

# The Need for Effective Information Security Awareness

Fadi A. Aloul

Department of Computer Science & Engineering

American University of Sharjah, Sharjah, UAE

Email: faloul@aus.edu

**Abstract**—Security awareness is an often-overlooked factor in an information security program. While organizations expand their use of advanced security technology and continuously train their security professionals, very little is used to increase the security awareness among the normal users, making them the weakest link in any organization. As a result, today, organized cyber criminals are putting significant efforts to research and develop advanced hacking methods that can be used to steal money and information from the general public. Furthermore, the high internet penetration growth rate in the Middle East and the limited security awareness among users is making it an attractive target for cyber criminals.

In this paper, we will show the need for security awareness programs in schools, universities, governments, and private organizations in the Middle East by presenting results of several security awareness studies conducted among students and professionals in UAE in 2010. This includes a comprehensive wireless security survey in which thousands of access points were detected in Dubai and Sharjah most of which are either unprotected or employ weak types of protection. Another study focuses on evaluating the chances of general users to fall victims to phishing attacks which can be used to steal bank and personal information. Furthermore, a study of the user's awareness of privacy issues when using RFID technology is presented. Finally, we discuss several key factors that are necessary to develop a successful information security awareness program.

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

## I. INTRODUCTION

Internet users in the Middle East have been continuously increasing in the past few years. According to the World Internet Usage Statistics News [1], while the Middle East constitutes 3.2% of the worldwide internet users, it has registered an internet usage growth of 1825% in the past 10 years, compared with the growth of 445% in the rest of the world. It also reported that Bahrain, UAE, and Qatar had the highest internet penetration rates in the Middle East as of June 30, 2010 with rates equivalent to 88%, 75.9%, and 51.8% of their population, respectively. This growth has attracted hundreds of online companies to conduct business in the Middle East and allowed many existing sectors, such as education, health, airline, and government, to move their operations online.

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.

The high number of internet penetration and credit card use growth, fueled by advances in the internet technology, has led to a significant increase in the number of online transactions, electronic data, and smart mobile devices. However, the last few years have also seen an increase in the number of cybercrime incidents in the Middle East. Local media occasionally report incidents of online fraud, attempts to hack banks, and websites being shut down or defaced. For example, in May 2008, Al-Khaleej Newspaper website, a reputable newspaper based in UAE, was defaced by hackers [4]. Later that year, in October 2008, Arabiya.net website, a reputable Middle East News Channel, was also defaced [5]. In both incidents, the hackers claimed to have conducted the attacks because of political reasons. In May 2008, the Bahraini Telco company was targeted by phishing attacks [6]. Later that year, the National Bank of Kuwait was also targeted by phishing attacks [7]. In January 2010, several UAE bank websites were a target of phishing attacks as reported by ITP [8]. In April 2010, it was reported that several users lost their UAE bank savings through internet fraud attacks [9]. In April 2010, the UAE Ministry of Education was infected by a computer virus [10]. In June 2010, Saudi Arabia's Riyad Bank website was hacked [11]. In June 2010, Al Jazeera Sport World's Cup broadcasting was also interrupted by hackers [12].

The worldwide increase in information technology (IT) security incidents is mainly due to the (1) increase in electronic data, (2) increase in mobile devices, (3) increase of organized cybercrime groups, (4) increase of intelligent external and internal IT security threats, (5) difficulty of tracing the attackers, (6) limited cybercrime laws, and (7) limited IT security knowledge among internet users. The hackers are also motivated by various reasons for conducting their attacks. Examples include:

(1) spreading a political message, (2) gaining financially (i.e. Theft), (3) stealing information, (4) causing damage and disturbance, and (5) achieving self satisfaction and fame.

The increase in IT security incidents has alerted governments to introduce federal laws to fight IT crimes, also known as e-crime or cybercrime. Many countries in North America, Europe, and Asia have already implemented and enforced such laws. A few Middle Eastern countries have already introduced such laws [13]. The UAE was one of the first Middle Eastern countries to introduce a cybercrime federal law in January 2006. The law consisted of 26 articles and covered the majority of cybercrime incidents. The penalty ranged from fines up to 100,000 UAE Dirhams and/or 15 years of imprisonment. Saudi Arabia followed by introducing a cybercrime federal law in October 2006. Such laws helped reduce the number of IT security incidents, but unfortunately incidents still occur in the region and are mainly because of the (1) lack of cybercrime laws in most of the Middle East countries, (2) limited enforcement of cybercrime laws, (3) lack of knowledge among residents of such cybercrime laws, and (4) few computer incident forensics teams that exist in the region.

