample according to (Gender)

Figure 22: Distribution of Pre-Assessment sample according to (Age)

Figure 23: Device Categories Used by the Pre-Assessment Sample
Figure (24) shows the first concept of Internet Security which is sharing personal information. As can be seen, the awareness testing of this concept targets the younger children from age 3 to 7 in particular. Thus, in the Pre-Assessment data, the nine younger children have the awareness that makes them decide to not share top private data such as financial information or Home and School addresses. Meanwhile, they still see that their personal information such as full name is shareable. The nickname, or username, is the top voted information; however, only five of the younger children realize this. The reason for the rest might be because they don’t have clear definition to what nicknames might be.

![Figure 24: Pre-Assessment Personal Information awareness level.](image-url)

In the next table, the measured level of Internet security awareness level among the selected subgroup sample is shown. As discussed in the Evaluation section, the questions are designed as a 3-point Likert scale. Each answer is given a weighted point; correct answers that represent a high level of awareness are given 3 points, medium level of awareness answers are given two points and answers that express a low level of awareness are given one point. In this testing pre-assessment data, the focus is on the older children who are in the age category 8 to 12 years old. The data of the younger children (3 to 7 years old) are
disregarded from the table since they will not be presented with the security concepts listed in the table. Disregarding some of the data resulted in a significant increase in the total awareness average point. The table shows the average points for each Security concept

Table 30: Sample's Internet security awareness Level (Pre-Assessment)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q8: Password Protection</td>
<td>1</td>
<td>2.87</td>
</tr>
<tr>
<td>Q9: Warning Message Symbol</td>
<td>2</td>
<td>2.68</td>
</tr>
<tr>
<td>Q6: Anonymous Advertisements</td>
<td>3</td>
<td>2.56</td>
</tr>
<tr>
<td>Q12: Secure Website Action</td>
<td>4</td>
<td>2.43</td>
</tr>
<tr>
<td>Q7: Anonymous Friend Request</td>
<td>4</td>
<td>2.43</td>
</tr>
<tr>
<td>Q10: Warning Message Action</td>
<td>5</td>
<td>2.31</td>
</tr>
<tr>
<td>Q13: Insecure Website Symbol</td>
<td>6</td>
<td>2.25</td>
</tr>
<tr>
<td>Q14: Insecure Website Action</td>
<td>7</td>
<td>2.12</td>
</tr>
<tr>
<td>Q11: Secure Website Symbol</td>
<td>8</td>
<td>2.06</td>
</tr>
</tbody>
</table>

N = 16 children (aged 8-12).
Not Applicable = 9 children (aged 3-7).

As shown, the average point of all security concepts is 2.41 which is higher when compared to the average of the total sample in the evaluation section. Regarding the security concepts individual averages, we can see that the Password Protection has once again ranked first. This indicated that the children already have a high awareness level to keep their passwords. On the other hand, the lower ranks are claimed by the Security Symbols concepts.

After having a clear understanding of the children’s level of Internet security awareness before receiving awareness knowledge through the proof-of-concept solution, the sample is ready to test and use the solution. The solution is an educational application designed to cover some of the Security Concepts that have low scores in the Pre-Assessment results.

The testing is conducted by introducing the solution application to each child individually. The child is told to go through the educational sessions appropriate for his/her age. After the end of the session, the child is asked to watch two awareness videos listed in the “Learn
59 | P a g e

More” page. Finally, the child is asked to retake the Evaluation survey and answer the questions based on their new acquired knowledge. With this step, the solution testing ends.

5.3. **Proof-of-Concept Solution Results:**

After completing the Awareness Enhancement Solution testing procedure, new data is collected and analyzed to present the “Post-Assessment” results. The applied data analysis process is similar to the analysis process of the “Pre-Assessment” data. In other words, the personal information concept is measured by the number of children chose to share the type of private information. In this particular test, the personal information training session targets the younger children from 3 to 7 years old. The other concepts are measured based on 3-point Likert Scale and target the older children from 8 to 12 years old. The following figure and table show the Internet security awareness level among the children who used the awareness solution and watched awareness videos.

![Bar Chart](image)

**Figure 25: Post-Assessment Personal Information awareness level**

In figure 25, the only two categories of personal information that were selected are “Full Name” and “Nickname”. Nearly 88% of the children chose to share their nickname or username. On the other hand, only 44% of the nine participating younger children chose to...
share their full name that includes first, middle and last name. The other more sensitive information such as home address, school address, financial information and surname were deemed to be non-shareable. This is a large enhancement, suggesting that the children learned more about protecting personal information.

**Table 31: Sample's Internet security awareness Level (Post-Assessment)**

<table>
<thead>
<tr>
<th>Question</th>
<th>Rank</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q8: Password Protection</td>
<td>1</td>
<td>3.00</td>
<td>.000</td>
</tr>
<tr>
<td>Q13: Insecure Website Symbol</td>
<td>2</td>
<td>2.87</td>
<td>.341</td>
</tr>
<tr>
<td>Q9: Warning Message Symbol</td>
<td>3</td>
<td>2.81</td>
<td>.543</td>
</tr>
<tr>
<td>Q11: Secure Website Symbol</td>
<td>3</td>
<td>2.81</td>
<td>.543</td>
</tr>
<tr>
<td>Q14: Insecure Website Action</td>
<td>3</td>
<td>2.81</td>
<td>.543</td>
</tr>
<tr>
<td>Q6: Anonymous Advertisements</td>
<td>4</td>
<td>2.75</td>
<td>.447</td>
</tr>
<tr>
<td>Q12: Secure Website Action</td>
<td>5</td>
<td>2.68</td>
<td>.704</td>
</tr>
<tr>
<td>Q10: Warning Message Action</td>
<td>6</td>
<td>2.56</td>
<td>.629</td>
</tr>
<tr>
<td>Q7: Anonymous Friend Request</td>
<td>7</td>
<td>2.50</td>
<td>.730</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.754</td>
<td>.497</td>
</tr>
</tbody>
</table>

N = 16 children (aged 8-12).
Not Applicable = 9 children (aged 3-7).

