UNIVERSITY OF TARTU
Institute of Computer Science
Cybersecurity Curriculum

Didier Dubey Suarez Medina

Assessment of Web-based Information Security Awareness Courses

Master's Thesis (30 ECTS)

Supervisor(s): Maria Claudia Solarte Vasquez
Co-supervisor; Raimundas Matulevičius

Tartu 2016

Assessment of Web-based Information Security Awareness Courses

Abstract:

Information security awareness web-based courses are commonly recommended in cyber security strategies to help build a security culture capable of addressing information systems breaches caused by user mistakes whose negligence or ignorance of policies may endanger information systems assets. A research gap exists on the impact of Information Security Awareness Web-Based Courses: these are failing in changing to a significant degree the behavior of participants regarding compliance and diligence, which translates into continuous vulnerabilities. The aim of this work is to contribute with a theoretical and empirical analysis on the potential strengths and weaknesses of Information Security Awareness Web-Based Courses and with two practical tools readily applicable for designers and reviewers of web-based or mediatized courses on information security awareness and education. The research design seeks to respond two research questions. The first on the formulation of a minimum set of criteria that could be applied to Information Security Awareness Web-Based Courses, to support their real impact on employee's diligence and compliance, resulting in eleven criteria for courses' assessment and a checklist. The second, about a controlled experiment to explore the actual impact of an existing course, in respect to diligence and compliance using phishing emails as educational tools, that reaffirms the theoretical assumptions arrived to earlier. The development of minimum criteria and their systematic implementation pursue behavioral change, emphasizes the importance of disciplinary integration in cyber security research, and advocates for the development of a solid security culture of diligence and compliance, capable of supporting the protection of organizations from information system threats. The results gathered in this study suggest that achieving positive results in the existing information security tests that follow security awareness courses does not necessarily imply that diligence or information security policies compliance are affected. These preliminary findings accumulate evidence on the importance of implementing the recommendations formulated in this work.

Keywords:

Awareness, information security, security policies, Learning Theories, Behavioral Theories, behavior, web-based course, social engineering, phishing email, security threat.

CERCS: P175 PHYSICAL SCIENCES - Informatics, systems theory

Hinnang veebipõhiste andmeturbe teadlikkuse kursustele

Lühikokkuvõte:

Veebipõhised Infojulgeoleku Teadlikkuse Kursused on tavapäraselt soovitatud küberjulgeoleku strateegiates, aitamaks konstrueerida julgeoleku kultuuri, mis oleks võimeline adresseerima infosüsteemi rikkumisi, põhjustatud kasutajate vigade poolt, kelle hooletus või eeskirjade teadmatus võib ohtu seada infosüsteemide vara. Veebipõhiste Infojulgeoleku Teadlikkuse Kursuste mõju uurimises esineb lõhe - need ei muuda osavõtjate käitumist olulisel määral, mis puudutab kuuletumist ja töökust, resulteerudes järjepidevates nõrkustes. Käesoleva töö eesmärk on panustada teoreetilise ja empiirilise analüüsiga Veebipõhiste Infojulgeoleku Teadlikkuse Kursuste potentsiaalsete tugevuste ja nõrkuste kohta. Samuti panustada kahe valmis rakendatava praktilise töövahendiga veebipõhiste või vahendatud andmejulgeoleku teadlikkuse ning õpetuse kursuste kujundajatele ja arvustajatele. Uuringu disain püüab vastata kahele uurimisküsimusele. Esimene on miinimumkriteeriumi formuleerimise kohta, mida saaks rakendada Veebipõhistes Andmeturbe Teadlikkuse Kursustes, et toetada nende tõelist mõju töötajate kuuletumisele ja töökusele, andes tulemuseks üksteist kriteeriumit kursuste hinnanguks ning kontrollnimekirja. Teine küsimus puudutab olemasoleva kursuse kuuletumise ja töökuse suhtes tõelist mõju uurivat reguleeritud katset, kasutades kalastusründe meile hariduslike vahenditena, mis kinnitab eelnevalt tehtud teoreetilisi oletusi. Miinimumkriteeriumi arendamine ning selle süstemaatiline rakendamine taotleb muutusi käitumises, rõhutab ditsiplinaarintegratsiooni tähtsust küberjulgeoleku uurimistegevuses ning propageerib kindla kuuletumise ja töökuse julgeoleku kultuuri, mis oleks võimeline toetama organisatsioonide kaitset infosüsteemi ohtude eest. Selles uurimuses näidatud tulemused pakuvad, et positiivsete tulemuste saavutamine olemasolevates infojulgeoleku testides, mis järgnevad julgeoleku kursustele, ei näita tingimata, et need töökust või infojulgeoleku eeskirjadele kuuletust mõjutaks. Need esialgsed järeldused koguvad tõendeid käesolevas töös sõnastatud soovituste rakendamise tähtsuse kohta.

Võtmesõnad:

Teadlikkus, küberjulgeolek, julgeoleku eeskirjad, Õppimisteooriad, Käitumisteooriad, käitumine, veebipõhine kursus, sotsiaalne korraldus, kalastusrünne, julegeolekuoht

CERCS: P175 REAALTEADUSED - Informaatika, süsteemiteooria

Table of Contents

1 Introduction

Information Systems (IS) security breaches have become a compelling concern for organizations due to the ever increasing rate of threats that can affect information assets. The way cyber criminals have improved their attack methods puts security information assets at a stake. Security systems management in enterprises have responded by strengthening technical security capacity, investing in advanced artifacts, software and also trainings designed to prevent, detect and protect information assets' Confidentiality, Integrity and Availability of being targeted from outside and inside. IS security breaches keep occurring regardless, affecting productivity, reputation and/or causing financial losses to organizations.

If organizations do not apply the required IS security measures sooner or later they may be targeted by malicious cyber attackers or become victims of their own employees whose lack of training or awareness regarding information technology security could create vulnerabilities that can open a free path for malicious attacks. The evolution on information technology has improved the ways data are stored, processed, shared and disposed, but at the same time it has increased vulnerabilities if security risks are not managed or/and mitigated.

The rapid evolution of information security threats encourage organizations to be up to date in relation to security updates and to be aware of the new attack vectors tendencies, which means that technical and managerial security measures must be implemented to face possible threats. Security measures can be based on technical automated, or organizational management solutions, focusing on protecting the organization's information assets from both: outsider or insider attacks. The literature review highlights that technology solutions by themselves are not enough to provide unbreakable levels of security so far, although research is conducted to develop smarter negligence alert programs. Regardless the great investment that organizations could make in technology security measures, security breaches keeps happening because misunderstanding or non-compliance with security policies. The previous reflections reflect this thesis's research problem that concerns employees who become Unintentional Insider Threats (UIT) for the organization, and more specifically those that are not influenced by training and awareness programs. These employees may fail to comply with security policies, which translates into continuous vulnerabilities, as even when warned in the Information Security Awareness Web-Based Courses (ISAWCs) about threats, they keep committing mistakes that can harm information assets.

The aim of this work is to contribute with a theoretical and empirical analysis on the potential strengths and weaknesses of ISAWCs. The scope of this work is focused in the way how security awareness messages are promoted and facilitated to the people through web-based training courses. Effectiveness for the purpose of this work will be understood as a positive change in participants' behavior towards information security policies compliance, and it will be measured in the corresponding section. Figure 1 presents the Research Questions (RQ) and how they are linked to the Research Tasks (RT) that were proposed during this study preparation phase.

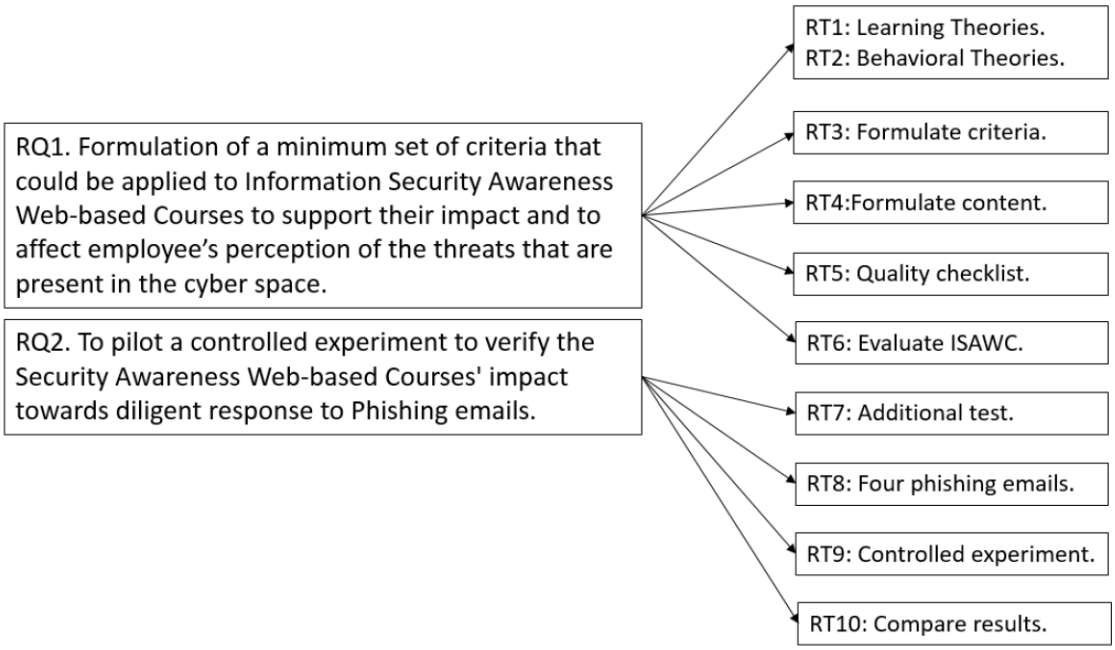


Figure 1. Research Questions and Task for the thesis (compiled by the author)

To achieve these aims 9 Research Tasks (RT) were set: RT1: Analysis of relevant documents and secondary data regarding to *Learning Theories* that can be applied to ISAWCs; RT2: Analysis of relevant documents and secondary data regarding to *Behavioral Theories* that can be used to shape human behavior towards security policies compliance; RT3: Formulate the criteria recommended to improve the impact of ISAWCs based on conceptual integration; RT4: Formulate the recommended content to be considered when designing ISAWCs; RT5: Develop a checklist to evaluate the quality of learning materials; RT6: Evaluate an ISAWC against the recommended criteria; RT7: Develop an additional test to test knowledge performance after taking an ISAWC; RT8: Develop four controlled phishing emails to be sent to a group of participants inside an experiment; RT9: Conduct an controlled experiment with two groups administering to them an additional test as well as exposing them to one of the most common and dangerous risks; and, RT10: Compare the experiments results to assess to which degree the ISAWCs affected the participant's behavior.

This work supports the opinion of cyber security experts and scholarly conversations that maintain that ISAWCs must be planned focusing not only on the current threats and how to mitigate them but also on the organization's mission, compliance with security policies, liability in case of security breaches, disciplinary sanctions, rewards and how to act or inform in case that an information security incident is detected. This is why this work proposes first that Learning and Behavioral Theories should be more carefully considered and incorporated in the planning of training courses to improve the way knowledge is promoted and facilitated, as well as shaping the participants' behavior towards information security policies compliance.

The present thesis is organized as follows: first, the theoretical foundations of awareness and education training programs will be studied; for this purpose relevant documents and secondary data on Learning and Behavioral Theories will be reviewed to establish their importance and identify the concepts that are chief to consider when designing ISAWCs.

Second, a conceptualization to improve the impact of ISAWCs will be presented integrating a careful choice of concepts from the Learning and Behavioral Theories reviewed. In this section, the set of criteria to improve the real impact of this courses will be proposed as well as the recommended learning materials that should be prepared when developing ISAWCs. An ISAWC will be compared against the set of criteria proposed and analyzed in connection with studies about web-based courses (taking into account the advantages and disadvantages of this modality over traditional face-to-face education). The third section of this work consists of a controlled experiment to collect empirical data about the impact of ISAWCs, the utility of the additional test, and to verify the suitability of the proposal for further studies and research on social engineering and training in cyber security. Methodology aspects will be detailed, the experiment that uses phishing emails is described, discussed and analyzed as well as the additional test announced previously. The fourth and last section of this thesis contains concluding remarks, reflects on the conceptual and practical contributions of the thesis, lists the perceived limitations of the research and underlines the avenues available for future research.

The outcome and main contribution resulting from this work is to inform on the development of those minimum criteria that are recommended to implement pursuing a change of behavior. The thesis insists on the importance of developing courses embracing theoretical applications of perspectives already consolidated in other fields, integrating concepts from diverse disciplines to be able to talk about genuine, dependable and palpable information security awareness. The same suggestion applies to building a solid and diligent security culture, capable protecting any organization from IS threats, while technical solutions reach a level of sophistication capable, without human intervention, of fully preventing these threats from arising

2 Conceptual Background and Theoretical Foundations

The present work argues that Information Security Awareness Web-Based Courses (ISAWCs) can be a powerful tool to raise employees' awareness towards compliance with security policies, it also argues that one course by itself is not enough to affect the behavior of all participants. Security awareness courses should be part of the cyber strategy of every organization nowadays. The courses must be aligned to security policies compliance, frequent so they can provide with sustained training, auditable, and be tested to verify their impact on the participant's performance and response. The integration of Learning Theories [1] [2], [3], [4], with Behavioral Theories [5], [6], [7], people learn, with already proven techniques that could influence human behavior. The relevance of online learning will be compared with the traditional classroom education also to help assessing learning outcomes. The awareness importance will be highlighted by revising International Standards that recommend awareness and training as an important tool to improve organizational security levels. To determine the set of criteria and learning material that should be considered when designing ISAWCs, an extensive theoretical research was conducted via literature review. In addition, one ISAWC was assessed to compare it with the recommendations and theoretical assumptions that were found the most relevant. The research design includes the collection of empirical data. A controlled experiment tested whether the participants' cognitive aspects (increased information and understanding) and their behavior towards information security policies compliance was affected by the course and to what extent. A group of participants were exposed to controlled phishing emails. An additional test was created to compare results and determine if a good test could be an indicator of raised diligence that means to verify whether that training as dispensed could achieve the intended behavioral change that it promises, namely, diligent response from trainees when facing real threats such as phishing emails.

Information security system breaches are commonly caused by errors in the security policies implementation, or human mistakes. Both involve human competences. As it was said by Bruce [8]: "Security is only as good as its weakest link, and people are the weakest link in the chain". For the purpose of this thesis the definition for UIT will be the one proposed by Team [9], "*An unintentional insider threat is (1) a current or former employee, contractor, or business partner (2) who has or had authorized access to an organization's network, system, or data and who, (3) through action or inaction without malicious intent, (4) unwittingly causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's resources or assets, including information, Information Systemss, or financial systems*."

To address the human factor is as important as any technical information security measure implemented to secure information assets. This understanding requires the Human Resources experts to be included in strategic planning discussions to implement the best practices recommended by International Standards on awareness [10], [11], [12], [13] starting with the hiring process to ensure that people are not only competent on the skills required for the job but also study their laboral background and planning an information security awareness program according to the organization's needs and the employee's skills. The awareness program must be auditable, periodic and continuously updated, so that the activities are repeated and changes in security policies and current threat trends are included at the same time that new employees are covered [14]. People's skills and competences need to be evaluated in the same way technology is, aiming to avoid negligent behavior that can harm the functionality of technical solutions and artifacts.

Constant changes in technology and the current trends on how information is communicated have opened path to different education methods such as television or radio courses which nowadays have been replaced by new online learning courses that give to the learners more possibilities of access to resources and materials as well as avoiding some barriers such as time or location to access to the learning materials. The real impact of online courses depends on the quality of instructional materials offered and the combination of the technology to be used with the implementation of E-learning theories. Relevant discussions about this topic are addressed in works by [1], [3], [2], [15].

2.1 Learning and Behavioral Theories

Investment in security solutions are increasing along with security risks and financial losses, which means that organizations need to address their situation regularly, to have a balanced return on security investment as suggested in articles such as *"A model for evaluating IT security investments"* [16]. To save resources such as labor costs, time and money, organizations have been changing educational methods and moving from traditional courses imparted in classrooms and led by a teacher, to Web-Based Trainings (WBT) that can be taken from the own employee's workstations or broadcasted from anywhere in the world. These are less expensive and seem not to affect productivity as much as the face-to-face courses would. WBT has changed the way knowledge can be transmitted. Learning environments are defined in time, place and space [1], extended this traditional definition to technology, interaction and control. WBT have adopted those six terms in the way that learners are not limited by geographic locations, they can determine the time and pace of the instruction, there are more materials and resources available, the technology can help to simulate real situations, the interaction between learners-to-learners and learners-to instructors can be done at any time by the use of email communication, chats or blogs, and give more learner control over the instructional presentation.

Although WBT seems to be a very effective way to share knowledge, not all researchers and educators agreed with the assumption that online education offers better results than traditional education. Online education has not always been so popular, Tom Conlon in his 1997 article *The Internet is not a Panacea* [17], stated that the skills of a good teacher cannot be underestimated, and that the internet is not the solution for difficult problems of teaching and learning [14], stated that media is just the vehicle that delivers instruction but do not influence achievement, only the content that is delivered can influence it. This means that the quality of the content to be taught, its design and the instructional techniques used are crucial to influence the teaching and learning processes.

"The best way to improve instruction is to begin with a research-based understanding of how people learn" [2]. Learning methods and cognitive development understandings have been in constant evolution in the way that learning theories have been also evolving from the Behaviorist, Cognitivist and Constructivist Theories to new ones, with diverse focus and techniques to enhance education systems. Researchers like Richard E. Mayer have contributed with Learning Theories to improve the education through technology media with theories like the Cognitive Theory of Multimedia Learning (CTML) where Mayer studied how the use of multimedia materials can affect the way people learn [4]. According to Mayer the CTML is based on three cognitive science principles of learning: (1)Humans can process information through two different channels (Visual/pictorial and auditory/verbal processing), (2) each channel has a limited capacity for processing information, and (3) active learning encompasses a coordinated use of cognitive processes such as selecting relevant words from the presented text or narration, selecting relevant

images from the presented illustrations, organising the selected words into coherent verbal representation, organizing the selected images to coherent pictorial representation and integrating new knowledge with prior knowledge. “The term cognitive refers to perceiving and knowing” [18].