Today, as organizations expand their use of advanced secure technologies, hackers are attempting to break into organizations by targeting the weakest link: the uneducated computer user [14]. According to [15], computer user mistakes are considered one of the top threats to IT security in organizations. In this paper, we will show the need for security awareness programs in schools, universities, governments, and private organizations in the Middle East by presenting results of several security awareness studies conducted among students and professionals in UAE in 2010. The first study, presented in Section 2, focuses on studying the chances of general users to fall victims to phishing attacks which can be used to steal bank and personal information. We present the results of an approved phishing audit made without notice within an academic organization. The study is the first-of-its-kind in UAE and has shown to be very useful in increasing the general security awareness. The second study, presented in Section 3, involves a comprehensive wireless security survey in which thousands of access points were detected in Dubai and Sharjah most of which are either unprotected or employ weak types of protection. In Section 4, we discuss the level of RFID security awareness in the UAE. In Section 5, we list the key factors necessary to develop a successful security awareness program in the Middle East. We finally conclude by showing examples of recent Middle Eastern governmental initiatives to spread security awareness among its citizens.

## II. PHISHING ATTACKS IN UAE

“Phishing” is a form of Internet fraud that aims at stealing valuable information such as credit cards, social security numbers, user IDs and passwords. The fraud starts by creating a fake website that looks exactly like

that of a legitimate organization but with a slightly different URL address. In many cases, the organizations are financial institutions such as banks. An email is then sent to thousands of internet users requesting them to access the fake website, which is a replica of the trusted site, to update their records by entering their personal details, including security access codes. The page generally looks genuine. Note that the email has a FROM address that is identical to the original organization address, e.g. Human Resource or IT director, to make users believe that the email is authentic. However, the FROM field in an email can be easily faked by a hacker and the email is actually coming from the hacker’s computer. Once the user enters his or her personal information into the fake website, the personal information is sent to the hacker, and the user is redirected to the legitimate website in order not to detect the fraud attempt.

According to the Anti-Phishing Working Group [16], the number of unique fake phishing websites exceeded 42,000 pages per month in 2009, compared to 23,000 pages per month in 2008. That is almost one new phishing website every one minute. The high number of phishing websites reflects the effectiveness of the phishing hacking method.

In the Middle East, cyber criminals are increasingly targeting UAE residents with advanced hacking methods, one of which is phishing scams [17]. Such scams have caused UAE banks to raise their IT security services in recent years. Although, UAE’s Cybercrime Law, Article #10, imposes a fine and an imprisonment for any person that steals or transfers money using online fraud, several phishing attacks against UAE were detected in 2009 [18]. One of the detected attacks involved a duplicate website of the UAE’s Ministry of Labor which had a URL of: <http://www.uaeministryoflabour.tk>. Note that the authentic URL of the Ministry is <http://www.mol.gov.ae>. The fake website was cheating people who wanted to find a job in the UAE [19].

General user education is considered one of the most important and widely-used approaches in fighting phishing attacks. Several organizations have launched awareness campaigns to educate the user on the meaning of phishing attacks and how to detect such attacks and avoid falling victims to them [20]. The campaigns can include various formats of communication such as emails, posters, in-class training, web seminars, games [21], etc. While such campaigns help companies meet the compliance requirements of security standards, such as ISO [22] and NIST [23], recent studies have questioned the effectiveness of such campaigns in protecting the general users from falling victims to phishing attacks [21]. The educational campaigns typically keep track of the users who took the training, i.e. the number of users who attended the awareness sessions, the number of users who passed the exams, etc. However, the campaigns fail to identify the impact of the awareness sessions, i.e. the number of users who might fall victims to real attacks after the awareness sessions or the usefulness of the awareness sessions.

