Why Strong Information Security Awareness Is Necessary

Mrs. V.ALEKHYA , Mr. KONCHADA BHANUCHAND , Mrs. K.JANSI
Assistant.Professor[1,2,3]
IT DEPARTMENT
Swarnandhara College of Engineering & Technology,Narsapuram-534275.

Abstract— An information security program's security awareness component is often disregarded. Normal users are the weakest link in any company because, despite businesses' efforts to improve the usage of sophisticated security technologies and regularly educate security specialists, relatively little is done to raise security awareness among these users. Consequently, modern-day organized cybercriminals are devoting a great deal of resources to studying and perfecting sophisticated hacking techniques that they may use to defraud unsuspecting individuals of their money and personal data. Cybercriminals find the Middle East an appealing target due to the region's high internet penetration growth rate and consumers' lack of security understanding.Using findings from many security awareness surveys administered to UAE residents in 2010 as evidence, this article will argue that educational institutions, public agencies, and private companies throughout the region need to implement security awareness programs. Among them is a thorough wireless security audit that uncovered hundreds of access points throughout Sharjah and Dubai, the vast majority of which are either unsecured or use inadequate forms of protection. The likelihood that average internet users would be the targets of phishing attempts designed to steal sensitive financial and personal data is the subject of an additional research. Additionally, a research is given on the user's understanding of privacy problems while utilizing RFID technology. We conclude by outlining a number of critical components for an effective information security awareness campaign.

***Index Terms*—Information Security, Security Awareness, Security Audits, Phishing Attacks, Wireless Security, RFID Security, UAE.**

I. Introduction

The number of people in the Middle East who use the internet has been steadily rising over the last few years. World Internet Usage Statistics News [1] reports that while the Middle East only accounts for 3.2% of the world's internet users, its internet usage has increased by 1825% over the last decade, outpacing the global average of 445%. According to the research, as of June 30, 2010, the internet penetration rates in Qatar (51.8%), Bahrain (88%), and the United Arab Emirates (74.9%) were the highest in the Middle East. As a result of this expansion, several established industries, including healthcare, education, transportation, and government, have begun to do more of their work online, and hundreds of internet firms have set up shop in the Middle East.Another study by the Arab Advisors Group [2] showed that the UAE had the highest e-commerce penetration rate in 2008. Specifically, 21.5% of UAE, 14.3% of Saudi Arabia, 10.7% of Kuwait, and 1.6% of Lebanon residents engaged in web commerce and in most cases such engagements required the use of credit cards. A study conducted by Lafferty Group [3] showed that the number of credit cards in the Middle East and North Africa region jumped by 24% in 2006 to 6.23 million and is expected to see a 51% increase in the number of credit card users in 2008 as compared to 2006.

There has been a meteoric rise in the volume of electronic data, smart mobile devices, and online transactions due to the proliferation of both the internet and credit cards. On the other hand, cybercrime in the Middle East has been on the rise in recent years. Online fraud, bank hacking attempts, website shutdowns, and defacements are periodically reported in local media. One example is the defacement of the website of the respected UAE-based Al-Khaleej Newspaper in May 2008 [4]. Also same year, in October 2008, the prominent Middle East news channel Arabiya.net had its website hacked [5]. The hackers in both cases said they were motivated by political motives when they launched the assaults. The Bahraini telecom business was the victim of phishing attempts in May 2008 [6]. Later in the same year, phishing attempts also hit Kuwait's National Bank [7]. According to ITP's reporting, many UAE bank websites were subjected to phishing attempts in January 2010 [8]. Multiple victims of online fraud in the United Arab Emirates lost their life savings in April 2010 [9]. The United Arab Emirates Ministry of Education was hit by a computer virus in April 2010 [10]. The Riyad Bank website, which is based in Saudi Arabia, was breached in June 2010 [11]. Hackers also disrupted the June 2010 broadcast of the World Cup by Al Jazeera Sport [12].

Some of the main reasons why there has been a rise in incidents involving information technology (IT) security around the world include: (1) more electronic data; (2) more mobile devices; (3) more organized cybercrime groups; (4) more intelligent external and internal IT security threats; (5) more difficulty in tracing the attackers; (6) fewer cybercrime laws; and (7) less IT security knowledge among internet users. Additionally, there are a variety of reasons why hackers launch assaults. Some examples are: (1)

disseminating a political message, (2) making money (i.e., stealing), (3) stealing data, (4) creating chaos and harm, and (5) being famous and satisfied with one's life.

