A Process Model for Phishing Prevention

Paulo Ribeiro do Nascimento
Student number: 1727435

Master's Dissertation
Executive Master's in Cyber Security Programme

Supervisors:
Prof. dr. Jan van den Berg &
Dr. Pieter Burghouwt M.Sc.

Leiden University
Faculty of Governance and Global Affairs
Cyber Security Academy The Hague

THE HAGUE, 26 JANUARY 2017

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

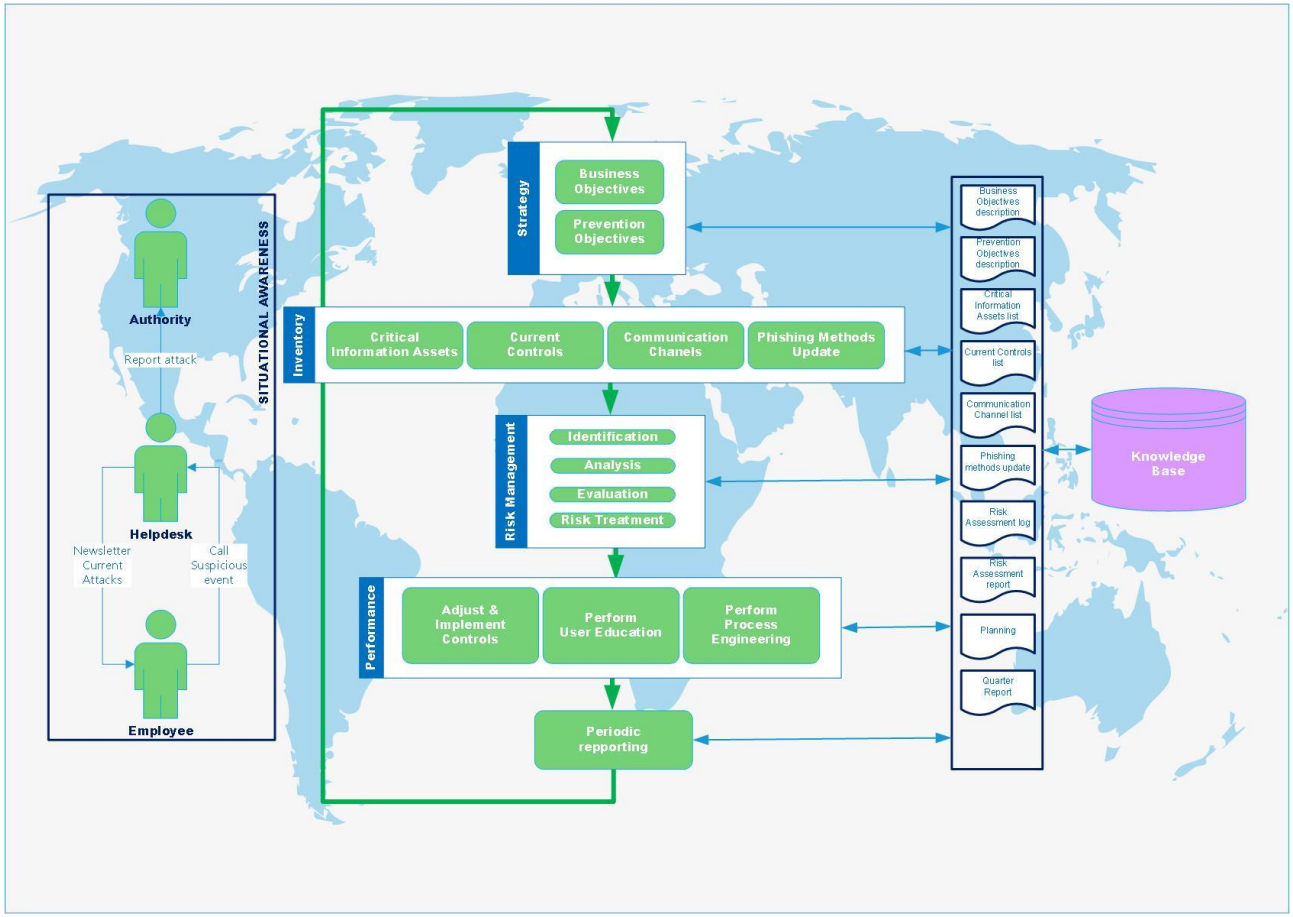
LIST OF ABBREVIATIONS

AOL	America Online
APWG	Anti-Phishing Working Group
AV	Attack Vectors
CERT	Computer Emergency Response Team
CIA	Critical Information Assets
CVE	Common Vulnerabilities and Exposures
ENISA	European Union Agency for Network and Information Security (ENISA)
IC3	Internet Crime Complaint Center
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Standardization Organisation
OWASP	Open Web Application Security Project
PDCA	Plan Do Check Act
SOC	Security Operations Center
UN	United Nations

"The real act of discovery consists not in finding new lands,
but in seeing with new eyes"
Marcel Proust

Abstract

Since the start of e-Commerce at large scale, companies have found that online scams pose a risk to their businesses. One particular kind of online scam commonly known as 'phishing' poses a great risk to the security of interactions between businesses, governments, and individuals in cyberspace. Phishing attacks have amounted to great economic loss, making it a serious threat to enterprises and governments. This study, therefore, aims to support phishing prevention efforts of organisations through the adoption of an organizational-level phishing prevention process. Through a "Design science approach", this research aims to contribute to cyber security in general and to phishing prevention in particular by providing a general process model and related guidelines, to guide cyber security professionals in the design and implementation of a phishing prevention process, adapted to the needs of the organisation and taking into account the existing strategic, tactical and operational processes within an organisation. The research will be carried out in the following sections: First, a literature study is conducted on related works, in order to assess the current state of this academic field of study. Second, the results of the literature study are used to assess the current practices in phishing prevention. Third, the findings from the literature study and the analysis of current practices, are synthesized into design requirements, followed by the design of the process model and guidelines. Finally, the opinion of cyber security experts regarding the outcomes of the research, are gathered from semi-structured interviews in order to validate the completeness, usability, and usefulness of method proposed.



Phishing Prevention Process Model

1 INTRODUCTION

The opening chapter of this study presents a general introduction to the concepts of cyberspace, the Internet, and cyber security. The motivation for the subject of choice will be discussed subsequently, followed by an exposition of the goal of the research. A description of the intended result is then given, followed by an explanation of the methodology adhered in the research and an elucidation of the Design Science research paradigm.

1.1 Background

The Internet made possible the creation of a new domain connecting the globe through computer networks dedicated to the exchange of information and other cyber activities. The domain of cyberspace is a realm of reality that – in contrast to other physical domains of land, air, sea and space – transcends the boundaries of national jurisdiction sovereignty established along the past centuries. Internet access is now widely available, the internet has reached many classrooms, offices, and homes. The mobile revolution brought the Internet to our pockets 24 hours a day (Grant, 2008). Together with the global increase in Internet access many businesses, governments and individuals discovered new opportunities for doing business online. e-Commerce is a growing business model, the expectations are that this trend will continue steadily for the foreseeable future (Marcus, 2016). Today most governments and companies use online services for reaching people through websites but also for automating business processes through web services. Since the start of e-Commerce at large scale, companies have found that online scams pose a risk to their businesses. One particular kind of online scam commonly known as 'phishing' poses a great risk to the security of interactions between businesses, governments, and individuals in cyberspace.

1.2 Motivation

The field of scientific study of cyber security is driven by communities of researchers and cyber security professionals. The interaction between this community and government, businesses, and universities have spurred the emergence of the study of cyber security. Phishing is widely recognized by the cyber security community as a growing problem, both in size and in complexity (Sheng, 2009). Phishing attacks are on the rise. The financial sector is impacted the most by this, causing them to be the most loss-making victims of phishing (Romanosky, 2016). The number of phishing websites observed by the Anti-Phishing Working Group (APWG) increased 250% from the last quarter of 2015 through the first quarter of 2016, leading to steadily growing economic losses (Manning, 2016). According to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3), from October 2013 through February 2016, phishing attacks amounted to more than $2.3 billion in losses (Schuetz, 2016). RAND corporation estimated the total costs from cyber events at approximately $8.5 billion annually and the mean loss for a cyber event caused by phishing attacks to be almost $6 million (Romanosky, 2016). These considerations form an imminent risk to organisations, governments, and individuals, especially for organisation actually experiencing prolonged and tailored phishing attacks.

1.3 Goal

This study aims to support phishing prevention efforts of organisations through the adoption of an organizational-level phishing prevention process. Organisations need a phishing prevention process that is tailored to their needs. This research recommends the development of a phishing prevention process based on a general process model. This study aims to contribute to cyber security in general and to phishing prevention in particular by providing a general process model and related guidelines, to guide cyber security professionals in the design and implementation of a phishing prevention process, adapted to the needs of the organisation and taking into account the existing strategic, tactical and operational processes within an organisation. The main goal of the research is to *design an organisational process model for phishing prevention.*

The process model aimed for consists of a *general* process and related guidelines, describing an approach to the design and implementation of a *useful* phishing prevention process within an organisation. Phishing prevention means in this context the mitigation of phishing-related risks through measures that avoid, inhibit the likelihood of these risks or diminishes its impact once these risks materialize. The concepts of general and useful are central in this context. By 'general' it is referred in the sense that it includes the main elements of phishing prevention, disregarding exceptions, being applicable to a broad range of organisations. 'Usefulness' means that it is a practical method that can be used in various circumstances, enabling the achievement of its purpose. Efforts to mitigate phishing-related incidents after the attack took place are explicitly out of the scope of this study.

1.3.1 Milestones

This sub-section aims to elaborate further on the goals of the research in order to enable the extraction of knowledge regarding the problem at hand from the research activities. Then, in order to synthesize the knowledge acquired into a method design, the following milestones (M) need to be met:

M1: *Understanding of what phishing is and what it's not;*

M2: *Understanding the current practice in phishing prevention;*

M3: *Determine requirements for the design of a process model;*

M4: *Design the process model;*

M5: *Validate the process model.*

The study of phishing (M1) and current practices in phishing prevention (M2) are undertaken in order to allow the expansion of the knowledge base of the problem domain within the research, which is required for the gathering of requirements (M3) for the design of the process model. The above-mentioned milestones enable the design (M4) and the validation (M5) of the process model, which in turn leads to the achievement of the main goal of the research.

1.4 What is a process model?

A *process* is a completely closed, timely and logical sequence of activities which are required to work on a process-oriented business object (Becker, 2013). A *model* is a physical, mathematical, or otherwise logical representation of a system or process. Simply put, models serve as representations of events and/or things that are natural or engineered (Sokolowski, 2010). In process engineering, a process model describes the common properties of a class of processes having the same nature, a process model is a description of a process at the type level (Rolland, 1998). Rolland defined process model as an abstraction, an artefact that represents a process at type level that can be repeatedly used for the development of process instantiations: “Since the process model is at the type level, a process is an instantiation1 of it. The same process model is used repeatedly for the development of many applications and thus, has many instantiations. One possible use of a process model is to prescribe "how things must/should/could be done" in contrast to the process itself which is really what happens. A process model is more or less a rough anticipation of what the process will look like. What the process shall, indeed, will be, however, determined during actual system development (Rolland, 1998). In this study, a process model means the abstraction or representation of the sequence of activities required for the design of a process. In the research, the process model is the representation of the structural method, from which a phishing prevention process can be deduced, designed and implemented.

1.5 Methodology

The research is conducted according to the ‘Design Science approach’ applied to the field of information systems research, as proposed by Hevner et al (2004). Design science research accommodates complex problem-solving and creative processes, in a build-and-evaluate loop continuum, able to catch-up with evolving problems. Design Science, when applied to information systems, intends primarily to “expand the boundaries of organisational capabilities by creating new and innovative artefacts”, this kind of research centres at the interaction between people, organisations, and technology (Hevner, 2004). The Design Science research paradigm is further explained in the following sections. The methodology of the research reflects the interdisciplinary nature of the Leiden University’s Executive Master’s programme in Cyber Security, for which it is also part of the requirements for the award of the degree of Master of Science (MSc). Based on the foundations of the Executive Master’s programme across the fields of cyber security, cyber security economics, risk management, cyber security governance and law, the research is constructed by the following components: First, a literature study is conducted on related works, in order to assess the current state of this academic field of study. Second, the results of the literature study are used to assess the current practices in phishing prevention. Third, the findings from the literature study and the analysis of current practices, are synthesized into design requirements, followed by the design of the process model and guidelines. Finally, the opinion of cyber security experts regarding the outcomes of the research, are gathered from semi-structured interviews in order to validate the completeness, usability, and usefulness of method proposed. The execution of each research methodology component listed above, contributes to each research milestone, generating knowledge gain and the achievement of the research goal.

1.5.1 Structure of the thesis

The relation between the goal and the milestones in the research, are intertwined in the division of the chapters and the sequence of research methodology components, as presented in the table below:

Chapter	Title	Design phase	Description
1	Introduction	Introduction to problem domain	Presents the motivation, goal, and methodology applied in the research.
2	Phishing	Phase 1: Understanding the problem domain	Description of the problem domain and current practice in the field of phishing prevention.
3	Prevention	Phase 2: Requirements gathering	Analysis of the problem domain and the requirements for the method design.
4	Process model	Phase 3: Design of the method	The design of the process model.
5	Validation	Phase 4: Method evaluation	Validation through observation and expert opinion.
6	Conclusion	Reflection	Summary of the contributions, conclusions and limitations of the research.

Table 1: Thesis structure

1.6 Design Science

Design Science is a scientific research paradigm where the main goal is the design of useful *artefacts* instead of developing and verifying theories (Hevner, 2004). Design Science purposefully addresses problems within unstable environments and information systems. Environments can be unstable due to complex interactions between its components, information systems can be unstable due to complex interactions between humans and machines. In this case, solutions have a strong dependency on human cognitive processes and social behaviour (Kulikova, 2012). The problem domain to be investigated in this study – *phishing attacks* – is an example of a complex problem within an unstable environment. The design of a *Process Model* for phishing prevention, the main goal of this research, is classified as a method according to the design science principles. According to Hevner, methods "define processes and provide guidance on how to solve problems, that is, how to search the solution space. These can range from formal, mathematical algorithms that explicitly define the search process to informal, textual descriptions of best practice approaches, or some combination" (Hevner, 2004). The result of this research – *a process model for phishing prevention* – entails a method, a tool for development of a solution in the form of an organizational-level process, containing a sequence of steps and activities that, when applied, enables the methodical study of the problem domain within an organisation, resulting in an approach to phishing prevention that is tailored to the organisation's needs. In the next section, a detailed description of the Design Science research framework is presented, together with a brief explanation on how the Design Science research framework is applied in the research.