In order to study the impact of awareness sessions and the vulnerability of general users to phishing attacks, several studies recommended the use of controlled in-house phishing audits. In [24], the authors discussed the urgent need for effective user privacy education to counter social engineering attacks on secure computer systems after they conducted a social engineering audit among 33 employees in an organization asking for their usernames and passwords in which 19 employees gave their passwords. The study also noticed that the level of user education against social engineering attacks was not uniform between the organization's departments. Another phishing audit was made among 576 office employees in London in 2008 [25]. Results showed that 21% of the respondents were willing to give their passwords out with the lure of a chocolate bar and 58% would reveal their password over the phone if the caller claimed he or she was from the IT department. The audit also noted that 43% of the respondents rarely or never changed their passwords and 31% of them used one password for all their accounts. In [21], the authors conducted a phishing audit among the employees of a Portuguese company that was followed by phishing training and another phishing audit. The authors noticed a failure rate of 42% in the initial experiment and 12% in the latter experiment which reflects the effectiveness of the phishing awareness training. Another group conducted a similar two-phase phishing experiment at the United States Military Academy at West Point, New York [26]. Experiment results also showed the ability of the participants to better identify the phishing attacks after the training sessions. The New York State Office of Cyber Security & Critical Infrastructure Coordination conducted a similar two-phase phishing experiment among their employees [27]. The experiment results also showed the ability of the employees to better identify the phishing attacks after the training sessions.

In order to study the vulnerability of users to phishing attacks in the Middle East, a controlled phishing experiment was conducted among the students, faculty, and staff of the American University of Sharjah (AUS) in UAE. The university consists of 5,000 students and 5,000 alumni in addition to 1,000 faculty and staff. The students come from 80+ nationalities. The university was founded in 1997 and offers 25 majors and 48 minors at the undergraduate's level and 13 master's degrees programs through four colleges (Arts and Science; Engineering; Architecture, Art and Design; Business and Management). The language of instruction at the University is English. The experiment was performed by three students and their advisor in coordination with the AUS IT Director and the approval of the University's Provost. No one else knew about this experiment in the University. A fake website was setup to look identical to an AUS website that is accessed by the users to change their AUS passwords (see Figures 1 and 2). Note that the phishing website URL address is different from the original website URL address (<https://passwords.aus.edu>). An email was sent to all AUS users asking them to urgently change their passwords due to a security

breach. The AUS FROM address was faked to look identical to the AUS IT Department email address. Once the email was received by the users, they were requested to click on a link <https://passwords.aus.edu> which redirected the users to the phishing website URL. The users were asked to enter their usernames and click on the *continue* button. They were supposed to be taken to a second page to enter their old and new passwords; however, to ensure that no passwords were entered, the users were directed to a second page with a timeout error and a message asking them to try again after an hour due to heavy system usage. A database was used to log all entered usernames with the corresponding date and time. User anonymity was ensured and no usernames were revealed. The goal was only to count the number of potential victims. The phishing website was left online for 10 days. The AUS IT Department typically sends a warning email to all AUS users whenever similar phishing emails are sent to AUS users. The Department also sends periodical emails alerting users to the latest IT security threats. In the experiment's case, the IT Department sent a warning email a few hours after the original phishing email. Despite the warning emails, 954 users out of the 11,000 AUS users entered their usernames to the phishing website. Of those, 96% were students. The number of male and female victims was almost equal. In terms of student levels, the victims also ranged from all levels, freshman to senior students. However, the highest number of victims was from the freshman level. Interestingly, over 200 users fell victims to the phishing experiment *after* the IT Department's warning email was sent. This shows that, unfortunately, some users ignore such warning emails and don't take them seriously. Furthermore, if this sophisticated attack was real or involved banking details, the consequences would have been severe.

At the end of the experiment, an illustrative website was setup explaining the details of the experiment, discussing the results, and advising users on what a phishing attack is and what they should do to avoid falling victims in future. The website was announced to all AUS users and published in the local media. The experiment results were daunting and showed the need for significant security awareness training, yet many users, especially the victims, became more aware of phishing attacks after the experiment.

To analyze the impact of the awareness sessions, another phishing audit was conducted two weeks later. Interestingly, only 220 users fell victims to the audit all of which were students. The second audit showed a drop in the number of victims from 9% to 2% which reflects the effectiveness of the conducted awareness sessions. The controlled phishing audit can identify the effectiveness of the information security awareness campaign.