In his research, Mayer also suggest two important principles to conceive a multimedia proposal for education: (1) coherent structure and (2) methodology; the message should provide guidance to the learner for how to build the structure. Mayer’s contributions settle down a series that need to be considered when creating online courses because this kind normally contain a significant amount of multimedia text. The real impact of this kind of courses relies on the quality of content to be taught and how this is structured in a multimedia format aiming to help the learners to learn how to apply lessons in practice.

One factor to be implemented is the reduction of the cognitive overload in multimedia learning. Cognitive overload occurs when processing demands evoked by the learning tasks exceed the processing capacity of the cognitive system [2]. Three cognitive processes described in Table 1 can contribute to increase the cognitive load. WBT must be designed in a way that cognitive load does not affect the learner’s learning performance. CTML is a very important tool that needs to be implemented when planning WBT.

Table 1. Three cognitive processes. Adapted from [19].

Process	**Observation**
Extraneous processing	Learner is exposed to cognitive processes that do not support the learning objective (when the material is presented in a confusing way or contains topics extraneous to the main objective).
Intrinsic processing	The learner is exposed to cognitive processing that is essential for comprehending the material (complexity of material gives more load).
Germane Processing	The learner faces deep cognitive processing such as organizing the material and relating it to prior knowledge (making sense of the presented material).

Achieving behavioral change is a complex task; a wide array of personal or environmental factors such as fear, mood, threat, economic conditions among others, can predispose behavior in a positive or negative way. Behavioral economics is an extensively field on its own, nested in the intersections between economics and the social sciences looking into ways to predict people’s behavior, and its impact on society. The Izec Ajzen’s Theory of Planned Behavior [5], for instance, helps to understand how people’s behavior can be predicted. Ajzen states that people’s intention captures the motivational factors that influence behavior, they point out how individual commitment forms, and how ingrained behavioral patterns could become. Table 2, indicates Ajzen’s three determinants of intentions.

Table 2. Ajzen's three determinants of intentions. Adapted from [5]

Intentions Determinant	**Observation**
Attitude Towards Behavior.	Referring to the degree to which a person has favorable or unfavorable evaluation of the behavior to be performed.
Subjective Norm.	Referring to the social pressure related to perform such behavior.
Perceived Behavioral Control.	Referring to the individual's perception of ease or difficulty to perform a behavior, the resources and opportunities available play an important role in the likelihood of behavioral achievement.

Tom Tyler and Steven Blader researched the effectiveness of regulation in the workplace by comparing two different strategies for achieving rule and policy compliance: an extrinsically oriented command-and-control model and an intrinsically oriented self-regulatory model [7]. The willingness to comply with information security policies can be influenced by both extrinsic and intrinsic motivators. Extrinsic motivators provide with external stimulus such as rewards to encourage the intended behavior or punishments to discourage the unwanted (sanction based). Intrinsic motivators in contrast, are self-regulatory mechanism that are developed when individuals perceive the legitimacy of the organization' rules and consistency with their own values. Both types of motivators are important in the success of employment regulations but employees are more likely to comply influenced by self-regulatory means. Herath and Rao coincide with these Tyler and Blader's findings. [20].

The General Deterrence Theory (GDT) has also been applied to security policies compliance strategies. [6] suggested that IS misuse intention can be more effectively reduced if employees perceive the severity, rather than the certainty of sanctions. Deterrence is defined as the preventive effect that the threat of punishment has upon potential offenders [21]. The theory suggests that employees are more likely to comply with security policies when they detect the severity of sanctions that could follow negligent behavior. Further studies have found that strategies based only on GDT do not always achieve the desired behavior in employees, but the consideration of tactics that derive from other theories could increase the desired compliance among employees [22], [23], [24], [25].

2.2 Face to Face Vs Online Education Study

The learning potential of online education and training vs. traditional face-to-face education are compared, taking into account that the present work narrows down to the impact of security awareness messages that are promoted and facilitated through web-based training courses. The online alternative has broken barriers facilitating accessibility to education from anywhere and anytime while interconnected using computing electronic devices and using a student-centered pedagogy. Updates can become available on real time and users/learners are supposed to have more control about their learning processes. Online learning is getting more acceptance at the same time that is beginning to substitute distance learning and traditional face-to-face classes [26].

Online education is gaining more acceptance worldwide thanks to the growing evolution of both technology and the internet which can give access to online material almost from everywhere and anytime. Allen & Seaman found that in the United States alone by the fall 2011, 6.7 million students were taking online courses, 572.000 more than a year before [27]. Online courses are being used in different levels of education from students in primary school to university and post-university level as well as training courses, for instance, the platform edX give free access to education to everyone with more that 5 million of learners in their community[1] or Coursera platform that provide access to education with worldwide partners and organizations [2]. The quality of online education has been extensively discussed in the literature and by practitioners such as [28], [29], [30], [31] and criticized by some who state that technology does not impact learning either positively or negatively, as found by a literature review conducted by Thomas Ramage in 2002 [32]. Katrina Meyer argues that some studies where the traditional and the distance models are compared, lack of deep analysis and are poorly designed. Such is the case of the book "No significant differences phenomenon" written by Thomas L Russell that reviewed 355 studies on distance education between 1928 and 1998 (only 40 of them include computer-based instruction), by comparing student outcomes using parameters such as grades [33]. This thesis relies on the assumptions advanced by Meyer's work who considers that higher grades/positive results obtained in a training course do not guarantee actual affectation of the learner's behavior.

Established the premise that online education is a prevailing method to facilitate knowledge when courses are designed according to the learning and behavioral theories revised, the work progresses onto the incorporation of institutional guidelines. International Standards that recommend awareness and training as a good practice to raise the organization's security awareness levels has been issued by [10], [11],[14], [12], [13], among others.

2.3 International Standards Study

International Organizations, aware of the negative consequences that security threats can cause, have developed different standards in which a set of "Best practices" for enhancing information security have been recommended. Drawing from the relevant documents consulted it may be stated that the following standards are common concerns about awareness training within the organizational information security strategy:

1. The National Institute of Standards and Technology (NIST) in its NIST Special Publication [10], provides a catalogue of security and privacy controls for Federal Systems and Organizations to protect organizational operations, organizational assets, individuals, other organizations, and the state from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors.
2. The Centre for Internet Security (CIS) developed the CIS Critical Security Controls for Effective Cyber Defence Version 6.0 of 2015 to illustrate about crucial management guidelines that every organization should be able to implement [11].
3. The Information Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) on its version ISO/IEC 27002:2013, emphasize the importance for Information Awareness trainings [14].

[1] https://www.edx.org/ Accessed on March 2016.
[2] https://www.coursera.org/about/ Accessed on March 2016.

4. The Information Systems Audit and Control Association (ISACA) developed the Control Objectives for Information and Related Technology (COBIT) Framework to provide guidelines and help organizations to create and assess Information Technology controls. In its fifth version, COBIT established seven enablers [12]. The enabler number 5 Culture, Ethics and Behavior highlights awareness as a Good practice to be considered.
5. The Payment Card Industry also have implemented standards to protect its IS security. The Payment Card Industry Security Standards Council (PCI SSC) developed the PCI Data Security Standard (PCI DSS) aiming at securing customer's data. In V 3.1 of 2015[3], the importance of awareness training is specified in the requirement 12.6 [13].

Theoretical developments also informs the elaboration of criteria formulated to design an ISAWC with higher impact and increased chances of success. The Sloan Consortium currently known as the Online Learning Consortium (OLC), an organization committed to the improvement of online education developed a quality enhancing framework[4].

Web-based trainings (WBT) are to be more than a collection of lessons, the content (besides than the quality) should be attractive to motivate the learner to navigate through the course materials, its completion, and implementation of the acquired knowledge. WBTs need a structure and should be designed in a way that offers the same or even more benefits than a traditional course could offer [35], in their book *The Online Learning Handbook: Developing and using Web-Based Learning*, refers to typical components found in a web-based learning environment. Table 3 summarizes those typical components.

Table 3. Typical components in web-based learning environments. Adapted from [34]

Typical component	**Observations**
Learning Event Plan.	Provides description and direction of the activities to be performed by the learner.
Learning materials presentation.	Instructional materials are presented to the learner.
Learning assessments.	Examinations will determine the learner progress, it is important to provide the learners with feedback regarding their outcomes.
Internet resources.	Can be used to assist the learner to complete the training event.
Instructional support.	Glossaries, Frequently Asked Questions, or forums can be created to guide the learners.
Technical support.	To support the learners in case of technical issues.

Another interdisciplinary model that combines various perspectives resulted from the research conducted by Ballew's et al, they worked on the development and delivery of WBT

[3] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf
[4] For more information refer to http://onlinelearningconsortium.org/about/olc-2/

for public health practitioners, and combined concepts from Information Technology, Health, Education, Business and the communication field [35].

2.4 Social Engineering and Phishing

One of the purposes of the present work is to use Social Engineering (SE) to support the learning material facilitated through ISAWCs. SE in some circles is known as the use of social interaction to obtain information about an user's electronic system or network, in many cases it will facilitate attacks that would not be possible through other means [36]. Mitnick and Simon defined SE as the use of influence and persuasion to deceive people by impersonating someone else or by manipulation to take advantage and obtain information without the use of technology [37]. Ian Mann says that it is used "To manipulate people, by deception, into giving out information or performing action" [38]. All definitions explain that in SE the source of information is a person. SE techniques can be shoulder surfing, pretexting, dumpster diving, online social engineering or phishing attacks, that is technology based or not [39]. Employees should be aware of the SE threat, but in practice this is not the case, as established the case study performed by Winkler, I. S., & Dealy, B. about social engineering threats [36].

The Anti Phishing Working Group reports that phishing does not show any signs of slowing in 2015[5]. [40] States that phishing is a SE technique that seeks to trick people into revealing classified information or installing malware on their electronic devices, targeting human vulnerabilities using social techniques that influence behavior. The phishing technique can be used as an educational tool in awareness training tests. Phishing has been studied by for a decade now by [41], [42], [43], for example.

Phishing has been used in different experiments to assess and improve information security awareness levels in different kinds of organizations [44], [45]. Recent experiments concluded that employees do not respond to phishing email according to security policies. It was the case of the audit report IT-AR-16-001[6] conducted in 2015 to assess the United States Postal Service's information security awareness training and phishing. Other studies had concluded similarly as the case of Dhamija et al where was demonstrated why phishing works [46].

The general considerations used by Dodge in a phishing experiment conducted in The United States Military Academy are a good example when implementing phishing experiments. Dodge's experiment succeeded in supporting a decrease vulnerability towards these attacks. [44].

2.5 Information Security Awareness Web-based Course Selection

In the second phase of this research, an ISAWC had to be selected, imparted, and assessed in terms of impact. "The Cyber Hygiene Course" (CHC) is the ISAWC chosen to proceed with this investigation. The CHC was commissioned by the Estonian and Latvian Ministries of Defence and developed by experts from BHC laboratory, Tallinn University of Technology and the Estonian and Latvian government. By the time this course was selected it was being implemented in different Ministries of Defence (MoD) from the European

[5] http://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf
[6] https://www.uspsoig.gov/sites/default/files/document-library-files/2015/IT-AR-16-001.pdf

Union such as Estonia, Latvia, Denmark, Netherlands, and Finland among others[7]. The course was based in its own Standard Document "Guidelines for Responsible IT-related Practices in Modern Organizations (Cyber Hygiene)" [47], when designed, the best practices recommended by national and international standards were considered. Mentioned guidelines aim to provide a universal approach to improve the information security by promoting a responsible human behavior to face the threats that can harm information assets.

The CHC was developed on the Integrated Learning, Information and Work Cooperation System (ILIAS). ILIAS is an open source Learning Management System (LMS) under the GNU General Public License (GPL) which means that end users are free to use it without any restriction. ILIAS has also been certified as compliant of the Sharable Content Object Reference Model (SCORM) in its versions 1.2 and 2004. ILIAS is a secure Learning Management System allowed to be implemented in NATO's intranet[8].

2.6 Evaluation of ISAWCs' Quality Learning Materials

Quality of learning materials may be said to be the top priority in teaching and learning projects. When the educational content is misleading or non-relevant to the course objectives it becomes frivolous [48]. The Multimedia Educational Resource for Learning and Online Teaching (MERLOT) considers among its evaluation standards three criteria to assess online materials, one of them is *"Quality of Content"* [49]. The course must combine accurate concepts, models and illustrations that are significant for the course objective. The design of learning materials must be audience centered, that is geared towards the learners' needs. Taking into account that ISAWCs are imparted mostly to adults, andragogy principles are applicable. Knowles et al, [50] affirmed that the six core adult learning principles are:

1. Learners need to understand: the Whys, Whats and Hows.
2. Self-concept of the learner: autonomous, self-directed.
3. Prior experience of the learner: resources and mental models.
4. Readiness to learn: life related, developmental task.
5. Orientation to learning: problem centered, contextual.
6. Motivation to learn: intrinsic value, personal payoff.

The use of verification techniques is recommended to keep in check that in creative processes the requirements of quality and formats are kept. Checklists are common tools that have supporters and detractors. Squires and McDougall claimed that checklist are limited by its focus on software attributes at the expense of consideration of educational issues [51]. But it does not necessarily have to be that way. Like Tergan states, they could be based on well-defined criteria and therefore become a practical method to evaluate of a course in the making [52]. In the design of learning materials, checklists help to iterate, and verify that quality requirements considered and implemented. P. Hosie et al [53], talk about the quality requirements of online courses in a framework of five categories as follows:

1. Accessibility: resources are logically structured and easy to navigate.
2. Currency: up to date.
3. Richness: learning material reflect a wide variety of perspectives.

[7] See more on this at: https://www.eda.europa.eu/info-hub/press-centre/latest-news/2015/05/19/initiative-to-mitigate-human-related-risks-in-cyber-space-signed
[8] http://www.ilias.de/docu/goto.php?target=cat_580&client_id=docu

4. Purposeful use of the media: well thought and chosen.
5. Inclusivity: diversity is integrated into the materials regarding social, cultural and gender factors.

Effective teaching and learning processes happen when courses rely on carefully designed learning materials that comply with consolidated quality standards. It can be argued that tools such as checklists are useful to facilitate the improvement of content and thus the ISAWCs' impact.

3 Conceptualization to Measure the Impact of ISAWCs

The methodology used to integrate the aforementioned theoretical foundations was a qualitative interpretative document analysis that relied on academic literature, and informal regulatory content such as manuals, codes of best practices and guidelines. This section develops these conceptual grounds, reasons and presents the criteria and standards to develop an ISAWC with real enhancing capacities impact. The way how people learn and how their behavior can be influenced must be considered in the same way other computer mediated courses are designed.

3.1 Interdisciplinary Connections

Developers of online learning courses and materials have to know how to capture the attention of learners, and maintain it throughout. Learning Theories are as relevant to design content as needed to conceive their delivery. As there is not one single Learning Theory to follow in all cases but many, a combination of concepts from several and a selection the most appropriate instructional to develop online training materials is the best current option [3]. A well thought mix attending both content and learning strategy could be effective to improve the learner's capacity to process information and become interested in improving capacity and skills. The media and method used in teaching and learning impacts the cognitive efficiency, so formulating proper questions becomes the most relevant embedding exercise. The questions are learning objects where valuable messages are contained [32]. Web-Based courses can support multimedia and interactive functions and thus, the consideration of the Cognitive Theory of Multimedia Learning for a balanced cognitive load can help prevent information overload that can affect cognitive process counterproductively. For instance, the multimedia content should be designed in a way that learners can focus on the message that is being transmitted by audio or video instead of getting distracted with subtitles, embellishments or unrelated pop-ups. Clearly, the content should support the learning objective without dispensing the learner with non-relevant information or noise, in the same way that the learning material should be presented in an understandable and intuitive format according to the learner's' capacity. For instance, training in the native language of the participants should be more effective than in a second or third, so translating the content is a rational investment in the betterment of courses.

As established earlier, technology by itself cannot yet guarantee a totally secure information environment, although current intelligent systems are being developed to reach that level. Advancements in machine learning, and artificial intelligence supported by big data studies could eventually render the human factor superfluous [54]. So far, it can be affirmed that the human factor should be also considered, and that it can only be partially addressed through security policies [55]. A simple example of common problems that arise relates to encryption. Information stored on mobile devices is protected with encryption algorithms, but when passwords are weak, predictable or written in a sticky note attached to the mobile device, then, the technology that protects the information stored on the mobile device is rendered useless [56]. Organizations should care about awareness, and consider informing their employees about the security policies they need to observe so they can begin implementing security measures to protect the organization's IT infrastructure. It is important that employees are not only aware about the security policies and guidelines in place, but also that they are convinced on that they should comply, and help to protect the organization's information assets against misuse, abuse and destruction [15]. Other aspect that needs to be considered is the fact that once employees had passed through an

information security training does not mean that policies, guides and recommendations will immediately be followed. User acceptance and internalization of information and knowledge/skills development must be viewed as gradual, and continuous improvement processes with long-term goals as M. Siponen noted [57].

Cybernetics and education share the same goal if to adhere to Hungerford & Volk [58] who state that: "The ultimate aim of education is shaping human behavior". When facilitating learning, courses should cater to behavioral changes and aspects beyond the cognitive. The TPB shows useful to guide the design of an awareness programme, because when the three determinants of intention are addressed, the likelihood of that employees will achieve the desired behavior is higher. In this case the desired behavior is compliance with information security policies and diligent action when facing IS threats. Employees need to know first, why the intended behavior represents a positive choice, for instance, briefs, workshops with examples, and incentives. Another factor can be explained as the sense of belonging, peer support and pressure. Employees need to feel that their colleagues as well as directors and staff within the organization also approve and comply with the same standards (Organization's security policies are to be implemented by everyone and the management needs to lead by example). Finally, once the legitimacy is established and employees' commitment achieved, the policy or rule has to be possible and easy to follow, (E.g. If the organization wants their employees to follow security policies, and management must transmit those policies in an understandable way, and provide software and hardware tools needed to comply)

When referring to security policies' impact, the common sign to look into is compliance. The employees' willingness to observe security policies measures the exposure level to security threats that an organization could face. To examine attitudes and emotions, attention have to be paid to the opinion and perception of the employees about the benefits of compliance as well as the consequences of noncompliance. Preventive measures include the creation of incentives and an environment that portrays the positive effects of due diligence and dutiful observance of rules and policies [59]. Security awareness education and training may be used to inform about security threats in particular and how to respond to these.