In the table shown above, we can see the big jump of concepts’ mean results compared to the previous “Pre-Assessment” results. The overall mean is 2.75 which is considered a quite high score. The concepts themselves show improvement in average results. As we can see, the password protection concept remained in the first rank as it indicate a very solid awareness level among the 16 children. The security symbol concepts advanced to the 2nd and 3rd ranks. This advancement suggests that the children became more aware of the symbols meanings. We can conclude that the “Post-Assessment” results indicate a pleasing increase in the subgroup’s Internet security awareness level.
6. DISCUSSION

When conducting this study and measuring the level of Internet Security among selected Saudi children and their parents, we found that most of the parents are well educated and use the Internet regularly. They also have sufficient awareness of protecting their children's safety online by activating the Parental Control feature and installing antivirus software on their children's devices. Also, they tend to check their children's online activities. The parents are doing a wonderful job to ensure the online safety of their children. Yet, they still do not pay much effort on educating the children themselves about Internet Safety. Therefore, it is necessary to focus on this aspect and work to increase the children's information about Internet threats; especially in areas such as dealing with anonymous friendship requests, providing personal information to unknown sources, and recognizing different security symbols that appear in the Internet Browsers.

On the other, when conducting the awareness evaluation and enhancement stages of this thesis, the children were found to have a solid background and experience of more recent applications and games; that in some cases, their knowledge in using the device might even exceed their parents'. The reason could be related to the children's heavy usage of games and applications. The children also appeared to already have questions and concerns about online safety. For example, a 9-year-old girl asked a question about the safety of using of the Chatting service found in one of the tablet games. Her question indicated that she already has an idea of what the service is, but she does not know if it is safe to use or not. The other question is from a 12-year-old girl who expresses her concern towards her frequent disabling of the protection software to be able to play a video game on the computer. Lastly, an 11-year-old boy, when asked what the viruses are, told that viruses are things that damage the computer, but he doesn't know how viruses get to the computer. These examples support that children have good background of the latest Internet technologies and applications; however, they seem to have a slight weakness in the perception of Internet threats and how to avoid falling for them.
The use of the proposed Awareness Enhancement solution significantly helped to increase the children's knowledge about online safety. Based on the Piaget's cognitive development theory, the program simplifies the basic Internet security tips and guidelines accommodate the perceptual differences between children's ages. The research methodology shows effectiveness in raising the selected children's Internet Security awareness; however, the study remains to have some flaws and shortcomings, which can be taken into account when working on future work. The flaws include a possibility of a bias in the study sample. The parents and children samples were randomly selected, which resulted an inequality in the demographic factors such as age and region. These differences might have a subtle effect on the overall awareness level. Another shortcoming is that the suggested solution was not tested for long-term efficiencies. In other words, it is hard to prove the effectiveness of the program after a long period of time since there the methodology design does not include a second post-assessment stage. Overall, the initial test of the suggested solution shows a potential development in the level of Internet security awareness level among the Saudi children.
7. RECOMMENDATIONS AND FUTURE WORK

7.1.1. Study Recommendations:

In the light of this study, we found that children have an excellent ability to learn and understand new concepts in Internet security. Thus, this is a list of recommendations that can be implemented to increase the children's awareness of the Internet threats:

1. Publishing new Internet security awareness materials which include simplified concepts targeting the children and supported by the Saudi technology Authorities such as Communications and Information Technology Commission (CITC), King Abdulaziz City for Science and Technology and the Saudi Computer Emergence Response Team.

2. Parents need to recognize the importance of discussing different Internet threats with their children and hear their questions; and not limit their security by protecting the device only.

3. Activating the role of schools and the communities in raising awareness among children through establishing a variety of workshops to educate children about common Internet threats.

7.1.2. Future Work:

This research is one of the researches that aim to enhance and raise the Internet security awareness among the children. It presents one of many possible solutions to spread the awareness. And given the significant contribution of the scientific researchers in solving problems and developing solutions, these are several suggestions for the future work in the same field:

1. Conduct a study with a controlled study sample that has specific equal numbers of people from different ages and regions.
2. A study that includes different Security concepts not mentioned in this study.

3. A study that focuses on the demographic factors to understand the nature of their relationship with the Internet security awareness level in Saudi Arabia.

4. Continuing to work on the proof-of-concept solution and simplify Internet security awareness guidelines so that children can comprehend them.
8. CONCLUSION

This study has explored the possibility of raising the Internet security awareness among a group of children from the age 3 to 12 years old through an interactive theory-based application. The main motivation of this thesis is to address the importance of educating the children in the field of Internet Security; especially after a number of studies confirmed the noticeable increase of the children's use of the Internet in the Middle East region, and in Saudi Arabia in particular. The necessity to educate the children and raise their Internet security awareness attributes to construct their ability to understand and avoid common Internet Security threats they may face during their use of the Internet.

The study approached the aforementioned goal in two steps: first, evaluating the current Internet security awareness level among the selected children and understand the nature of their Internet usage through a specifically-designed survey targeting the children and their parents. Second, based on the awareness evaluation results from the first step, an electronic Awareness Enhancement application is designed as a proof of concept. The design of this application is based on one of the most significant Educational Psychology's theories, which is Piaget's cognitive development. The theory helped in forming the Internet security awareness content to fit the children's different ages and mental capabilities.