Note that universities have always been a target for cyber criminals since universities typically have a large number of computing stations, fast internet bandwidth, and allow guest access [14]. Yet, very few universities are known to offer IT security awareness sessions to its students and staff [28]. Recently, several researches have

been exploring the factors that affect information security awareness in universities [28, 29].

As users, today, are becoming familiar with phishing attacks, hackers are launching more sophisticated phishing attacks known as *Spear Phishing*. The idea is to send a phishing email targeting specific names in governments or financial enterprises. The emails typically belong to senior executives and include personally identifiable information that is collected of public websites or social pages, e.g. Facebook or LinkedIn. Only a limited number of emails are sent to make the emails look credible and avoid publicizing the attack. Such attacks usually end up with the victim passing his/her personal information and passwords.

Another advanced phishing attack is referred to as *Pharming* where the hacker tampers the domain name server (DNS) system such that the user would be redirected to the fake website while displaying the original legitimate URL address. This makes it more difficult for the user to identify the fraud attempt.

A new advanced phishing attack known as *Real-Time Phishing* targets two-factor authentication systems, such as one-time passwords or tokens. The attack works by immediately using the captured password from the phishing website to access the bank website and commit the fraud as opposed to using the password at a later time.

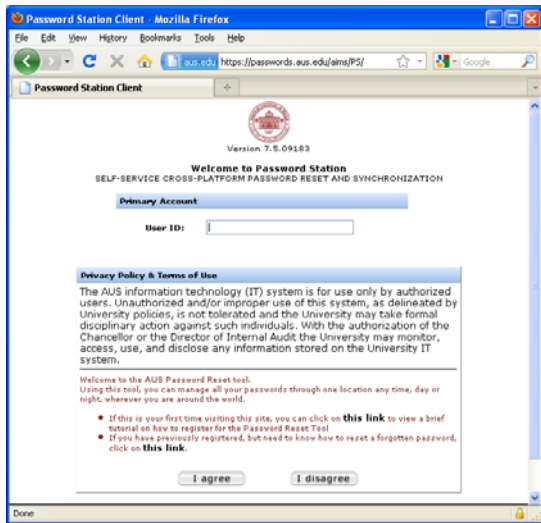


Figure 1. Original Password Portal Website for the American University of Sharjah.



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

### III. WIRELESS SECURITY IN UAE

Wireless internet users are on the rise. According to Computer Industry Almanac Inc, 38.7% of the world internet users used wireless networks in 2008 and the number will increase to 65.7% in 2014 [30]. Wireless networks allow for easy access to the internet and reduces the need for wires. Most PDAs, phones, and laptops today have wireless internet devices that allow users to connect to wireless hotspots. Today, wireless access points are sold in normal supermarkets for less than \$100 and are deployed in most homes, companies, universities, hospitals, airports, etc.

Nevertheless, using the wireless access point without changing its default configuration allows for data to be exchanged between the access point and the wireless device, e.g. laptop, in clear air unencrypted. In most cases, users don't read the access point manual or spend the time on changing the default configuration. When no encryption is used, an attacker can easily eavesdrop on any exchanged communication and steal the user's private data, such as emails or bank account info. An attacker can also connect to the internet via the access point and use it to avoid paying internet charges or more seriously to conduct attacks against others and hide the attacker's identity.

Today, several wireless encryption systems exist. Examples include WEP and WPA [31]. The WEP system, which was introduced in 1999, has been shown to have security flaws and security consultants are continuously advising customers not to use WEP. An attacker can easily break into the WEP system and identify the WEP password with *freely* available tools. WPA is considered the newest and most secure wireless encryption system.

In 2010, a wireless security assessment was conducted in two cities of UAE: Dubai, and Sharjah. Residential and commercial areas were assessed for the number of

wireless access points and the percentage of users that employ any type of encryption. The study found 12,000 access points in the two cities, of which 40% employed WPA encryption, 38% employed WEP encryption, and 22% had no encryption (see Figure 3).