It is firmly established in the literature that volition or intention plays a crucial role regarding policy compliance in general, an individual's willingness to implement IS controls may be influenced by whether the asset to protect is perceived as worth the effort to be protected [60]. Information and security awareness training is at one end of the problem of cyber security threats while at the other end stands the individual with limited capacity to act rationally or acting based exclusively on the information that has obtained [61]. It is the intentions level the one that deserves greater attention, and where techniques involving concepts and theories from other disciplines can be attempted. Security awareness trainings can adapt to the specific policies that each organization follows and its own sets of incentives, reward and sanctions. It is noticed that leadership affects motivation on information security compliance and that leading by example is more persuasive than dispensing instructions alone.

The aspects mentioned above encourage the organizations to create understandable information security policies, but not only, also to find incentives of influence motivators to comply. While security policies, and information about current threats and incident handling are communicated, incentives to increase the due diligence should care to address personal, social and labour expectations. Behavioral theories revised such as the Theory of Planned Behavior (TPB) and the General Deterrence Theory (GDT), can be useful in the design information security awareness programmes. It can be claimed that these, when combined

with Learning Theories and applied to information security awareness programs, improve the impact of courses by influencing acquisition and use of the knowledge as well as the perception of legitimacy of regulations on information security, which in turn, facilitates commitment.

In summary, it is recommended to combine the GDT with TPB along with CTML to address both, the learners' cognitive process and to shape the expected behavior after the web-based course is finished. The integration of theories recommended are illustrated in Figure 2.

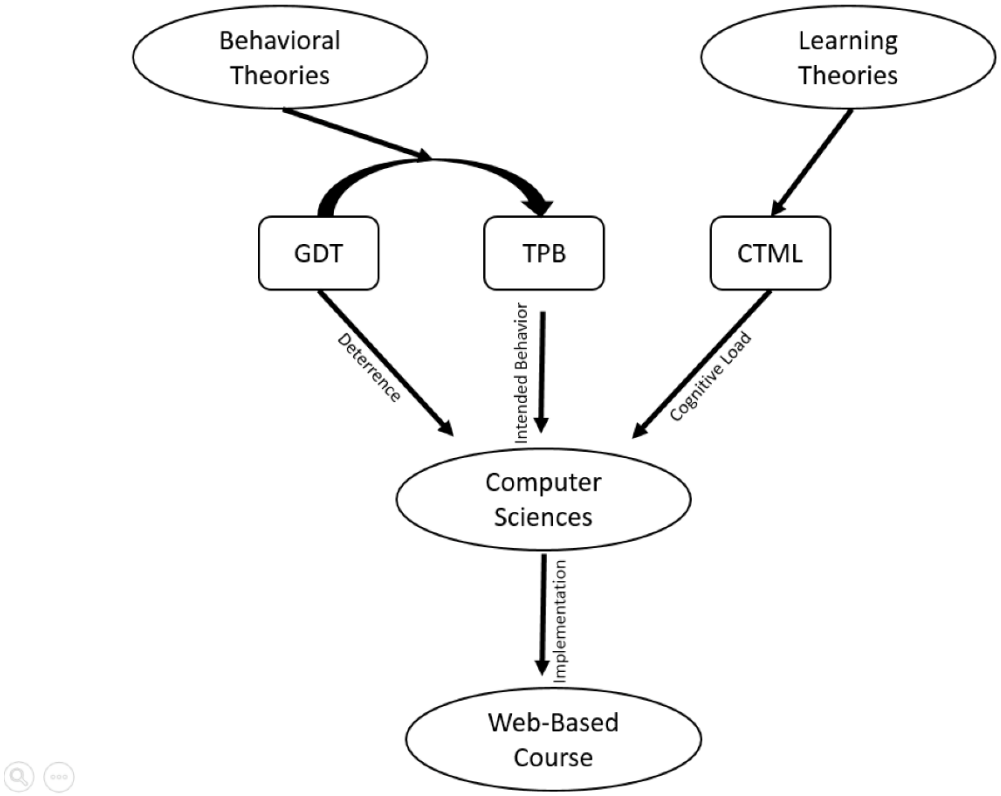


Figure 2. Integration of theories recommended.

3.2 Face to Face Vs Online Education

Face-to-face education herein referred to as traditional education, has been affected by the sociotechnical paradigm transformation that the telecommunications' development has imposed. The widespread use of internet and mobile technologies was the first step towards innovative educational technologies [23]. Blackboards and chalk are replaced by acrylic boards and markers, most recently already responding to the phase of the Internet of Things by smart boards that count with their own operative system and a variety of features embedded. Slide projectors were changed by digital video projectors with capabilities of reproducing not only slides but also video and audio improving the learning experience by using multimedia formats. New path for distance and asynchronous education are open, through which learners hold control of their learning process and experience, contrasting with the face-to-face educational format. Nowadays computer-mediated communication changed physical classrooms for virtual environments using Asynchronous Learning Networks (ALNs). ALNs facilitate the way learners exchange information and get support

without physical barriers using a student-centred approach [24]. Online education implies that learners are physically separated from instructors and connected through the use of a computer and network or internet link. The learning process is no longer fully held in traditional classroom where instruction is direct, time and place bound, typically consisting on face-to-face interaction, conducted in an educational setting and primarily following a lecture/note taking model [25].

A comparative analysis of the two educational models shows that they differ on their delivery and operative systems, and that web-based or at least mediatized (by technology) teaching and learning enjoys a growing popularity around the world. However, the quality of web-based and mediatized education is yet to be proven to match the levels reached in traditional formats. Research about the topic are still controversial [62], [63]. Technology modifies the way how knowledge is transmitted/facilitated, but the actual impact is affected by many other factors and variables such as age, motivation, education level, profession, experience, workload, availability of tools that facilitate the learning process, etc., that translate into the knowledge's use, processing and application. The positive aspects of web based and mediatized education benefit instructors as well as institutions. The repository of resources and pool of information that is created can be made accessible for long periods of time, be reused and distributed at ease, generate statistics as it is developed and be tracked for record keeping and monitoring. Grading progress can be made more efficient as well, with the use of technology [64].

The traditional training impact depends on the quality of material and content presented to the learners, both the skills and teaching strategies implemented by the instructor or the environment where the class takes place (temperature, noise, comfort, etc.), in the case of web-based mediatized learning environments, the impact relies on the quality of content selected, the techniques used when designed the online material as well as the learner's skills and personal qualities as motivation, independence and self-sufficiency as a learner and the goal of learning a degree [33]. Convenience and cost are factors that make web-based and mediatized learning more attractive. According to a research performed by Terry, desertion rates are higher in online courses than traditional campus courses, because online learning requires self-control and independent time management, rather than presential courses that require attendance to classes as precondition to pass [34].

The quality of learning materials in cyber security awareness, and the learner's commitment to process it are both crucial to obtain positive learning outcomes, security policies need to be designed carefully considering legal and ethical factors, employees are more likely to comply with them if they perceive its legitimacy along with ethical leadership [65]. Quality refers to the content relevance regarding the topic and its applicability. Good, usable content should be up to date, transmitted in a friendly way facilitating the learner's comprehension without degrading the subject or diminishing its importance. Learning materials should involve the learner by forcing him to think and apply the knowledge that is being transmitted, for example with practical exercises where the learner needs to take decisions in controlled scenarios created with threats that he/she could face in practice. Commitment can be articulated as an advantage to all, but first to the learner by showing the advantages or disadvantages of course completion and compliance with principles and regulations. The consequences of non-compliance with information security policies can go from simple reprimands to legal actions against the offenders and should be made clear. At the same time, good outcomes resulting from compliance must be stressed.

3.3 Compilation of International Standards Recommendations

The compilation of recommendations of this section focuses on standards that can improve web-based and mediatized methods for teaching, training and learning.

-Awareness and training (AT) was selected among the security controls established by the NIST Sp-800-53 that can be implemented by organizations [10]. This control addresses security awareness on policies, procedures, and role based security awareness training to final users. The policies should consider the purpose, scope, roles and responsibilities regarding to information security and the procedures are meant to facilitate the implementation of the information security training. The role based awareness training need to address specific security requirements of the organization, such as training to final users, specialists or system administrators or management.

-The importance of information security awareness training is highlighted in the Critical Security Control (CSC) 17: "*Security Skills Assessment and Appropriate Training to Fill the Gaps"* [11]. This control addresses the awareness training by analyzing employees' skills and behaviors searching for gaps that can harm information assets building a baseline roadmap for the employees, the training is to be delivered and implemented into a security awareness programs that is to be validated periodically to monitor their impact namely measurable improvements in awareness levels. Periodic test can be used to monitor the awareness level among employees as well to measure the training impact in the time.

-The ISO/IEC 27002:2013 highlighted the importance of awareness and training in control number 7.2.2 on information security awareness, education and training [10]. Employees of the organization and where relevant, other stakeholders should receive appropriate awareness education and training and regular updates about organizational policies and procedures connected to their functions and roles. Training material should be updated as much as needed, changes in security policies, procedures or new trends in security threats should be considered and included.

-COBIT Enabler number 5: "*Culture, Ethics and Behavior"* [12], suggests that awareness is necessary to create, encourage and maintain the organization's desired behavior, in this case, due diligence and compliance with the organization's security policies. Information security policies are a safeguard for information assets which can be jeopardized if employees do not comply with those policies.

-The Payment Card Industry in V 3.1 of 2015 specified the importance of awareness training in requirement 12.6 [13]. The implementation of an awareness program is recommended to educate personnel at least annually regarding compliance of security policies and procedures. The assumption is that untrained people, create vulnerabilities. Security safeguards and processes that have been implemented may become ineffective because of UITs. The training frequency is also highlighted admitting that key security processes and security policies can be forgotten or bypassed especially when training and education operate only at the cognitive level.

-Besides the good practices recommended by International Standards, the OLC has developed a framework to advance in the quality of online learning consisting in five principled Pillars that supports quality learning environments [66]. Table 4 summarizes the framework.

Table 4. OLC's Five Quality Pillars. Adapted from J.C. Moore 2005 [66]

Pillar	**Goal**
Learning Effectiveness.	The quality of learning online should meet or exceed, institutional, industry or community standards.
Scale (Cost effectiveness).	Institutions continuously improve services while reducing costs. Tuition rates provide fair return to the provider and best value to the learners at the same time.
Access.	All learners interested in online learning can have a reliable access.
Faculty Satisfaction.	Faculty are pleased with teaching online, participating and supporting online education.
Student Satisfaction.	Students are satisfied with their educational online experience. Learning outcomes should match the learners' expectations.

The overview that OLC made takes into account key aspects to consider when designing web-based courses. These are listed in the right column of the table. Each one of them requires amenable approaches that may differ but at the end can be integrated toward the same end: the facilitation of equal or better learning outcomes than those achieved through traditional classroom education [67].The column on the right explains the objectives of the key aspects that the pillars uphold.

Earlier, integrative and interdisciplinary research has already been conducted in this field. The study by Ballew's et al, is an example where concepts from Information Technology, Health, Education, Business and the Communication field were combined, resulting in a list of eight recommendations to design and implement a successful WBT course [35].

Table 5 summarizes the researchers' recommendations.

Table 5. Recommendations to design and implement successful WBT. Compiled from Ballew et al 2013 [35]

Characteristic	**Observations**
Formative research.	• Baseline knowledge, learning needs and technological capabilities must be determined before the WBT. • The organizational priorities should be evaluated and includes into the course design.
Design and layout.	• Clear and consistent format. • Visual appeal. • Proper use of multimedia formats. • Software compatibility with different platforms. • Flexibility with the pace of learning. • Implement functions to allow participants to learn from their mistakes.
Content.	• Include training background information. • Use concrete real-life examples (relevance). • Provide external links to access to additional information.
Interactivity.	• Functional features that allow users to interact with the training. • Add communication spaces for learners to interact with each other and with trainers.
Technical support.	• Enable technical support to help user's troubleshooting.
Feedback and follow up.	• Offer user feedback to participants during the training. • Allow users to contribute with feedback about the training
Marketing and promotion.	• Inform about the trainings through the organizations with posters, newsletter, brochures, staff meetings, etc.
Incentives.	• Grant certifications of completion. • Reward and/or recognition for course completion should be available.

The column on the left refers to the recommended concepts to design and implement a successful WBT course according to the Ballew's findings, the right column explain more detailed the components that should be considered for each concept.

Established that information security awareness represents an important tool for information security in organizations, and so is the need for periodical training and education offerings. According to recognized International Standards, awareness can be increased in various ways but web-based and/or mediatized (by technology) training constitutes a current trend that academic research is committed to enrich. All the frameworks consulted coincide on the importance of designing a detailed awareness training programme, aligned with the organization's information security strategy and policies, with attention to the sort of information to be protected as well as the procedures that have been already implemented for the same purpose. Employees' roles and skills must be also taken into consideration. Awareness trainings can be expected to have impact when offered periodically, and updated regularly. Continuous monitoring is required to keep instructional material in line with organizational policies and procedures. Materials and objects of study could and should be built on lessons learnt from information security incidents, so the importance of feedback is underlined [14]. Thomas R. Peltier says that an effective security awareness must take into account the company's mission and business objectives, written security policies and standards and matching the architecture of the security program with the infrastructure that supports it [68].

3.4 Phishing as an Educational Tool

Phishing can jeopardize organization's information assets easily, a negligent unaware employee is enough to create vulnerabilities and incur in information security breaches with catastrophic consequences. Phishing emails target people posing as candid and legitimate messages with intriguing and tempting offers. Typically, a phishing victim will click on links, reveal credentials or other sensitive information, feed with it into a fake website give out their credentials in a fake website, reply or download malware into their devices. This work argues that controlled phishing drills can be used to support learning and raise information security awareness among employees. In addition the method can be used to research on a diversity of field that converge in this activity: regulations, behavior, learning, human computer interaction and all areas that inform the computational social sciences. However, a phishing testing exercise should be planned in detail and carefully structured to prevent ethical or legal misconduct. Soghoian advises on this respect and suggests the following [69]:

- To inform and seek the assistance of the institutional review board as well as the information technology department or anyone else who can approve or desist about the experiment,
- Be aware of the laws applicable in the place where the experiment will be held or to the people that will participate,
- Consider terms of service of platforms and user accounts before accessing the site's useful data,
- Anonymize research data before publishing to protect the reputation of organizations that have been spoofed,
- Studies should not be conducted for profit,
- No experiment should cause any harm to participants and sensitive information must be protected.

Despite efforts by organizations to reduce the amount of incidents linked to phishing attacks, it is alarming that users are still deceived these fraudulent emails or spoofed websites [9] [46], Dhamija et al, researched the reasons why phishing works and concluded that scams happen due to:

1. Insufficient knowledge and information about computer systems and security indicators: some users do not understand the syntax of domain names and cannot differentiate fake Uniform Resource Locators (URLs).
2. Visual deception: Images and logos are copied perfectly.
3. Bounded attention: Users fail to notice all security indicators or their absence but once some are recognized the need for more caution is overridden [46].

Conducting phishing drills is a practical and telling tool that both researchers and organizations can use to educate or train people to be ready to face the threat and overcome the problems identified that can harm information assets. Jakobsson et al, stated that researchers commonly use three approaches to quantify phishing studies: surveys, in-lab experiments and naturalistic (field) experiments. Surveys usually underestimate damages, sometimes victims are unaware that an attack occurred or just are not comfortable disclosing that they fell for it. In-lab experiments can affect the outcome because of expectancy bias. Naturalistic experiments offer the most accurate outcomes, because they mimic a real attack, but this kind of experiment poses ethical concerns: if the experiment resembles accurately the reality, then the experiment represents a real fraud attempt itself [70]. Conducting this kind of experiments can represent a legal risk for the person or organization that sponsors it, they can get extremely close to the line that separates legal or fair use from copyright or trademark infringement, privacy violation, computer hacking and other wrongful actions that are associated to sending phishing emails [69].

3.5 Theoretical Contribution

Issues of quality assurance of learning materials arise for every institution, in regard to all formats of instruction and delivery. Two practical recommendations respond to these concerns, assuming that content quality is a chief responsibility of the developer of web-based and mediatized courses, during the design process. Tools such as the criteria recommended to improve ISAWC's impact and the Checklist on the quality of learning materials (Based on the content proposed by this thesis) consolidate the theoretical contributions of this study.

3.5.1 Criteria Recommended to Improve ISAWCs Impact

The topicality, importance and relevance of information security awareness and training has been demonstrated, and the existing standards revised. This section introduces a set of criteria that draws from the principles and standards already discussed, and that is recommended to conceive and design ISAWCs. The following contribution also integrates the notions of Learning and Behavioral Theories that were reviewed above.