Governments have responded to the alarming rise in IT security events by passing federal legislation to combat IT crimes, e-crime, and cybercrime. Such laws are already in place and being enforced by a number of nations in Asia, Europe, and North America. Such legislation has previously been passed by a handful of Middle Eastern nations [13]. When it came to cybercrime, the United Arab Emirates was an early adopter of a federal legislation in January 2006. Most instances of cybercrime were addressed under the 26 provisions that made up the statute. Fines of up to one hundred thousand UAE Dirhamsand/or imprisonment for up to fifteen years were possible consequences. In October 2006, Saudi Arabia was the second country to pass a federal legislation criminalizing cybercrime. Even though these laws did a good job of lowering the number of IT security incidents, there are still a lot of them in the Middle East. This is due to four main reasons: (1) not enough cybercrime laws, (2) not enough enforcement, (3) not enough awareness of the laws among locals, and (4) not enough computer incident forensics teams.

Hackers are trying to breach enterprises by focusing on the most vulnerable point: the computer user without proper education [14]. This is happening even though firms are increasingly using sophisticated security solutions. One of the greatest risks to an organization's information technology security is human error, as stated in [15]. Using findings from many security awareness surveys administered to UAE residents in 2010 as evidence, this article will argue that educational institutions, public agencies, and private companies throughout the region need to implement security awareness programs. Section 2 presents the results of the first research, which looked at the likelihood that regular users would be victims of phishing attempts designed to obtain sensitive financial and personal data. Here, we provide the findings of a covert phishing audit that was authorized by an academic institution. As the first of its type in the UAE, the research has been crucial in raising people's level of security awareness. Section 3 presents the second research, which is a thorough wireless security assessment that found thousands of access points throughout Sharjah and Dubai, the majority of which were exposed or used inadequate forms of protection. We go over the UAE's RFID security awareness level in Section 4. We outline the critical elements needed to create an effective security awareness campaign in the Middle East in Section 5. Lastly, we wrap up by illustrating how governments in the Middle East have recently worked to raise security awareness among their populations.

2. Attacks on UAE Users by Phishers

"Phishing" refers to a kind of online fraud that targets sensitive information including login credentials, credit card details, and social security numbers. An imposter website mimicking the appearance of a real company's site (down to the last detail) is where the scam begins.

website address. Financial institutions, such as banks, are often the entities in question. Afterwards, thousands of people who use the internet will get an email asking them to update their records by inputting their personal data, including security access credentials, on a phony website that looks just like the real one. It seems to be a real page. To trick consumers into thinking the email is legitimate, the FROM address is the same as the real organization's, such as the HR or IT director. Hackers may easily trick email systems into thinking the FROM address is from their own machine by forging that address. In order to keep the user's identity hidden, the fraudulent website sends their personal information to the hacker once they input it. Then, the user is sent to the real website.

The Anti-Phishing Working Group said that in 2009, there were more than 42,000 unique pages per month of false phishing websites, up from 23,000 pages per month in 2008. Every minute, there is almost a new phishing website. An indication of how successful the phishing hacking approach is is the large number of phishing websites.

Hackers in the Middle East are using sophisticated techniques, such as phishing schemes, to target people in the United Arab Emirates [17]. In response to these types of frauds, financial institutions in the UAE have increased the importance of information technology security measures in recent years. A number of phishing attempts were identified in 2009 targeting the United Arab Emirates [18], despite the fact that the country's Cybercrime Law, Article #10, punishes individuals with fines and jail terms for engaging in online money theft or transfers. An assault that was noticed featured a website that looked identical to the UAE Ministry of Labor and had the URL http://www.uaeministryoflabour.tk. Take note that http://www.mol.gov.ae is the real address of the Ministry. Anyone looking for work in the UAE was lied to by the phony website [19].

One of the most effective and extensively utilized strategies to combat phishing attempts is general user education. In an effort to raise user knowledge about phishing attacks, their definition, and how to recognize and avoid falling prey to them, a number of organizations have initiated awareness campaigns [20]. Emails, posters, online seminars, in-class instruction, games, etc. are all possible campaign communication methods [21]. A number of studies have cast doubt on the efficacy of such efforts in protecting end users against phishing attempts, even if they assist businesses in meeting the compliance requirements of security standards like ISO [22] and NIST [23]. Typical metrics for educational programs include the total number of users who completed the training (i.e., how many people showed up to the awareness sessions, how many people got a passing score on the examinations, etc.). But the campaigns don't know how effective the awareness sessions were or how many people would be targeted in actual assaults after attending them.