After the design and development of the Awareness Enhancement application, a test was conducted to prove the application's efficiency in enhancing the children's awareness level. The user test was applied on a small sample of the children from the original study sample. A remarkable increase of the Internet security awareness level was witnessed as the children became more familiar with the most common Internet threats and how to deal with them. With this revelation, the main objective of this study, which is measuring and aiming to raise the level of the Internet security awareness among a group of Saudi children, is successfully achieved.
9. BIBLIOGRAPHY


Jistice Reference Service:


10. APPENDIX A:

MEASURING THE INTERNET SECURITY AWARENESS LEVEL AMONG SAUDI CHILDREN (SURVEY)

10.1. Parents Survey:

Greetings, this is a survey conducted to understand and measure the current security awareness level of Saudi Children when using the Internet. Kindly take your time to clearly answer the following questions. Any given information will be ONLY used for the mentioned purpose. Your participation is appreciated. Thank you.

A. Demographic Information:

1. Are you the: هل أنت
   o Mother الأم
   o Father الأب
   o Guardian الوصي الشرعي

2. Which age group do you belong to? ما هي الفئة العمرية التي تنتمي إليها؟
   o Under 20 تحت العشرين
   o 20-29
   o 30-39
   o 40-49
   o 50 and Over فوق الخمسين

3. Where do you currently live? أين تعيش الآن؟
   o Inside Saudi Arabia داخل المملكة العربية السعودية
   o Outside Saudi Arabia خارج المملكة العربية السعودية

4. Which region are you from? من أي مناطق السعودية أنت؟
   o Northern region المنطقة الشمالية
   o Southern region المنطقة الجنوبية
   o Eastern region المنطقة الشرقية
   o Western region المنطقة الغربية
   o Central region المنطقة الوسطى

5. What is the highest level of education you have received? ما هي أخر درجة علمية حصلت عليها؟
   o Less than high school degree المتوسطة أو أقل
   o High school degree or equivalent الثانوية العامة
6. Are you currently working? هل تعمل الآن؟
   - Yes نعم
   - No لا

7. If yes, what is your current occupation field? ماهو مجال عملك الحالي؟
   - Administration إدارة
   - Advertising, marketing and PR إعلان وتسويق
   - Animal and plant resources موارد نباتية وحيوانية
   - Arts, design and crafts الفنون والتصميم
   - Construction and property management البناء وإدارة العقارات
   - Counselling, social and guidance services الاستشارات والخدمات الاجتماعية
   - Education, teaching and lecturing التعليم
   - Engineering الهندسة
   - Finance and management consultancy الاستشارات الإدارية والمالية
   - Health care الصحة
   - Hospitality and events management الفندقية
   - Human resources and employment الموارد البشرية
   - IT, economics, statistics and management services الخدمات الإدارية والأحصائية
   - Information services الخدمات المعلوماتية
   - Insurance and pensions and actuarial work التأمين
   - Law enforcement and public protection الامن العام
   - Legal services الخدمات القانونية
   - Leisure, sport and tourism السياحة والرياضة
   - Logistics and transport خدمات النقل
   - Manufacturing and processing التصنيع والمعالجة
   - Natural resources and the environment الموارد الطبيعية والبيئية
   - Publishing, media and performing arts الإعلام والفنون المسرحية
   - Sales, retail and buying المبيعات
   - Scientific services الخدمات العلمية
   - Other أخرى
   - I don’t work أنا لا أعمل

8. Do you have children younger than 13 year-old? هل لديك أطفال تحت الثالثة عشر؟
   - Yes نعم
   - No لا

9. Which age group does your child belong to? من أي مرحلة عمرية ينتمي طفلك؟
   - 3-5 years old (Preschoolers) من 3 إلى 5 سنوات (الطفلة المبكرة)
   - 6-8 years old (Middle Childhood) من 6 إلى 8 سنوات (الطفلة المتوسطة)
   - 9-12 years old (Late Childhood) من 9 إلى 12 سنة (الطفلة المتاخرة)
10. Is your child a male or a female? هل طفلك ذكر أم أنثى؟
   - Male ذكر
   - Female أنثى

B. General information about Internet Usage:

11. Do you use the Internet? هل تستخدم الانترنت؟
   - Always دائماً
   - Sometimes أحيانًا
   - Rarely نادراً
   - Never أبداً

12. Does your child use Internet-enabled devices? هل يستخدم طفلك جهاز متصل بالانترنت؟
   - Yes نعم
   - No لا

13. Does your child use the Internet? هل يستخدم طفلك الإنترنت؟
   - Always دائماً
   - Sometimes أحيانًا
   - Rarely نادراً
   - Never أبداً

14. What type of device does your child use? ما هو نوع الجهاز الذي يستخدمه طفلك؟
   - Desktops/Laptops جهاز حاسوبي
   - IPad/IPOD/Android Tablets جهاز لوحي
   - Smart Phones هاتف ذكي

15. What is the main purpose for which your child uses the device? ما هو الغرض الرئيسي لاستخدام طفلك للجهاز؟
   - Entertainment (To play) للعب
   - Education (To do Homework) لاداء الواجبات المنزلية

16. Do you consider the device specifications before you buy it for your child? هل تقوم بدراسة مواصفات الجهاز قبل شرائه لطفلك؟
   - Yes نعم
   - No لا

17. Do you depend on the specifications or the price when buying a device for your child? هل يعتمد قرارك لشراء جهاز إلكتروني لطفلك على مواصفات الجهاز أو سعر الجهاز؟
   - Device’s specifications مواصفات الجهاز الإلكتروني
   - Device’s Price سعر الجهاز الإلكتروني
18. On average, how many hours a day does your child use the Internet?
   - Up to 1 hour a day.
   - 1 to 3 hours a day.
   - 4 to 7 hours a day.
   - More than 7 hours a day.

19. Do you teach your child any kind of device management?
   - Yes, a minimum knowledge (such as adjusting device’s volume).
   - Yes, a limited knowledge (such as visiting websites, opening applications and powering the device on or off).
   - Yes, my child knows how to set up a password or connect to new networks.
   - No, my child depends on me to manage the device.