1.6.1 Design science research framework

The Design Science research paradigm can be applied to the field of information systems research, as postulated by Hevner et al. In this context, some concepts are used to explain how knowledge is created through the performance of each research methodology component. These components and their interactions describe the process of investigating, analysing and understanding the practical problem, in order to extract the requirements and create the design of the artefact, which is then validated against the requirements. As shown in the picture below, the Design Science research paradigm is dependent on the *environment* – which is composed of people, organisations, technology and regulations, the environment defines the business needs. The Design Science research paradigm is also dependent on to the *knowledge base* – which defines the practice-oriented theories, the knowledge base defines the applicable knowledge. At the centre of the figure below, the Design Science research domain contains both practical and knowledge problems. *Knowledge problems* are solved by applying knowledge available in the knowledge base or by generating this knowledge through research. *Practical problems* are solved by understanding the problem domain and by aggregation, association, and binding of the knowledge created by solving knowledge problems (Kulikova, 2012), resulting in the application of *artefacts* in the appropriate environment. In the figure below these elements and their interactions are displayed.

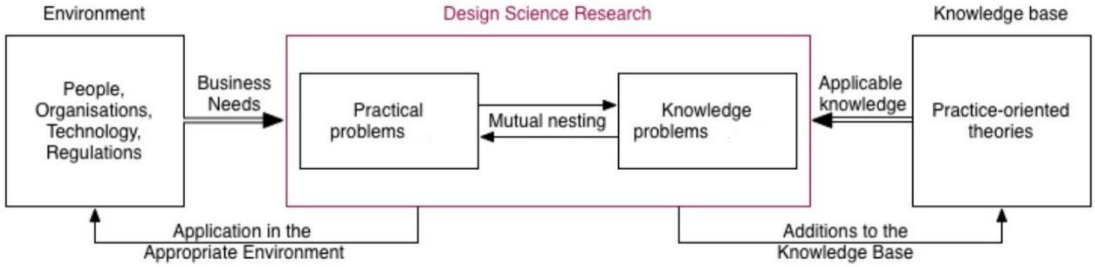


Figure 1: Design Science Research Framework. Source: Kulikova (Kulikova, 2012)

1.6.2 Practical problem and knowledge sub-problems

Hevner et al. proposed a research framework, applied to information systems research and based on the Design Science research paradigm. According to the framework, design science research is, in general, composed of a main goal and sub-goals. The main goal is a *practical problem*, logically divided into a cluster of sub-goals or *knowledge problems*, encapsulated within the main problem, for which a practical solution is required. In this study, the main goal is represented by milestone four (M4), which encapsulates a cluster of knowledge problems or sub-goals, represented in this study by remaining milestones. Milestone four (M4) is achieved when the *practical problem* of designing an organizational process model for phishing prevention is solved. In order to achieve the main goal, the practical problem is sub-divided into a set of knowledge problems or sub-goals, in this study represented by milestones (M1, M2, M3, and M5). The knowledge problems regarding *phishing* and the *current practices in phishing prevention* are the starting point in the research, where an understanding of the problem domain is acquired. These two sub-goals are followed by the knowledge problems regarding the creation of *requirements for the design* of the process model, where the knowledge gained in the previous sub-goals are synthesized into new knowledge. The produced knowledge allows the solution of the main goal represented by milestone four (M4), which allow the solution of the final sub-goal. Finally, the fifth milestone (M5) is achieved.

1.6.3 Milestones in the thesis structure

The first milestone (M1) is addressed in the second chapter of this study, where phishing is defined and its history briefly discussed, followed by an exposition regarding the attackers, their techniques, and motives. The second milestone (M2) is also addressed in the second chapter. The third milestone (M3) is addressed in the third chapter, where requirements for the design of the process model is gathered from the general findings and the identified challenges. Milestone four (M4), the main goal or practical sub-problem, is addressed in chapter four, where the design process is outlined and the resulting design of the process model is presented, together with the corresponding guidelines. Each recommendation in the guidelines reflects a process step in the process model. Milestone five (M5) is addressed in the fifth chapter where a validation of the process model is performed, based on the results of semi-structured interviews with cyber security experts. In figure 2 below the relationship between milestones and chapters are visualized.

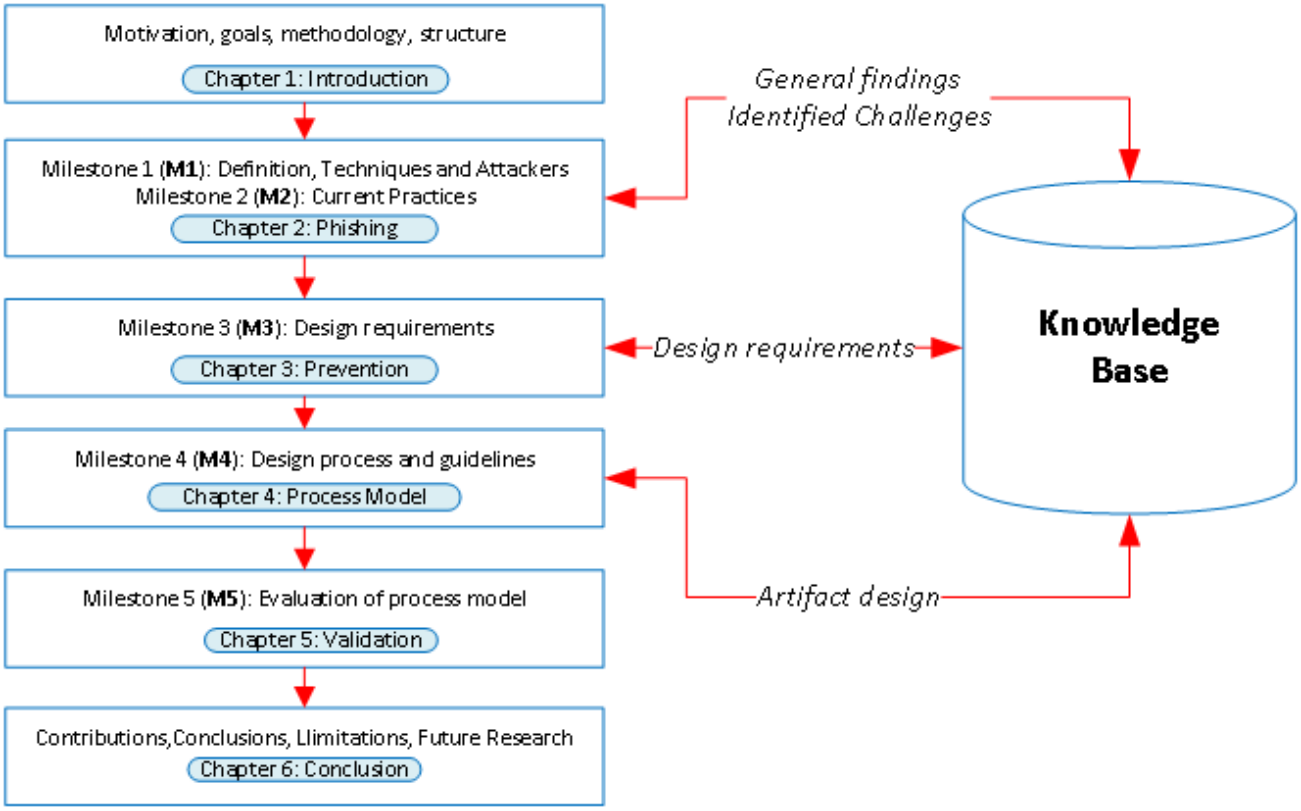


Figure 2: Design Science Thesis Structure

2 PHISHING

In this second chapter of this research, an investigation on the literature will be performed concerning the phenomenon of *phishing*, in order to gain an understanding of what phishing is and what it's not. First, a couple of different definitions for the term 'phishing' are presented. Second, the history of phishing in the last two decades is briefly summarized. We then proceed to describe, on the basis of the threat landscape of the European Union, the threat agent groups launching phishing attacks. Third, we explain their motivation, capabilities, and skills, together with an explanation of the several methods, techniques, and vectors utilized to conduct phishing attacks. Various technological and psychological instruments used to execute phishing attacks are exposed. Fourth, the current practices in the field of phishing prevention are discussed, followed by a discussion on the literature related the phishing prevention. Finally, the knowledge gained by the literature study is synthesized in a set of general findings regarding phishing prevention.

2.1 Definition

The term phishing is a homophone of the word fishing. The words have related meanings. In cyberspace, the attackers (*phishers*) make use of automated social engineered messages (*bait*) to get the fish (*naive user*) to bite their 'hook'. Phishing is, therefore, an allusion to the activity of catching fish. Phishing definitions in the literature are not consistent as we can see in the following examples: Khonji classified phishing under the semantic attacks and gave phishing the following definition: "Phishing is a type of computer attack that communicates socially engineered messages to humans via electronic communication channels in order to persuade them to perform certain actions for the attacker's benefit" (Khonji, 2013). This definition is broad in the sense that it doesn't limit the attacker's actions (undefined 'certain actions') or the benefits for the attackers. A broader definition of phishing was compiled from 113 distinct definitions of phishing by Lastdrager: "Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target" (Lastdrager, 2014). The Anti-Phishing Working Group (APWG) defines phishing including both social engineering and technical subterfuge as follow: "Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit websites that trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account usernames and passwords -- and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes) (Manning, 2016). Within this study, phishing is defined according to the extensive but comprehensive definition above given by the APWG, because this definition includes both the social engineering and technical aspects common to advanced phishing attacks like spear phishing.

2.2 A brief history of phishing

The term phishing first appeared 20 years ago on the '*alt.2600*' hacker newsgroup in January 1996 (Bose, 2007). Phishing was originally used to describe the theft of America Online (AOL) user accounts and corresponding passwords (Clayton, 2005), those stolen accounts were known in the early hacker scene as *phish*. The origins of the use of the old-fashioned (*ph*) combination instead of the modern letter (*f*) are explained as a part of the early hacker community slang use when the community was busy hacking into telephone networks just for free calls, something the community coined as *Phone Phreaking*. As a result, (*ph*) became a concept on itself when it stands in for (*f*) (Bose, 2007). From 2004 onwards a progressive increase in diversity and technical sophistication of phishing attacks was set, already including technically advanced attacks that used malicious code to spy on targets and collect sensitive authentication information (Milletary, 2005). Phishing distribution spread to other communication channels (*attack vectors*) then email to include SMS, instant messaging, social networking sites and more (Hong, 2012). Today *phishers* still exploit primal human emotions – like curiosity, fear and empathy – but combine their social engineering skills with advanced technical subterfuge to *phish* on carefully selected targets, in a type of attack known as *spear phishing*. Using the wide available contextual information to customize these attacks against high-level corporate and public officials, in a type of attack now called *whaling* – which is, in short, the art of chasing and catching a very big fish (Chaudhry, 2016). Phishing attacks in the second quarter of 2016 shatter all previous records to reach an all-time high peak. According to APWG, the total number of unique phishing sites observed in the second quarter of 2016 was 466,065. This was 61% higher than the previous quarterly record in the fourth quarter of 2015 (Manning, 2016).

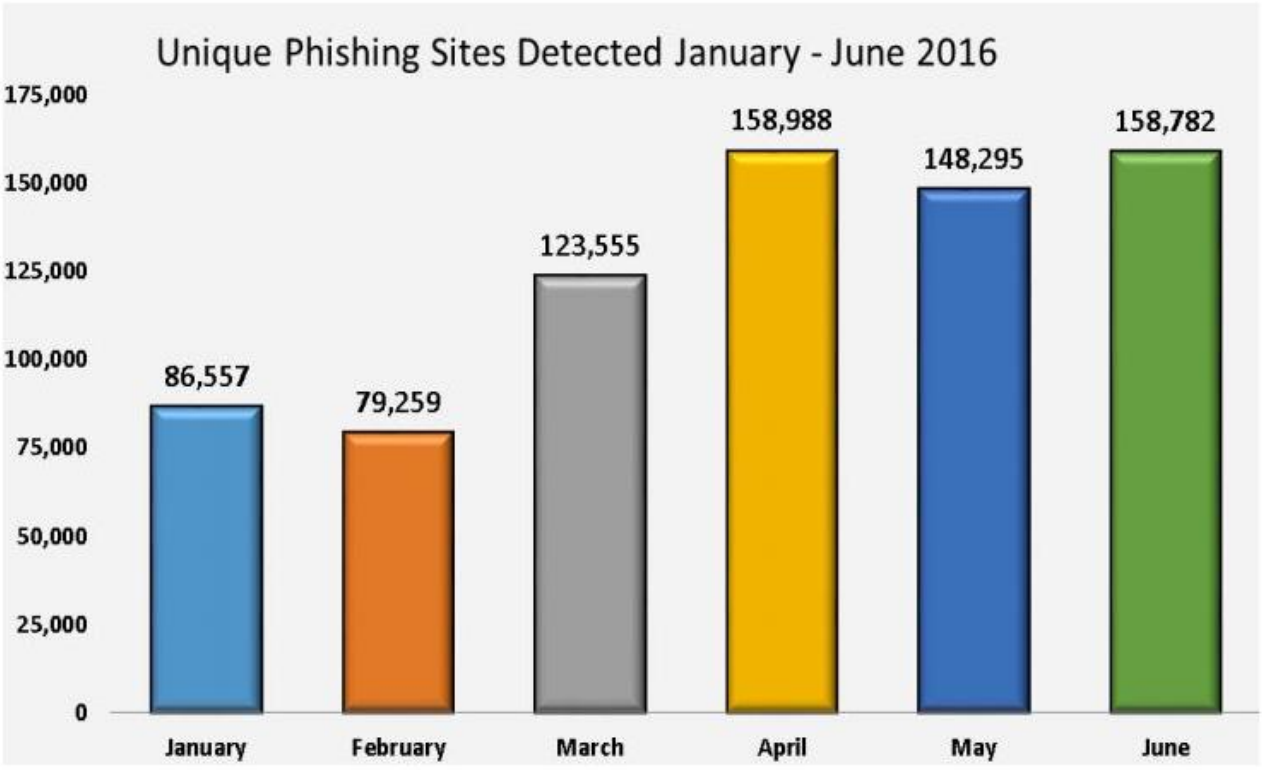


Figure 3: All-time high records phishing sites in Q2 2016. Source: APWG.