A similar survey was conducted in 2008 in the three cities of UAE: Abu Dhabi, Dubai, and Sharjah [32]. The 2008 study found 15,000 access points in the three cities, of which 35% employed WPA encryption, 33% employed WEP encryption, and 32% had no encryption (see Figure 4). While clearly the number of access points with no encryption dropped by 10%, the number of access points with the *weak* WEP encryption increased. This shows the limited wireless security awareness among some users and the need for additional education.

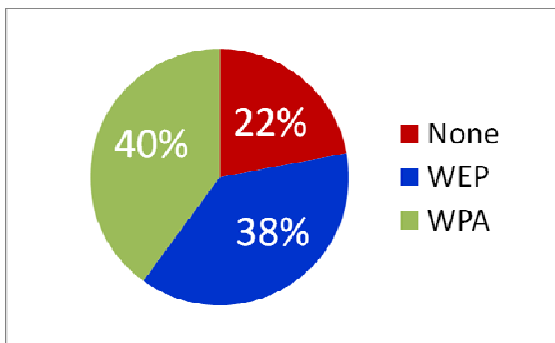


Figure 3. Percentage of Wireless Access Point Encryption Types in the 2010 UAE Survey.

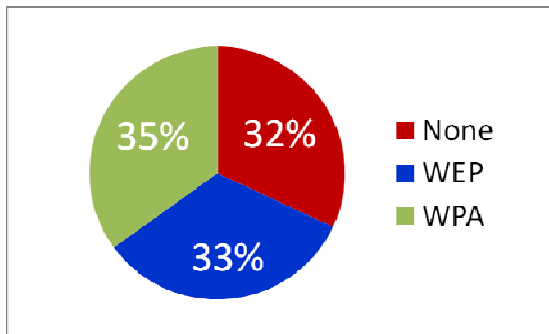


Figure 4. Percentage of Wireless Access Point Encryption Types in the 2008 UAE Survey.

#### IV. RFID SECURITY IN UAE

Radio Frequency Identification (RFID) is a new technology used for identifying and tracking objects, known as RFID tags. The tags are typically applied into products, animals, or humans. An advantage of the RFID tag is its ability to be identified beyond the line of sight of the reader and up to hundreds of meters away. Organizations from all over the world have been heavily investing in RFID to help them reduce their operation cost, improve their business, and increase their revenue.

The Middle East has seen a rise in RFID applications in the past few years. Dubai in United Arab Emirates started using RFID gates for e-tolling. The Saudi Post Corporation uses RFID tags to track valuable mail. Emirates Motor Company, the world's largest Mercedes Benz facility, uses RFID tags to reduce the amount of time needed to locate the vehicles in its large service centers. Jewelry shops use RFID tags for fast detection of missing items. UAE Universities, such as the American University of Sharjah, are placing RFID tags on the diplomas that they issue to ensure the validity of the certificate. Child stores, such as Barou in Kuwait, are using RFID tags to allow parents to track their children while playing in the store. Several organizations in the oil & gas, construction, and health industries are using RFID tags for access management.

According to VDC Research, the market of RFID services in the Middle East was estimated at \$29.4 million in 2009 and expected to reach \$69.1 million in 2012 [33]. In contrast, the RFID services' markets in North/South America and Asia-Pacific are expected to reach \$1.28 billion and \$1.6 billion, respectively, in 2012. Although the RFID market in the Middle East is still small, the growth rate is high.

Unfortunately, the introduction of new technologies always comes with a byproduct, which is the abuse of the technology. Today, several security researchers have already highlighted various security weaknesses in RFID systems, mainly being the illicit tracking of RFID tags. In addition to privacy concerns, RFID tags can be used for user profiling without the user's knowledge. For example, access to RFID tags can reveal reading habits in the case of tagged books or the financial situation in the case of tagged banknotes. Such weaknesses call for the need of public awareness of RFID technology and the understanding of its benefits, challenges, and risks.

According to [34], the general awareness regarding RFID is low in both the United States and Europe. The RFID awareness in the Middle East is also limited. The last few years, have seen a few RFID-based conferences hosted in the Middle East, but more is needed to increase the general awareness among the public with respect to how the RFID technology works and its security and privacy concerns.