20. Do you check on your child's activates on the device?
   - Yes, Always.
   - Yes, Sometimes.
   - Yes, Rarely.
   - No, Never.

21. If the answer is yes, do you do that while or after he/she uses the device?
   - While using the device.
   - After using the device.

C. Information about Security Practices and Awareness:

22. Have you ever heard of the Computer Emergency Response Team, which is a part of the Saudi Communication and Information Technology Commission?
   - Yes.
   - No.

23. Have you ever read any awareness publications from the Computer Emergency Response Team?
   - Yes.
   - No.

24. Have you ever read any Information Security Awareness publications from any other sources?
   - Yes.
   - No.
25. Is there any Internet Security software installed on your child's device?
هل تستخدم برامج الحماية والأمان على جهاز اطفالك؟
○ Yes نعم
○ No لا

26. If the answer is yes, do you regularly update the software?
اذا كان الجواب نعم .. هل تقوم بالتحديث الدوري للمطلوب لهذه البرامج؟
○ Yes, on a regular basis. نعم، على نحو مستمر
○ Yes, the auto-update is enabled. نعم، استخدم التحديث التلقائي
○ No, I don't remember the last time I updated it. لا، لا اتذكر

27. Do you verify the credibility and safety of the sites and applications your child visits and uses?
هل تتحقق من مصداقية وامان المواقع التي يزورها طفلك؟
○ Yes نعم
○ No لا

28. Do you give your child an overview of the Internet Security Threats? (Such as viruses, spam, phishing)
هل تقوم بتعليم الأطفال نبذة عامة عن مشاكل الانترنت ؟(مثل مخاطر الفيروسات والتجسس والتصيد المعلوماتي)
○ Yes نعم
○ No لا

29. Do you use Parental Control settings on your child's device?
هل تقوم بتفعيل اعدادات الرقابة الابوية على جهاز طفلك؟
○ Yes نعم
○ No لا
○ I do not know

30. Does your child have the privilege to download applications or games on the device?
هل تعطي طفلك الصلاحية لتنزيل التطبيقات أو الالعاب على الجهاز؟
○ Yes نعم
○ No لا

31. Does your child know the password used to download programs and games?
هل يعرف طفلك كلمة المرور المستخدمة لتنزيل التطبيقات على الجهاز؟
○ Yes نعم
○ No لا

32. Has your child ever encountered any problems related to the information security when using the Internet?
هل سبق وواجه طفلك مشكلة من المشاكل المتعلقة بأمن المعلومات؟
○ Yes. نعم
○ No. لا
33. What type of security problems has your child encountered? (You can check more than one choice)
   □ Spyware
   □ Viruses
   □ Worm
   □ Spam
   □ Trojan horse
   □ Adware
   □ Phishing
   □ Intrusions
   □ Masquerade / impersonation attack (e.g. stolen passwords or someone sending emails in your name)
   □ Cyberbullying

34. Have these problems once and for all been solved?  
   □ Yes
   □ No

35. Who was the individual who solved these problems?
   □ Parents (or other adults).
   □ The Child.

36. What is the top Internet Security Threat from which you want to protect your child?
   □ Game Addiction and using the device for a long time.
   □ Cyberbullying (such as exposure to blackmail, intimidation and verbal abuse)
   □ Personal and Financial information theft.
   □ Access to inappropriate content such as gambling and pornography.
   □ Exposure to malware and penetration attacks.
   □ Communicating with strangers

37. In your opinion, who do you think is primarily responsible for securing your child's device?
   □ I am the one responsible for securing it by using security software.
   □ The ISP (Internet Service Provider).
   □ The Operating System that I’m using (e.g. Windows, MacOS, Linux...).
38. On a scale of 1-5 (1 being "very poor" and 5 being "excellent"), what is your assessment of your child's awareness of the Internet security?

- 1
- 2
- 3
- 4
- 5

39. Finally, would you be interested in introducing Internet security awareness solutions to your child?

- Yes
- No

The End

References:

10.2. Children Survey:
We are doing a research study about how much children are aware of Internet security threats. A research study is a way to learn more about people. If you decide that you want to be part of this study, you will be asked to answer a multiple-choice questions on a website. The questions will take 10-15 minutes of your time. You do not need to worry because there is no risk or harm in this study. Not everyone who takes part in this study will benefit. A benefit means that something good happens to you. We think these benefits might be for you to know more about security threats and be careful when you use the Internet. When we are finished with this study we will write a report about what was learned. This report will not include your name or that you were in the study. You do not have to be in this study if you do not want to be. If you decide to stop after we begin, that’s okay too. Your parents know about the study too. If you decide you want to be in this study, please choose “I agree”.

- Yes, I agree to participate
### Section 1: General Information:

1. **You are a:**
   - ![Girl](image)
   - ![Boy](image)

2. **How old are you?**
   - ![3](image)
   - ![4](image)
   - ![5](image)
   - ![6](image)
   - ![7](image)
   - ![8](image)
   - ![9](image)
   - ![10](image)
   - ![11](image)
   - ![12](image)

3. **You have a:**
   - ![Laptop](image)
   - ![Tablet](image)
   - ![Smart Phone](image)
4. Which online websites do you visit? (You can choose more than one answer)

☐ Google play
☐ App store
☐ YouTube

☐ Instagram
☐ Facebook
☐ YouTube kids

☐ Baraem.net
☐ MBC3 website
☐ Friv Game

Section 2: Using the Internet:

5. Which information do you think is okay to give to the websites on the Internet?
☐ Full name
☐ Surname
☐ Nickname
☐ Home address
☐ School address
☐ Credit card number
6. When a commercial of a new game appears on the screen while you are playing, what do you do?