2.3 Phishers

In this section, the criminal profiles of the most infamous threat agents, those allegedly carrying out significant phishing campaigns in cyberspace, are presented. This information is published by the European Union Agency for Network and Information Security (ENISA) in its Threat Landscape 2015. Through the analyses of the available information regarding the threat agent motivations, capabilities, skills and alliances, it is possible to estimate how much effort the attacker is able to produce. Taking into account the knowledge available in the Threat Landscape 2015, it can be argued that – in the context of phishing prevention – cyber security professionals need to counteract at least four different threat agent groups. Each threat agent groups have its own characteristics in terms of capabilities, skills, motivations and alliances. All threat agent groups are capable of setting advanced phishing campaign in motion. The following four categories of threat agents are relevant for phishing prevention: cyber criminals, online-social hackers, cyber spies and hacktivists. In the next sections a brief description of each threat agent group is presented.

2.3.1 Cyber criminals

Cyber criminals are not placed at the top of the list by coincidence. According to ENISA, most of the observed incidents caused by phishing attacks have been attributed to cyber criminals. Their sole motivation is profit, illegal monetisation on the detriment of the target misfortune. Their capabilities encompass the access to large amounts of money, time and resources. Cyber criminals are at the same time technically highly skilled and well equipped. Cyber criminals join alliances with other threat agent groups, either as the provider of cybercrime capabilities for rent (cybercrime-as-a-service) or as the outsourcer of part of its cybercrime operations to other threat agent groups (espionage-as-a-service).

2.3.2 Online-social hackers

ENISA added this threat agent group to the Threat Landscape in 2013. The term ‘online-social hacker’ seems to be little known outside ENISA publications, the number of references to this term found outside ENISA publications is negligible. Its motivations are not explicitly mentioned by ENISA, only its capabilities make it discernible from the category of cyber criminals. Online social hackers are highly skilled in social engineering, analysis, and understanding of human behaviour and psychology, possessing low technical skills. ENISA expects that, with increasing use of social media, the importance of this threat agent group will grow in the near future.

2.3.3 Cyber spies (Nation states or corporations sponsored)

The threat agent group of cyber spies is believed to hold a significant operational advantage in cyberspace, both in terms of available capabilities and advanced skills. This group has demonstrated to be capable of disrupting cyber-physical systems through the unleash of state-of-art cyber weapons like Stuxnet. Cyber spies are highly motivated by their sense of duty towards their nation and employer. Driven by common interests, especially when it comes to economic espionage, cyber spies from both governments and corporations could actually be operating in a symbiotic alliance on areas of national interest like high-tech or defence industries.

2.3.4 Hacktivists

Hacktivists groups like Anonymous often display their capabilities and skills to the general public by hacking governments and multinationals, motivated by the desire to disseminate classified information about people in power, to embarrass them and to raise public awareness about alleged wrongdoings. Recently hacktivists have decided to attack terrorist groups by identifying and exposing around 10 thousand Twitter and Facebook accounts used by those terrorist groups for propaganda dissemination and recruitment. The accounts were deleted soon after. Hacktivists found themselves fighting the same target as security agencies, bringing the possibility of a cooperative alliance between the cyber rebels and government in the case of a major cyber-attack.

2.4 1st Summary: definition, history, and actors

Before we start the discussion on the methods, techniques and vectors currently used in phishing attacks, we list below the findings identified in the previous sections of this chapter. From the study of phishing definition, it's history and the threat agent groups, we identified the following challenges to phishing prevention:

- *Phishing is hard to define*. On the one hand, phishing attacks can be composed of a vast number of possible combinations of methods, techniques, and vectors, making the phenomenon of phishing hard to define in anatomical terms. On the other hand, phishing attacks are characterised by the use of automated social-engineered messages.
- *Human behaviour impacts phishing prevention*. Effective phishing prevention requires automation and the deployment of technical controls, but technical controls can only counteract the automated part of a phishing attack. Phishing prevention depends on human behaviour and other unpredictable factors like human cognition, awareness, suspiciousness and even chance, in order to counteract the social-engineered part of a phishing attack. The use of automated social-engineered messages – the single feature that characterizes phishing – forms at the same time a remarkable challenge to phishing prevention.
- *Phishing is evolving*. Phishing is not a new phenomenon. After approximately twenty years, phishing is constantly mutating and evolving throughout the years.
- *Phishing prevention needs to be continuous*. Cyber criminals are the most prolific *phishers* but other threat agent groups like cyber spies and hacktivists pose a threat to organisations. The continued exposure of organisations to the following risks justify a continuous effort to mitigate the risks: Financial losses related to cyber security incidents caused by phishing attacks are remarkably high. The number of confirmed phishing websites continues to grow. Forecasts predicts the rise of ever more advanced phishing attacks, phishing is becoming more complex and advanced.
- *Communication channels are vulnerable*. Cyber criminals adapt their phishing attacks methods to every new emerging communication technology, targeting not only login credentials and other sensitive information, but using phishing attacks to implant malware on the target computers. Communication channels (*attack vectors*) acts as the entry point for phishing attacks into the organisation premises.

2.5 Phishing Techniques

In this section, the techniques used in the execution of phishing attacks are described. These techniques were developed to enable the deployment of both social-engineering schemes and technical subterfuge. The described techniques are constantly being rearranged, modified and reused for the development of novel phishing attack methods. The exhibition of phishing techniques presented in this section do not intend to be exhaustive or conclusive, a detailed description of phishing techniques is, in the context of this study, required only as a demonstration of the arsenal available to cyber criminals and other threat agent groups, necessary for a better understanding of how phishing works. This study does not intend to provide specific solutions to this multitude of techniques. Figure 3 gives an overview of phishing methods, techniques, and attack vectors.

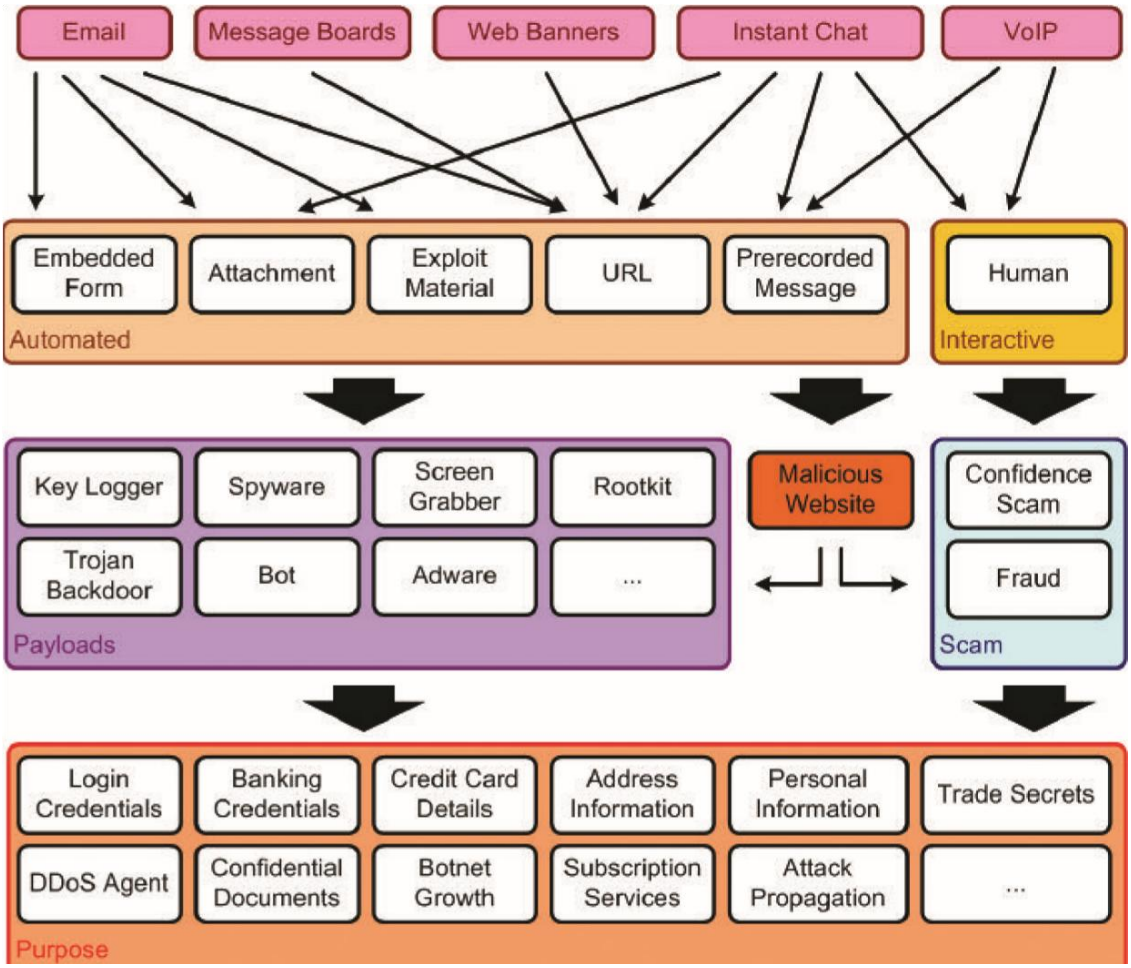


Figure 4: Phishing Methods. Source IBM (Ollmann, 2007)

2.5.1 Phishing e-mail

Perhaps the most known phishing attack method. Sometimes sent by the thousands, this delivery method works quite the same as spam mail does. In phishing e-mail, the message contains a social-engineered persuasion, arousing feelings of fear and a sense of urgency, urging the target to act immediately. Usually, such e-mail messages are crafted to make it seems like the message was originated from a source that is trusted by the target. The e-mail message usually contains also a link to a counterfeit website, resembling in everything the alleged trusted sources of the message. If the target follows the instructions, login credentials could be stolen or malware could be installed on the target's computer. In an example attack scenario, the attacker – the 'phisherman' – buys from spammers hundreds of thousands of email addresses. With this mailing list, he sends out a hundred thousand email messages to random targets – called the 'phools'. In the email message, the attacker pretends to be an employee of a major commercial bank. The message instigates the targets to follow a link in the email message by claiming their accounts will be expired and blocked if no action is taken immediately. The 'phools' that happen to believe in such a claim, click the link and are forwarded to a phishing website – in looks and feel identical to the real bank website - which is totally controlled by the attacker. The targets perform the authentication procedure as they are used to, and by doing so, they provide their authentication credentials for their online bank accounts to the cyber criminals running the scam. The credentials acquired are used to get online access to the bank account and ultimately all savings of this *phool* suddenly vanishes. The phishing e-mail attack can be combined with a series of techniques like sending malware as attachments etc.

2.5.2 Spoofing e-mail messages, addresses, and websites

Cyber criminals utilize, among others, counterfeit websites, e-mail addresses or e-mail messages to fool their targets. Spoofing refers to the imitation of an original website, e-mail address or e-mail message. While 'spoofing' e-mail messages and e-mail addresses could convince the target that the message – and the call for immediate action – comes from a trustable source, 'spoofing' a website could reaffirm the target's confidence that the message is indeed sent by a trustable website. Spoofing means in this context, simply put, to impersonate or masquerade as someone else, through e-mail messages, e-mail addresses, and websites.

2.5.3 Web based delivery

Another method of executing a phishing attack can be launched through the dissemination of malicious website content. The malicious website content could either reside on a website controlled by the attacker or be inserted into a third-party website. One example of malicious content would be a counterfeit advertisement of a major commercial bank, containing a link to a phishing website, distributed through popular websites or discussion forums (Ollmann, 2007). The goal behind the scam is to select and attract customers of a specific bank – instead of sending bulk e-mail messages. Through malicious content, an attacker could exploit vulnerabilities in the web browser in order to install malware for espionage like key-loggers, back-doors, screen-grabbers or other Trojan horse malware (Ollmann, 2007). The spyware, once installed, would reveal the authentication credentials from the targets. Ultimately all savings in the targets bank account would suddenly disappear.

2.5.4 Social phishing

'Social phishing' is the phishing attack method in which the target receives a message containing a link to a phishing website through an instant message in social media programs like Facebook, Twitter, Instagram etc. These social media networks allow embedded content such as web links, to be sent to individual users, groups etc. One example of a malicious attack through social media would be an automated program – a 'bot' – running a counterfeit profile, adding as many people as possible to its network – and sending messages through social media networks, announcing the availability of 'embarrassingly attractive' pictures of celebrities. Intelligent bots are even able to 'chat' with the targets. Once the link is visited, instead of the promised pictures, malware is installed through vulnerabilities in the web browser of the target.

2.5.5 Man-in-the-middle

'Man-in-the-middle' refers to a phishing technique where the attacker places a phishing server in the middle of the communication channel, between the target's computer and the web server of the bank, the phishing server then acts as a proxy between the target computer and its online bank account. The target seemingly makes a connection to the real bank website, but in reality, the connection is made to the phishing server, which relays the connection to the real bank website in real-time. The attacker is able to intercept all the communication between the parties, usually replaying the communication in real-time, being able to change sensitive information like account numbers and amount to withdraw. Ultimately all savings in the targets bank account disappear, never to be found again.

2.5.6 URL Obfuscation

'URL obfuscating' refers to all kinds of techniques used in phishing attacks, in order to get the target to follow a link to the attacker's web server instead of the real online banking web server. For example, attackers use 'bad domain names' – which are domain names that are very similar in name to the real website domain – to make targets believe the domain they're logging in is legitimate.

2.5.7 Cross-Site Scripting (XSS)

Making use of code injections through customized URL's containing HTML substitutions, inline embedding of scripting content, loading external scripts etc. In this kind of advanced phishing attack, targets are directed and connected to the real website of the bank, but the elements of the page that handle transactions, are originated from a malicious website. The target has no way of knowing some parts of the page is not legitimate.