Controlled in-house phishing audits have been suggested by many studies as a means to investigate the efficacy of awareness sessions and the susceptibility of average users to such assaults. The authors of [24] conducted a social engineering audit among 33 employees of a company, asking for their login credentials; 19 employees complied, prompting the authors to discuss the critical need of user privacy education in preventing social engineering attacks on protected computer systems. Additionally, the research found that different divisions within the company had varying degrees of user education about protection against social engineering assaults. The year 2008 saw yet another phishing assessment of 576 London office workers [25]. The results indicated that 21% of the participants would divulge their credentials in exchange for a chocolate bar, and 58% would do the same over the phone if the caller identified themselves as an IT agent. A quarter of respondents changed their passwords very seldom, and a third of those people used the same password for all of their accounts, according to the audit. The authors of [21] trained a Portuguese company's staff to recognize and avoid phishing attempts, then ran another audit to confirm the training's efficacy. The authors found that the phishing awareness training was beneficial, as the failure rate dropped from 42% in the first trial to 12% in the second. At New York's United States Military Academy at West Point, another group ran a phishing experiment with two stages [26]. The findings of the experiment also shown that the participants were able to better recognize phishing attempts after the training. In a similar two-stage phishing attempt, the New York State Office of Cyber Security & Critical Infrastructure Coordination exposed its staff [27]. Employees' improved capacity to recognize phishing attempts after training was also shown by the outcomes of the experiments.

Students, teachers, and staff at the American University of Sharjah (AUS) in the United Arab Emirates participated in a controlled phishing experiment to learn more about Middle Eastern users' susceptibility to such assaults. Five thousand current students, five thousand alums, and one thousand staff members make up the university. The pupils represent more than 80 different countries. Established in 1997, the institution's four colleges—Arts and Science, Engineering, Architecture, Art and Design, and Business and Management—offer a total of thirteen master's degree programs in addition to twenty-five undergraduate majors and forty-eight minors. At this university, English is the medium of instruction. Three students and their adviser carried out the experiment with the help of the AUS IT Director and the University's Provost, who gave their clearance. At the university, no one else was aware of this trial. To imitate the AUS website that customers visit to reset their passwords, a phony website was created (see to Figures 1 and 2). Keep in mind that https://passwords. aus.edu is not the same as the phishing website's URL address. Because of a security breach, an email was issued to every AUS user requesting that they change their passwords immediately. breach. The AUS FROM address was spoofing such that it seemed to be the email address of the AUS IT Department. Users were tricked into visiting the phishing website by being asked to click on a link in the email that led to https://passwords.aus.edu. After entering their usernames, users were prompted to click the proceed button. To make sure no passwords were submitted, the users were sent to a second page with a timeout error and a message requesting them to try again in an hour due to excessive system demand. They were meant to be sent to a second page to input their old and new passwords. The date and time of each username entry was recorded in a database. All users' identities remained hidden, guaranteeing their privacy. Counting the number of possible victims was the primary objective. After being up for ten days, the phishing website was taken down. When the AUS IT department receives a phishing email that seems to be from someone trying to trick AUS users, they usually send out a warning email to everyone. Additionally, users are informed of the most recent IT security concerns via frequent emails sent by the Department. A few hours subsequent to the first phishing email, the IT department in the experiment issued a warning email. A total of 954 out of 11,000 Australian consumers fell for the phishing scam, even though they were warned via email. Students made up 96% of that group. There were almost as many male and female casualties as female. The casualties also came from various academic years, from freshmen to seniors. But first-year students made up the bulk of the casualties. Curiously, after the IT department's warning email, more than 200 people were tricked into falling for the phishing exercise. Unfortunately, this demonstrates that some people do not pay attention to and disregard such warning letters. Moreover, serious repercussions would have ensued had this sophisticated assault been genuine or had included financial information.

After the experiment was over, a helpful website was built up to explain everything that had happened, go over the findings, and provide people advice on how to recognize a phishing attempt and stay safe in the future. Publications in the local media informed all AUS users about the website. Even though the experiment's findings were frightening and demonstrated the need for extensive security awareness training, many users—particularly the experiment's victims—became more vigilant against phishing attempts as a consequence.