- Click Enter
- Close Window
- Ask Parents

7. When you get a new message from a stranger who wants you to add them as a friend in the game, what do you do?

- Click Accept
- Click Decline
- Ask Parents
8. When your friend asks you to tell him the secret password to open your device, what do you do?

- Tell your friend the password
- Do not tell your friend

9. What do you think about this symbol? Is it something Good? Bad?

- Good
- Bad
- I don’t know
10. What do you think is the right thing to do when the first symbol appears?

- Click Okay
- Close Window
- Ask Parents

11. What do you think about this symbol? Is it something Good? Bad?
   Second Symbol:

- Good
- Bad
- I don’t know

12. What do you think is the right thing to do when the second symbol appears?

- Do Nothing
- Close Window
- Ask Parents

13. What do you think about this symbol? Is it something Good? Bad?
   Third Symbol:
14. What do you think is the right thing to do when the third symbol appears?

- Do Nothing
- Close Window
- Ask Parents

Thank you for participating in this survey. You did a great job

Survey References:

- Untrusted website icon. Retrieved from: http://wiki.threadfix.googlecode.com/git-history/8e5e3089e1247eda0b13669058a9800cf7171479/GettingStarted.wiki
- Other icons. Licensed and retrieved from: http://www.vectorstock.com/
11. APPENDIX B:

AWARENESS ENHANCEMENT SOLUTION’S CODE AND INTERFACES:

Welcome Screen:

Hello Champions,
In this series, you will be able to play games and learn new things about how to stay safe when you use the Internet.

Before we start, which age group do you belong to?

3-7 Years Old  8-12 Years Old

Public Class f1main
  Private Sub Button1_Click(sender As Object, e As EventArgs) Handles Button1.Click
    f2little.Show()  
  End Sub

  Private Sub Button2_Click(sender As Object, e As EventArgs) Handles Button2.Click
    f3older.Show()  
  End Sub

  Private Sub Button4_Click(sender As Object, e As EventArgs) Handles Button4.Click
    f4more.Show()  
  End Sub

  Private Sub ExitButton_Click(sender As Object, e As EventArgs) Handles ExitButton.Click
    ExitButton.Click
    Close()  
  End Sub
End Class
Preschoolers’ Awareness Session:

What do you want to do today?

Learn New Terms

Learn about Personal Information

Public Class f2little
    Private Sub f2little_Load(sender As Object, e As EventArgs) Handles MyBase.Load
        End Sub
    
    Private Sub TabControl1_SelectedIndexChanged(sender As Object, e As EventArgs) Handles TabControl1.SelectedIndexChanged
        End Sub
    
    '========================
    'TAB TRANSITIONS (NEXT, PREVIOUS,
    'EXIT)========================
    
    Private Sub Button21_Click(sender As Object, e As EventArgs) Handles Button21.Click
        TabControl1.SelectTab(1)
        End Sub
    
    Private Sub Button24_Click(sender As Object, e As EventArgs) Handles Button24.Click
        TabControl1.SelectTab(0)
        End Sub
    
    Private Sub Button1_Click(sender As Object, e As EventArgs) Handles Button1.Click
        TabControl1.SelectTab(2)
        End Sub
    
    Private Sub Button2_Click(sender As Object, e As EventArgs) Handles Button2.Click
        TabControl1.SelectTab(1)
        End Sub
    
    Private Sub Button3_Click(sender As Object, e As EventArgs) Handles Button3.Click
TabControl1.SelectTab(3)
End Sub

Private Sub Button4_Click(sender As Object, e As EventArgs) Handles Button4.Click
TabControl1.SelectTab(2)
End Sub

Private Sub Button5_Click(sender As Object, e As EventArgs) Handles Button5.Click
TabControl1.SelectTab(4)
End Sub

Private Sub Button6_Click(sender As Object, e As EventArgs) Handles Button6.Click
TabControl1.SelectTab(3)
End Sub

Private Sub Button7_Click(sender As Object, e As EventArgs) Handles Button7.Click
TabControl1.SelectTab(5)
End Sub

Private Sub Button9_Click(sender As Object, e As EventArgs) Handles Button9.Click
TabControl1.SelectTab(4)
End Sub

Private Sub ExitButton_Click(sender As Object, e As EventArgs) Handles ExitButton.Click
ExitButton.Click
Close()
End Sub

'========================================START

Private Sub Button22_Click(sender As Object, e As EventArgs) Handles Button22.Click
TabControl1.SelectTab(1)
End Sub

Private Sub Button23_Click(sender As Object, e As EventArgs) Handles Button23.Click
TabControl1.SelectTab(4)
End Sub

'=====================================NEW SECURITY
WORDS=================================

Private Sub PictureBox2_Click(sender As Object, e As EventArgs) Handles PictureBox2.Click
PictureBox2.BackgroundImage = My.Resources.virus
PictureBox2.BackgroundImageLayout = ImageLayout.Center
Label2.Visible = True
Dim virus As New Media.SoundPlayer
virus.Stream = My.Resources.virus5
virus.Play()
End Sub

Private Sub PictureBox3_Click(sender As Object, e As EventArgs) Handles PictureBox3.Click
PictureBox3.BackgroundImage = My.Resources.hacker
PictureBox3.BackgroundImageLayout = ImageLayout.Center
Label3.Visible = True
Dim hacker As New Media.SoundPlayer
hacker.Stream = My.Resources.hacker3
hacker.Play()

End Sub

Private Sub PictureBox4_Click(sender As Object, e As EventArgs) Handles PictureBox4.Click
    PictureBox4.BackgroundImage = My.Resources.password
    PictureBox4.BackgroundImageLayout = ImageLayout.Stretch
    Label4.Visible = True
    Dim pass As New Media.SoundPlayer
    pass.Stream = My.Resources.password3
    pass.Play()
End Sub