2.5.8 Cross-Site Request forgery (CSRF)

'Cross-Site Request Forgery' (CSRF) refers to the targeting of web application users. In this kind of attack, the attacker causes the target to perform an unwanted action on a trusted website via a malicious link or other content (Lin, 2009). Simply put, the attacker is able to send requests to the target web browser and from there to a legitimate website that are currently being visited by the target.

2.5.9 Client-side Vulnerabilities

This kind of phishing attack techniques refers to any attack exploiting vulnerabilities in the web browser or other web-based software like Flash Player, etc. As the name of the technique shows, this attacks exploit vulnerabilities in the client-side of the connection, through vulnerabilities in web applications which resides on the target computer.

2.5.10 Key-loggers

Key loggers refer to hardware, malware or scripting code used to record inputs to the keyboard. The information recorded is then sent to the attacker, who will gain access to passwords and other types of login credentials (Goring, 2007). This technique is used to steal login credential and personal information.

2.5.11 Screen-grabbers

Screen-grabbers refer to malware that is able to take screenshots of the data that is entered into a web-based application such as online banking. Used to steal login credential and personal information.

2.5.12 Spear Phishing

Spear phishing is a term use to describes a phishing campaign, designed and executed targeting a specific organisation, business, group, or government agency. Contrasting with the massive spam-like phishing e-mail campaigns, spear phishing attacks are more elaborated, the attacker possesses some information about the target and can use that information to social-engineer the target. A variation of spear phishing is called whaling, which means that a high profile senior executive is targeted by spear phishing.

2.6 2nd Summary: phishing techniques

Before diving into the current practices in phishing prevention, this section lists the findings identified in the previous sections. From the study of phishing techniques, the following are recognized challenges to phishing prevention:

- *Phishing attacks can target all employees*. Complex interactions between computer networks, cyber criminals, employees and organisations, make phishing prevention not only difficult to define but also to investigate and to prevent.
- *Phishing attack methods are changing constantly.* Phishing methods, techniques, and attack vectors are constantly changing, becoming more sophisticated, being adjusted to overcome preventive measures. This arms race, together with the impact of phishing attacks, make it necessary for organisations to adopt a flexible yet methodical, continuous approach to phishing prevention.

2.7 Current practices in phishing prevention

In this section, an investigation on the current practices in phishing prevention is presented. The discussion presented in this section is essential for the identification of challenges to phishing prevention. The identified challenges will help in the discovery of general patterns in the current practices in phishing prevention, these general patterns could be used in the design of the process model for phishing prevention. It is important to note that this study does not intend to be conclusive or exhaustive, nor to evaluate the current practices in phishing prevention.

2.8 Related work

Current phishing prevention measures are often of a purely technical nature. Technical measures are essentially algorithms that automate tasks, deployed in hardware and software, operating without human assistance. Blocking spam senders or filtering e-mail messages that match some predefined heuristics (Khonji, 2013) are examples of technical measures. Technical measures discussed in the literature can be classified in one of the following areas: Network protection, authentication, client side tools and server side filters. *'Network protection'* measures act at the network level by blacklisting malicious IP-ranges or fraudulent domains. *'Authentication'* measures perform among others, verification of e-mail sender's identity. '*Client side tools'* includes anti-phishing toolbars for Internet browsers. '*Server-side filter classifiers'* performs content-based filtering of e-mail messages based on machine-learning algorithms (Almomani, 2013). It is also interesting to note that many different machine learning approaches have been proposed to counter phishing (Purkait, 2012).

User education is an approach to phishing prevention with a strong focus on the 'human factor'. User education approaches rely on learning, in order to instruct the user to recognize clues in phishing messages and to act accordingly. Employees are expected to properly identify and effectively act upon each and every phishing e-mail. Even if employees are successful in acting upon clues in phishing e-mails, phishing attacks are not static. Phishing attacks develop according to a process cycle (Parno, 2006). Every improvement in terms of new solutions triggers a new episode in the arms race between defenders and attackers. If defenders come up with an effective solution, attackers feed on the information loop to develop a slightly different variation of the attack, enabling it to circumvent the (by then obsolete) solution. Phishing attacks becomes more sophisticated, attackers create new techniques in order to adjust their strategies (Kumaraguru, 2007). Phishing attacks are delivered not only through e-mail messages but from a multiplicity of channels among others instant messaging and web advertisement, using identity theft and social engineering techniques to impersonate a trustable source (Sheng, 2009).

Although many technical and user education approaches to phishing prevention are studied, there is a perceived gap in the literature regarding approaches to phishing prevention at the organisational level, addressing both the business needs as the characteristics of phishing. Currently available anti-phishing solutions are not effective against phishing attacks because the attack methods are continuously being improved (Zeydan, 2014). Chaudhry et al. argue that process engineering constitutes the third branch of phishing prevention, adjusting the business process to eliminate authentication loopholes in procedures (Chaudhry, 2016).

2.8.1 Technical approaches

As demonstrated in the previous section, most approaches to phishing prevention consists of technical measures. These technical measures can prevent the delivery of phishing e-mail to employees by filtering e-mail messages that matches some predefined heuristics (Khonji, 2013). Other technical approaches are concerned with securing communication channels at network level. Examples of this approach are the blacklisting of malicious IP ranges and fraudulent domains. Authentication is yet another approach to phishing prevention, this approach consists in the verification of the identity of e-mail senders to prevent untrusted sources from delivering phishing e-mails to the organisation. Client side tools are another example of a phishing prevention approach based on technical measures. This approach is deployed within web applications at the user's computer. A practical example of this approach are the anti-phishing toolbars that can be installed in Internet browsers. Server side filter classifiers are yet another approach to phishing prevention based on technical measures, this approach consists in the content-based filtering of e-mail messages, performed by machine-learning algorithms (Almomani, 2013). Many different machine learning algorithms have been proposed (Purkait, 2012). Next to the technical approaches that were developed specially for phishing prevention, there are cyber security measures that can improve phishing prevention: Anti-virus, anti-spam filters, password management tools, SSL/TLS, digital signature, 2-factor authentication etc. (Bose, 2007) are examples of cyber security controls that could help prevention phishing attacks.

2.8.2 User education approaches

User education is an approach to phishing prevention that is not based on technical measures. User education is a part of the current practice in phishing prevention that is concerned with the responsibility of users to properly identify and act upon a phishing attack accordingly. User education training teaches users, among others, how to identify clues in phishing e-mails. Some approaches are based upon direct training using game techniques (Kumaraguru, 2007). Other user education solutions are focused on theoretically teaching what phishing is and how it works. On the other hand, some studies have demonstrated that improvement in user security awareness is hard to measure (Dodge, 2007). The user education approach can prepare employees to recognize certain clues in phishing e-mails, but only those patterns of clues that were trained. Even when users are able to detect and act accordingly in 100% of the phishing attacks, they might not be able to identify yet unknown phishing methods as these new methods couldn't possibly have been learned at previous training.

2.9 3rd Summary: current practices and related work

In this section we summarize the findings identified through the study of related works, technical approaches and user education approaches in the previous sections. These findings were synthesized from the recommendations found in the literature, by organizing the recommendations in cluster of related topics. Below we list the identified challenges to phishing prevention:

- *Cyber security controls contribute to phishing prevention.* Cyber security controls are crucial for counteracting common phishing attacks, cyber security tools assist phishing prevent. The following tools could be deployed as technical measures against phishing prevention: Anti-virus, anti-spam filters, password management tools, SSL/TLS, digital signature, 2-factor authentication etc.
- *Combine technical and user education approaches*. Current practices are either directed to technical solution or user education. Phishing prevention needs to combine both and to add process engineering to the set of phishing prevention approaches. Process engineering can be used to discover and correct loopholes in business processes and authentication protocols.
- *Current practices are no guarantee for the future*. Emerging practices in phishing prevention needs to be perfected and integrated in the organisation, user education need to incorporate newly discovered phishing attack methods as soon as possible.
- *Security controls impact usability of information systems.* Phishing prevention needs to take this into account when selecting appropriate controls.
- *User education has its limits.* The efficiency of user education in preventing phishing is hard to measure. We argue that user education cannot prevent all attacks, even if user is able to act properly on 100% of phishing attacks, due to novel phishing attack methods not being part of received user education training.

2.10 Findings from the problem domain

In this section, we summarize the twelve findings identified in the previous sections into a single set of findings, by combining and organizing the findings in clusters of related topics. The findings presented below shall be further detailed in the next chapter, resulting in a set of identified challenges to phishing prevention. The resulting challenges to phishing prevention will then elaborated and synthesized into design requirements for the development of a process model for phishing prevention.

	Finding description
F1	Phishing is the collective name given to a variety of cyber-attacks that employ automated social-engineering methods and exploit the human – machine interface.
F2	Phishing can be executed through different methods, using various techniques and being propagated by multiple attack vectors. There are many possible combinations of methods, techniques, and attack vectors.
F3	Current mitigation effort produced countermeasures that are either of a purely technical nature or only directed to user education. Process engineering could be added to the effort.
F4	There is an arms race going on between attackers and defenders. Every new solution triggers a subsequent new variation of phishing attacks. The requirements for solutions are constantly changing. Phishing prevention needs to be adaptive, incremental and continuous.
F5	Prevention measures can cause a decrease in efficiency, usability and security in information systems due to a complex interaction with users.
F6	Cyber criminals are designing and executing phishing campaigns mainly for the purpose of stealing login credentials, credentials that can be used to seize control of financial and informational assets. Protecting this asset is crucial for phishing prevention.
F7	Cyber criminals and other threat actors like cyber spies and hacktivists are making use of phishing attacks. Phishing prevention needs to be persistent.
F8	Emerging communication technologies like Social Media, Instant Messengers etc. quickly becomes an attack vector for phishing propagation.
F9	Next to targeting login credentials to steal, phishing is also used to install malware at the target end. This malware can be used for many purposes, including spying the target, recording data from I/O components, running a botnet, ransomware etc.
F10	Techniques like cross-site scripting and cross-site request forgery can trust website, the target has no way of knowing that the website has been compromised.
F11	Current practices are directed at stopping phishing e-mail entering the organisation, password management, black-listing phishing web servers and websites, applying two-factor or multi-channel authentication and user education. This practices all adds to successful phishing prevention.
F12	User education training utilizes demonstrations of currently known phishing attacks. Unknown attacks are a blind-spot that need to be addressed through prevention.

Table 2: Findings from the Problem Domain

3 PREVENTION REQUIREMENTS

In this chapter the findings from the previous chapter will be further discussed. The discussion is organised around the following topics: Main challenges to prevention, business objectives and prevention objectives, attack vectors, situational awareness, critical information assets, risk management and incident management. The topics were created in order to facilitate the deduction of design requirements, acting as a bridge between findings and design requirements. The discussion on each topic is then synthesized into a single design requirement, to be used in the development of the process model in the next chapter.

3.1 Linking findings to discussion topics

In this section the findings presented in the previous chapter are linked to the topics discussed in the next sections.

Finding 1 - *Phishing is the collective name given to a variety of cyber-attacks that employ automated social-engineering methods and exploit the human – machine interface*. (F1), exposes the complex challenges to effective phishing prevention. Those challenges are further investigated in section 3.2 Challenges to prevention, section 3.3 Business Objectives, section 3.4 Prevention Objectives, section 3.6 Situation Awareness and section 3.7 Risk Management.

Finding 2 - *Phishing can be executed through different methods, using various techniques and being propagated by multiple attack vectors. There are many possible combinations of methods, techniques and attack vectors* (F2), exposes the need of a phishing prevention process that is continuous, integrating a changing landscape into the process. These aspects are further investigated in section 3.2 Challenges to prevention, section 3.5 Attack Vectors Inventory, section 3.6 Situation Awareness and section 3.7 Risk Management.

Finding 3 - *Current mitigation effort produced countermeasures that are either of a pure technical nature or only directed to user education* (F3), exposes the need for an approach to phishing prevention that combines and aligns both technical controls and user education approaches. These aspects are further investigated in section 3.2 Challenges to prevention and section 3.7 Risk Management.

Finding 4 - *There is an arms race going on between attackers and defenders. Every new solution triggers a subsequent new variation of phishing attacks. The requirements for solutions are constantly changing. Phishing prevention needs to be adaptive, incremental and continuous* (F4), exposes the need for an approach to phishing prevention that is adaptive, incremental and continuous. These aspects are further investigated in section 3.4 Prevention Objectives, section 3.6 Situation Awareness, section 3.7 Risk Management and section 3.9 Incident Management.

Finding 5 - *Prevention measures can cause a decrease in efficiency, usability and security in information systems due to a complex interaction with users* (F5), exposes the need for an approach to phishing prevention that takes into account the impact on the usability of information systems. These aspects are further investigated in section

3.2 Challenges to prevention, section 3.5 Attack Vectors, section 3.6 Situation Awareness and section 3.7 Risk Management.

Finding 6 - *Cyber criminals are designing and executing phishing campaigns mainly for the purpose of stealing login credentials, credentials that can be used to seize control of financial and informational assets. Protecting these assets is crucial for phishing prevention* (F6), exposes the need for an approach to phishing prevention that centres in the assets being targeted. These aspects are further investigated in section 3.8 Critical Information Assets.

Finding 7 - *Cyber criminals and other threat actors like cyber spies and hacktivists are making use of phishing attacks. Phishing prevention needs to be persistent* (F7), exposes the need for an approach to phishing prevention that is persistent. These aspects are further investigated in section 3.2 Challenges to prevention, section 3.3 Business Objectives, section 3.9 Incident Management and 3.7 Risk Management.

Finding 8 - *Emerging communication technologies like Social Media, Instant Messengers etc. quickly becomes an attack vector for phishing propagation* (F8), exposes the need for an approach to phishing prevention that incorporates emerging technology in the process. These aspects are further investigated in section 3.3 Business Objectives, section 3.6 Situation Awareness and section 3.7 Risk Management.

Finding 9 - *Next to targeting login credentials to steal, phishing is also used to install malware at the target end. This malware can be used for many purposes, including spying the target, recording data from I/O components, running a botnet, ransomware etc.* (F9), exposes the need for an approach to phishing prevention that includes risks like malware, ransomware etc. in the process. These aspects are further investigated in section 3.2 Challenges to prevention, section 3.7 Risk Management and section 3.9 Incident Management.