[9] http://usa.kaspersky.com/about-us/press-center/press-releases/2015/kaspersky-lab-spam-and-phishing-q2-2015-report-exploiting-world

The criteria that this study encourages to be used to improve instruction and increase the impact of ISAWCs, are the following:

1. Course materials should be developed based on the organization's objective, audience needs and skills. Previous assessment need to be conducted to identify such needs. (Coinciding with Merlot"s standards [49])
2. Course materials should possess quality attributes that strengthen ISAWCs' impact towards diligent information security behavior such as being relevant and focused to the topic, up to date, clear and consider organization's security policies.
3. Behavioral theories such as the Theory of Planned Behavior and the General Deterrence Theory should be considered to address the participant's behavior towards compliance with security policies (similar to Hosie et al [53]). The TPB suggest to know what people are willing and be able to do and how behaviors are perceived by communities. For example a rule against the use of memory sticks at the office is more likely to be obeyed if employees see it as an acceptable expectation, if the rule is commonly observed by the majority and if other tools can replace the functionality of the memory stick, for instance cloud computing. In the absence of these legitimizing characteristics, rules and policies are unlikely to be observed.
4. Web-base course materials should have passed a usability test and hence exploiting the full potential of the medium.
5. Learners should be actively involved in the learning process. Practical exercises or labs, according to real life scenarios and flipped classrooms for online audiences where learners are producing content themselves, are examples of involvement. Learning by doing.
6. The interoperability of technical features and availability to support should be guaranteed (An online helpdesk should be active to guide users to troubleshoot any technical issue)
7. Communication between instructors and peers needs to be reliable.
8. The CTML concepts should inform how learning happens through computer systems (mediatization).
9. Feedback should be recorded during and after the course completion for continuous updates.
10. The course evaluation should be auditable. Organizations should be able to use information about their employees' performance and implement changes needed to improve the information security environment.
11. Periodicity is key. ISAWCs must be available frequently, for example twice a year. It reinforces the cognitive aspects of the training and consolidates perceptions on the importance of policies and regulations. It keeps employees up to date about information security policies as well as on security threats. Figure 3 illustrates the recommended web-based course structure.

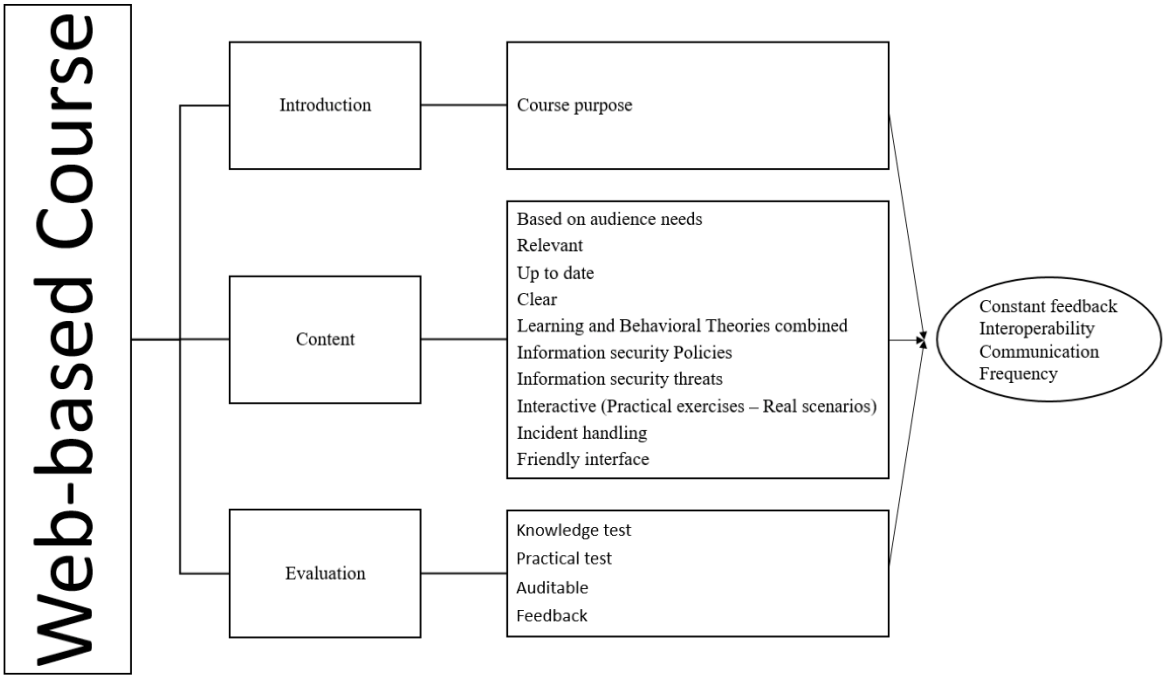


Figure 3. Recommended web-based course structure.

The recommended web-based course structure divides the course in three components (Introduction, Content and Evaluation) were the criteria recommended to improve ISAWCs impact should be implemented assuring constant feedback, interoperability and communication during the whole course. The course should be designed to be updated and to follow a periodicity.

3.5.2 Recommendations on ISAWCs' Quality Content Development

The task of determining high quality study materials that can strengthen ISAWCs' impact on participants regarding diligence and compliance should aim at proposing substance with improved quality attributes, and be presented as legitimate. These are the two general qualitative and nominal measuring categories relevant to this study. The learning material selection process and a checklist for self-assessment and verification purposes will be discussed further below.

3.5.2.1 Learning Material Recommended

Johnson stated that to rise information security awareness, course should cover first information on the organization's security policies, then, the major risks than can jeopardize information assets together with other current threats, basic countermeasures as well as preventive tactics (good use of security passwords, incident reporting and handling), and proper internet, intranet and messaging systems and risks. [71].

Other researchers such as Kruger and Kearney spoke of six critical areas or "Golden Rules": strict adherence to company policies, secure management of passwords and pins, secure use of internet and email, caution when using mobile devices, information security incident reports, and responsibility and accountability, understanding on that all actions carry consequences [72]. Among the topics recommended by the NIST are: Password use and management, protection from viruses and malware, visitor control and physical access to spaces, spam and unknown email attachments, internal policy and implications of non-compliance, access control, mobile devices security, changes in system environment (e.g.,

water, fire, dust or dirt, physical access), social engineering techniques, incident handling, use of encryption and transmission of sensitive information [73].

The European Union Agency for Network and information Security (ENISA), in its report ENISA Threat Landscape 2015 [74], presented the current threat trends in a list of the prevailing 15 cyber-threats based on a comparison of those identified in the period 2014/2015. Table 6 represent the list of threats and thematic categories, and showing which involve directly end users and can be mitigated through awareness training.

Table 6. Current threat landscape, adapted from ENISA Threat Landscape 2015.

No.	Threat	Thematic Categories	Mitigation Strategy
1	Malware	Protection from viruses and malware [72].	Technical / User awareness
2	Web based attacks	Secure use of internet, [71] [72].	Technical / User awareness
3	Web application attacks	Secure use of internet, [71] [72].	Technical / User awareness
4	Botnets	--	Technical
5	Denial of Service	--	Technical
6	Physical Damage/theft/loss	Changes in system environment [73].	Technical / User awareness
7	Insider threat (malicious, unintentional)	Access control, social engineering, visitor control and physical access to spaces [73].	Technical / User awareness
8	Phishing	Secure use of internet, [71] [72]. Secure use of mail [71], [72], [73]. Social engineering[73].	Technical / User awareness
9	Spam	Secure use of mail [71], [72], [73].	Technical / User awareness
10	Exploit kits	--	Technical
11	Data breaches	Secure management of passwords and pins [71], [72], [73]. Visitor control and physical access to spaces, access control [73].	Technical / User awareness
12	Identity theft	Secure management of passwords and pins [71], [72], [73]. Visitor control and physical access to spaces, access control [73].	Technical / User awareness
13	Information leakage	Secure management of passwords and pins [71], [72], [73]. Visitor control and physical access to spaces, access control [73].	Technical / User awareness
14	Ransomware	Secure use of internet [71], [72].	Technical / User awareness
15	Cyber espionage	Access control, social engineering, visitor control and physical access to spaces [73]. Secure management of passwords and pins[71], [72], [73]. Social engineering [73].	Technical / User awareness

The middle column on the table shows the thematic category where the threat would belong, according to theory, while the last is added to denote the type of strategy that can be used for mitigation. By technical is meant the intervention that is hardly connected if at all with awareness training because it does not require only the involvement of end users or does not depend on due diligence or compliance with policies. Most of the threats that can be reduced with improved security awareness training, and education as shown on the table above, the corresponding to ENISA 1-3, 6-9, and 11-15. The learning material recommended must concern, first of all information on all the threats but extend on those that can be managed by the learners. This is a suggestion that also has to do with relevance as a quality attribute, and the first criteria on impact explained in section 3.5.1., above.

Bulgurcu and Cavusoglu stated that Information security policies are the set of roles and responsibilities that guide employees to safeguard the information assets of their organizations [59], in fact, it can be claimed, that intended to shape behavior and the creation of a diligent and compliant information security culture. For that reason the second primordial recommendation in respect to the choice of learning materials is the inclusion of organizational security policies. The rest reflect the mainstream considerations that researchers agree upon: passwords security, behavior when managing internet or emails, Incident handling, current information security threats and social engineering techniques. Table 7 shows the complete list of recommended content to be included in an ISAWC.

Table 7. Content recommended to be included in an ISAWC

Thematic categories combined	Observations
Information security policies.	• What is and is not allowed regarding to ISs manage in the organization. • Consequences of compliance and noncompliance of security policies.
Password security.	• How to create strong passwords. • How to securely store and manage passwords.
Internet and emails.	• What is phishing, how it works and how to avoid it? • Proceedings with unwanted emails. • Malicious URLs and spoofed websites.
Social networks.	• Threats, and consequences of using social networks without precaution.
Social engineering.	• Definition, techniques and recommendations to avoid it.
Incident handling.	• What to do in case of information security incident and who to report.
IS threats.	• Current threats and how to face them.
USB related risk.	• Risks of using USB sticks.
Wi-Fi Risk.	• Risks of using open Wi-Fi.
Securing information.	• Use of passwords and encryption. • Backups.
Self- discipline.	• What to do when leaving the workstation. • Information cannot be at open sight. • Use of shredders. • Security when printing or copying documents. • Precautions when sending emails (CC and CCO). • It is not recommended to store organization's information on personal devices. • Etc.
Bring your own device.	• Personal devices are more exposed to threats because lack of security measures or freeware use.
Communication culture.	• Report to Information security officer about suspicious behaviors in the systems. • Friendly communication with IT specialists.

The content categories on the table belong to a combination of the the themes grouped by ENISA [74], Johnson [71], the "Golden Rules" by Kruger & Kearney [72], and the list by Wilson & Hash. The observations' column expand the categories in some detail. Information security policies, together with techniques for security risks mitigation as content and under the subthemes of the table are consistent with criteria on impact 1, 2, 4 and 5. from the section 3.5.1. These recommendations do not stand alone, they can be associated with principles and assumptions that derive from the CTML and this way proceed with the interdisciplinary connections this thesis advocates for. For example, the amount of content has to be carefully weighed, not to overload the learners. The same goes for the length of the training sessions. The longer it extends, the more it is likely to result in ineffective training because excess, tiredness and boredom would diminish the attention and retention span of participants [75].

Following the recommendation on the selection of material systematizes the process of design and preparation of courses and can be a valuable guide if the relevance of the topics and the thematic categories are regularly updated. However, there are no guarantees of success in a vacuum, and effectiveness measurements can become statistically meaningful only after testing, experimentation, implementation, or all of the above, if research on the field continues.

3.5.2.2 Checklist on the Quality of Learning Materials

To revise the content of the final product, a self-assessment questionnaire that can be used as research evaluation tool when or if implemented with a Likert scale, was designed considering andragogy principles, the criteria recommended to improve ISAWCs' impact and the framework proposed by P. Hosie et al [53]. Table 8 illustrates the proposed checklist.

Table 8. Learning material quality checklist.

No	Statement	1	2	3	4	5
1	The learning material was prepared according to the audience needs.					
2	The learning objectives are understandable (Why, what and how).					
3	The user interface is easy to manage.					
4	The learning materials are relevant to the course objective.					
5	The organization's information security policies were considered.					
6	Incident handling regarding to current information security risks were considered.					
7	The learning materials are up to date.					
8	The learning materials involve the learners with practical exercises.					
9	If practical exercises are considered, they are applicable to real life situations.					
10	The multimedia materials were used according CTML.					
11	The course evaluation is auditable.					
12	Communication tools are embedded.					
13	Feedback was considered through the course.					
14	The learning materials avoid any kind of discrimination. (Sex, religion, age, culture, etc.)					
15	The course is designed to follow a periodicity.					
	Comments.					

The quality level could be measured using the Likert scale of 5 points where 1 is poor, 2 is fair, 3 is good, 4 very good, and 5 is excellent.

The checklist consists of 15 Lines that capture the content and selection of learning materials recommendations as follows: Lines 1, 3-4, 7-13 and 15 stem from criteria recommended to improve Information Systems Awareness Web-based Courses' impact from section 3.5.1; line number 2 was gathered from recommendation number 1 stated by Knowles et al [50] in section 2.6; line number 5-6 were compiled from the Content recommended to be included in an ISAWC from section 2.5.2.1; line 14, although is not mentioned in the recommended criteria or content, was added to the checklist because it addresses the audience and their needs.

3.5.3 Assessment of an ISAWC against the Recommended Criteria

The ISAWC selected for the assessments that the present paper proposes is a Cyber Hygiene Course (CHC). These type of courses give organizations an overview of the employees' awareness and compliance patterns, and statistical information that can be used for the improvement of information security levels. The CHC is expected to raise the employees' awareness levels or diligence, and with it increase the number of reports on information security incidents/breaches. That, in turn, would mean that the detection capacity of the employees and their commitment to organizational policies and regulations have increased.

The CHC selected follows the principles set forth in the Guidelines for Responsible IT-related Practices in Modern Organizations [47], the course address four areas: (1) Categories of personnel which address potential trainees into 3 categories: Users, Managers and Specialists. Only the Users category of personnel section of the training is under observation in this thesis. (2) Areas of concern or the so called Threat Vectors, they are in constant change, the current situation should be analyzed to know actual problems to deal with. If users are irresponsible the threat vectors will be more effective. (3) Human risk behavior, this is a key section with typical scenarios that illustrate and discuss some simple actions that cause problems. These representations match threat vectors and many more elements of the training content. (4) Training shall ensure that all the human behavioral risks are addressed and mitigated.

The CHC conceived for users is divided in three modules:

1. A questionnaire with 12 questions that tests the initial awareness level of participants. Statistics are also gathered at this point.
2. The core materials of the course, where the threat vectors and the human risk behavior are addressed in 14 chapters. Every chapter begins with an introductory video showing information security breach situations, and follows with questions. Feedback is provided when answers are mistaken, whereas when answered correctly the user can gain access to the chapter content.
3. A test that can evaluate the participants' cognitive capacity with a traditional scoring system. Scores in numbers and percentages are shown after the test is completed, and a function is enabled for participants to learn about their mistakes..

It is unlikely that this test can be fully relied upon to understand whether the capacities of participants were enhanced or as a conclusive indication of commitment to policies and regulations.

The CHC was evaluated against the criteria recommended earlier on this paper, using the checklist from section 5.2.2.2, because it has already integrated all recommendations and can refer to all thematic categories. Table 9 illustrates the results of the assessment.

Table 9. CHC coincidences with the criteria and standards recommended. Use of the checklist.

No	Statement	1	2	3	4	5
1	The learning material was prepared according to the audience needs.	X				
2	The learning objectives are understandable (Why, what and how).					X
3	The user interface is easy to manage.					X
4	The learning materials are relevant to the course objective.					X
5	The organization's information security policies were considered.	X				
6	Incident handling regarding to current information security risks were considered.			X		
7	The learning materials are up to date.					X
8	The learning materials involve the learners with practical exercises.	X				
9	If practical exercises are considered, they are applicable to real life situations.	X				
10	The multimedia materials were used according CTML.					X
11	The course evaluation is auditable.					X
12	Communication tools are embedded.					X
13	Feedback was considered through the course.					X
14	The learning materials avoid any kind of discrimination. (Sex, religion, age, culture, etc.)					X
15	The course is designed to follow a periodicity.					X
	Comments.					

The content verification was performed as a research task but the results were triangulated with the outcome of the same revision by two other cybersecurity experts and a trainer in adult education, with credentials in andragogy. Despite the different perspectives all of them made the same annotations, as indicated in the table 9.

The CHC fails to conform to the recommended criteria in four aspects. First, the material learning was not designed as the result of previous assessment conducted in order to identify particular organizational needs. Second, the regulations and policies of organizations on information security cannot be adopted by the training model either. The CHC's philosophy conforms to an universal scheme applicable to any kind of organization. This work disfavors universal approaches that by definition are inconsistent with recommendation number 1 and 2, from the criteria recommended to Improve ISAWC Impact. These were consolidated

recommendations inspired on the literature that tackle on people's diligence and on the clear understanding about the status of the organization and security compliance patterns at all times. The matter was strongly emphasized in the corresponding section 3.5.1. Regular assessments help to keep the situation in check for an accurate overview of the obligations, needs and interests of the parties involved, and thus, are necessary, or the course structure should be dynamic. The third and fourth mismatches, show that the CHC ranked low in the scale because it does not actively or sufficiently involve the participants. The questionnaire that features in the first module is limited in reach and seeks to obtain information, rather than input, then delivers the learning materials and finishes with a final test. Practical exercises or labs where not included in this initiative. This contradicts recommendation 5 from the section 3.5.1. That relates to the concept of learning by doing and the newest trends in education and training be it mediatized by technology or not: co-creation, flipped classrooms, the learner generates most content, project based learning, and so on.

The remaining of the course appears to comply satisfactorily with the rest of the criteria. During the revision there was no need to use very precisely the scale because the purpose was not to gather data for statistical or quantitative analysis. However with minor adjustments this can be turned into a questionnaire for expert evaluation and continuing research of such type.

The course materials were relevant in the use of examples that were topical and recognizable as well as updated to the most current threats available (recommendation 2 - partially). In terms of the usability aspects of the interface, although no special test was used, no difficulty was salient during the revision, navigation was flawless and the functionality of the platform and the course arrangements seemed intuitive and well mapped, user-friendly (recommendation 4). The course was compatible with different web browsers and performed well in all of them (recommendation 6). The communication between participants, instructors and peers, occurs through an internal mail service component (recommendation 7). The course also complies with the postulates of the CTML; learning materials are not overloaded with irrelevant information, unnecessary subtitles or complicated formats that could negatively affect the cognitive process (recommendation 8). The TPB was considered, the typical scenarios used to exemplify common mistakes committed by unaware users were designed to show ordinary behaviors using different characters trying to avoid racial or any kind of discrimination, in the same way the behaviors recommended by the course are commonly accepted to safeguard information assets, participants can have control over the recommended behavior considering that the course also advise the participants how to comply (recommendation 3). Feedback was constantly available throughout the text and during the course, the chapters end with a question and after each participant's answer an information box appears explaining why the answer is correct or incorrect, once the final test is completed the participant receives a summary as well as a reflections per question on the expected answers, so the participant can have a detailed report on performance (recommendation 9). The organization can access participants' individual reports and collect group results on the whole or about specific topics to study and monitor potential breaches, vulnerabilities, negligence patterns and security gaps. These observations are the first step in addressing prevention challenges, preparing to confront problems, and shielding the information assets against detected and foreseeable vulnerabilities (recommendation 10). The course can be performed periodically, although the exact frequency should be established by the organization based in the analysis of the participants' performance and the security gaps discovered (recommendation 11). Periodicity in the training is important to influence a behavioral change, the CHC is not long

enough to repeat messages inside the course content, and for this reason regularity on the trainings and continuous education is suggested.