Private Sub PictureBox5_Click(sender As Object, e As EventArgs) Handles PictureBox5.Click
    PictureBox5.BackgroundImage = My.Resources.shield2
    PictureBox5.BackgroundImageLayout = ImageLayout.Center
    Label5.Visible = True
    Dim anti As New Media.SoundPlayer
    anti.Stream = My.Resources.antivirus
    anti.Play()
End Sub

Private Sub PictureBox6_Click(sender As Object, e As EventArgs) Handles PictureBox6.Click
    PictureBox6.BackgroundImage = Image.FromFile("C:\")
    PictureBox6.BackgroundImage = My.Resources.lock
    PictureBox6.BackgroundImageLayout = ImageLayout.Center
    Label6.Visible = True
    Dim securitylock As New Media.SoundPlayer
    securitylock.Stream = My.Resources.securitylock
    securitylock.Play()
End Sub

'==============================NEW WORDS TAB

Private Sub Button8_Click(sender As Object, e As EventArgs) Handles Button8.Click
    PictureBox7.Image = My.Resources.evirus
End Sub

Private Sub Button10_Click(sender As Object, e As EventArgs) Handles Button10.Click
    PictureBox7.Image = My.Resources.ehacker
End Sub

Private Sub Button11_Click(sender As Object, e As EventArgs) Handles Button11.Click
    PictureBox7.Image = My.Resources.Passcode
End Sub

Private Sub Button12_Click(sender As Object, e As EventArgs) Handles Button12.Click
    PictureBox7.Image = My.Resources.enlockGIF
End Sub

Private Sub Button13_Click(sender As Object, e As EventArgs) Handles Button13.Click
    PictureBox7.Image = My.Resources.ENanti
End Sub

'========================================================================NEW WORDS TAB
3=====================================================================

Private Sub PictureBox_Click(sender As Object, e As EventArgs) Handles
  PictureBox12.Click, PictureBox11.Click, PictureBox10.Click
  PictureBox8.BackgroundImage = My.Resources.ewrong
  PictureBox8.BackgroundImageLayout = ImageLayout.Center
  Dim wrong As New Media.SoundPlayer
  wrong.Stream = My.Resources.awrong
  wrong.Play()
End Sub

Private Sub PictureBox9_Click(sender As Object, e As EventArgs) Handles
  PictureBox8.BackgroundImage = My.Resources.ecorrect
  PictureBox8.BackgroundImageLayout = ImageLayout.Center
  Dim correct As New Media.SoundPlayer
  correct.Stream = My.Resources.acorrect
  correct.Play()
End Sub

'=================================================================================================

Private Sub Button14_Click(sender As Object, e As EventArgs) Handles
  Button14.Click
  PictureBox13.BackgroundImage = My.Resources.names
  PictureBox13.BackgroundImageLayout = ImageLayout.Center
End Sub

Private Sub Button15_Click(sender As Object, e As EventArgs) Handles
  Button15.Click
  PictureBox13.BackgroundImage = My.Resources.age
  PictureBox13.BackgroundImageLayout = ImageLayout.Center
End Sub

Private Sub Button16_Click(sender As Object, e As EventArgs) Handles
  Button16.Click
  PictureBox13.BackgroundImage = My.Resources.ehomeaddress
  PictureBox13.BackgroundImageLayout = ImageLayout.Center
End Sub

Private Sub Button17_Click(sender As Object, e As EventArgs) Handles
  Button17.Click
  PictureBox13.BackgroundImage = My.Resources.family
  PictureBox13.BackgroundImageLayout = ImageLayout.Center
End Sub

Private Sub Button18_Click(sender As Object, e As EventArgs) Handles
  Button18.Click
  PictureBox13.BackgroundImage = My.Resources.tele
  PictureBox13.BackgroundImageLayout = ImageLayout.Zoom
End Sub

Private Sub Button19_Click(sender As Object, e As EventArgs) Handles
  Button19.Click
  PictureBox13.BackgroundImage = My.Resources.eschool
  PictureBox13.BackgroundImageLayout = ImageLayout.Center
End Sub
Private Sub Button20_Click(sender As Object, e As EventArgs) Handles Button20.Click
    PictureBox13.BackgroundImage = My.Resources.emoney
    PictureBox13.BackgroundImageLayout = ImageLayout.Zoom
End Sub

Private Sub PictureBox7_Click(sender As Object, e As EventArgs) Handles PictureBox7.Click
End Sub

Private Sub TabPage6_Click(sender As Object, e As EventArgs) Handles TabPage6.Click
End Sub

Private Sub PictureBox8_Click(sender As Object, e As EventArgs) Handles PictureBox8.Click
End Sub
End Class

Elementary School awareness sessions:

![Image of an educational software interface with options to learn about Security Symbols and Checking Sources.]

Public Class f3older

    '=============TABS TRANSTIONS (NEXT, PREVIOUS, EXIT)=================================

    Private Sub Button11_Click(sender As Object, e As EventArgs) Handles Button11.Click
End Sub

92 | Page
TabControl1.SelectTab(1)
End Sub

Private Sub Button18_Click(sender As Object, e As EventArgs) Handles Button18.Click
    TabControl1.SelectTab(0)
End Sub

Private Sub Button3_Click(sender As Object, e As EventArgs) Handles Button3.Click
    TabControl1.SelectTab(2)
End Sub

Private Sub Button12_Click(sender As Object, e As EventArgs) Handles Button12.Click
    TabControl1.SelectTab(1)
End Sub

Private Sub Button1_Click(sender As Object, e As EventArgs) Handles Button1.Click
    TabControl1.SelectTab(3)
End Sub

Private Sub Button4_Click(sender As Object, e As EventArgs) Handles Button4.Click
    TabControl1.SelectTab(2)
End Sub

Private Sub Button5_Click(sender As Object, e As EventArgs) Handles Button5.Click
    TabControl1.SelectTab(4)
End Sub