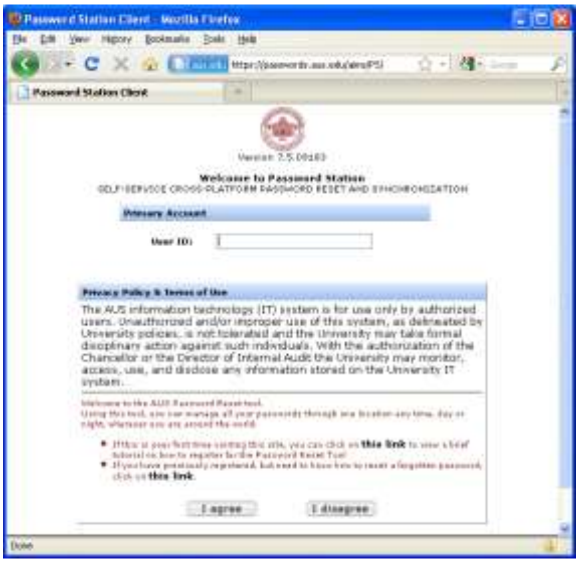
Two weeks subsequent to the awareness training, a second phishing audit was executed in order to assess their efficacy. Curiously, out of all the users affected by the audit, only 220 were students. The success of the awareness seminars was shown by the second audit, which indicated a decrease in the number of victims from 9% to 2%. The information security awareness campaign's efficacy may be determined by conducting a controlled phishing audit.

Keep in mind that cybercriminals have long targeted educational institutions like colleges because to the abundance of computers, high internet speeds, and guest access that these establishments usually provide [14]. Despite this, there aren't many schools that educate their employees and students about the need of information technology security [28]. Quite a few studies have recently been investigating what influences university students' knowledge of information security risks [28, 29].

Hackers are resorting to increasingly complex phishing techniques, called Spear Phishing, as consumers get used to these types of assaults. Sending a phishing email to specified individuals in government or financial institutions is the plan. Typical recipients are high-ranking executives, and the emails include sensitive information gleaned from public sources like Facebook or LinkedIn. So as not to draw attention to the assault, just a small number of emails are sent in an effort to make them seem authentic. The typical outcome of these types of assaults is for the victim to divulge sensitive information and passwords.

Pharming is another sophisticated kind of phishing in which the hacker manipulates the DNS system to redirect users to a malicious website while still showing them the real, valid URL. The user will have a harder time detecting the effort at fraud because of this.

Figure 1. Original Password Portal Website for the American University of Sharjah.


Password Station Client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://passwords.aus.edu/ams/PS/
Password Station Client
I agree
I disagree
Done

Version 7.5.00163

Welcome to Password Station
SELF-SERVICE CROSS-PLATFORM PASSWORD RESET AND SYNCHRONIZATION

Primary Account

User ID:

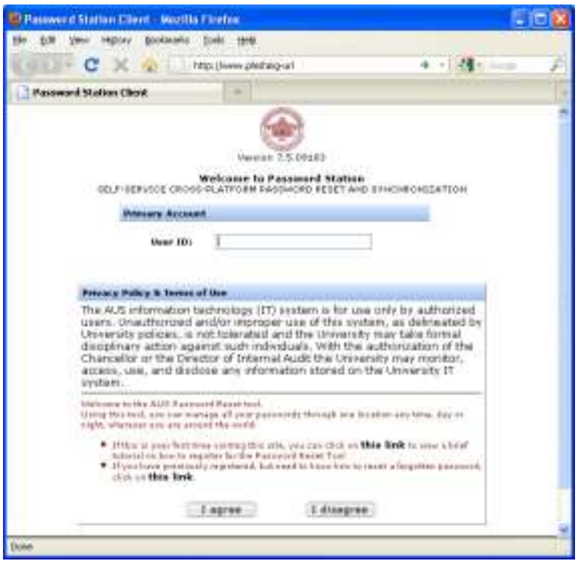
Privacy Policy & Terms of Use

The AUS information technology (IT) system is for use only by authorized users. Unauthorized and/or improper use of this system, as delineated by University policies, is not tolerated and the University may take formal disciplinary action against such individuals. With the authorization of the Chancellor or the Director of Internal Audit the University may monitor, access, use, and disclose any information stored on the University IT system.

Welcome to the AUS Password Reset tool.
Using this tool, you can manage all your passwords through one location any time, day or night, wherever you are around the world.

- If this is your first time visiting this site, you can click on **this link** to view a brief tutorial on how to register for the Password Reset Tool.
- If you have previously registered, but need to know how to reset a forgotten password, click on **this link**.

Tokens and one-time passwords are examples of two-factor authentication systems that are the focus of a new kind of sophisticated phishing attacks called Real-Time Phishing. The assault is successful because, instead of waiting to use the stolen password, the perpetrator uses it to enter the bank's website and carry out the fraud right away.


Password Station Client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.phishing-url
Password Station Client
I agree
I disagree
Done

Version 7.5.00163

Welcome to Password Station
SELF-SERVICE CROSS-PLATFORM PASSWORD RESET AND SYNCHRONIZATION

Primary Account

User ID:

Privacy Policy & Terms of Use

The AUS information technology (IT) system is for use only by authorized users. Unauthorized and/or improper use of this system, as delineated by University policies, is not tolerated and the University may take formal disciplinary action against such individuals. With the authorization of the Chancellor or the Director of Internal Audit the University may monitor, access, use, and disclose any information stored on the University IT system.