Traditional learning principles cannot be put aside, interaction with the instructor is necessary at least at the beginning and the end of the training session in order to give guidance and resolve questions regarding to both the process and the content of the course.

If ISAWCs are consciously and systematically designed, centered on the users and on the organization's needs, they could be powerful prevention tools to mitigate information security breaches occurrence. Awareness about information security threats could be raised and also commitment to rules and policies issued by the organization in connection to ethical codes and legitimacy. Learning materials included in web-based or mediatized courses should be kept current, relevant to the course objective, in-depth, culturally sensitive, and should hold the same quality level and scope and of traditional face-to-face courses [67].

4 Information Security Awareness Web-Based Course Assessment

An experimental study was designed to produce an empirical contribution that complements this study, suggesting an approach to the use of diagnostic tests in determining the effectiveness of ISAWCs. The proposal is exploratory at this stage and does not intend to confirm hypotheses. More experiments of varied content, using the same testing model are necessary to reach conclusive results. However, the preliminary outcomes obtained from this limited exploration are consistent with observations made earlier, on that it is unlikely that this additional test, or any other alone, can determine if the diligence of participants was enhanced or provide certainty about people's commitment to policies and regulations.

The experiment was designed to indicate an option to research effectiveness with an Additional Test (AT), and to help the evaluation of impact of an ISAWC while at the same time looking into the value of phishing as educational technique. A convenience group, divided into two subgroups that underwent training during the same period of time, but were exposed to moot threats and given the AT (Appendix I) in different opportunities. This design permitted to observe and compare the responses of the subgroups and collect data regarding changes in the participants' behavior. The experiment was telling of the many avenues of research and implementation of educational technologies that are open in the field of cyber security awareness training and education.

4.1 Methodology

The type of data that the research task at hand needs to collect to answer the research question 2, benefits from using experimental methods. The methodological approach in this phase of the research was quantitative. Because the experiment is exploratory, it may be considered a pilot testing exercise, especially taking into account the limitations imposed by the convenience group composition, the time constraints and the impossibility to conduct additional experiments in comparable and dissimilar settings. More data would have also allowed the use of more sophisticated analytical tools such as probabilistic analysis (Bayesian). Two assessment mechanisms were linked to this experiment, both resulting from the planning and design of the research and unique. The first was an Additional Test (AT) on the cognitive aspects that the ISAWC was supposed to consolidate. The other involved the careful use a common threat to have an account of the signs of behavioral changes that the course expects to motivate.

4.2 The Additional Test

The AT is an original instrument, an evaluation tool drafted exclusively for the purpose of this exploration. The AT consists of 20 questions that address only cognitive aspects such as the users' understanding of basic information security concepts. Understandably, people who are not informed could be assumed to be more susceptible to security threats. Lack of familiarity with terms and conceptual understanding could also render some additional awareness material useless. For example, a poster warning about phishing emails will not have the same effect if users do not know what the term phishing means, or if they are not familiarized with the activities that can be affected by it [76]. The list of threats on the 2015 security report by ENISA, the content of the CHC that was the ISAWC used for the experiment, and the theoretical assumptions revised in section 3 were consulted to compose an accurate and comprehensive instrument.

The AT was drafted in a questionnaire format posing only closed questions, in consideration to the needs and interests of the audience as well as the type of verification sought after. Closed questions do not allow the respondent to speak his mind, but it was considered that the students are not yet experts or experienced enough as to be able or willing to contribute with long reflections. Also, close questions are easier to process and analyze [77]. The questionnaire included three simple open questions regarding demographics (age, sex and semester of enrolment) that required unambiguous answers, and 20 multiple choice questions weighed each with 5 points for a total of 100. The main capacity of this test was to corroborate vocabulary proficiency and application to different scenario situations related to information security.

4.3 Threat Experiment

The ISAWC selected to perform the experiment was the CHC, a course on cyber hygiene that aims "*to provide a universal approach for a better information protection by promoting responsible human behavior to avoid exposure to the threats emanating from the cyber space*" [47]. Access to the entire course was granted by the developer[10] but the relevance of this choice is highlighted by the widespread use of this ISAWC in trainings across Europe, by organizations and institutions such as Ministries of Defense[11]. The theoretical part of this study regarding the content quality, impact and components uncovered that the CHC conforms to certain learning theories postulates and principles, as well as to some formulation standards, but fails to adhere to others (see section 3.5.3). For instance, the course did not appear to be adaptable to the specific needs and particularities of the audience and there was no clear evidence of active involvement of the participants in the development of the course itself (co-creation or responsiveness based on feedback). However, the need for empirical evidence is acknowledged in this work, thus a search for data should be added to the conceptual revision on theoretical grounds already completed.

4.4 Design and Description

The CHC promises to be an effective ISAWC that is supposed to increase understanding of participants about information security and most importantly to change behaviour, promoting diligence, and compliance, in particular in the presence of threats. Earlier in this section the assumptions on effectiveness were problematized. It was said that it is unlikely that a follow up test of an ISAWC could be fully relied upon to understand whether the capacities of participants were enhanced or as a conclusive indication of commitment to policies and regulations. One of the main assumptions that has been put forward by this study is the need to add reflection and monitoring mechanisms that would justify and corroborate the impact of the courses, and eventually inform the development of effectiveness' measuring instruments and research. Consequently, the experiment's purpose led the design of its organization and content towards the collection of data that could permit the evaluation of the impact that the course could have had over the participants on cognitive and behavioral aspects, completing with it the RT8.

[10] The CHC was developed by experts from BHC laboratory, Tallinn University of Technology and the Estonian and Latvian government.

[11] See more on this at: https://www.eda.europa.eu/info-hub/press-centre/latest-news/2015/05/19/initiative-to-mitigate-human-related-risks-in-cyber-space-signed

A convenience sample group that initially consisted of 101 students was chosen from the bachelor level population that were enrolled in Cyber Security studies at Tallinn University of Technology (TTU), but not necessarily belonging to that specific minor within the Computer Sciences program. The group was divided in two subgroups (Group I and Group II) 40 participants belonged to Group 1, and 41 formed Group II. 20 students gave up a portion of the experiment, so the sample was reduced to 81 participants. Whereas the two groups were assessed in different times, using the same evaluation tools, all of the participants had to take the CHC while available during the same period of time.

The phishing experiment conduction conforms with Soghoian's recommendations [68]. Four controlled phishing emails to be distributed in two waves, were created. The first wave (Phishing emails No.1 and 2) was sent only to Group I while the second wave (Phishing emails No. 3 and 4) was sent to both groups. The participants' behavior who have not taken the CHC was evalauted after the first phishing wave; these results were also compare with the outcome of the second phishing wave that was sent after both groups had completed the CHC. Some variations should be noticeable as to assert the extent to which the course had impact on the student's diligence and compliance. The AT, on the other hand, was used to assess the participants' knowledge only and administered to both groups. The test results looked into cognitive improvements by comparing the results obtained before and after the training course. The CHC was left an assignment for course ITX0040, and the students could cover all materials on their own considering that conducting the experiment in a computer lab could had affected the experiment results because the participants would know exactly when and how they were tested. Participants were exposed to the phishing emails without warning to conduct the experiment in a realistic manner for more accurate results. The phishing technique was selected among the various social engineering threats because its high impact in information security taking into account that when well designed it can trick even well trained personnel [46]. Previous researches had proven that practical exercises such as phishing email drills can contribute to raise the participant's awareness about a given the threat [44], [45].

Modified URLs were created using the software BIND[12], the Web Server used to host the domain was nginx 0.7.[13] In order to identify the participants who click on the fake links, an unique identification code consisting in eight random characters was created using the Linux application pwgen and then edited to match each participant's email. The URLs were designed in such way that when a participant clicks on the link, he/she will be redirected to specific (virtual) locations of Tallinn University of Technology Website, where the following information will be sent back to the hosting server from where the records are consulted:

- Timestamps (Data and time when a event was recorded by a computer).
- Unique identification code created (Created to individualize participants' email addresses).
- User agent. (Line of text that identifies the browser and operating system to the web server).

The information that the web mail server collects is shown in Figure 4.

[12] See more on this at: https://www.isc.org/downloads/bind/
[13] See more on this at: https://www.nginx.com/resources/wiki/

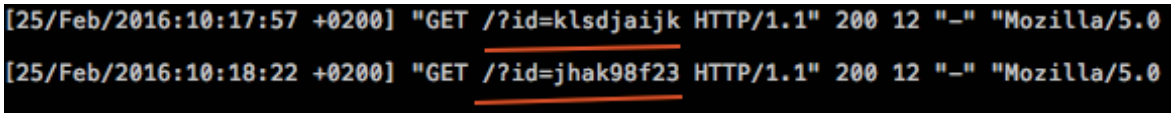


Figure 4 Cropped snapshot with an example of phishing logs.

In the cropped snapshot the data shown consists on information on the date and time when the participant clicked on the modified URL, the unique identification code created for the experiment per participant, and the user agent logs. Each click will disclose the unique identification code that will match one of the specific email address created for the experiment. Table 10 illustrates an example of the email addresses matching a URL with an unique ID code. The clicking on these fake URLs did not represent any harm to the participants, the university or anyone else that may get involved (third parties responding on behalf of the student).

Table 10 Distribution of Unique ID codes

URLs with unique ID	Email address	Result
http://ttu.stiestonia.eu/?eiyoTh1u	Participant1@ttu.ee	
http://ttu.stiestonia.eu/?echoV1ee	Participant3@ttu.ee	X
http://ttu.stiestonia.eu/?Moop5pho	Participant6@ttu.ee	
Total		1

The first column from the left side of the table lists the links with the fake component or the threat vector that include the identification of the student who received the phishing. The middle column shows the institutional participant's email and the right column whether a response followed, to complete the phishing task, four email addresses were created using the domain myttu.eu which was purchased at the Domain Registar and web hosting company GoDaddy[14].

As each Unique ID code belongs to an unique email address, the phishing emails were created one by one according to each recipient and they were sent during working hours aiming to not raise suspicion about the emails. Table 11 illustrates the email accounts created matching their specific modified URL.

Table 11. Modified URLs and Email accounts created.

No	Email account	URL
1	**Helpdesk Maili** <helpdesk@myttu.eu>	http://ttu.stiestonia.eu/?uniqID/html
2	**Stipendiumid Maili** <stipendiumid@myttu.eu>	http://baltech.stiestonia.eu/?uniqID/stipendiumid
3	**Õppeinfosüsteem Helpdesk** <oppeinfosusteem@myttu.eu>	http://ois.ttu.stiestonia.eu/?uniqID/ITX0040
4	**Heydi Kivilo** <arengufond@myttu.eu>	http://arengufond.stiestonia.eu/?UniqID/stipendiumikonkurss

[14] Visit the corresponding page at: https://uk.godaddy.com

The procedures and substance to perform the phishing experiment were endorsed by the university and received ethical and legal clearance after permission was requested from the Dean's office of the Faculty of Information Technology (as well as IT Department), provided that the participants' email addresses to be targeted belonged to the @ttu.ee domain, which they did.

The four fake email accounts were created emulate as closely as possible, TTU's email accounts (using the domain @myttu.eu), the email's subjects were chosen using information gathered from TTU's website. Topics such as scholarships, changes in curriculum and courses info were the sort of interests that could be used to "deceive" the participants that due to their student status could spark interest. The selected group of students were enrolled in the Electronics and Telecommunications program of Tallinn University of Technology as of the dates of the experiment, so the content of the message was decided to be related to university events. The body of the message was written in Estonian because the target group were Estonian speaking students. If the messages would had been not been sent in the official language of the country, it would had raised suspicions and affected the experiment results. A translator drafted the message and it was adjusted twice. The pre-modified URLs were created using: (1) the "http" protocol, (2) a subdomain according to the phishing email topic, for instance "//arengufond", (3) the domain was ".stiestonia", (4) the top domain was ".eu", (5) the category corresponded to the unique ID code and (6) the subcategory was added as a distraction. Figure 5 illustrates an example of the modified URLs created.

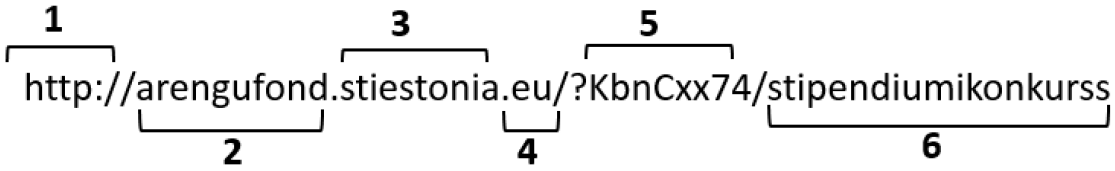


Figure 5 Example of the modified URLs created.

The figure above shows the link created for the experiment as it appears clickable inside the phishing email. Some features that were incorporated when designing the email body, were meant to signal the existence of phishing. These are marked in Figure 6.

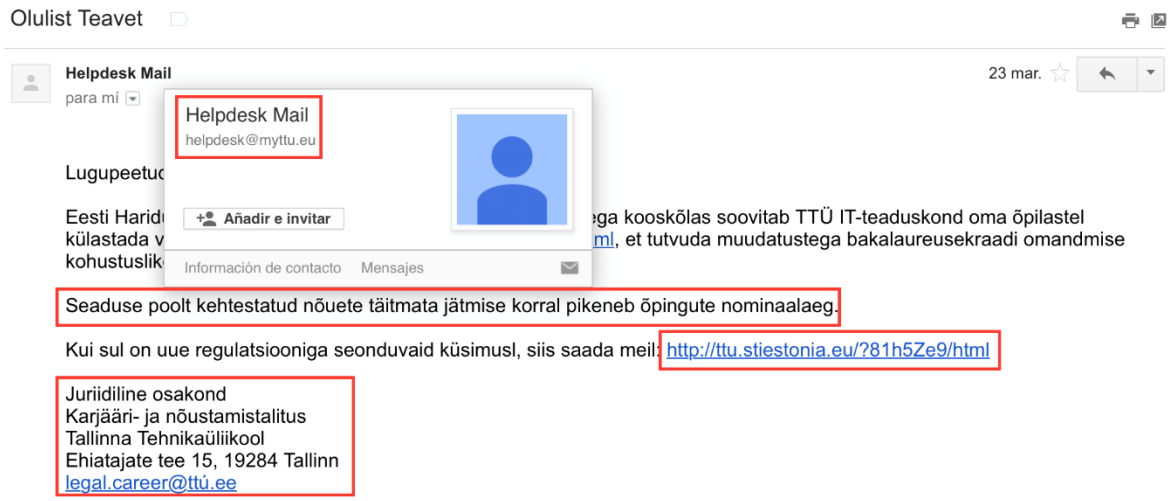


Figure 6 Phishing Email No. 1

The red squares illustrate the features that could help participants suspect about the authenticity of the message, such as urging immediate action, the domain used in the provided URL link, which does not match the TTU's real domain, false contact information as well as the inclusion of typos. The four phishing emails created are added to the thesis as Appendix II.

The experiment was conducted according to the schedule in Table 12.

Table 12. Experiment's schedule.

GROUP I	**GROUP II**
Participants: 40	Participants: 41
Design and planning: 18.01.16 - 10.04.16	
Phishing 1-2 (1st wave) (24.03.16)	--
Additional Test (26.03.16)	--
CHC (13.04.16)	CHC (13.04.16)
Phishing 3-4 (2nd wave) (14.04.16)	Phishing 3-4 (2nd wave) (14.04.16)
--	Additional Test (20.04.16)
Data analysis: 21.04.16	

Group I, under the heading in the column on the left took the AT once, prior to the CHC but received two waves of phishing emails. The schedule of the Group II appears in the column to the right. The second group was not subject to threats or tested before the Course but received the phishing emails and took the AT later, after the CHC was completed. The records on how many of the participants tried to open a link originated from an unknown source were gathered for the experiment between 24.03.2016 and 15.04.2016. The whole experiment developed in a lapse of 3 months including the planning and analysis stages; on the rows the exact dates of the activities are specified.

The groups' level of cognitive capacity related to security threats and diligence when exposed to phishing emails could be tested for both groups, and data could be successfully collected on the reaction of the groups to the phishing email waves and the results were compared in regards to both assessments. The statistical results collected after the completion of the CHC and the additional test were supposed to give account of the participant's knowledge acquisition and improved performance when finishing a security awareness training course; in the same way, the statistics collected with the phishing attacks can be compared to detect the correlations between course completion and participant's behavior when exposed to these threats. The experiment was designed to complete the RT8, conducted to complete the RT9 and help answer the RQ2.

4.5 Results

The experiment took place as planned and described without inconveniences. The schedules were kept accordingly. The mismatch between AT scores and appropriate behaviour became

evident in some cases, for instance: three participants from Group I (P18, P32 and P34), who scored 100% in the AT, failed to refrain from clicking on both fake emails when exposed to phishing wave No 1. In total, 13 participants from Group I were tricked in the first phishing email wave. When Group I was exposed to phishing email wave No. 2., five participants (P5, P10, P15, P18 and P31) were deceived, all of them with the exception of P15 fell for both phishing emails 3 and 4.