Private Sub Button6_Click(sender As Object, e As EventArgs) Handles Button6.Click
    TabControl1.SelectTab(3)
End Sub

Private Sub Button7_Click(sender As Object, e As EventArgs) Handles Button7.Click
    TabControl1.SelectTab(5)
End Sub

Private Sub Button22_Click(sender As Object, e As EventArgs) Handles Button22.Click
    TabControl1.SelectTab(4)
End Sub

Private Sub Button21_Click(sender As Object, e As EventArgs) Handles Button21.Click
    TabControl1.SelectTab(6)
End Sub

Private Sub Button29_Click(sender As Object, e As EventArgs) Handles Button29.Click
    TabControl1.SelectTab(5)
End Sub

Private Sub Button28_Click(sender As Object, e As EventArgs) Handles Button28.Click
    TabControl1.SelectTab(7)
End Sub

Private Sub Button9_Click(sender As Object, e As EventArgs) Handles Button9.Click
    TabControl1.SelectTab(6)
End Sub
Private Sub ExitButton_Click(sender As Object, e As EventArgs) Handles ExitButton.Click
    Close()
End Sub

'===================================================================
PAGE===================================================================
Private Sub Button10_Click(sender As Object, e As EventArgs) Handles Button10.Click
    TabControl1.SelectTab(1)
End Sub

Private Sub Button8_Click(sender As Object, e As EventArgs) Handles Button8.Click
    TabControl1.SelectTab(3)
End Sub

'====================================================================
SECURITY ICONS
====================================================================
Private Sub Button2_Click(sender As Object, e As EventArgs) Handles Button2.Click
    PictureBox26.BackgroundImage = My.Resources.arrow
    PictureBox26.Visible = True
    Label6.Text = "The Green color means safety. It means that the website is" & vbCrLf & "secure. Also, locked padlocks are used to show that the website" & vbCrLf & "does not have any problems. These symbols make us sure" & vbCrLf & "that we are away from Dangers. Be sure to " & vbCrLf & "find them when using the Internet.""
    Label6.Location = New Point(124, 113)
    PictureBox14.BackgroundImage = My.Resources.locked
    PictureBox4.BackgroundImageLayout = ImageLayout.Center
    PictureBox15.BackgroundImage = My/Resources/secured
    PictureBox16.BackgroundImage = My/Resources/lock
End Sub

Private Sub Button13_Click(sender As Object, e As EventArgs) Handles Button13.Click
    PictureBox26.BackgroundImage = My/Resources/arrow
    PictureBox26.Visible = True
    Label6.Text = "The red color means security problems. It means that" & vbCrLf & "the website is not safe. Also, the unlocked padlocks are" & vbCrLf & "used to show that the website may be harmful to us and" & vbCrLf & "our computers. Make sure to close and stay away from" & vbCrLf & "websites with these symbols."
    Label6.Location = New Point(154, 113)
    PictureBox14.BackgroundImage = My/Resources/unlocked
    PictureBox15.BackgroundImage = My/Resources/insecure
    PictureBox16.BackgroundImage = My/Resources/unlocked
End Sub

'====================================================================
MATCHING GAME
====================================================================
'/////////Matching Game Setup///////////
Private random As New Random
Const RevealCycleWaitTime As Integer = 1
'Add 6 different pictures twice in an ImageList:
Private imgs = New List(Of Image) From {My/Resources.locked, My/Resources.locked, My/Resources.unlocked, My/Resources.unlocked,
'Add 6 different Image Tags twice in a String List:
Private ImageNames = New List(Of String) From {"locked", "locked", "unlocked", "unlocked", "hacker1", "hacker1", "shield1", "shield1", "virus1", "virus1", "malmail1", "malmail1"}

'Creating a class to randomly assign 12 pictures to 12 PictureBoxes:
Private Sub AssignImagesToSquares()
    For Each control In Panel1.Controls
        Dim imgbox = TryCast(control, PictureBox)
        If imgbox IsNot Nothing Then
            If imgbox.BackColor <> Color.Beige Then
                Dim randomNumber = random.Next(imgs.Count)
                imgbox.BackgroundImage = imgs(randomNumber)
                imgbox.Tag = ImageNames(randomNumber)
                imgbox.BackgroundImageLayout = ImageLayout.Zoom
                ImageNames.removeAt(randomNumber)
                imgs.RemoveAt(randomNumber)
            End If
        End If
    Next
End Sub

'Activating the class to assign the pictures at form start:
Private Sub f3olderr_Load(sender As Object, e As EventArgs) Handles MyBase.Load
    AssignImagesToSquares()
End Sub

'Initiate the creation of table at form start:
Private Sub Panel1_Paint(sender As Object, e As PaintEventArgs)
End Sub

'///////////Start the real work///////////
'Player's First Choice:
Dim FirstPicture As PictureBox = Nothing
'Player's Second Choice:
Dim SecondPicture As PictureBox = Nothing

'This class receives all click events on covering objects
Private Sub PictureBox9.Click(sender As Object, e As EventArgs) Handles PictureBox9.Click, PictureBox7.Click, PictureBox5.Click, PictureBox4.Click, PictureBox32.Click, PictureBox31.Click, PictureBox3.Click, PictureBox29.Click, PictureBox2.Click, PictureBox12.Click, PictureBox11.Click, PictureBox1.Click
    'ignore clicks while the timer is running
    If Timer1.Enabled Then
        Beep()
        Exit Sub
    End If

    'hide the object that was clicked on
    Dim width As Integer = sender.Width
    While sender.Width > 0
        sender.Width = sender.Width - 1
        Threading.Thread.Sleep(RevealCycleWaitTime)
        Application.DoEvents()
    End While
sender.Visible = False

' reset the width to normal now that the object is invisible
sender.Width = width