Finding 10 - *Techniques like cross-site scripting and cross-site request forgery can fake trusted website, the target has no way of knowing that the website has been compromised* (F10), exposes the need for an approach to phishing prevention that includes risks coming from trusted sources. in the process. These aspects are further investigated in section 3.2 Challenges to prevention, section 3.7 Risk Management and section 3.9 Incident Management.

Finding 11 - *Current practices are directed at stopping phishing e-mail entering the organisation, password management, black-listing phishing webservers, and websites, applying two-factor or multi-channel authentication and user education. This practices all adds to successful phishing prevention* (F11), exposes the need for an approach to phishing prevention that includes current practices in the process. These aspects are further investigated in section 3.2 Challenges to prevention, section 3.4 Prevention Objectives, section 3.6 Situation Awareness and section 3.7 Risk Management.

Finding 12 - *User education training utilizes demonstrations of currently known phishing attacks. Unknown attacks are a blind-spot that need to be addressed through prevention* (F12), exposes the need for an approach to phishing prevention that includes communicating real-time developments in phishing attacks to users. These aspects are further investigated in section 3.2 Challenges to prevention, 3.7 Risk Management and section 3.9 Incident Management.

3.2 Main Challenges

In this section we argue that the main challenges to phishing prevention are: The dynamic nature of the problem domain, the possible impact of phishing prevention on usability and the alignment of different approaches into phishing prevention efforts. The discussion on these three topics results in three design requirements.

3.2.1 Dynamic requirements arms race

The design of a solution in information systems engineering is often based upon predefined requirements. In the case of the design of a process model for phishing prevention, the requirements are derived from the understanding of the environment (the organisation) and the problem (phishing). Both the organisation and the problem are constantly subject to change (F1 and F2). In the case of the organisation, technological developments, and market forces are constantly exercising pressure for change, which will sometimes result in the modification of its business processes and information systems. In the case of phishing, a constant arms race, as described in the general findings (F4), keep the requirements constantly changing. Every solution in phishing prevention will trigger the development of adjusted phishing methods and techniques (F7, F9, F10). This challenge requires the process model to be adaptive, incremental and continuous.

- Requirement*:* Phishing prevention must be adaptive, incremental and continuous.

3.2.2 Impact of prevention on usability

Cyber security measures and solutions can sometimes conflict with the usability, efficiency and efficacy of the use of information systems by employees. An example of these conflicting requirements is the difficulty employee experience in memorizing a vast number of passwords. Eventually, a password will be forgotten, preventing the employee from accessing the information system in the exact moment the employee needed access to the system the most. The intended increase in efficiency that motivates the adoption of information technology in organisations, can be reverted by user-unfriendly security controls (F5). Organisations can face conflicting requirements between cyber security and the usability of information systems (F11). This challenges need to be overcome in order to come up with an appropriate design of a process model for phishing prevention. Usability is important because, in general, systems with poor usability design tend to evoke a greater degree of user resistance (Al-Gahtani, 1999), what in turn could be contra-productive for the efforts of phishing prevention in the organisation. According to Sasse, "*usability problems are the root cause of many of today's IT security incidents. Security mechanisms are often too time-consuming for people to bother with, or so complex that even those willing to use them make mistakes*" (Sasse, 2016). Sasse also postulates that to be efficient, any security mechanism design needs to take in consideration the tasks users perform through their interactions with information systems. These interactions need to be efficiently designed to allow task performance to be quick as possible, without waste of energy, time or resources (Sasse, 2016). This challenge requires the process model to include an evaluation of the impact of security measures on usability of information systems.

- Requirement: Security controls are adopted only if no considerable impact in usability is evident.

3.2.3 Alignment of different approaches

As exposed by the general findings (F3 and F12), current solutions in phishing prevention are either pure technical in nature of directed only towards user education. It is argued that a phishing prevention approach that align technical measures, user education and process engineering have a greater probability of being effective against phishing attack. This challenge involves alignment of the phishing prevention process with existing technical security measures, user education efforts, and process engineering. A risk assessment approach would help catalogue and prioritize the implementation of technical measures, user education, and process engineering activities. For this reason, risk assessment should be the core activity within the process model for phishing prevention.

- Requirement: Technical measures, user education, and process engineering approaches must be aligned, based on risk assessment, within phishing prevention process.

3.3 Business objectives

Business objectives elucidate what goals the organisation is striving to achieve. These business objectives are the departing point for the gathering of requirements for the design of a phishing prevention process, by providing the context in which the organisation operates, what interactions with the environment takes place, who the organisation communicates with stakeholders etc. (F8). Then main reason for including an investigation of business objectives in the phishing prevention process is to determine what the approach of the organisation regarding quality management actually is (F7), and what this approach means to phishing prevention. The investigation of business objectives must be a part of the phishing prevention process, as it would help to determine or to adapt the length of the phishing prevention improvement cycle for the organisation. A complete cycle should last, we argue, three months or a quarter of a year, usually in parallel with the reporting period of the organisation.

- Requirement: Phishing prevention must be embodied in the improvement cycle of the organisation.

3.4 Prevention objectives

Prevention objectives help elucidate the necessities, possibilities and maturity level of the organisation regarding cyber security and phishing prevention. An investigation of the prevention objectives, we argue, would help the organisation to determine its goals regarding phishing prevention, taking into account the business objectives established, as discussed in the previous section (F4). Prevention objectives are the strategic goals the organisation wants to pursue regarding phishing prevention. The prevention objectives are high-level (strategic statements on organisational-level), intended to support the decision-making process during the design of a phishing prevention process, setting realistic goals to be persuade by the organisation, according to business needs, possibilities and maturity in the area of cyber security and phishing prevention (F11).

- Requirement: The Phishing prevention improvement cycle should be short, preferably a quarter of a year.

3.5 Attack vectors

Attack vectors (AV) are the channels through which a phishing message is delivered. In the previous chapter, some of the AV commonly used in phishing attacks were described. E-mail is by far the most used attack vector in phishing attacks. It is important to perform an inventory on the communication channels available in the organisation that could be used as attack vectors, whether these AV are available to the general public or have an authorized-only audience (F2). The attack vectors are a crucial step in phishing attacks, the identified AV should be listed and included in the risk assessment, be enumerated and prioritized. Prioritizing the AV could, we assert, help also in the decision-making regarding the impact of security measures on the usability of communication facilities (F5).

- Requirement: The organisation knowledge of emerging phishing methods, techniques, and attack vectors, is up-to-date and its impact in the organisation can be quickly assessed.

3.6 Situational awareness

The cyber security professionals involved in the design and management of a phishing prevention process, we argue, need to engage the organisation in several knowledge-sharing channels in order to keep track of the emerging phishing methods, techniques and attack vectors, as well as the emerging solutions (F1, F2, F4, F5, F8 and F11). Example of these knowledge sharing channels are: National CERT, regional SOC, local OWASP chapter, the Common Vulnerabilities and Exposures (CVE) community, the Anti-Phishing Working Group (APWG) etc. Communication with these channels, we argue, needs to be established and maintained. The input received from those channels is used with risk assessments, helping determine the likelihood and impact of emerging phishing attacks, as well as to evaluate new solutions, and as input for the adjustment of the phishing prevention programme.

- Requirement: Every presumption of a phishing attack is investigated, every confirmed attack is communicated to all employees, to the authorities and, if possible, the attacker(s) prosecuted.

3.7 Risk Management

Risk Management is currently a proved method for dealing with business risks, including cyber security risks (Blakley, 2001). In our opinion, we assert that this approach can be replicated to phishing prevention. The application of risk management in phishing prevention, based on the ISO31000 standard, represents also the introduction of the organisation improvement cycle of Plan Do Check Act (Deming, 1986) in the field of phishing prevention. The international standard for Risk Management was published in 2009 by the International Standardization Organisation (ISO) and is based upon the PDCA cycle of Deming. The ISO31000:2009 standard is, in fact, the global standard and "*has been adopted as a national standard by more than 50 national standards bodies covering over 70 % of the global population. It has also been adopted by a number of UN agencies and national governments as a basis for developing their own risk-related standards and policies*" (Tranchard, 2005). By relying on the popularity of ISO31000, we expect to save effort required to introduce yet another standard approach in an organisation. From the standard, a subset of elements will be selected, based on its suitability for phishing prevention. In the definition of the standard, risk is the "*effect of uncertainty on objectives*". Simply put, managing risk is "*a process of optimization that make the achievement of objectives more likely*" (Purdy, 2010). By applying risk management, the organisation put risks in considerations in the process of decision-making, adjusting decision according to the risks at hand. We postulate that phishing prevention is risk management at micro-level. Using risk management for phishing prevention, it is possible to break-down the high-level cyber security risk identified simply as 'phishing' into small fragments, adjusting each fragment of risk to the current used phishing methods, techniques and attack vectors. Those small fragments of risk can then be treated independently of each other, limiting the impact on operations as much as possible, keeping the phishing prevention manageable.

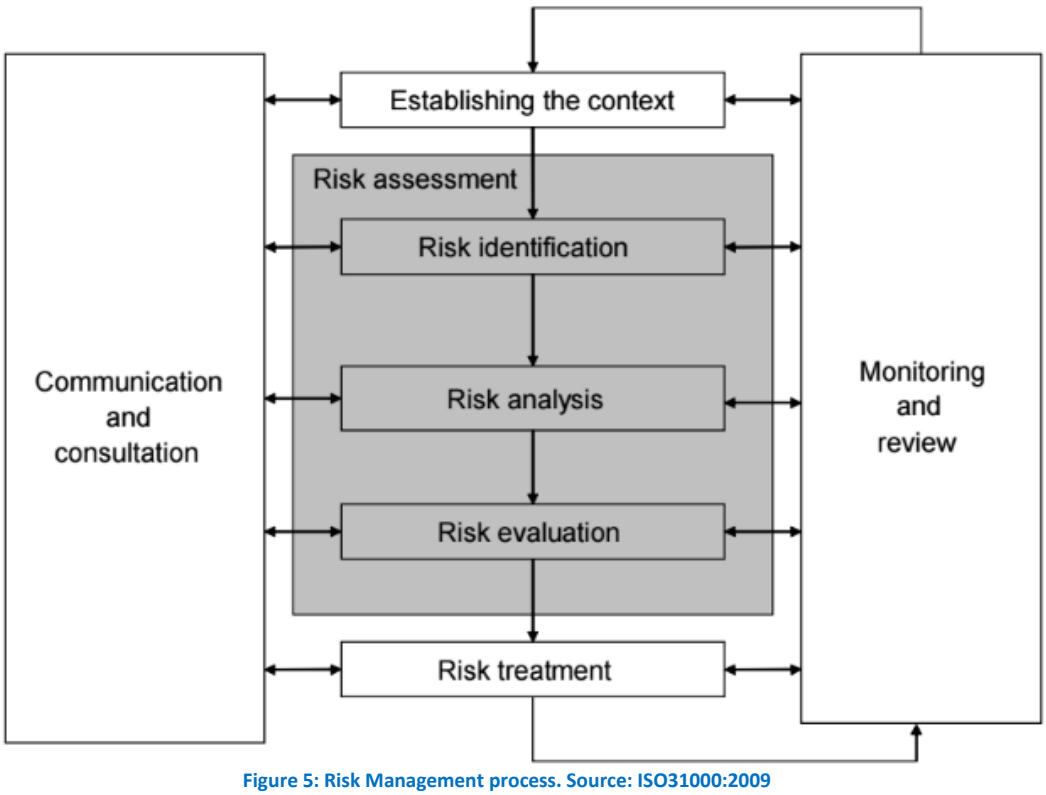


Figure 5: Risk Management process. Source: ISO31000:2009

3.7.1 Risk Management and phishing prevention

As discussed in the previous section, we argue, that risk management can be applied in order the help the management of phishing prevention efforts in an organisation. The Risk Management process proposed in the standard ISO31000:2009, as shown in figure 5 above, has two elements which requires continuous execution, 'communication and consultation' and 'monitoring and review'. These continuous execution elements relate well to the challenge of shifting requirements, as described in the general findings (F2, F4, and F8). *Communication* relates to phishing prevention in that employees need to be periodically informed about the emerging phishing methods, techniques, and attack vectors, in order to allow them to act effectively in the case of a phishing attack. *Consultation* is related to phishing prevention in that employees need to report every presumption or occurrence of a phishing attacks, in order to enable the organisation to take effective measures. The Risk Management process, as proposed by the standard ISO31000:2009, has also elements which requires not continuous but periodically recurrent execution. Two of these elements, Risk Assessment, and Risk Treatment, we argue, are suitable for being adapted and incorporated in a process model for phishing prevention. *Risk Assessment* is the process of identification, analysis and evaluation of risks, this activity relates to phishing prevention in that emerging phishing methods, techniques, and attack vectors need to be identified, analysed and evaluated, in order to enable the organisation to find a balanced risk mitigation approach regarding phishing prevention (F1, F2, F4, F5, F7 and F8). *Risk Treatment* is the process of improving current controls or introducing new controls to match the current level of risks (F11), it relates to phishing prevention in that emerging methods, techniques and attack vectors requires revision of the currently applied solutions, in order to adapt defences to emerging attacks. Based on the argumentation above we argue that phishing prevention, to be effective, needs to be based on risk management.

- Requirement: Phishing prevention must be based on Risk Management.

3.7.2 Risk Assessment

Risk Assessment is the core activity within risk management. Risks assessments are usually performed in a systematic way, following a prescribed methodology. There are thirty-one risk assessment techniques listed on Annex B of the ISO/IEC 31010 to choose from, this guide "*provides guidance on selection and application of systematic techniques for risk assessment*" (IEC, 2009). From the thirty-one risk assessment techniques, we argue, the Bow Tie is to be considered the most appropriate risk assessment techniques to the tasks of investigating risks related to phishing, for the following reasons: First, the application of the method results in a simple diagram, describing the path risk travels, from cause to consequences, having a focus on the barriers between the cause and the risk, and between the risk and the consequences (F1), which translates well to phishing prevention in the sense that those barriers (cause/risk/consequences) are the attack vector and the technique deploy in the phishing attack (F2). Second, the Bow Tie risk assessment can also be constructed directly from the input in a workshop or brainstorm session, making its adoption simpler than other methods (F7). Finally, the only information required to perform an assessment are the cause, the consequences and the barriers to prevent or mitigate the risk (F4). The goal is to perform risk assessment from a phishing prevention perspective, at micro-

level, breaking down the high-level risk of a phishing attack into the smallest fragment possible to include its methods, techniques and attack vectors. Those little risk fragments can then be treated independently of each other, limiting the impact on operations as much as possible and keeping the process manageable.