Welcome to the AUS Password Reset tool.
Using this tool, you can manage all your passwords through one location any time, day or night, wherever you are around the world.

- If this is your first time visiting this site, you can click on **this link** to view a brief tutorial on how to register for the Password Reset Tool.
- If you have previously registered, but need to know how to reset a forgotten password, click on **this link**.

Figure 2. Phishing Password Portal Website for the American University of Sharjah. Note that the URL address is different from theoriginal URL address in Figure 1.

II. Wireless Security in UAE

A growing number of people are opting to utilize wireless internet. In 2008, 387 million people throughout the globe utilized wireless networks; by 2014, that figure would have risen to 655.7 million, according Computer Industry Almanac Inc. [30]. There is less need for cables thanks to wireless networks, which make internet access easier. You can connect to wireless hotspots with most modern PDAs, phones, and laptops thanks to their built-in wireless internet devices. Most houses, businesses, schools, hospitals, airports, etc. already have wifi access points installed, and you can get them in regular supermarkets for less than $100. Nevertheless, data may be transferred between the wireless access point and a wireless device, such a laptop, in plain air without encryption if the default configuration is not altered. Changing the default settings or reading the access point documentation are tasks that consumers seldom undertake. Without encryption, a hacker could simply listen in on any conversation between two parties and steal sensitive information like bank account details or email correspondence. By connecting to the internet via the access point, an attacker may mask their identity, commit assaults against others, or even avoid paying internet expenses.

There are a number of wireless encryption methods available today. As an example, there are protocols like WEP and WPA [31]. Security experts have long warned clients against using the 1999-introduced WEP system because to its proven vulnerabilities. The WEP password is readily discoverable by an attacker using publicly accessible techniques, and the system may be quickly breached. Wireless Protected Access (WPA) is the latest and greatest in wireless encryption technology.

Sharjah and Dubai, two cities in the United Arab Emirates, were the sites of a wireless security audit in 2010. A study was conducted to determine the number of wireless access points in residential and business regions, as well as the proportion of users that use encryption. Four in ten (12,000) access points in the two cities used WPA encryption, 38 percent used WEP, and 22 percent did not use encryption at all (see Figure 3).

Abu Dhabi, Dubai, and Sharjah were the sites of a comparable poll in 2008 [32]. Of the 15,000 access points identified in the three cities in the 2008 research, 32% were unencrypted, 33% used WEP, and 35% used WPA (see to Figure 4 for details). Although there was a noticeable 10% decline in the number of unencrypted access points, there was an increase in the number of access points using poor WEP encryption. This highlights the need for more education and the fact that some users have low levels of wireless security awareness.

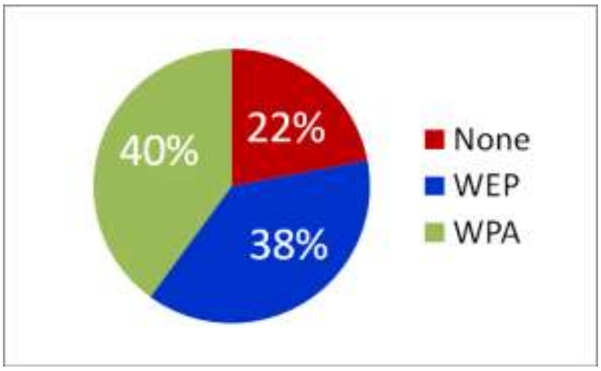


Figure 3. Percentage of Wireless Access Point Encryption Types in the2010 UAE Survey.

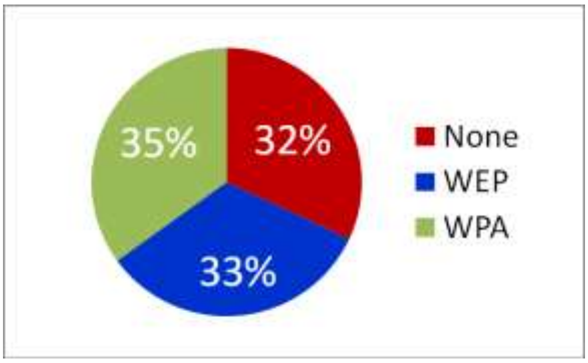


Figure 4. Percentage of Wireless Access Point Encryption Types in the2008 UAE Survey.