' if this is the first of a pair of pictures, just retain it and exit
If FirstPicture Is Nothing Then
    FirstPicture = sender
    Exit Sub
End If

' the second of a pair of pictures has been revealed
SecondPicture = sender
Timer1.Start()
End Sub

Private Sub Timer1_Tick(sender As Object, e As EventArgs) Handles Timer1.Tick
    Timer1.Enabled = False

    ' determine whether the two visible items match or not
    If FirstPicture IsNot Nothing And SecondPicture IsNot Nothing Then
        Dim pb1 As PictureBox = Nothing
        Dim pb2 As PictureBox = Nothing

        ' identify the pictures that correspond to the two revealed boxes
        For Each control In Panel1.Controls
            If TypeOf (control) Is PictureBox Then
                Dim pb As PictureBox = control
                If pb.BackColor.Name = "Transparent" Then
                    If pb.Location = FirstPicture.Location Then pb1 = pb
                    If pb.Location = SecondPicture.Location Then pb2 = pb
                End If
            End If
        Next

        ' Winner()
        ' compare the two pictures
        If pb1.Tag = pb2.Tag Then
            Dim correct As New Media.SoundPlayer
            correct.Stream = My.Resources.acorrect
            correct.Play()
            pb1.Visible = False
            pb2.Visible = False
            FirstPicture = Nothing
            SecondPicture = Nothing
            Exit Sub
        End If

        ' re-hide the pictures
        Dim width As Integer = FirstPicture.Width
        FirstPicture.Width = 0
        SecondPicture.Width = 0
        FirstPicture.Visible = True
        SecondPicture.Visible = True

        While FirstPicture.Width < width
            FirstPicture.Width = FirstPicture.Width + 1
            SecondPicture.Width = SecondPicture.Width + 1
            Threading.Thread.Sleep(RevealCycleWaitTime)
            Application.DoEvents()
        End While
    End If
End Sub
While FirstPicture = Nothing
SecondPicture = Nothing
End If
End Sub

'Check for winning
'Private Sub Winner()
'For Each Control In Panel1.Controls
'Dim mgbox = TryCast(Control, PictureBox)
'If mgbox IsNot Nothing AndAlso
'mgbox.Visible = True Then Exit Sub
'Next
'MessageBox.Show("Congats!!")
'End Sub

'================================GAME 2: SECURE AND INSECURE
CONTENT==================================

'PICTURE #1: SPAM MAIL.
'SECURE OPTION:
Private Sub Button15_Click(sender As Object, e As EventArgs) Handles Button15.Click
PictureBox13.BackgroundImage = My.Resources.eWrong
PictureBox13.BackgroundImageLayout = ImageLayout.Center
Dim wrong As New Media.SoundPlayer
wrong.Stream = My.Resources.aWrong
wrong.Play()
End Sub

'INSECURE OPTION:
Private Sub Button14_Click(sender As Object, e As EventArgs) Handles Button14.Click
PictureBox13.BackgroundImage = My.Resources.eCorrect
PictureBox13.BackgroundImageLayout = ImageLayout.Center
Dim correct As New Media.SoundPlayer
correct.Stream = My.Resources.aCorrect
correct.Play()
End Sub

'PICTURE #2: TRUSTED CONTACT (SCHOOL).
'SECURE OPTION:
Private Sub Button17_Click(sender As Object, e As EventArgs) Handles Button17.Click
PictureBox19.BackgroundImage = My.Resources.eCorrect
PictureBox19.BackgroundImageLayout = ImageLayout.Center
Dim correct As New Media.SoundPlayer
correct.Stream = My.Resources.aCorrect
correct.Play()
End Sub

'INSECURE OPTION:
Private Sub Button16_Click(sender As Object, e As EventArgs) Handles Button16.Click
PictureBox19.BackgroundImage = My.Resources.eWrong
PictureBox19.BackgroundImageLayout = ImageLayout.Center
Dim wrong As New Media.SoundPlayer
wrong.Stream = My.Resources.aWrong
wrong.Play()
End Sub

'PICTURE #3: ADWARE.
'SECURE OPTION:
Private Sub Button24_Click(sender As Object, e As EventArgs) Handles Button24.Click
    PictureBox22.BackgroundImage = My.Resources.ewrong
    PictureBox22.BackgroundImageLayout = ImageLayout.Center
    Dim wrong As New Media.SoundPlayer
    wrong.Stream = My.Resources.awrong
    wrong.Play()
End Sub

'INSECURE OPTION:
Private Sub Button23_Click(sender As Object, e As EventArgs) Handles Button23.Click
    PictureBox22.BackgroundImage = My.Resources.ecorrect
    PictureBox22.BackgroundImageLayout = ImageLayout.Center
    Dim correct As New Media.SoundPlayer
    correct.Stream = My.Resources.acorrect
    correct.Play()
End Sub

Private Sub PictureBox13_Click(sender As Object, e As EventArgs) Handles PictureBox13.Click
End Sub
End Class

Learn More Screen:

Here, you can get more information on the Internet
Click on the link and enjoy watching :)

Sesame Tales and Internet Security
https://youtu.be/LmbVCbjag_U

8 Tips to protect yourself from Internet Dangers
https://youtu.be/0lqofUcQNo8

Public Class f4more
    Private Sub Button3_Click(sender As Object, e As EventArgs) Handles Button3.Click
        Close()
    End Sub
Awareness Enhancement Solution References:

- A child with tablet icon. Retrieved from:
  http://images.amazon.com/images/G/01/toys/detail-page/c26-B008DS1M58-4-1.jpg
- Green and Red Buttons. Retrieved from:
  https://mikeclayton.files.wordpress.com/2013/11/redbuttongreenbutton.png
- Birthday Numbers icons. Retrieved from:
  http://tubes.toutimages.com/festivite/anniversaire/index.htm