- Requirement: Risk assessment must be the core activity within the phishing prevention process.

3.7.3 Risk Treatment

After identifying, analysing and evaluating the risks, the risk treatment process enables the organisation to perform decision-making regarding the adjustment of existing controls and/or the development and adoption of new controls to prevent risks materializing. The activities of adjustment of existing controls (F11) and/or the development and adoption of new controls (F5, F8, and F12) within risk treatment, are also applicable in the phishing prevention process. The ISO31000:2009 standard propose a list of options for risk treatment (Purdy, 2010):

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- Removing the risk source;
- Changing the likelihood;
- Changing the consequences;
- Sharing the risk with another party or parties;
- Retaining the risk by informed decision.

3.8 Critical information assets

In the previous chapters, many characteristics of phishing attacks were discussed. One of these characteristics are the pursue of attackers to take over login credentials. Through many different combinations of phishing techniques, attackers aim at login credentials, special credentials regarding online banking or other online financial services (F6). In order to be able to design an effective phishing prevention process, we argue that an overview of critical information assets should be maintained by the organisation, this CIA inventory will be incorporated in the risk assessment process. Critical information assets can encompass many kinds of data: From bank accounts number to credit card details to intellectual property. In the context of phishing, Critical Information Assets (CIA) are any piece of information that would be crucial for helping the attacker achieve its goals.

- Requirement: Access to Critical Information Assets is restricted to employees who 'need-to-know'.

3.9 Incident Management

Most organisations that utilize Information Systems in the performance of its business processes have an Incident Management process in place. This process is often managed by a helpdesk or a shared service centre and acts as a single point of contact between all employees and IT operations. The incident management process, we argue, need to be adjusted in order to assist the phishing prevention process in the communication with employees. This two-way communication channels should be used by employees to rapport all presumptions of phishing attacks, transmitting the necessary details for the assessment of the suspected attack, leading to a confirmation or refute. On the other hand, the two-way communication channels should also be used to inform employees about confirmed phishing attacks. One of the recommended modification would be to include the dispatch of a general communication note to all employees, every time a phishing attack is reported and confirmed (F4, F9, F10, and F12). The notice should be short and concise and only include extra explanatory information in the case that an unprecedented type of attack is reported. The integration of the phishing prevention process within Incident Management aims at the acceleration of knowledge dissemination within the organisation with respect to previously unknown phishing attack methods, techniques, and attack vectors.

- Requirement: Users are informed about emerging social-engineering methods, techniques and vector attacks and in case of confirmed attacks against the organisation.

3.10 Summary of design Requirements

In the previous sections, the identified challenges to phishing prevention were elaborated, these challenges were extracted from the findings in previous chapters. From the analysis of each identified challenges, design requirements were synthesized. In the table below we present a summary of the requirements for the design of the process model for phishing prevention, which will be exposed in the next chapter.

#	Requirement description
R1:	Phishing prevention must be adaptive, incremental and continuous.
R2:	Phishing prevention should be embodied in the organisation improvement cycle.
R3:	Phishing prevention must be based on Risk Management.
R4:	Risk assessment should be the core activity within the phishing prevention process.
R5:	The organisation knowledge of emerging phishing methods, techniques, and attack vectors, is up-to-date and its impact in the organisation can be quickly assessed.
R6:	Employees are educated about emerging social-engineering methods, techniques and vector attacks, and quickly informed in case of a confirmed attacks against the organisation.
R7:	Access to Critical Information Assets (CIA) is restricted to the employees who 'need-to-known'.
R8:	The organisation implements current proven (technical) solutions as soon as possible.
R9:	Security controls are adopted only if no considerable impact in usability is evident.
R10:	The Phishing prevention improvement cycle should be short, preferably a Quarter of year.
R11:	Every presumption of a phishing attack is investigated, every confirmed attack is communicated to all employees, to the authorities and, if possible, the attacker(s) prosecuted
R12:	Technical measures, user education, and process engineering approaches must be aligned, based on a risk assessment, with the phishing prevention process.

Table 3: Design Requirements for the creation of a Process Model for Phishing Prevention

In the previous chapters, knowledge regarding the problem domain and the current practices in phishing prevention were aggregated. This knowledge was summarized, leading to the identification of the general findings. The findings were subsequently analysed, resulting in the identification of a set of challenges in phishing prevention. The identified challenges were then elaborated, analyzed, combined and synthesized into a set of design requirements. In this chapter, the design process pursued will be presented, as the resulting process model, together with a methodological justification of how each requirement was addressed during the development of the process model and the accompanying guidelines. The process model and guidelines are the fulfillment of the main goal of this research.

4.1 DESIGN PROCESS

In the introduction chapter, the process model has been defined to be developed as *an abstraction and representation of the sequence of activities required for the design of a process dedicated to the prevention of phishing in an organisational environment*. The proposed process model is thus a blueprint, the representation of a generalized phishing prevention process, designed to be customizable, in order to be useful as a model for the design of a specific phishing prevention process, tailored for a specific organisation, allowing phishing prevention efforts within an organisation to be managed as an improvement cycle. The process model, when applied to a specific organisation by a cyber security practitioner and in combination with the guidelines, enables the methodological investigation of the problem environment, through the execution of the initial steps in the process model. The study of the problem environment made plausible our argumentation that the Risk Management process – as proposed by the ISO standard for risk management ISO31000:2009 – have common characteristics with the process required to manage phishing prevention within an organisation. The risk management process can thus be expanded, adapted and transformed, resulting in a phishing prevention process that is familiar to many organisations and could help making uncertainties around phishing attacks manageable. As demonstrated in section 3.7 and based on the findings, challenges and the design requirements presented in the previous chapter, we argue that some components of the risk management process have evident similarities with the components required in a phishing prevention process. In the figure 6 below, the components identified as necessary in a phishing prevention process, in line with the design requirements, are arranged in superimposition of the risk management process.

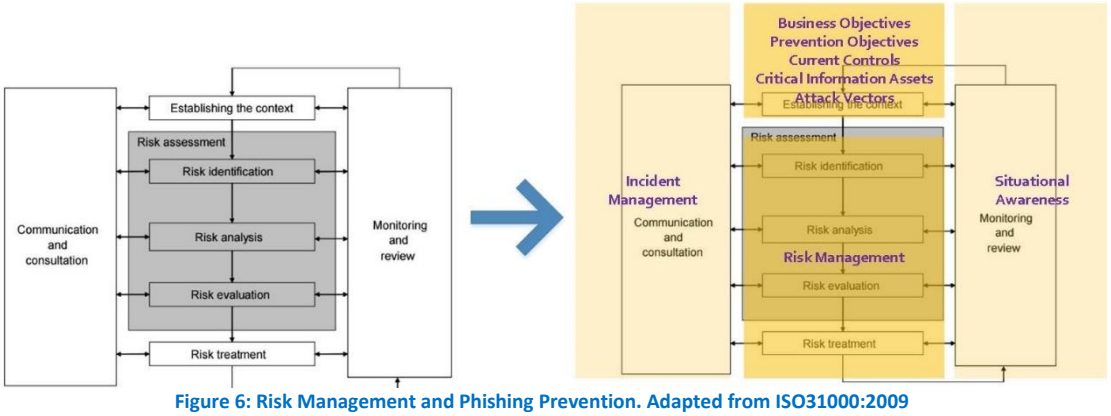


Figure 6: Risk Management and Phishing Prevention. Adapted from ISO31000:2009

4.1.1 Design Process methodology

Based on the investigation of each the identified challenges presented in section 3.1 and the requirements presented in section 3.10, the concepts related to the sequence of events and activities belonging to the phishing prevention process were one-by-one plotted on the risk management process. By reasoning on the suitability of each necessary component in a phishing prevention process, to a particular place within the risk management process, both the continuously active and the recurring components had its place in the structure of the process assigned. The next step was set, based on the requirements and risk management process knowledge, by reasoning on the appropriate sequence of components. We argue that placing Business Objectives before Prevention Objectives is a logical sequence for the inaugural components, equating those components to *Establishing the context* in the risk management process. The next components to be placed in the sequence were the components that assists in the investigation of the problem environment, because those components are responsible for the initial production of knowledge that is subsequently required as input for the risk assessment components: Critical Information Assets inventory, Current Practices and Controls inventory, Communication Channels inventory and Phishing Methods inventory.

These four inventories can be performed in parallel and provide input for the next components in the sequence. The product of each inventory consists of an overview or a list to be stored in the Knowledge Base. With the product of the six initial components being stored in the Knowledge Base and available for consultation, the core activity in the phishing prevention process can have its central place in the sequence assigned: Risk Assessment. The risk assessment element here contains exactly the same steps as in the risk management process: Risk Identification, Risk Analysis and Risk Evaluation. This activities are performed sequentially, the Risk Assessment component produces output in the form of a report, containing a prioritized list of risks and an account of the information generated during the workshops sessions. The output of the risk assessment is stored in the Knowledge Base as well. The prioritized list is the necessary input for the component obviously placed next in the sequence: Risk Treatment. In the risk treatment step, the prioritized list is used in the decision-making process regarding the adjustment of existing security controls or the implementation of new security controls. The output of Risk Treatment consists of an updated prioritized list, which is then stored in the Knowledge Base.

The components to be placed next in the sequence are the performance steps, which are responsible for the actual implementation of prioritized preventive measures in the organisation. With the updated prioritized list being available for consultation, the performance components can be executed in parallel: Perform Adjustment/Implement Controls, Perform User Education and Perform Process Engineering. The output of the previous steps consists of an updated list of current controls to be stored in the Knowledge Base. When the duration of the improvement cycle is coming to an end, a report on the ending improvement cycle is produced, which is also stored in the Knowledge Base and distributed to management and employees in the organisation.

4.1.2 Optimization of the Process Model

In the previous section the design process methodology observed during the development of the process model first draft, was discussed in detail. In this section, the first draft of the Process Model undergoes an incremental iteration, required for both the optimisation of the information traffic with the Knowledge Base, as to the addition of requirements missing in the first draft.

Situational Awareness

Situational Awareness, a continuous activity that includes communication with the outside world, is place on the right side of the process model. Incoming communication represents updates from partners in the cyber security community and authorities, regarding alerts, news, technical descriptions, rapports etc. Outgoing communication represents updates to partners in the cyber security community and authorities, regarding information disclosure on phishing attacks, filing complaints to the authorities against cyber criminals etc., in fulfilment of the requirement that all confirmed phishing attacks must be communicated to the authorities and if possible, the attacker undergo prosecution.

Incident Management

Incident Management is an existing process in most organisations relying in information technology to the execution of business processes. Based on the design requirements, the incident management process should be integrated within the Situational Awareness component on the right side of the process model, represented by the image of a helpdesk employee. Incoming communications in the form of a service call represents users contacting the helpdesk to report a suspicious event that could be part of a phishing attack. Outgoing communication in the form of a newsletter represents employees being informed about confirmed phishing attacks against the organisation and about novel phishing methods, techniques, and attack vectors.

Knowledge Base

The output of the process model components can be further detailed in order to indicate the information stored in the knowledge base. At the end of the improvement cycle period, the knowledge base should contain the following information:

- Description of the Business Objectives
- Description of the Prevention Objectives
- Critical Information Assets List
- Current Controls list
- Communication Channels list
- Phishing methods update
- Risk Assessment log
- Risk Assessment report
- Planning (for the implementation of preventive measures)
- Periodical rapport (on phishing prevention)

4.2 Guidelines

Based on the description of the process model presented from the previous section, in this section, the guidelines for application of the process model are discussed. As in the case of the process model itself, these guidelines were induced from the findings in chapters 2 and the discussion of the topics in chapter 3. The study of Risk Management contributed to the creation of the guidelines, resulting in description of the main ingredients of each process step in the process model. The guidelines aim to provide guidance to the use of the process model, providing guidance during the development and implementation of the phishing prevention process.

4.2.1.1 Guideline 1: Business Objectives

In the inaugural step of the process model, an overview of the strategic business goals of the organisation is collected. This step is at the same time intended as a preliminary investigation into the feasibility of the project. The collected business objectives are the departing point for gathering requirements for the customization of the phishing prevention process. Business objectives provide the context in which the organisation operates, its stakeholders, relations with society etc. In this step, it's important to determine which approach the organisation adheres regarding quality, risk and security management. The nominal length of the improvement cycle is also set in this step, preferably in sync with the reporting period adopted in the organisation. The results of this step are stored in the Knowledge Base, in the form of a description of the business objectives.

4.2.1.2 Guideline 2: Prevention Objectives

In the second step of the process model, the business needs regarding phishing prevention are established. It is important that in this step the prevention objectives are aligned with the business objectives in the previous step. Different organisations require different prevention objectives, a commercial bank, and other financial services providers have different prevention objectives than government agencies. This step is also intended as a preliminary investigation into the feasibility of the project. In this step, it is important to establish the scope of the project, the Key-Performance Indicators (KPI) and unambiguous goals for prevention. The results of this step are stored in the Knowledge Base, in the form of a description of the prevention objectives.

4.2.1.3 Guideline 3: Critical information assets inventory

In this process step an inventory of the critical information assets is made. The list is important in order to discover what the "Crown jewels" of the organisation are and how the responsibility for the critical information assets is regulated within the organisation. In general, the inventory should contain a quantitative estimation of the monetary value of each critical information asset. Critical information asset like login credentials, online banking details, credit card details, should be listed together with Intellectual Property and other information that might be crucial for phishing attackers to be successful in stealing value from the organisation. This list is used as input to the risk assessment. The results of this step are stored in the Knowledge Base, in the form of a critical information assets list.

4.2.1.4 Guideline 4: Current controls inventory

In this process step an inventory of the currently adopted cyber security controls is made. The list will be used as input to the risk assessment and risk treatment steps. It is important in this step to differentiate between currently *adopted* controls and currently *available* controls. One of the requirements demands currently available controls to be deployed as soon as possible, while the implementation of these controls is addressed in the Adjust/Implement Controls step. The results of this step are stored in the Knowledge Base, in the form of a current controls list.