#### V. CYBER SECURITY AWARENESS

Hackers are continuously identifying new means of stealing information. Unfortunately, the presence of "uneducated" users in an organization makes them an easy target for hackers and vulnerable to privacy attacks [35]. User education and training is a must to combat IT security threats. Users should not only learn the material but they should also apply it in their daily life. This is not a simple task to achieve and not the sole responsibility of the user or the organization. Many groups have to be involved to produce an IT security-aware resident. We summarize some of the recommendations below:

- **Governments** – should produce cybercrime laws and enforce them. They should also work closely with

other governments since many attacks can be conducted from abroad. They should also establish Computer Emergency Response Teams (CERT) that are dedicated to the detection, prevention, and response of cyber security incidents.

- **Computer Emergency Response Teams (CERT)** – should be established to enhance the security awareness among residents. CERT can also help establish new cybercrime laws, train computer forensic teams, and assist organizations and users in fighting cybercrime. They can declare a cyber security awareness month that can help increase the public's attention to the importance of cyber security awareness. In the Middle East, UAE, Saudi Arabia, and Qatar have recently introduced CERT centers [36, 37, 38].
- **Police Departments** – should have computer forensics teams that are specialized in obtaining, recovering, examining, analyzing, and presenting electronic evidence stored on computers or electronic devices.
- **Enterprises** – should offer security training to its employees and clients. This could be online or onsite training or a combination of both. The training should be done regularly, e.g. twice a year, since new IT security threats appear constantly. The enterprise management should endorse and financially support the training. The enterprise should also have a local awareness campaign by distributing posters and emailing newsletters to alert users to the latest IT security threats. Note that the method of *preparing* the awareness material is very important and the content needs to be customized for different users. For example, language and culture must be taken into consideration when preparing the awareness material. Similarly, the method of *delivering* the awareness material is very important and the communication process needs to be customized for different users. For example, in a university, social media websites, such as Facebook, can be used to deliver the awareness material since a large number of students are likely to be using social media websites. In order to be compliant with standards that require awareness programs, e.g. ISO 27001, learning management systems can be used to track the user's learning activity. Audits, similar to the one conducted at the American University of Sharjah and reported in Section 2, should also be conducted to measure the level of security awareness among the users and the effectiveness of the security awareness campaign and training. Such audits must be carefully planned and implemented to meet their goals, while protecting the privacy and the personal data of the assessed users. A central point of contact regarding IT security related matters should be established to ease the communication with the users. The education material should cover the organization's IT security policies and the penalties for not following the rules. Finally, enterprises should adopt a

*proactive* rather than a *reactive* approach to security awareness.

- **Telecommunication companies (ISPs)** – should offer advices on how to use the internet safely or configure any internet device securely.
- **Media** – should continuously post IT security advices, report IT security incidents, and the penalty that the attackers got.
- **Users** – should train themselves by constantly reading magazines, books and online articles on IT security threats and what to do to protect themselves from such threats.
- **Non-Governmental Organizations (NGOs)** – should lead IT security awareness campaigns and provide support for those who have questions or have security problems.
- **Schools and Universities** – should offer security awareness campaigns and integrate IT security topics into their computer courses curriculum.

In 2008, a new initiative has been proposed to fight cyber terrorism by bringing governments, businesses, and academia together from all over the world. The initiative, known as the International Multilateral Partnership Against Cyber Terrorism (IMPACT) [39], consists of the international partnership of more than 30 countries to study and respond to high-level cyber security threats.

## VI. CONCLUSIONS

As Middle East organizations expand their use of advanced security technology and use the latest hardware and software, it is becoming more difficult to conduct technical attacks. Similarly, the organizations are developing well-written complete security policies and hiring IT security experts that are also helping in reducing the number of possible attacks. Unfortunately, little is used to secure the weakest link, i.e. the users. This is pushing attackers to gain unauthorized access to information by exploiting user's trust and tendency to help. The paper discussed the security awareness among users in the Middle East and reported the findings of several IT security awareness studies conducted among students and professionals in UAE. It discussed the importance of assessing the security awareness by running controlled audits. Several key factors to help increase the security awareness among users were also presented.

## ACKNOWLEDGMENT

The author would like to thank Ahmed El Zarka, Arsalan Bhojani, Jamshaid Mohebzada, Maram Jibreel, Rayan Al-Omran, and Rim Zakaria for collecting some of the data.