III. RFID SECURITY IN UAE

New technology called Radio Frequency Identification (RFID) allows for the identification and tracking of things through tags. Tags are usually attached to goods, creatures, or even people. The RFID tag has the benefit of being able to be detected from up to hundreds of meters away, even when the reader is not in direct line of sight. Worldwide, companies are pouring resources into RFID in the hopes that it would boost their bottom line, enhance their operations, and save operational costs.

The use of radio frequency identification (RFID) has increased in recent years throughout the Middle East. The e-tolling system in Dubai, United Arab Emirates, has begun using RFID gates. The valuable mail is tracked by the Saudi Post Corporation using RFID tags. To speed up the process of finding automobiles in its massive service facilities, Emirates Motor Company—the biggest Mercedes-Benz facility in the world—uses radio frequency identification tags. In order to quickly find lost jewelry, stores utilize RFID tags. Diplomas issued by universities in the United Arab Emirates, such the American University of Sharjah, are being equipped with radio frequency identification tags to guarantee their authenticity. Stores like Baroue in Kuwait that cater to children are using RFID tags so parents can keep tabs on their kids while they play. Radio frequency identification tags are being used for access control by a number of businesses in the construction, health, and oil and gas sectors.

In 2009, the Middle Eastern RFID market was valued at $29.4 million, and by 2012, it was projected to reach $69.1 million, according to VDC Research [33]. By comparison, analysts predict that the North and South American RFID services market will be worth $1.28 billion in 2012, while the Asia-Pacific market will be worth $1.6 billion. The Middle Eastern RFID market is currently rather tiny, but it is growing at a rapid pace.

As unfortunate as it is, the introduction of new technologies always leads to their misuse. Several security experts have already brought attention to several RFID security flaws today, the most prominent of which is the illegal monitoring of RFID tags. There are already privacy issues with RFID tags, and now there's the added risk of unwitting user profiling. When it comes to tagged books, for instance, access to RFID tags may expose reading patterns; when it comes to marked currencies, it can reveal financial situations. In light of these shortcomings, it is imperative that the general population learn about RFID technology and its advantages, disadvantages, and potential dangers.

There is a lack of RFID knowledge among the general public in both Europe and the US, as stated in [34]. Even in the West, few people in the Middle East know about RFID. While the Middle East has played home to a handful of RFID-related conferences in recent years, more effort is required to educate the public about the technology's inner workings and the privacy and security risks it poses.

IV. Cyber Security Awareness

- The methods that hackers use to steal data are always evolving. The presence of "uneducated" people in a company leaves it open to privacy breaches and hacking attempts [35]. Combating risks to information technology security requires user education and training. Not only should users study the content, but they should also put it into practice on a regular basis. Neither the user nor the company should be held solely responsible for this difficult job. To create a resident who is knowledgeable about IT security, several different organizations must work together. Below, we have outlined a few suggestions:
-
- Cybercrime laws should be enacted and strictly enforced by governments. Since many attacks may be carried out from outside, it is important for them to collaborate closely with foreign countries. There has to be a system in place to identify, prevent, and respond to cyber security problems, and they should form Computer Emergency Response Teams (CERT).
- To raise people's level of security awareness, it is recommended that Computer Emergency Response Teams (CERT) be formed. On top of that, CERT may aid in the formation of new cybercrime statutes, the education of computer forensic teams, and the combatting of cybercrime by both people and enterprises. To bring more emphasis to the significance of cyber security awareness, they might proclaim a cyber security awareness month. Qatar, the United Arab Emirates, and Saudi Arabia are the newest Middle Eastern countries to establish CERT centers [36, 37, 38].
- It is imperative that law enforcement agencies establish computer forensics units whose only purpose is to collect, restore, analyze, and present digital evidence found on digital devices.
- Businesses should provide security training to their staff and customers. It may be a mix of online and in-person instruction, or it might be entirely virtual. Given the ever-present nature of emerging IT security risks, the training should be conducted on a regular basis, preferably twice yearly. Training should have the full backing of the company's upper management. Additionally, the business should launch a local awareness campaign informing people about the most recent IT security dangers via the distribution of posters and newsletters sent via email. Keep in mind that the approach to creating the awareness materials is crucial, and that various users need different information. When making the awareness materials, for instance, it's important to think about things like language and culture. Similarly, the communication process has to be tailored to individual consumers, and the way of providing the awareness material is crucial. For instance, because many college students use Facebook and other social media sites, it would be an excellent platform to disseminate awareness materials in a campus setting. By keeping tabs on the user's learning activities, learning management systems may help ensure compliance with standards that demand awareness programs, such ISO 27001. It is important to monitor the impact of security awareness campaigns and training by conducting audits like to the one mentioned in Section 2 from the American University of Sharjah. These audits will help determine the degree of user security awareness. Protecting the privacy and personal data of the users being audited is of the utmost importance throughout the planning and execution of such audits. It would be helpful to have one person that consumers can talk to about any issues with IT security. The training materials have to go over the company's policies on information technology security as well as the consequences for breaking those policies. Lastly, businesses should prioritize security knowledge and take a proactive strategy instead of a reactive one.