4.2.1.5 Guideline 5: Communication channels inventory

In this process step, an inventory of the communication channels available in the organisation is made, prioritized by the dependency of business operations on each channel. This list is important for the whole process and functions as input to the risk assessment step. With this list, the impact of new phishing methods, techniques and attack vectors (communication channels) can be estimated. With the list, an overview can be made of disclosed vulnerabilities impacting each channel. The results of this step are stored in the Knowledge Base, in the form of a communication channels list.

4.2.1.6 Guideline 6: phishing methods update

In this process step an update is performed regarding the currently known trends in phishing methods, techniques, and attack vectors. Actual trends in phishing methods, techniques and attack vectors, should be included in the update, together with the description of the *modus operandi* of each method, technique and attack vector. This list is important for the whole process and functions as input to the risk assessment step. With this list, the efficacy of current controls can be evaluated. The results of this step are stored in the Knowledge Base, in the form of a phishing methods update.

4.2.1.7 Guideline 7: Risk Assessment Identification

In this step, the execution of a risk assessment begins. The risk assessment steps Identification is performed in accordance to the risk assessment technique of choice. The risk assessment technique of choice should help the participants to envision what possible developments could damage the business objectives, how those developments could materialize and when. The first step of the risk assessment is crucial for determining the level of risk the organisation is exposed to. The results of this step are stored in the Knowledge Base in the form of a risk assessment log and are used in the execution of the next step in the sequence.

4.2.1.8 Guideline 8: Risk Assessment Analysis

In this step, the execution of a risk assessment proceeds with the investigation of each identified risk separately. This investigation aims to estimate the possible consequences (impact) and the likelihood of each identified risk becoming reality. Estimations of impact (consequences) and chance (likelihood) can be expressed either as a quantitative, semi-quantitative or qualitative value. It is important to use the current controls list, produced in the previous step, to estimate the reliability of currently *deployed* controls. Identified risks which are already mitigated by existing controls, can be marked as acceptable risk. In case the existing controls are judge insufficient, the risk should be further evaluated in the next step. The results of this step are stored in the Knowledge Base in the form of a risk assessment log and are used in the execution of the next step in the sequence.

4.2.1.9 Guideline 9: Risk Assessment Evaluation

In this step, the execution of a risk assessment is completed with the prioritization of the analysed risks, based on the estimations of impact and likelihood defined in the previous step. It is important to maintain a helicopter view of all identified risks estimations of impact and likelihood and the reliability of currently deployed controls. In order to achieve an adequate prioritization, the values expressing impact and likelihood should be equally distributed between all risks, allowing the participants in the risk assessment sessions to evenly rate each risk separately. A common practice in risk assessment is to divide the spectrum of possible values expressing impact and likelihood into three categories: Low, Medium, and High. The results of this step are stored in the Knowledge Base in the form of a risk assessment log and are used in the execution of the next step in the sequence.

4.2.1.10 Guideline 10: Risk Treatment

In this step decisions are made concerning the adjustment of existing controls and/or the adoption of new controls. In this step the modified and/or new controls are investigated for impact regarding the usability of information systems, as well as efficient alignment of technical, user education and process engineering measures. In this step, it is also important to develop the planning for implementation of the proposed measures. The prioritized risk assessment log produced in the risk assessment, functions as input for this step. The output of this steps is an updated risk assessment log, containing the measures to be taken and a planning for implementation of the proposed measures. The results of this step are stored in the Knowledge Base.

4.2.1.11 Guideline 11: Adjust and Implement controls

In this step, the adjusted and/or new controls – which were prioritized and planned in the previous step – are actually implemented in the organisation. This steps might include interaction with other processes within the organisation. Each adjusted and/or new control needs a different approach, depending on how the control is implemented in the organisation. For example, if a new control requires changes in a business application, a request for change might be applicable. Results are stored in the Knowledge Base.

4.2.1.12 Guideline 12: perform user education

In this step, the activities related to user education are deployed. The performance of these activities could take place in workshops, newsletters, master classes etc. Results are stored in the Knowledge Base.

4.2.1.13 Guideline 13: perform process engineering

In this step, the process engineering solutions are implemented. The execution of this steps might depend on interaction with other business processes. In example, the verification procedure for accessing the corporate online banking account could be modified to prevent login credentials being stolen. A process engineering solutions would then require interaction with the change management process, in order to add extra assurance in the verification procedure. Results are stored in the Knowledge Base.

4.2.1.14 Guideline 14: Periodic reporting

A report is written at the end of the improvement cycle. This report containing an account on the progress achieved during the period. The report is distributed within the organisation, informing management and employees about the performance of the phishing prevention process. The end of an improvement cycle period marks the beginning of the next round.

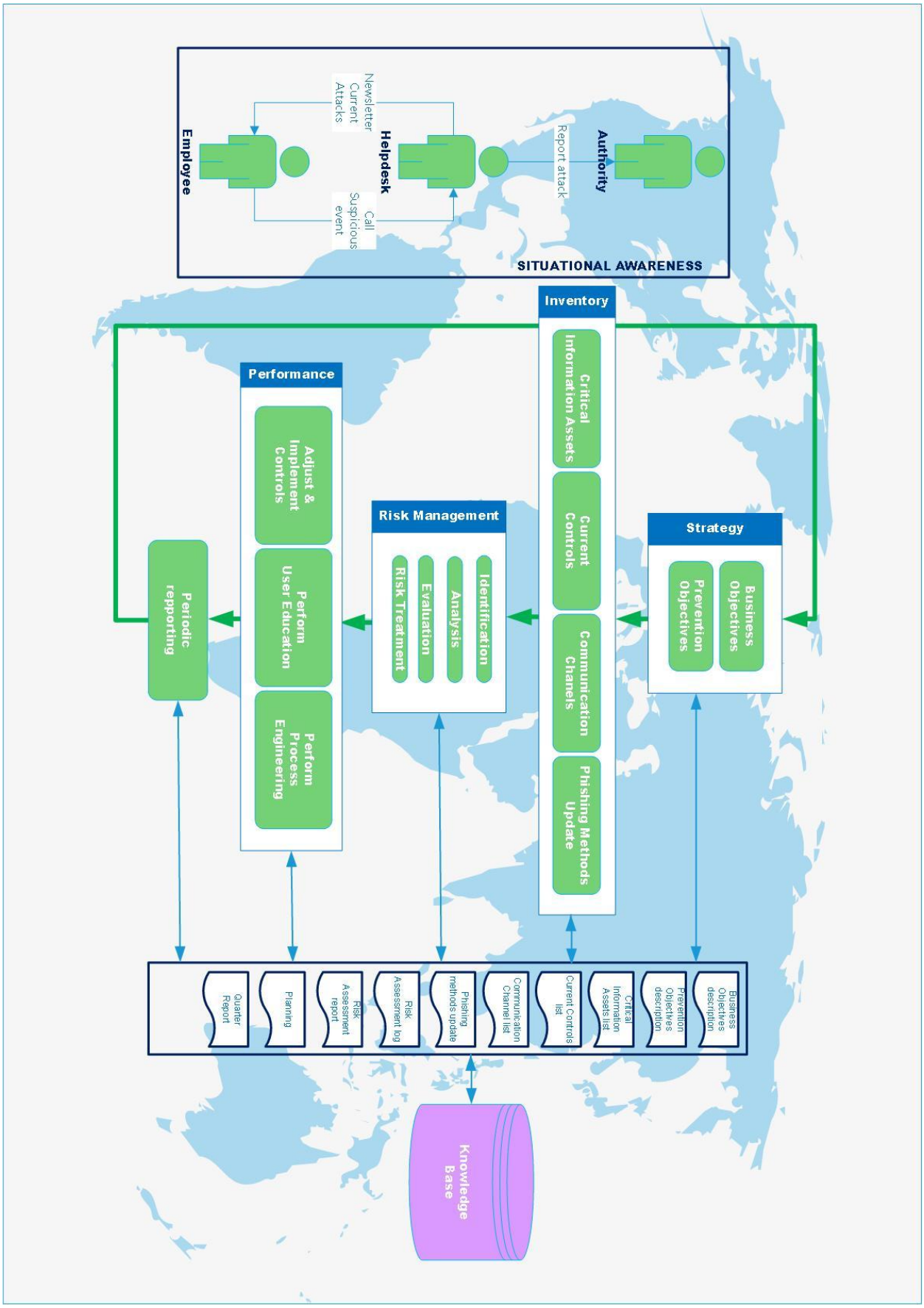
4.2.1.15 Guideline 15: Situational awareness

Situational Awareness is a part of the phishing prevention process that coordinates communication and therefore needs to be is always on stand-by in case of an emergency. Implementing situational awareness means interacting with other business processes and with the outside world. In the process model, incoming communication represents updates from partners in the cyber security community and authorities, regarding alerts, news, technical descriptions, rapports etc. Outgoing communication represents updates to partners in the cyber security community and authorities, regarding information disclosure on phishing attacks, filing complaints to the authorities against cyber criminals etc.

4.3 Resulting process model

As a result of the previous sections and the reoccurring analysis, this section present the resulting process model. There are four core elements in the process model: *Strategy, Inventory, Risk Management* and *Performance*. Next to the core elements, two peripheral elements compose the process model: *Knowledge Base* and *Situational Awareness*. The core elements contain *sequential* and *parallel* process steps. Strategy consists of two sequential process steps: *Business Objectives* and *Prevention Objectives*. Inventory contains four parallel process steps: *Critical Information Assets, Current Controls, Communication Channels* and *Phishing Methods Update*. Risk Management contains four sequential process steps: *Identification, Analysis, Evaluation* and *Risk Treatment*. Performance contains three sequential process steps: *Adjust & Implement Controls, Perform User Education* and *Perform Process Engineering*. Situational Awareness deals with internal and external communication and the links with the existing processes in the organisation, while the Knowledge Base represents a container in which the output of the activities are stored.

Figure 7: Phishing Prevention Process Model based on previous analysis



4.4 Implementation of the process model in practice

In the previous sections we presented the guidelines and the process model for phishing prevention. In this section we discuss the implementation of the process model in practice. We argue that the implementation of the process model in practice should be conducted in a project basis, because the framework and tools provided by project management methodologies can be helpful in the planning and execution of the task. Project management is a best-practice, widely used in the IT industry (White, 2002). The project manager is responsible for the scope, planning and execution of all activities required for the development and deployment of the phishing prevention process in the organisation. We argue that the project should contain at least the following four distinct phases:

- *Initiation*

The initiation phase regards the feasibility, scope and planning of the project. The process steps *Business objectives* and *Prevention objectives* can be executed in this phase, the results will determine the feasibility of the project and constitutes the basis for the development of the phishing prevention process.

- *Development*

Through the customization of each process steps, a bespoke process can be developed. Tooling required for the support of the process, including storage for the *Knowledge base,* can be selected in this phase. The internal and external communication processes within *Situational awareness* can be developed, including the instructions for employees responsible for handling communication.

- *Execution*

Starting with the parallel process steps *Critical information assets, Current controls, Communication channels and Phishing methods update*, followed by the sequential process steps *Identification, Analysis, Evaluation and Risk treatment* and by the parallel process steps *Adjust & implement controls, Perform user education and Perform process engineering*, the phishing prevention process is executed for the first time, being finalized with the first periodic reporting.

- *Transfer*

The phishing prevention process is embedded in the regular organisation through the transferring of the project deliverables to the business unit responsible for further execution of the phishing prevention process.

4.5 mitigation of phishing-related risks

In the previous section we discussed the application of the process model in practice. In this section we discuss how the process model can support organisations in the mitigation of phishing-related risks. We argue that the process model presented in this study can support organisations in the mitigation of phishing-related risks by introducing a risk management approach to phishing prevention: In this approach, organisations are required to keep information updated about its communication channels, critical information assets, current security controls and phishing attacks. This information enables organisations to quickly assess the impact and likelihood of recently discovered phishing attacks. The process model requires organisations to perform recurring risk assessments. The organisations are also required to mitigate phishing-related risk using technical, user education and process engineering measures.

5 VALIDATION

In this chapter, the validation of the proposed process model is presented. The most important question to be answered here is whether the developed process model is a useful tool against phishing. The process model is examined through the application of two assessment methods. First, the *design* of the process model is tested against the design requirements. The resulting process model must, in order to be considered valid, fulfill all the requirements. Second, the *utility* of the developed process model is evaluated through a consultation of cyber security experts regarding the process model completeness, usability, and usefulness. The opinions of Cyber security experts were collected using semi-structured interviews in which, simultaneously, the research results were communicated to those members of the cyber security community and relevant feedback about this study was provided.

5.1 Design validation

In this section, a first attempt to evaluate the proposed process model is made, beginning with a validation of the *design* of the process model. This validation aims to demonstrate that all the identified challenges are addressed in the design of the process model and that all requirements have been fulfilled. The test setup consists in cataloguing the identified challenges, requirements, and components of the process model, in order to demonstrate which component fulfilled which requirement addressing which challenge. Table 4 below evidences exactly which challenge is addressed by which requirement, displaying which requirement is fulfilled by which component in the process model. The validation is to be considered successful when all identified challenges have been addressed by the requirements and all the requirements have been fulfilled by the components in the design of the process model.