## REFERENCES

- [1] Miniwatts Marketing Group, 2010 Internet World Stats. Available at: <http://www.internetworldstats.com/stats.htm>.

- [2] "B2C e-commerce volume exceeded US\$ 4.87 billion in Kuwait, Lebanon, Saudi Arabia and UAE in 2007", *Arab Advisors Group Report*, 2008. Available at: <http://www.arabadvisors.com/Pressers/presser-040208.htm-0>.
- [3] "Explosion in popularity of credit cards in the Middle East", Lafferty Group Report, 2007. Available at: [http://www.lafferty.com/pdffiles/Lafferty%20MENA%20cards%20-%20press%20release%20180607%20\\_3\\_.pdf](http://www.lafferty.com/pdffiles/Lafferty%20MENA%20cards%20-%20press%20release%20180607%20_3_.pdf).
- [4] "Leading UAE newspaper's website hacked", *Arabian Business*, 2008. Available at: <http://www.arabianbusiness.com/519982-leading-uae-newspapers-website-hacked>.
- [5] "Al Arabiya hit by Sunni-Shiite hacking war", *Al Arabiya News Channel*, 2008. Available at: <http://www.alarabiya.net/articles/2008/10/10/57995.html>.
- [6] "Batelco internet subscribers targeted by phishing attack", *Arabian Business*, 2008. Available at: <http://www.arabianbusiness.com/520459-batelco-internet-subscribers-targeted-by-phishing-attack>.
- [7] "NBK online banking customers targeted by phishing attacks", *Arabian Business*, 2008. Available at: <http://www.arabianbusiness.com/522781-nbk-online-banking-customers-targeted-by-phishing-attack>.
- [8] "UAE bank targeted in major phishing attacks", *ITP*, 2010. Available at: <http://www.itp.net/579059-uae-bank-targeted-in-major-phishing-attack>.
- [9] "Phishing raid empties bank accounts", *The National*, 2010. Available at: <http://www.thenational.ae/apps/pbcs.dll/article?AID=/20100405/NATIONAL/704049912&SearchID=73398739698056>.
- [10] "Internet virus infects Ministry of Education", *UAE Today*, 2010. Available at: <http://www.emaratayoum.com/local-section/accidents/2010-04-12-1.106891>.
- [11] "Riyad bank website hacked", *AMEinfo*, 2010. Available at: <http://www.ameinfo.com/235378.html>.
- [12] "Al Jazeera blames hackers for World Cup interruption", *The National*, 2010. Available at <http://www.thenational.ae/apps/pbcs.dll/article?AID=/20100613/NATIONAL/706129867&SearchID=73402848695382>.
- [13] *International Cyber Crime Law*. Available at: <http://www.cybercrimelaw.net/laws/alfabetic/s-t.html>.
- [14] F. Katz, "The effect of a university information security survey on instructing methods in information security", in *Proc. of the Annual Conference on Information Security Curriculum Development*, pp. 43-48, 2005.
- [15] M. Whitman and H. Mattord, "Principles of Information Security", *Course Technology*, 2<sup>nd</sup> edition, 2007.
- [16] APWG, *Phishing Activity Trends Report, Q4 2009*. Available at: [http://www.antiphishing.org/reports/apwg\\_report\\_Q4\\_2009.pdf](http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf).
- [17] "Emirates vulnerable to internet attacks", *The National*, 2008. Available at: <http://www.thenational.ae/apps/pbcs.dll/article?AID=/20080814/NATIONAL/420302377&SearchID=73402849474210>.
- [18] "UAE cybercrime squad gunning forward", *Arabian Business*, 2009. Available at: <http://www.Arabianbusiness.com/553470-uae-cybercrime-squad-gunning-forward>.
- [19] "Phishing website of bogus recruitment agency blocked", *Gulf News*, 2008. Available at: <http://gulfnews.com/news/gulf/uae/employment/phishing-website-of-bogus-recruitment-agency-blocked-1.84296>.
- [20] D. Timko, "The Social Engineering Threat", *Information Systems Security Association Journal (ISSA)*, January 2008.
- [21] P. Kumaraguru, S. Sheng, A. Acquisti, L. Cranor, and J. Hong, "Lessons From a Real World Evaluation of Anti-Phishing Training", in *Proc of the IEEE eCrime Researchers Summit*, pp. 1-12, 2008.
- [22] ISO/IEC 27001:2005 - Information technology – Security techniques – Information security management systems – Requirements. Published by *International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)*, October 2005.