• Internet service providers (ISPs)—they should provide guidance on how to use the internet securely or how to set up any device to access the internet securely. Information technology (IT) security events, tips for preventing them, and the consequences faced by those responsible should all be regularly included in news articles.

To better prepare themselves for potential IT security risks, users should read periodicals, books, and internet articles on a regular basis.

• Non-Governmental Organizations (NGOs)—should spearhead initiatives to raise awareness about IT security and provide assistance to individuals with inquiries or issues related to security.

Security awareness initiatives and the incorporation of information technology security subjects into computer science curricula should be offered by educational institutions.

An international coalition of governments, corporations, and universities has been formed to combat cyber terrorism since 2008. More than 30 nations have joined together in an effort to investigate and counteract catastrophic cyber threats; they call it the International Multilateral Partnership Against Cyber Terrorism (IMPACT) [39].

V. Conclusions

Technical assaults are getting more difficult to execute as Middle Eastern firms increase their use of cutting-edge protection equipment and software. In a similar vein, businesses are minimizing the amount of potential assaults by creating comprehensive security policies and employing IT security specialists. Regrettably, very little effort is made to protect the users, who are the weakest link. This encourages hackers to take advantage of people's generosity and trust in order to get sensitive information. Several research on IT security awareness among UAE students and professionals were described in this article, which covered user security awareness in the Middle East. The significance of conducting controlled audits to gauge security knowledge was covered. Also covered were a number of important aspects that might raise consumers' level of security awareness.

REFERENCES

[1] As stated in the 2010 Internet World Stats by the Miniwatts Marketing Group. Visit http://www.internetworldstats.com/stats.htm for further information.

[2] “B2C e-commerce volume exceeded US$ 4.87 billion in Kuwait, Lebanon, Saudi Arabia and UAE in 2007,” according to a 2008 report by the Arab Advisors Group.For more information, visit http://www.arabadvisors.com/Pressers/presser-040208. htm-0.

[3] "The Middle East's credit card industry is experiencing explosive growth," according to a 2007 report by the Lafferty Group. Yours to peruse at this location: http://www.lafferty.com/pdffiles/Lafferty%20MENA %20ca rds%20-%20press%20release%20180607%20_3_.pdf.

[4] The website of a prominent UAE newspaper was compromised in 2008, according to Arabian Business. You can get this information at: http://www.arabianbusiness. com/519982-leading-uae-newspapers-website-hacked.

[5] In 2008, the Al Arabiya News Channel said that the country was "hit" by a cyber war between Sunnis and Shiites.Find it at: http://www.alarabiya.net/articles/2008/10/10/57995.html.

[6] [6] "Phishing attack targets Batesco internet subscribers," Arabian Business, 2008.Read the full story at: http://www.arabianbusiness.com/520459-batelco-internet-subscribers-targeted-by-phishing-attack.

[7] Arabian Business reported in 2008 that phishing assaults were targeting NBK internet banking users.Link: http://www.arabianbusiness.com/522781-nbk-online-banking-customers-targeted-by-phishing-attack.

[8] U.A.E. bank hit by massive phishing assaults, according to ITP (2010). Visit http://www.itp.net/579059-uae-bank-targeted -in-major-phishing-attack for more information.

[9] [9] "Bank accounts emptied in phishing raid," The National, 2010. It may be accessed at this URL: http://www.thenational.ae/apps/pbcs.dll/article?AID=/201 00405/NATIONAL/704049912&SearchID=73398739 6980 56.

[10] [10] "Viral infection targets UAE Ministry of Education," UAE Today, 40 October 2010. This information may be accessed at: http://www.emaratalyoum. com/local-section/accidents/2010-04-12-1.106891.

[11] [11] "Internet security breach at Riyad Bank," AMEinfo, 2010. Visit http://www.ameinfo.com/235378.html to get the information.

[12] "Al Jazeera accuses hackers of disrupting World Cup coverage," The National, 2010. You can access this article at this link: http://www.thenational. ae/apps/pbcs.dll/article?AID=/20100613/NATIONAL/ 7061 29867&SearchID=73402848695382.