Group II was subject to the second wave of phishing emails only, and registered more mistakes than Group I. While five Group I participants (P5, P10, P15, P18, and P31) clicked on the fake URL from email No. 3, nine Group II participants (P1, P2, P4, P7, P9, P11, P13, P18 and P20) incurred in negligent behavior. Regarding phishing email No. 4, four participants from Group I (P5, P10, P18 and P31) were deceived, while five participants from Group II (P1, P4, P9, P13 and P34) fell for the same phishing email.

Due to the sample size, gender was not considered to drawn a pattern for susceptibility to phishing threats. For Group I, 10 of the 40 participants were female. 1 woman fell in the first phishing wave while 13 males did it. For the second phishing wave 1 woman and 4 males did it. For Group II, 9 of the 41 participants were female. 2 women fell in the corresponding phishing wave while 8 males did.

The summary of the experiment results is visible in Table 13 and the detailed results are available in Appendix III and IV showing the outcome for groups I and II, respectively.

Table 13. Experiment results.

GROUP I		GROUP II	
Phishing 1	13 = 32.5%	Phishing 1	--------
Phishing 2	6 = 15%	Phishing 2	--------
Additional Test	Average: 92.35 Max. : 100 Lower : 69	Additional Test	Average: 93.36 Max. : 100 Lower : 67
CHC	Average: 97,75 Max. : 100 Lower : 83	CHC	Average: 98,41 Max. : 100 Lower : 67
Phishing 3	5 = 12.5%	Phishing 3	9 = 21.95%
Phishing 4	4 = 10%	Phishing 4	5 = 12.19%

The outcome of the experiment shows that although both groups obtained high average grades on the AT (Group I, 92,35 - Group II 93,26) and CHC final test (Group I, 97,75 - Group II 98,41), the rate of participants deceived by the phishing emails was high considering the number of participants.

In respect to the outcome of the behavioral assessment part of the experiment, Group I obtained more favorable results after the CHC, acting more diligently and complying with the policies on phishing emails, it must be reminded that Group II had not taken the AT prior the completion of the Course. Figure 7 consigns the phishing results after everyone has successfully passed the CHC.

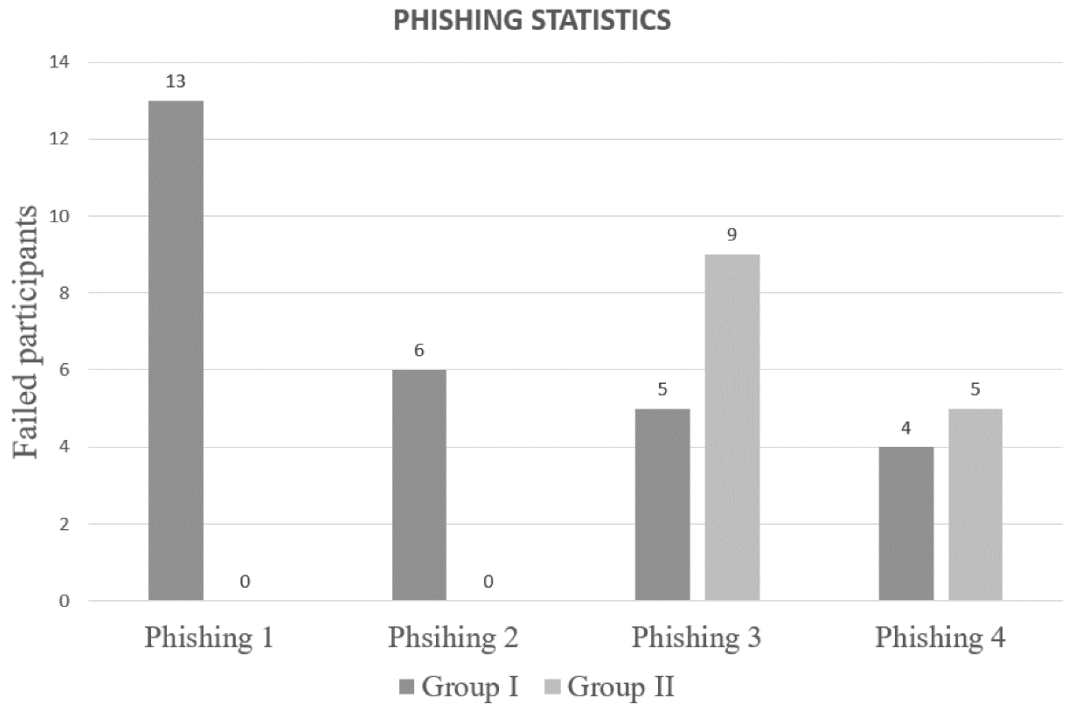


Figure 7 Phishing email results.

The statistics revealed in figure 7 illustrate how the groups responded to the four phishing emails. In the first phishing wave, phishing email No. 1 was the most clicked, with 13 participants deceived in contrast to 6 participants that were tricked by phishing email No. 2 in Group I. On the second phishing wave, phishing email No. 3 deceived more participants in Group II with 9 students phished, while from Group I, 5 showed negligence. Phishing email No. 4 showed the lowest rate of response with 4 participants phished from Group I and 5 participants from Group II.

4.6 Discussion

The findings on this first experiment using the AT for knowledge combined with exposure to simulated threats for testing the behavioral changes, displayed by this specific group, are worrisome. The number of participants who were tricked by the phishing emails, was elevated when looking at the characteristics of the phishing emails (with warning signs too obvious not to have been detected), the controlled group characteristics, the number of failures on diligence in respect to the size of the group, the fact that the same participants for the most part have obtained excellent results in the AT where the cognitive capacity was tested, and most importantly, that everyone had been informed and trained by the CHC so recently.

High test scores in the Additional Test and Cyber Hygiene Course were expected, under the assumption that being the participants students enrolled on a technical faculty and taking a cyber security course from Computer Sciences Department, possessed an advantage. The unexpected experimental finding had to do with the amount of participants who fell for the phishing threat. This outcome is consistent with the theoretical claims and reflections that the conceptual contribution put forward and suggests that the correlations that can be concluded between high scores in tests and behavioral change are not straightforward positive. These may be indicative of the lack of impact of ISAWCs as they are conceived at

the moment and an alarming signal on that the CHC course that was object of this study may not have the effectiveness that it could, if improved on the grounds of the cognitive and behavioral sciences. After Group I finished the CHC, the rate of participants who fell for second wave of phishing emails No. 3 and No. 4 was lower but still considerable, taking into account that the negligence of only one person in an organization regarding information security policies is capable of creating a security breach of catastrophic dimensions. The participant's behavior is affected, but it cannot be considered that the changes were significant.

Students from Group I could have been better at reacting to the fake emails because they submitted one AT extra plus one additional phishing wave that gave the participants the possibility to learn from the experiences and predict the nature of these messages. The improvement of their cognitive capacities cannot be said to have been a factor in this case.

Phishing emails continue to represent a dangerous threat to organizations and can trick even well trained, knowledgeable employees. The design of the experiment should be revised leaving these results as indicators of proficiency of the phishing emails for education purposes and first collection of data to aggregate on evidence that could show how the purposes of some educational models do not successfully translate into results. Correctives can be applied to these ISAWCs so their potential can be unleashed. This study has made claims on proposals that are well structured and possess theoretical validity (consult section 3.5.2). These are worth incorporating into the CHC, to move onto a perfected research scheme that could consider variables of interest such as age, cultural components, organizational sectors, etc., and determine much more clearly the significance of demographic variables such as gender in the context of qualitative research using critical discourse analysis, for example.

5 Concluding Remarks

The aim of the present thesis to perform a theoretical integration and to recommend a set of criteria that could be applied to Information Security Awareness Web-based Courses was achieved. It focused on producing real impact on the participants' behavior and to affect people's perception of security policies, vulnerabilities and the continuously evolving cyber threats. The impact Assessment of ISAWC's and its capacity to influence participants' behavior, was performed as an empirical research using the phishing email technique. The Research Questions proposed were answered as follows:

RQ1. The formulation of a minimum set of criteria that could be applied to Information Security Awareness Web-Based Courses to support their impact and affect employees' perception of the threats that are present in the cyberspace was possible.

The acceptance of online education has grown at the same pace that internet and technology have, which gives relevance to online education design and delivery. A set of criteria was developed into guidelines for the design of ISAWCs, pursuing not only to improve the learning process and study materials but also to influence the participant's behavior toward compliance with information security policies. Learning Theories such as the CTML should facilitate the learning of multimedia content, and Behavioral Theories such as TPB and GDT should be mixed in to address the interest of influencing people's behavior towards information security policies compliance.

RQ2. A pilot test of a controlled experiment successfully matched the principles that were followed and worked to verify the Information Security Awareness Web-Based Courses' influence on the participants' response to phishing emails.

It was argued that online education's efficiency cannot be judged only by comparing student outcomes and using parameters such as grades [30], it is important that the way how the learners behave when applying the acquired knowledge could be represented. To achieve high scores in a course is important, but even more important is behavioral change on the basis of volition and commitment. The experiment confirmed the departing assumption on that higher scores do not necessarily mean that the course's objectives were achieved. The participants of the experiment were exposed to phishing emails, the experiment results showed that even the participants that obtained a high score in the tests could fail to act more diligently when exposed to threats. The experiment also demonstrated that ISAWCs are a good tool to raise cognitive awareness among the course participants, but do not rank well in shaping most participant's behavior towards information security policies compliance. For instance, in Group I the participants' behavior improved soon after the experiment, which was demonstrated when the rate of participants who fell in the phishing email dropped from 19 to 9, but still a considerable amount of negligence was detected.

It can be stated that quality and relevance of the learning content as well as the use of practical exercises to involve the participants into the course are important topics to consider when trying to help participants understand the applications of their lessons learned. For instance, the second phishing wave results from both groups demonstrated that the Group I performance was better than the performance of Group II. This outcome can be attributed to the fact that Group I was submitted to an extra phishing email round as well as an Additional Test that reinforced their learning and skills.

In summary, this thesis persuades on the arguments it has put forward: that the proposed set of criteria can help to improve ISAWC's impact on behavior and behavioral change, especially regarding information security policy compliance. Learning Theories as well as Behavioral Theories combined, the quality and relevance of learning materials, and practical exercises are important the core aspects to consider in the design of ISAWCs. The efficiency of this kind of courses can be improved in time, by analyzing the course results and by focusing on enhancing the security topics where the participants are showing low performance indicators.

One of the main limitations of the present work was the sample size, which nevertheless could yield valuable results as a pilot test to support the preparation of future research work. The foreseeable future holds promising opportunities for the present research to be expanded to other groups, of differing composition, using a diversity of exploratory techniques and simulating other threats. Alos, ethical concerns should be more carefully contrasted with academic regulations in place so institutions can develop these insights safely and prevent any harm from being inflicted on participants. A second pilot test could benefit researchers if with a more with a more representative sample of participants that for instance should think about organizational policies as well as the general information that ISAWCs dispense. ISAWC's should be updated through the time aiming to include oncoming changes in security policies or current threats and so should the impact assessment and testing tools.

6 References

[1] G. Piccoli, R. Ahmad, and B. Ives, "Web-Based Virtual Learning and a Research Framework Environments : a Preliminary Assessment of Effectiveness in Basic It Skills Training," *MIS Q.*, vol. 25, no. 4, pp. 401–426, 2001.

[2] R. Mayer and R. Moreno, "Nine ways to reduce cognitive load in multimedia learning," *J. Educ. Psychol.*, vol. 38, no. 1, pp. 43–52, 2003.

[3] M. Ally, "Foundations of educational theory for online learning," *Theory and Practice of Online Learning, 2nd Edition*, vol. 2. p. chapter 1 15–44, 2008.

[4] R. E. Mayer, "Cognitive Theory of Multimedia Learning," *Cambridge Handb. Multimed. Learn.*, pp. 31–48, 2005.

[5] I. Ajzen, "The theory of planned behavior," *Organ. Behav. Hum. Decis. Process. VO - 50*, no. 2, p. 179, 1991.

[6] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Inf. Syst. Res.*, vol. 20, no. 1, pp. 79–98, 2009.

[7] T. O. M. R. Tyler and S. L. Blader, "Can Businesses Effectively Regulate Employee Conduct ? the Antecedents of Rule Following in Work Settings," *Acadamy Manag. J.*, vol. 48, no. 6, pp. 1143–1158, 2005.

[8] B. Schneier, "'Secrets and lies: digital security in a networked world' International Hydrographic Review.," vol. 2, pp. 103–104, 2001.

[9] C. E. R. T. (CERT), "Unintentional Insider Threats : A Review of Phishing and Malware Incidents by Economic Sector," no. July, p. 41, 2014.

[10] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations," *Sp-800-53Ar4*, p. 400+, 2014.

[11] Center for Internet Security, "The CIS critical security controls for effective cyber defense," p. 106, 2014.

[12] Isaca, *"COBIT: A Business Framework for the Governance and Management of Enterprise IT."* 2013.

[13] PCI SSC, "Requirements and Security Assessment Procedures v3.1," 2015.

[14] International Organization for Standardization, *Information technology Security techniques Code of practice for information security controls*. 2014, p. 11,12.

[15] S. Pahnila, M. Siponen, and A. Mahmood, "Employees' behavior towards IS security policy compliance," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 1–10, 2007.

[16] H. Cavusoglu, B. Mishra, and S. Raghunathan, "A model for evaluating IT security investments," *Commun. ACM*, vol. 47, no. 7, pp. 87–92, 2004.

[17] T. Conlon, "The Internet is not a Panacea," vol. 29, no. Scottish educational review, pp. 30–38, 1997.

[18] S. D. Sorden, "The cognitive theory of multimedia learning," *Handb. Educ. Theor.*, pp. 1–31, 2012.

[19] K. E. DeLeeuw and R. E. Mayer, “A comparison of three measures of cognitive load: Evidence for separable measures of intrinsic, extraneous, and germane load,” *J. Educ. Psychol.*, vol. 100, no. 1, pp. 223–234, 2008.

[20] T. Herath and H. R. Rao, “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness,” *Decis. Support Syst.*, vol. 47, no. 2, pp. 154–165, 2009.

[21] J. C. Ball, “The Deterrence Concept in Criminology and Law,” *J. Crim. Law. Criminol. Police Sci.*, vol. 46, no. 3, p. 347, 1955.

[22] J. Lee, Y. Lee, and J. Lee, “A holistic model of computer abuse within organizations A holistic model of computer abuse within organizations,” pp. 57–63, 2006.

[23] Siponen Mikko and Vance Anthony, “Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations,” *Siponen, Mikko, Vance, A.MIS Q. Mikko, Vance, A.MIS Q.*, vol. 34, no. 3, pp. 487–502, 2010.

[24] J. D’Arcy and T. Herath, “A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings,” *Eur. J. Inf. Syst.*, vol. 20, no. 6, pp. 643–658, 2011.

[25] L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai, “Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory,” *Comput. Secur.*, vol. 39, no. PART B, pp. 447–459, 2013.

[26] S. R. Hiltz and M. Turoff, “Education Goes Digital: The Evolution of Online Learning and the Revolution in Higher Education,” *Commun. ACM*, vol. 48, no. 10, pp. 59–64, 2005.

[27] I. E. Allen and J. Seaman, “Changing course: ten years of tracking online education in the United States,” *Nurs. Stand.*, vol. 26, p. 47, 2013.

[28] A. T. Clarke and Hermens, “Corporate developments and strategic alliances in e-learning.,” *Educ. Train.*, vol. 43, no. 4/5, pp. 256 – 267, 2001.

[29] R. H. Wild, K. a. Griggs, and T. Downing, “A framework for e-learning as a tool for knowledge management,” *Ind. Manag. Data Syst.*, vol. 102, pp. 371–380, 2002.

[30] D. Newton and A. Ellis, “Effective implementation of e-learning: a case study of the Australian Army,” *J. Work. Learn.*, vol. 17, no. 5/6, pp. 385–397, 2005.

[31] S. Bartley, “Evaluating the Cost Effectiveness of Online and Face-to-Face Instruction,” *Online*, vol. 7, pp. 167–175, 2004.

[32] T. R. Ramage, “The’No Significant Difference'Phenomenon: A Literature Review,” *J. Instr. Sci. Technol.*, 2002.

[33] K. Meyer, “Quality in Distance Education,” *ASHE-ERIC Higher Education Report*, vol. 29, no. 4. p. 155, 2002.

[34] D. Jolliffe, A., Ritter, J., & Stevens, *“The online learning handbook: Developing and using web-based learning”. Routledge. pp 16-19.* 2012.

[35] P. Ballew, S. Castro, J. Claus, N. Kittur, L. Brennan, and R. C. Brownson, “Developing web-based training for public health practitioners: What can we learn from a review of five disciplines?,” *Health Educ. Res.*, vol. 28, no. 2, pp. 276–287, 2013.

[36] I. S. Winkler and B. Dealy, “Information Security Technology?...Don’t Rely on It A

Case Study in Social Engineering," *Sci. Appl. Int. Corp.*, no. June, pp. 1–6, 1995.

[37] K. D. Mitnick and W. L. Simon, "The Art of Deception: Controlling the Human Element in Security," *BMJ Br. Med. J.*, p. 1., 2003.

[38] M. Mann, *"Hacking the human: social engineering techniques and security countermeasures". Gower Publishing, Ltd.* 2012.

[39] X. Luo, R. Brody, A. Seazzu, and S. Burd, "Social Engineering," *Inf. Resour. Manag. J.*, vol. 24, no. 3, pp. 1–8, 2011.

[40] J. Hong and J. Hong, "The Current State of Phishing Attacks The Current State of Phishing Attacks," *Commun. ACM*, vol. 55, no. 1, pp. 74–81, 2012.

[41] P. Kumaraguru and S. Sheng, "Getting Users to Pay Attention to Anti-Phishing Education : Evaluation of Retention and Transfer," *Proc. anti-phishing Work. groups 2nd Annu. eCrime Res. summit*, pp. 70–81, 2007.

[42] S. A. Robila and J. W. Ragucci, "Don'T Be a Phish: Steps in User Education," *SIGCSE Bull.*, vol. 38, no. 3, pp. 237–241, 2006.