- [23] NIST – An Introduction to Computer Security. Published by *National Institute of Standards and Technology (NIST)*, 2004.
- [24] G. Orgill, G. Romney, M. Bailey, and P. Orgill, "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems", in *Proc. of the 5<sup>th</sup> Conference on Information Technology Education*, pp. 177-181, 2004.
- [25] "Women 4 times more likely than men to give passwords for chocolate", *Infosecurity Europe*, 2008. Available at: <http://www.infosec.co.uk/page.cfm/T=m/Action=Press/PressID=1071>
- [26] R. Dodge, C. Carver, and A. Ferguson, "Phishing for User Security Awareness", *Computers and Security*, 26(1), pp. 73-80, February 2007.
- [27] New York State Office of Cyber Security & Critical Infrastructure Coordination, "Gone Phishing. A Briefing on the Anti-Phishing Exercise Initiative for New York State Government. Aggregate Exercise Results for public release", 2005.
- [28] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study", *Computers and Security*, 27 (7-8), pp. 241-253, 2008.
- [29] A. Marks, "Exploring universities' information systems security awareness in a changing higher education environment", *Ph.D. Thesis, University of Salford*, 2007.
- [30] Computer Industry Almanac Inc, *Wireless Internet Users*, <http://www.c-i-a.com/pr032102.htm>
- [31] J. Edney and W. Arbaugh, "Real 802.11 Security: Wi-Fi Protected Access and 802.11i", *Addison-Wisley*, 2003.
- [32] A. Kalbasi, O. Alomar, M. Hajipour, and F. Aloul, "Wireless security in UAE: A survey paper", in *Proc. of the IEEE GCC Conference*, 2007.
- [33] "Middle East RFID market heats up", *RFID Journal*, 2009. Available at: <http://www.rfidjournal.com/article/view/4618>
- [34] "RFID and Consumers: What European Consumers Think About Radio Frequency Identification and the Implications for Business", *Cap Gemini*, Paris, 2005. Available at: <http://www.us.capgemini.com/DownloadLibrary/requestfile.asp?ID=450>.
- [35] Z. Khattak, J. Manan, and S. Sulaiman, "Analysis of Open Environment Sign-in Schemes-Privacy Enhanced & Trustworthy Approach", in *Journal of Advances in Information Technology*, 2(2), pp. 109-121, May 2011.
- [36] UAE-CERT. Available at: <http://www.aecert.ae/>.
- [37] Saudi Arabia-CERT. Available at: <http://www.cert.gov.sa/>.
- [38] Qatar-CERT. Available at: <http://www.qcert.org/>.
- [39] International Multilateral Partnership Against Cyber Terrorism (IMPACT). Available at: <http://www.impact-alliance.org/>.



**Fadi Aloul:** Dr. Aloul is currently an Associate Professor of Computer Science & Engineering at the American University of Sharjah, UAE. Dr. Aloul holds a Ph.D. and M.S. degrees in Computer Science & Engineering from the University of Michigan, Ann Arbor, USA, respectively, and a B.S. degree in Electrical Engineering *summa cum laude* from Lawrence Technological

University, Michigan, USA. He is a Certified Information Systems Security Professional (CISSP). He was a post-doc research fellow at the University of Michigan during summer 2003 and a visiting researcher with the Advanced Technology Group at Synopsys during summer 2005.

Dr. Aloul received a number of awards including the prestigious Sheikh Khalifa, UAE's President, Award for Higher Education, the Semiconductor Research Corporation Research Fellowship, and the AUS CEN Excellence in Teaching Award. He has 80+ publications (available at <http://www.aloul.net>) in international journals and conferences, in addition to 1 US patent. His current research interests are in the areas of design automation, combinatorial optimization, and computer security. He is a senior member of the Institute of Electrical and Electronics Engineers (IEEE) and the Associate of Computing Machinery (ACM). He is the founder and chair of the UAE IEEE Graduates of Last Decade (GOLD) group.