[13] [13] Cybercrime Law on a Global Scale. Visit http://www.cybercrimelaw.net/laws/alfabetic/s-t.html for more information.

[14] [14] In the Proceedings of the Annual Conference on Information Security Curriculum Development, 2005, F. Katz discusses "The effect of a university information security survey on instructing methods in information security" (pp. 43-48).

[15] In their 2007 second edition of "Principles of Information Security," M. Whitman and H. Mattord wrote the book Course Technology.

[16] [...] APWG's Phishing Activity Trends Report, Fourth Quarter 2009. The report may be seen online at: http://www.antiphishing.org/reports/apwg_ report_Q4_2009.pdf.

[17] [17] "The National: Emiratis at risk of cyberattacks," 2008. Link to the article: http://www.thenational.ae/apps/pbcs.dll/article?AID=/ 20080814/NATIONAL/420302377 &SearchID=73402849474210.

[18] Article from 2009 in Arabian Business on the UAE cybercrime team. You may get the article at this link: http://www.Arabianbusiness. com/553470-uae-cybercrime-squad-gunning-forward.

[19] According to Gulf News in 2008, a phishing website for a fake recruiting firm was disabled. The website of a fake recruiting agency was blocked: http://gulfnews.com/news/gulf/uae/employment/phishing-website-of-bogus-agency-blocked-1.84296.

[20] 20. "The Social Engineering Threat," in the January 2008 issue of the ISSA Journal, written by D. Timko.

[21] ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements (P. Kumaraguru, S. Sheng, A. Acquisti, L. Cranor, and J. Hong, 2008) and the Proceedings of the IEEE eCrime Researchers Summit (pp. 1-12) are cited as sources. Originally published in October 2005 by the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO).

[22] [23] TheNIST - An Introduction to Computer Security. The National Institute of Standards and Technology (NIST) published this in 2004.

[23] [24] "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems" (P. Orgill, G. Romney, M. Bailey, and G. Orgill, 2004), in Proceedings of the 5th Conference on Information Technology Education, pages 177–181.

[24] [25] The"Passwords for chocolate are given by women four times more often than men," Infosecurity Europe, 2008. See it at:

http://www.infosec.co.uk/page.cfm/T=m/Action=Press /Pre ssID=1071.

[25] [26] "Phishing for User Security Awareness" (R. Dodge, C. Carver, and A. Ferguson, 2007) published in Computers and Security, vol. 26, no. 1, pages 73–80.

[26] - "Gone Phishing" (New York State Office of Cyber Security & Critical Infrastructure Coordination, 2017). A Report on the State of New York's Anti-Phishing Exercise Program. Exercise Summary for the General Audience, 2005.

[27] [28] In their 2008 article "Information Security Awareness in Higher Education: An exploratory study," Y. Rezgui and A. Marks discuss the topic in Computers and Security, volume 27, issues 7 and 8, pages 241-253.

[28] 28. A. Marks, "Exploring universities' information systems security awareness in a changing higher education environment," Ph.D. Thesis, University of Salford, 2007.

[29] Computer Industry Almanac, Inc., Worldwide Users of Wireless Internet Connections,

[30] At the following URL: http://www.c-i-a.com/pr032102.htm

[31] [31] "Real 802.11 Security: Wi-Fi Protected Access and 802.11i" (Addison-Wisley, 2003), by J. Edney and W. Arbaugh.

[32] [32] "Wireless security in UAE: A survey paper" in 2007's Proceedings of the IEEE GCC Conference by A. Kalbasi, O. Alomar, M. Hajipour, and F. Aloul.

[33] [33] "RFID market in the Middle East is heating up," RFID Journal, 2009.

[34] The paper may be seen online at: http://www.rfidjournal.com/article/view/4618.

[35] on page 34The 2005 Cap Gemini report "RFID and Consumers: What European Consumers Think About Radio Frequency Identification and the Implications for Business" surveyed consumers in Europe. Find it at: http://www.us.capgemini.com/DownloadLibrary/requestfil e.asp?ID=450.

[36] Journal of Advances in Information Technology, 2(2), pp. 109-121, May 2011, by Z. Khattak, J. Manan, and S. Sulaiman, "Analysis of Open Environment Sign-in Schemes—Privacy Enhanced & Trustworthy Approach" [35].

[37] You may find UAE-CERT at http://www.aecert.ae/.

[38] Referenced as [37] on the Saudi Arabian CERT website (http://www.cert.gov.sa/).

[39] It is the Qatar-CERT. The International Multilateral Partnership Against Cyber Terrorism (IMPACT) is accessible online at http://www.qcert.org/. Visit http://www.impact-alliance.org/ for more information.