[43] I. Kirlappos, A. Beautement, and M. A. Sasse, "'Comply or die' is dead: Long live security-aware principal agents," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7862 LNCS, pp. 70–82, 2013.

[44] R. C. Dodge, C. Carver, and A. J. Ferguson, "Phishing for user security awareness," *Comput. Secur.*, vol. 26, no. 1, pp. 73–80, 2007.

[45] J. G. Mohebzada, A. El Zarka, A. H. Bhojani, and A. Darwish, "Phishing in a University Community," *2012 Int. Conf. Innov. Inf. Technol.*, pp. 249–254, 2012.

[46] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," pp. 581–590, 2006.

[47] B. Laboratory, *"Guidelines for Responsible IT-related Practices in Modern Organizations (Cyber Hygiene),"* no. 1. 2015, pp. 3–15.

[48] T. L. Leacock and J. C. Nesbit, "A Framework for Evaluating the Quality of Multimedia Learning Resources," *Educ. Technol. Soc.*, vol. 10, pp. 44–59, 2007.

[49] S. Reisman, "Multimedia Educational Resource for Learning and Online Teaching," *Calif. State Univ. Fullert.*, no. July 2000, pp. 1–11, 2007.

[50] M. Knowless, E. Holton, and R. Swanson, *"The adult learner: The definitive classic in adult education and human resource development". Routledge.* 2014.

[51] D. McDougall and A. Squires, "Software evaluation: a situated approach," *J. Comput. Assist. Learn.*, vol. 12(3), pp. 146–161, 1996.

[52] S. Tergan, "'Checklists for the evaluation of educational software: critical review and prospects,'" *Innov. Educ. Train. Int.*, vol. 35, no. 1, pp. 9–20, 1998.

[53] P. Hosie, R. Schibeci, and A. Backhaus, "A framework and checklists for evaluating online learning in higher education," *Assess. Eval. High. Educ.*, vol. 30, no. 5, pp. 539–553, 2005.

[54] M. Pantic, A. Pentland, A. Nijholt, and T. Huang, "Machine understanding of human behavior," pp. 13–24, 2007.

[55] N. Sohrabi Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput. Secur.*, vol. 56, no. March, pp. 1–13, 2016.

[56] G. Bunker, “Technology is not enough: Taking a holistic view for information assurance,” *Inf. Secur. Tech. Rep.*, vol. 17, no. 1–2, pp. 19–25, 2012.

[57] M. T. Siponen, “A conceptual foundation for organizational information security awareness,” *Inf. Manag. Comput. Secur.*, vol. 8, no. 1, pp. 31–41, 2000.

[58] H. R. Hungerford and T. L. Volk, “Changing Learner Behavior through Environmental Education,” *Journal of Environmental Education*, vol. 21, no. 3. pp. 8–21, 1990.

[59] I. B. B. Bulgurcu, H. Cavusoglu, “Information Security policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness.,” *MIS Q.*, vol. 34, no. 3, pp. 523–548, 2010.

[60] M. Workman, W. H. Bommer, and D. Straub, “Security lapses and the omission of information security measures: A threat control model and empirical test,” *Comput. Human Behav.*, vol. 24, no. 6, pp. 2799–2816, 2008.

[61] J. Abawajy, “User preference of cyber security awareness delivery methods.,” *Behav. Inf. Technol.*, vol. 33, no. 3, pp. 236–247, 2014.

[62] Scott D. Johnson, S. R. Aragon, and N. Shaik, “Comparative Analysis of Learner Satisfaction and Learning Outcomes in Online and Face-to-Face Learning Environments,” *J. Interact. Learn. Res.*, vol. 11, no. 1, pp. 29–49, 2000.

[63] J. J. Summers, A. Waigandt, and T. A. Whittaker, “A comparison of student achievement and satisfaction in an online versus a traditional face-to-face statistics class,” *Innov. High. Educ.*, vol. 29, no. 3, pp. 233–250, 2005.

[64] J. L. M. Brown, “ONLINE LEARNING: A Comparison of Web-Based and Land-Based Courses.,” *Q. Rev. Distance Educ.*, vol. 13, no. 1, pp. 39–42, 2012.

[65] L. K. Treviño, G. R. Weaver, D. G. Gibson, and B. L. Toffler, “Managing Ethics and Legal Compliance: What Works and What Hurts,” *California Management Review*, vol. 41, no. 2. p. 131, 1999.

[66] J. C. M. C. Moore, “The Sloan Consortium Quality Framework and the Five Pillars. The Sloan Consortium,” 2005.

[67] F. Zhao, “Enhancing the quality of online higher education through measurement,” *Qual. Assur. Educ.*, vol. 11, no. 4, pp. 214–221, 2003.

[68] T. R. Peltier, “Social Engineering: Concepts and Solutions,” *Edpacs*, vol. 33, no. September 2013, pp. 1–13, 2006.

[69] C. Soghoian, “Legal risks for phishing researchers,” *eCrime Res. Summit, eCrime 2008*, 2008.

[70] M. Jakobsson, N. Johnson, and P. Finn, “Why and how to perform fraud experiments,” *IEEE Secur. Priv.*, vol. 6, no. 2, pp. 66–68, 2008.

[71] E. C. Johnson, “Security awareness: Switch to a better programme,” *Netw. Secur.*, vol. 2006, no. 2, pp. 15–18, 2006.

[72] H. A. Kruger and W. D. Kearney, “A prototype for assessing information security awareness,” *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006.

[73] J. Wilson, M., & Hash, “Building an information technology security awareness and training program.,” *NIST*, vol. 800–50, pp. 7–39, 2003.

[74] European Network and Information Security Agency (ENISA), “ENISA Threat Landscape 2015,” no. December, pp. 67–70, 2016.

[75] E. T. Welsh, C. R. Wanberg, K. G. Brown, and M. J. Simmering, “E-learning: Emerging uses, empirical results and future directions,” *Int. J. Train. Dev.*, vol. 7, no. 4, pp. 245–258, 2003.

[76] H. Kruger, L. Drevin, and T. Steyn, “A vocabulary test to assess information security awareness,” *Inf. Manag. Comput. Secur.*, vol. 18, no. 5, pp. 316–327, 2010.

[77] A. N. OPPENHEIM, “‘Questionaire design and attitude measurement.,’” *sot 1*, 1966.

Appendix I. Additional Test

The following test was designed to test the participant's information security awareness. Please feel free to answer the questions according to your knowledge. The results will be anonymized and used only for research purposes. The results of the present test will not affect your course grade.

Thank you so much for participating. Each question has a 5 points value.

DEMOGRAPHICS (No points)

Please provide the following information. (The gathered information will be anonymized and used only for research purposes)

a. Age:

b. Gender:

c. Semester:

PASSWORDS (no points)

Please give an example of the passwords you use.

1. PHISHING

When receiving an e-mail that appears to be coming from your bank asking you to go to a specific web link to confirm your personal details, what is the correct action? (Choose all best actions)

a. If the bank's logo, address and all other information on the e-mail and webpage are correct, I will provide the required information.

b. I will click on the link. Having personal information updated is very important.

c. If my colleagues received the same request and if they have provided their details, I will do the same.

d. I will ignore the email.

e. I will report it to our company's IT department.

---

2. DATA LOSS

What is the best way to protect information stored in external storage devices? (USB, hard disks, CD ROM, DVD, etc.)

a. Having information backups in other devices.

b. Using password to protect the files.

c. Encrypting the information and protecting it with password.

d. Camouflaging the information with fake names.

e. Storing the information in compressed formats.

---

3. SOCIAL ENGINEERING

The following are measures for preventing social engineering attacks except:

a. Do not respond to email solicitations asking for personal or financial information.

b. Do not share sensitive information on social networks. (Personal, financial, health, etc.)

c. Do not lock your computer when leaving your workstation.

d. Never click on embedded links in emails from unknown senders.

e. Do not share sensitive information by phone.

---

4. PASSWORDS

According to your knowledge, which one is the more secure password?

a. P@ssw0rd

b. 54321abc

c. strong_p@ssw0rds_ are_too_long

d. AdminAdmin

e. All of the above

---

5. PHISHING:

The term Phishing means:

a. The use of an email message that appears to be from a legitimate trusted source and intends to persuade someone to give away confidential information by clicking in the link provided.

b. The act of going through someone's trash to find out important information.

c. Type of malware that prevents of limits users from accessing their systems.

d. Tracking and recording every stroke entry made on a computer without the knowledge of the user.

---

6. USB

When you are at work and you find an abandoned USB device at your desk or someone gives it to you, the correct action is:

a. Use it only for personal purposes.

b. Format it before using it.

c. Open the USB to see if there is something suspicious.

d. Take it to the organization's IT department.

e. Connect it to the computer and run an antivirus before using it, the USB could be infected.

---

7. INCIDENT HANDLING

When you think that something suspicious is happening with your system, the correct action is:

a. Restarting the computer, and keep working. Maybe you did something wrong.

b. Try to figure out what is happening, google the problem and find out a solution.

c. Reporting the incident immediately to the IT department.

d. Asking others if the same has happened to them, if so, then is normal.

e. Wait and see if something wrong happen. Is not good idea to create panic. IT department has more important things to take care of.

---

8. PASSWORDS

In which situations it is accepted to share your passwords?

a. When a trusted colleague is trying to access to some information and his/her password is not working.

b. When your colleagues have shared their passwords with you.

c. When everyone in the office has the same kind of security access to the system.

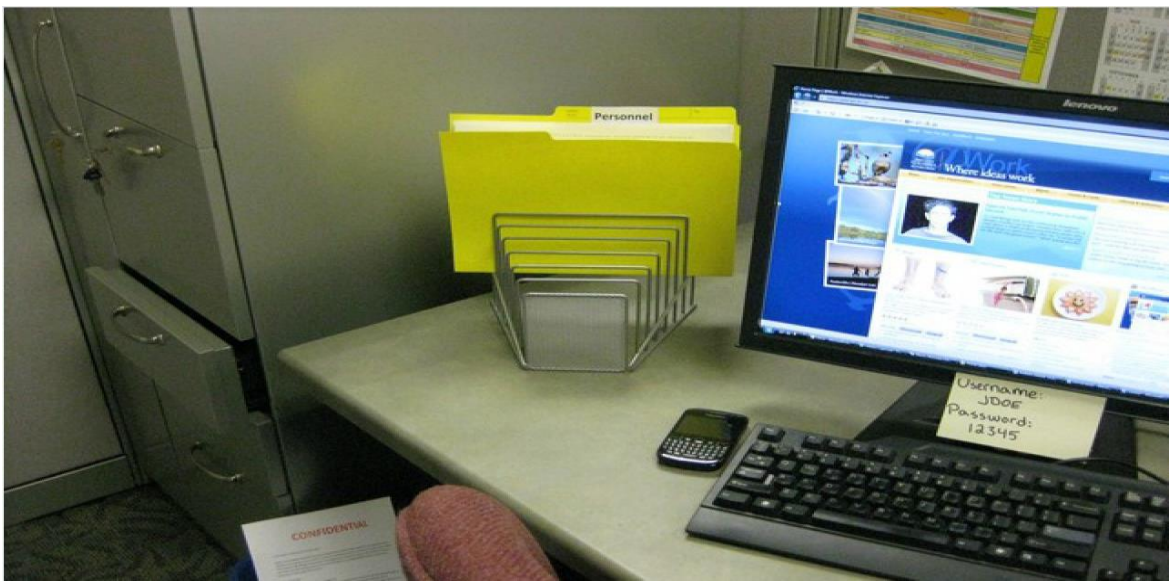
d. When someone with higher rank in the organization ask for it.

e. None of the above.

---

9. SELF DISCIPLINE

According to the picture, which information security policies could be harm by user's lack of self-discipline? Please provide at least 5 mistakes.



http://www.cio.gov.bc.ca/local/cio/informationsecurity/November2015Quiz_CleanDesk/November2015Quiz_CleanDesk.htm

Possible correct answers:

a. Filing cabinet left opened with unattended keys.

b. Personnel file with documents information left accessible.

c. User did not lock or log off from his account before left his/her desk.

d. ID and password written in a sticky note attached to the computer screen.

e. Sensitive information posted in the wall.

f. Confidential documented in recycled bin. .

g. Cell Phone left unattended

h. Using Internet Explorer.

---

10. MALWARE:

The term malware is refers to:

a. a. Computer program that was poorly designed resulting in errors by no compatibility.
b. b. Computer program designed to restore deleted files.
c. **c. Computer program designed to do harmful or unwanted things to a computer's legitimate user.**
d. d. Computer program used to update your protection software.
e. e. Computer program designed to secure your hardware.

---

11. SOCIAL NETWORKS

When you visit your social networks sites, you are expose to:

a. Identity theft.

b. Reputation damage.

c. Nothing, the social networks sites are secured by password and privacy settings.

d. Violation of privacy.

e. Malware.

---

12. SHOULDER SURFING

The term Shoulder Surfing is related to:

a. Using the internet without any precautions.

b. Surfing the internet quickly without clicking on any suspicious site.

c. Spying on the user of any electronic device to obtain information.

d. Surfing the internet covering the computer's camera with a dark tape.

e. Covering your mobile device's with your shoulder to hide what you are typing.

---

13. MALICIOUS SITE

Which of the following sites is free of malware:

a. Governmental web pages.

b. YouTube.

c. Daily news portals.

d. Banks' websites.

e. None, any site can contain malware.

---

14. B.Y.O.D.

Using your own device for related work purposes can put your systems at risk. Choose the correct statements:

a. Corporate data can be exposed if software security updates are not applied.

b. Charging a smartphone directly from a work computer does not represent any security risk.

c. Mobile devices are safer than workstations.

d. Corporate data ca be exposed If a mobile device is lost and is not properly protected with passwords and encryption

e. If my mobile device gets infected, it will represent a threat to me not to the organization.

---

15. SELF DISCIPLINE

At the end of the workday is recommended:

a. To switch off the computer monitor.

b. Leave an active download running and lock the computer.

c. To log off from the computer.

d. To unplug the keyboard and mouse.

---

16. PHISHING

When receiving a phone call asking for specific technical information related to the brand of hardware or software your organization is using, what is the correct way to proceed?

a. Take note of the caller's ID and give the information.

b. If the person says that the information is needed to solve an emergency, I will provide the information.

c. I will not provide technical information by phone.

d. I will ask information about the caller, if I check that the person is related to the organization I will provide the information.

e. If the person is listed on organization's phone list, I will provide the information.

17. OPEN WI-FI

Which of the following statements about free internet connections are correct:

a. Free internet access points are not a threat if I only visit https web sites.

b. My information is protected because I use strong passwords.

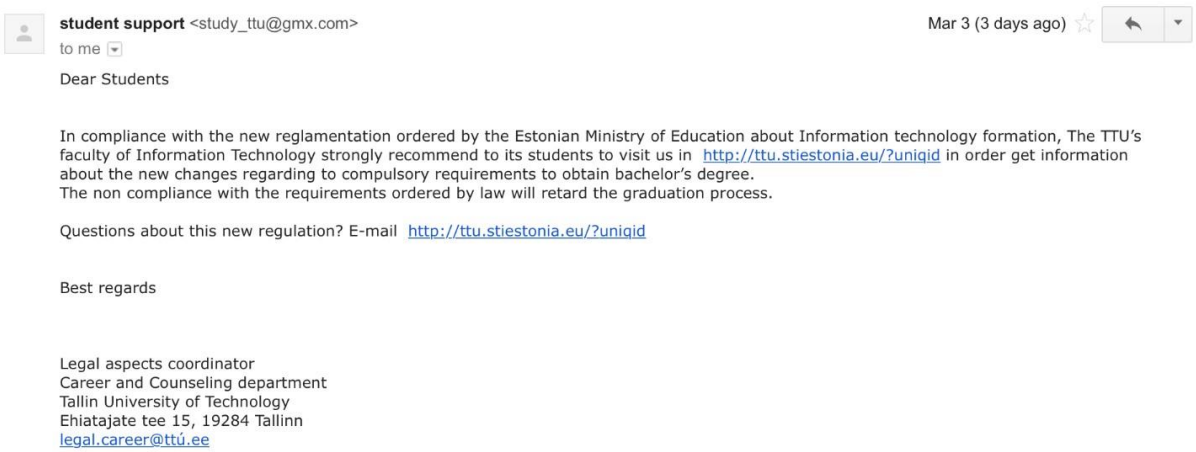
c. A hacker can be between you and the connection point.

d. Unsecure Wi-Fi connection can be used to distribute malware.

e. Credentials cannot be sniffed when listening traffic through an open Wi-Fi network.

18. PHISHING

The following picture represent an example of a Phishing email. How could you, as student of TTU determine that this email is Phishing? Please provide at least three reasons.



student support <study_ttu@gmx.com> Mar 3 (3 days ago)

to me

Dear Students

In compliance with the new reglamentation ordered by the Estonian Ministry of Education about Information technology formation, The TTU's faculty of Information Technology strongly recommend to its students to visit us in http://ttu.stiestonia.eu/?uniqid in order get information about the new changes regarding to compulsory requirements to obtain bachelor's degree.
The non compliance with the requirements ordered by law will retard the graduation process.

Questions about this new regulation? E-mail http://ttu.stiestonia.eu/?uniqid

Best regards

Legal aspects coordinator
Career and Counseling department
Tallin University of Technology
Ehiatajate tee 15, 19284 Tallinn
legal.career@ttú.ee

Possible correct answers:

a. The email domain's sender does not correspond to the TTU's domain.

b. The contact email address contains a domain *tt*ú.ee instead of ttu.ee

c. The University address provided is not real.

d. The URL embedded to the email does not correspond to a TTU' domain.

19. MALWARE

Which of the following are signs to suspect that your computer is infected by malware: (select

a. Several pop-ups emerging on your screen.

b. Suddenly the computer performance has slow down.

c. Standard maintenance programs does not work. (For example updates are disabled)

d. Your browser redirects to unfamiliar URLs.

e. Post you did not write appears on your social media pages.

---

20. <u>SECURE BEHAVIOR</u>

The term Dumpster Diving refers to:

a. Cleaning the recycle bin to free disk space.

b. Gathering information sources from the trash with the purpose of planning cyber-attacks.

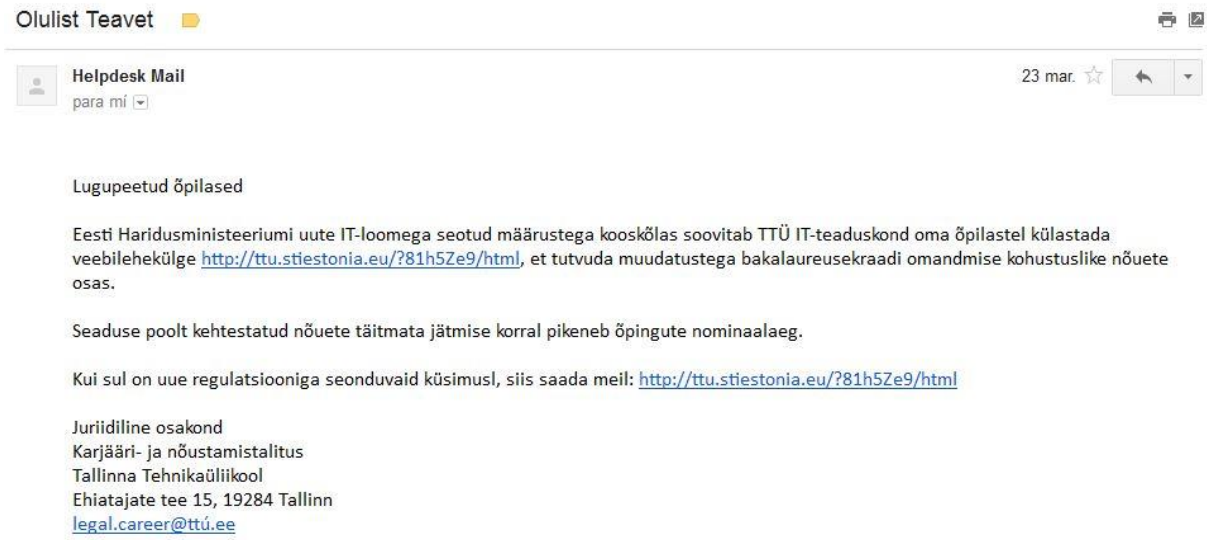
c. Shredding documents before to discard them.

d. Impersonating a trash collection company with the purpose of stealing information through a phone call.

e. Proper formatting of devices before being discarded.

Appendix II. Phishing emails created.

Phishing email No.1



Olulist Teavet

Helpdesk Mail
para mí

23 mar.

Lugupeetud õpilased

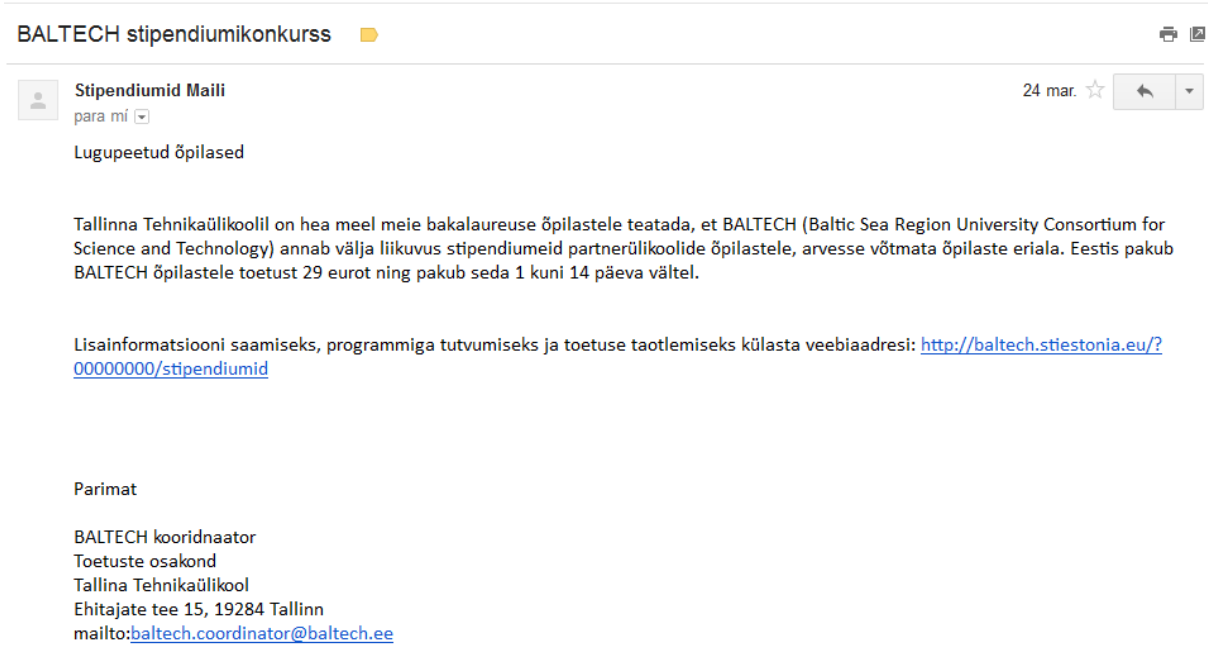
Eesti Haridusministeeriumi uute IT-loomega seotud määrustega kooskõlas soovitab TTÜ IT-teaduskond oma õpilastel külastada veebilehekülge http://ttu.stiestonia.eu/?81h5Ze9/html, et tutvuda muudatustega bakalaureusekraadi omandmise kohustuslike nõuete osas.

Seaduse poolt kehtestatud nõuete täitmata jätmise korral pikeneb õpingute nominaalaeg.

Kui sul on uue regulatsiooniga seonduvaid küsimusl, siis saada meil: http://ttu.stiestonia.eu/?81h5Ze9/html

Juriidiline osakond
Karjääri- ja nõustamistalitus
Tallinna Tehnikaülikool
Ehiatajate tee 15, 19284 Tallinn
legal.career@ttú.ee

Phishing email No. 2



BALTECH stipendiumikonkurss

Stipendiumid Maili
para mí

24 mar.

Lugupeetud õpilased

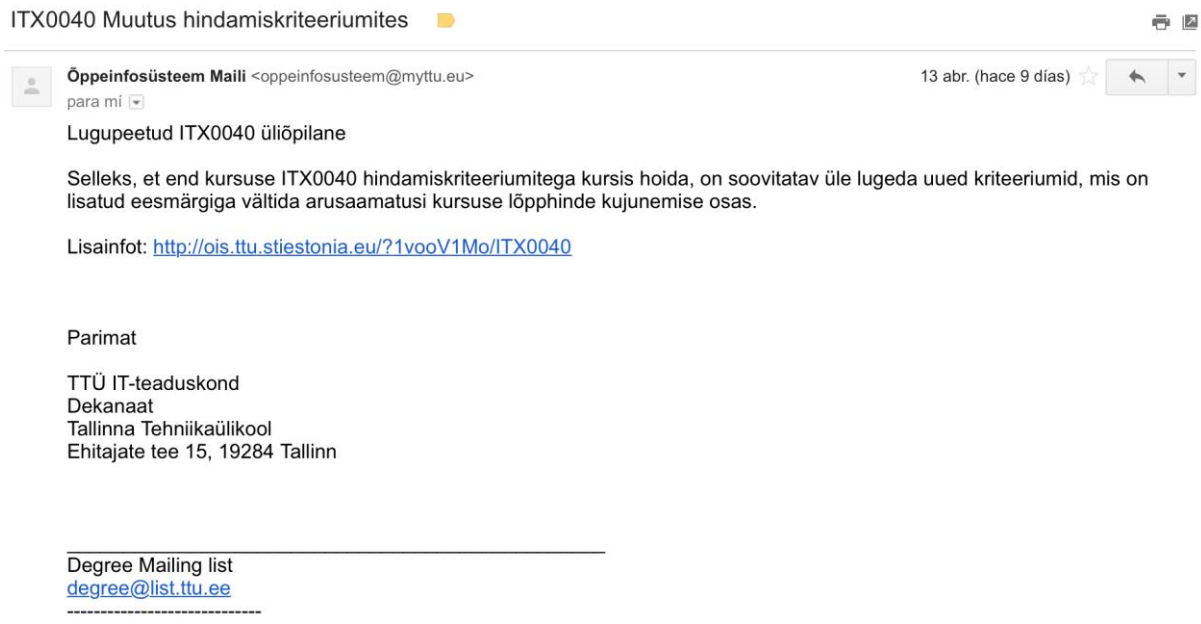
Tallinna Tehnikaülikoolil on hea meel meie bakalaureuse õpilastele teatada, et BALTECH (Baltic Sea Region University Consortium for Science and Technology) annab välja liikuvus stipendiumeid partnerülikoolide õpilastele, arvesse võtmata õpilaste eriala. Eestis pakub BALTECH õpilastele toetust 29 eurot ning pakub seda 1 kuni 14 päeva vältel.

Lisainformatsiooni saamiseks, programmiga tutvumiseks ja toetuse taotlemiseks külasta veebiaadresi: http://baltech.stiestonia.eu/?00000000/stipendiumid

Parimat

BALTECH kooridnaator
Toetuste osakond
Tallina Tehnikaülikool
Ehitajate tee 15, 19284 Tallinn
mailto:baltech.coordinator@baltech.ee

Phishing email No. 3



ITX0040 Muutus hindamiskriteeriumites

Õppeinfosüsteem Maili <oppeinfosusteem@myttu.eu> 13 abr. (hace 9 días)
para mí

Lugupeetud ITX0040 üliõpilane

Selleks, et end kursuse ITX0040 hindamiskriteeriumitega kursis hoida, on soovitatav üle lugeda uued kriteeriumid, mis on lisatud eesmärgiga vältida arusaamatusi kursuse lõpphinde kujunemise osas.

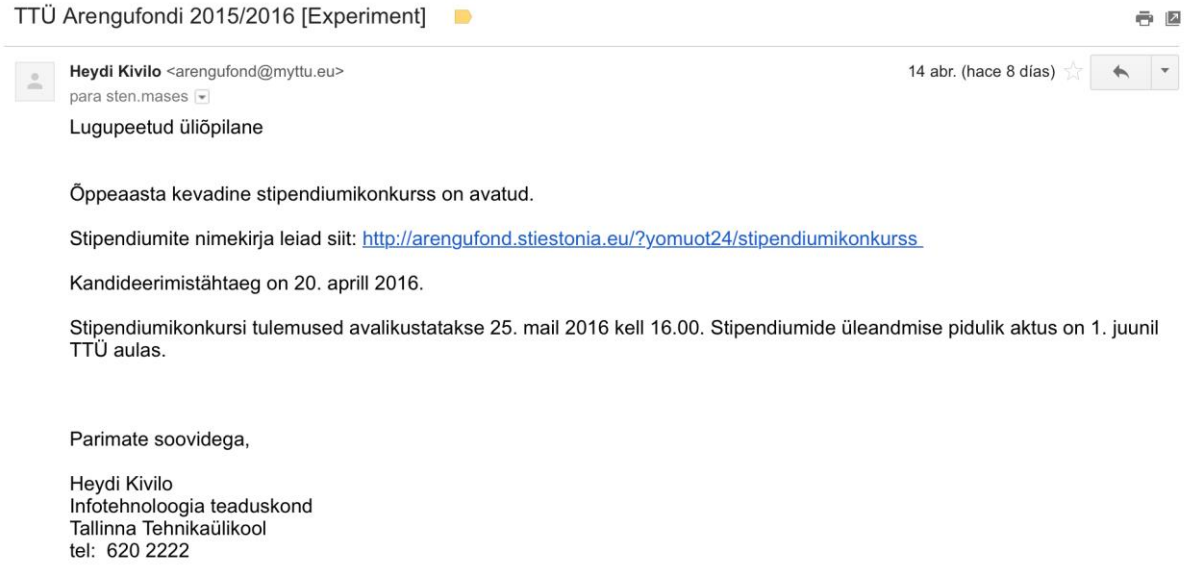
Lisainfot: http://ois.ttu.stiestonia.eu/?1vooV1Mo/ITX0040

Parimat

TTÜ IT-teaduskond
Dekanaat
Tallinna Tehniikaülikool
Ehitajate tee 15, 19284 Tallinn

_____
Degree Mailing list
degree@list.ttu.ee

Phishing email No. 4



TTÜ Arengufondi 2015/2016 [Experiment]

Heydi Kivilo <arengufond@myttu.eu> 14 abr. (hace 8 días)
para sten.mases

Lugupeetud üliõpilane

Õppeaasta kevadine stipendiumikonkurss on avatud.

Stipendiumite nimekirja leiad siit: http://arengufond.stiestonia.eu/?yomuot24/stipendiumikonkurss

Kandideerimistähtaeg on 20. aprill 2016.

Stipendiumikonkursi tulemused avalikustatakse 25. mail 2016 kell 16.00. Stipendiumide üleandmise pidulik aktus on 1. juunil TTÜ aulas.

Parimate soovidega,

Heydi Kivilo
Infotehnoloogia teaduskond
Tallinna Tehnikaülikool
tel: 620 2222

Appendix III. Group I detailed results

No.	Gender	Age	Sem.	Phish 1	Phish 2	A.T. Score	CHC score	Phish 3	Phish 4	Phis total
1	1	20	2	0	0	100	92	0	0	0
2	1	21	6	0	0	87	100	0	0	0
3	1	19	2	0	0	89	100	0	0	0
4	1	24	4	0	0	73	100	0	0	0
5	1	22	2	1	0	91	100	1	1	3
6	2	21	2	0	0	98	100	0	0	0
7	2	19	2	0	0	95	100	0	0	0
8	1	19	2	0	0	75	100	0	0	0
9	1	19	2	0	0	96	100	0	0	0
10	2	20	2	1	0	92	100	1	1	3
11	2	22	6	0	0	98	100	0	0	0
12	1	19	2	0	0	98	100	0	0	0
13	1	20	2	1	0	99	100	0	0	1
14	1	20	2	0	0	95	83	0	0	0
15	1	19	2	1	0	93	100	1	0	2
16	2	21	2	0	0	100	83	0	0	0
17	1	23	6	0	0	98	100	0	0	0
18	1	20	2	1	1	100	100	1	1	4
19	1	19	2	1	0	98	92	0	0	1
20	2	21	6	0	0	90	100	0	0	0
21	2	20	2	0	0	95	100	0	0	0
22	1	20	2	0	1	78	100	0	0	1
23	1	67	4	0	0	95	100	0	0	0

24	1	20	2	0	0	85	100	0	0	0
25	2	19	2	0	0	69	92	0	0	0
26	1	19	2	1	0	100	100	0	0	1
27	1	29	2	0	0	87	100	0	0	0
28	1	22	6	0	0	86	100	0	0	0
29	1	20	2	0	0	85	100	0	0	0
30	2	19	2	0	0	90	92	0	0	0
31	1	22	2	1	0	99	100	1	1	3
32	1	24	2	1	1	100	100	0	0	2
33	1	19	2	0	0	95	92	0	0	0
34	1	20	2	1	1	100	100	0	0	2
35	1	20	2	1	0	95	92	0	0	1
36	1	21	2	0	0	100	100	0	0	0
37	1	23	2	1	1	95	100	0	0	2
38	1	18	2	0	0	90	100	0	0	0
39	2	27	2	0	0	100	92	0	0	0
40	1	20	1	1	1	85	100	0	0	2
Average Result:				32,5%	15%	92.35	97.75	12,5%	10%	28

Item	Description.
No.	Participant.
Gender 1	Male.
Gender 2	Female.
Sem.	Semester.
A.T.	Additional Test.
Phish	Phishing Email.
CHC	Cyber Hygiene Course.

Appendix IV. Group II detailed results

No.	Gender	Age	Sem.	CHC score	A.T. Score	Phish 3	Phish 4	Phish total
1	1	19	2	100	79	1	1	2
2	1	19	2	100	96	1	0	1
3	2	21	6	100	95	0	0	0
4	2	20	2	100	85	1	1	2
5	2	19	2	100	98	0	0	0
6	1	20	2	100	100	0	0	0
7	1	24	2	100	100	1	0	1
8	1	20	2	92	75	0	0	0
9	1	19	2	100	100	1	1	2
10	1	20	2	100	95	0	0	0
11	2	19	2	100	98	1	0	1
12	1	20	2	100	98	0	0	0
13	1	20	2	100	98	1	1	2
14	1	19	2	100	98	0	0	0
15	2	19	2	100	100	0	0	0
16	1	20	2	92	93	0	0	0
17	1	19	2	92	95	0	0	0
18	1	20	2	100	95	1	0	1
19	2	22	6	100	98	0	0	0
20	1	20	2	100	98	1	0	1
21	1	22	6	100	98	0	0	0
22	2	20	2	100	85	0	0	0
23	1	20	2	100	98	0	0	0
24	1	19	2	100	95	0	0	0
25	1	19	2	100	94	0	0	0

26	1	20	2	100	98	0	0	0
27	2	19	2	100	100	0	0	0
28	1	19	2	100	89	0	0	0
29	1	20	2	92	98	0	0	0
30	1	19	2	100	100	0	0	0
31	2	21	2	100	93	0	0	0
32	1	20	2	100	75	0	0	0
33	1	20	2	100	95	0	0	0
34	1	20	2	100	67	0	1	1
35	1	21	6	100	93	0	0	0
36	1	19	2	100	90	0	0	0
37	1	21	2	100	100	0	0	0
38	1	20	2	100	88	0	0	0
39	1	21	2	100	93	0	0	0
40	1	19	2	67	90	0	0	0
41	1	19	2	100	95	0	0	0
Average Result:				98,41	93,41	21,95%	12,19%	14

Item	Description.
No.	Participant.
Gender 1	Male.
Gender 2	Female.
Sem.	Semester.
A.T.	Additional Test.
Phish	Phishing Email.
CHC	Cyber Hygiene Course.

Appendix V. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Didier Dubey Suarez Medina**

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:
   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and
   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

Of my thesis

Assessment of Web-based Information Security Awareness Courses,

Supervised by Maria Claudia Solarte,

Raimundas Matulevičius

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **27.05.2016**