Identified Challenges	*Requirements*	*Component*
Phishing is the collective name given to a variety of cyber-attacks that employ automated social-engineering methods and exploit the human – machine interface.	Phishing prevention must be adaptive, incremental and continuous (R1).	Whole the process model addresses this challenge and fulfill this requirement. The process model was adapted from risk management to support an adaptive, incremental and continuous process.
Phishing can be executed through different methods, using various techniques and being propagated by multiple attack vectors. There are many possible combinations of methods, techniques, and attack vectors.	Phishing prevention should be embodied in the organisation improvement cycle (R2).	Almost all process steps address this challenge and fulfill this requirement, specially the following steps: Organisation Objectives, Risk Management and Periodic Reporting.
Current mitigation effort produced countermeasures that are either of a pure technical nature or only directed to user education. Process engineering could be added to the effort.	Phishing prevention must be based on Risk Management (R3).	The process step Risk Management addresses this challenge and fulfill this requirement.
There is an arms race going on between attackers and defenders. Every new solution triggers a	Risk assessment should be the core activity within the phishing prevention process (R4).	The process step Risk Management addresses this challenge and fulfill this

subsequent new variation of phishing attacks. The requirements for solutions are constantly changing. Phishing prevention needs to be adaptive, incremental and continuous.		requirement.
Prevention measures can cause a decrease in efficiency, usability and security in information systems due to complex interaction with users.	The organisation knowledge of emerging phishing methods, techniques and attack vectors, is up-to-date and its impact in the organisation can be quickly assessed (R5).	The process steps Situational Awareness, Current Controls, Communication Channels, Critical Information Assets and Phishing Methods Update all addresses this challenge and fulfill this requirement.
Cyber criminals are designing and executing phishing campaigns mainly for the purpose of stealing login credentials, credentials that can be used to seize control of financial and informational assets. Protecting this assets is crucial for phishing prevention.	Employees are educated about emerging social-engineering methods, techniques and vector attacks, and quickly informed in case of a confirmed attacks against the organisation (R6).	The process steps Situational Awareness and Perform User Education both addresses this challenge and fulfill this requirement.
Cyber criminals and other threat actors like cyber spies and hacktivists are making use of phishing attacks. Phishing prevention need to be persistent.	Access to Critical Information Assets (CIA) is restricted to employees who 'need-to-know' (R7).	The process steps Critical Information Assets and Perform Process Engineering both addresses this challenge and fulfill this requirement.
Emerging communication technologies like Social Media, Instant Messengers etc. quickly becomes attack vector for phishing propagation.	The organisation implements current proven (technical) solutions as soon as possible (R8).	The process steps Adjust & Implement Controls and Risk Management both addresses this challenge and fulfill this requirement.
Next to targeting login credentials to steal, phishing is also used to install malware at the target end. This malware can be used for many purposes, including spying the target, recording keystrokes, running a botnet, ransomware etc.	Security controls are adopted only if no considerable impact in usability is evident (R9).	The process steps Adjust & Implement Controls and Risk Management both addresses this challenge and fulfill this requirement.
Techniques like cross-site scripting and cross-site request forgery can trusted website, the target has no way of knowing that the website has been compromised.	The Phishing prevention improvement cycle should be short, preferably a Quarter of year (R10)	The process step Periodic Reporting addresses this challenge and fulfill this requirement.
Current practices are directed at stopping phishing e-mail entering the organisation, password management, black-listing phishing webservers and websites, applying two-factor or multi-channel authentication and user education. This practices all adds to successful phishing prevention.	Every presumption of a phishing attack is investigated, every confirmed attack is communicated to all employees, to the authorities and, if possible, the attacker(s) prosecuted (R11)	The process step Situational Awareness addresses this challenge and fulfill this requirement.
User education training utilizes demonstrations of currently known phishing attacks. Unknown attacks are a blind-spot that need to be addressed through prevention.	Technical measures, user education and process engineering approaches must be aligned, based on a risk assessment, with the phishing prevention process (R12)	The process steps Adjust & Implement Controls and Risk Management both addresses this challenge and fulfill this requirement.

Table 4: Validation Identified Challenges and Requirements

5.2 Utility validation

In the previous section the design of the proposed process model was the subject of validation. In this section the quality of the process model is evaluated in terms of utility. The utility of the process model is evaluated though a consultation of cyber security experts. The ordeal of those experts was collected using semi-structured interviews in which the research results were communicated to those members of the cyber security community. The interviews were conducted with the collaboration of four experienced cyber security experts, providing relevant feedback for this study. The interviews had an average duration of ninety minutes, the interviewee received the survey questions and the summary of the research prior to the interview. All four interviewees have at least 5 to 10 years of experience in cyber security operations, cyber security management, consultancy and IT audit, working in multinational corporations, government agencies and consulting firms in the Netherlands. Their privacy is guaranteed, names nor affiliations are disclosed. The survey questionnaire used in the semi-structured interviews can be found in the Annex A. In Annex B a summary of the research can be found, which was used to communicate the results of the research to the interviewees. In the following sub-sections, the opinions expressed by the majority of the experts during the interviews are presented.

5.2.1 Expert opinion: Design Requirements

In this section the opinion the interviewees concerning the design requirements is summarized. Based on the answers given by interviewees to the questions regarding the design requirements, it is evident that cyber security experts regard user education as the most important requirement (requirement #6) for phishing prevention. Their choice was justified in part because phishing attacks can only be successful though the mislead of an employee, in part because technical measures alone are not able prevent *all* users being misled *all the time*. Cyber security experts expect – despite all present and possible future technical solutions – user education to remain a crucial priority and concern in the field of phishing prevention. Next to user education, keeping the organisation's knowledge about phishing methods, techniques and vectors up to date (requirement #6), is seen as almost equally important as user education. Interviewees also selected mandatory adaptive, incremental and continuous prevention (requirement #1) as one of the top-three most important requirements, together with a short phishing prevention improvement cycle (requirement #10). According to the interviewees, one specific requirement should be added to the list of requirements: *Prevention should be automated through monitoring*. This monitoring should include phishing prevention triggers, those triggers should raise red flags alerts to the organisation whenever certain signals indicating possible abuse are detected. The triggers must be continuously updated to incorporate signals of abuse discovered in previous and current attacks.

5.2.2 Expert opinion: Risk Management

Based on the answers given to the questions regarding the use of the risk management process as the basis for the design of a process model for phishing prevention, it is evident that experts are unanimously positive about an approach based on risk management. The reason for being positive about the proposed approach was the expected advantages of the familiarity of risk management to most organisations, ranging from a potential straightforward adoption and implementation of the process model to the possible use of the proposed approach for the prevention of other high-risk threats than phishing only. According to the experts, the proposed process model might be an effective approach to prevention of other high-risk threats, being useful not only for phishing prevention but also for other high-risks threats like espionage or Advanced Persistent Threats (APT). Furthermore, the interviewees expressed the opinion that they recognized all elements of the risk management process – in one way of another – in the proposed phishing prevention process model. In their opinion, the process steps are well adjusted to the challenges of phishing prevention. The most obvious advantage of the proposed approach is that it might be simple and quick to implement – following the assumption that most organisations have adopted risk management in their decision-making process – bringing about the possibility of (re)utilization of resources already available in the organisation.

5.2.3 Expert opinion: The Process Model

Based on the answers given by cyber security experts regarding the process model, it can be said that the process model is valued as useful in their opinion. The majority of the experts were able to identify a flaw in the design of the process model, which could be perfected by the addition of an extra step dedicated to the improvement of the process itself, at the end of the process. The interviewed experts expressed the opinion that the process model can be useful in practice, even if it's not officially adopted by the organisation and is used solely as a guideline for cyber security professionals, being also useful in facilitating communication about phishing prevention in the organisation. As mentioned earlier, the interviewees expressed the opinion that the process model can be useful for the prevention of other high-risk threats, not only for phishing prevention. In the case of government agencies, the process model might also be effective for the organisation's amenability to government leaders and parliament members, especially in the case the government is required to justify its actions regarding the prevention of a high-risk threat: Instead of pointing out to the general cyber security efforts, government agencies could vindicate with a prevention process, specific tailored to the threat in question. Experts expressed the opinion that the proposed process model should be easily implementable in organisations that already have a well-established risk management process, for the process model is recognizable for the most organisations, this familiarity being inherited from the risk management process – an advantage that could lead to a quick and simple adoption and implementation.

6 CONCLUSION

6.1 Conclusions

The research main conclusion regards the design of a process model for phishing prevention. The process model is designed to help cyber security professionals in the development of a phishing prevention process. Based on the judgment of experienced cyber security experts, we conclude that the process model presented in this study is a useful tool for organisations in the fight against phishing. The process model is accompanied by guidelines, explaining the relevance, the activities, the necessary input and output of each process step. The design of the process model was validated by matching the process model to the design requirement, safeguarding the rigidity in the design process of the artefact produced in this study. The process model itself was validated by expert opinion, gathered through semi-structured interviews with cyber security experts, safeguarding the relevance and utility of the artefact produced this in study.

6.2 Contributions

In this study the phenomenon of phishing attacks is investigated. This investigation evidenced the necessity of the adoption of a phishing prevention process in organisations. Through the study of phishing prevention in the literature, a set of general findings was identified. The findings were investigated, resulting in a set of challenges for phishing prevention. Based on the identified challenges, a set of design requirement was synthesized. The design requirements were then used in the design of the process model. This research contributes to cyber security in general and to phishing prevention in particular, by proposing a general process model that can be adjusted to the specific business needs of a wide range of organisations. The proposed process model is based on risk management, having risk assessment as its core activity, integrating phishing prevention into existing processes in the organisation. Another contribution of this research can be found in the expansion of the use of risk management in organisations, making the process of risk management suitable for the task of preventing phishing. At last but not at least, the research contributes to phishing prevention by providing a guideline for the process model, facilitating the alignment of technical, user education and process engineering approaches to existing processes in organisations.

6.3 Future research

We recognized a few opportunities for future research in this study. A future research opportunity could lie in the expansion of the process model's guideline, the creation of detailed template set or the development of a software tool that facilitates the management of the phishing prevention process. We also recognize an opportunity for the experimental use of the proposed process model, in the creation of a tailored phishing prevention process, adapted to the specific business needs. Consequently, this context could be used in the generation and analysis of empiric data, for both the improvement of the process model as for the empirical validation of its applicability and efficacy. We also recognize a future research opportunity in the development of a novel risk assessment method and approach, adjusted to the dynamic nature of phishing prevention.

6.4 Limitations

As an experimental, explorative attempt, this research provided conclusions based on the results obtained in fulfillment of the main goal of the research, as described in the first chapter. Next to conclusions, contributions and suggestions for future research, it's important to acknowledge in this last chapter's section that this study was not completely free of limitations. This is important to mention because those limitations might as well have influenced the results. The research was limited by a number of factors, varying from the ambiguity of the research subject to the absence of experimental implementation of the process model in an organisational context. The first limitation concerns the ambiguity of the research subject, namely phishing prevention. The term phishing itself, as demonstrated in the second chapter of this study, refers to a phenomenon in the cyber security discourse that can be interpreted in many different ways, embracing a wide range of methods, techniques, and attack vectors. The quest for prevention of a phenomenon that is not precisely defined resulted in limitations to the scope of the research. Within this context, the research was limited to those appearances of phishing that were found in the literature concerning the automated deployment of social engineering methods in cyber-attacks. The research was also limited by the lack of experimental performance measurements of the proposed process model in an organisational context. This limitation constitutes in itself an opportunity for future research, as mentioned in the previous section. The lack of an experimental implementation of the process model in an organisational context limited the research in its capacity to prescribe the contents of the proposed process model in a more detailed fashion. The experimental implementation of the process model would require commitment and availability of organisational resources, in order to produce empirical data, next to an explicit permission of the organisation for the use of this data in the research and consequently in the publication of the research results. The experimental implementation of the process model was unfeasible to manage during the timespan of this research. Despite the ambiguity of the subject and lack of empirical testing, the research was still able to provide a useful process model for phishing prevention.

Al-Gahtani, S. S., & King, M. (1999). Attitudes, satisfaction and usage: factors contributing to each in the acceptance of information technology. Behaviour & Information Technology, 18(4), 277-297.

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. *IEEE communications surveys & tutorials*, *15*(4), 2070-2090.

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., ... & Ou, X. (2010). Cyber SA: Situational awareness for cyber defense. In Cyber Situational Awareness (pp. 3-13). Springer US.

Barnes, S. J. (2002). The mobile commerce value chain: analysis and future developments. *International journal of information management*, *22*(2), 91-108.

Becker, J., Kugeler, M., & Rosemann, M. (Eds.). (2013). *Process management: a guide for the design of business processes*. Springer Science & Business Media.

Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104). ACM.

Bose, I., & Leung, A. C. M. (2007). Unveiling the mask of phishing: Threats, preventive measures, and responsibilities. *communications of the Association for Information Systems*, *19*(1), 24.

Ceesay, E. N. (2008). *Mitigating phishing attacks: a detection, response and evaluation framework*. University of California at Davis.

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing Attacks and Defenses. *International Journal of Security and Its Applications*, *10*(1), 247-256.

Clayton, R. (2005, April). Insecure real-world authentication protocols (or why phishing is so profitable). In *International Workshop on Security Protocols* (pp. 89-96). Springer Berlin Heidelberg.

Cyber Threat Source Descriptions, [online] Available: https:llics-cert.us-cert.gov/content/cyber-threat-source-descriptions.

Deming, W. E. (1986). Out of the crisis, Massachusetts Institute of Technology. *Center for advanced engineering study, Cambridge, MA*, *510*.

Denning, D. E. (2012). Stuxnet: what has changed?. *Future Internet*, *4*(3), 672-687.

De Querol, R. R., & Kappler, K. E. (2013). Looking for the Social Hackers. In *VaSCo@ WebSci* (pp. 1-12).

Eisen, O. (2012). *U.S. Patent No. 8,151,327*. Washington, DC: U.S. Patent and Trademark Office.

Forte, D. (2009). Anatomy of a phishing attack: a high-level overview. *Network Security*, *2009*(4), 17-19.

Goring, S. P., Rabaiotti, J. R., & Jones, A. J. (2007). Anti-keylogging measures for secure Internet login: an example of the law of unintended consequences. *Computers & Security*, *26*(6), 421-426.

Grant, A. E. (2008). The mobile revolution. *Communication Technology Update and Fundamentals*, 343-350.

Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys (CSUR)*, *48*(3), 37.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81.

IEC, I. (2009). ISO 31010: 2009-11. *Risk management–Risk assessment techniques*.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.

Jakobsson, M. (2005, February). Modeling and preventing phishing attacks. In *Financial Cryptography* (Vol. 5).

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials*, *15*(4), 2091-2121.

Kruck, G. P., & Kruck, S. E. (2006). Spoofing–a look at an evolving threat. *Journal of Computer Information Systems*, *47*(1), 95-100.

Kulikova, O., Heil, R., van den Berg, J., & Pieters, W. (2012, December). Cyber Crisis Management: A decision-support framework for disclosing security incident information. In *Cyber Security (CyberSecurity), 2012 International Conference on* (pp. 103-112). IEEE.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, April). Protecting people from phishing: the design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 905-914). ACM.

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(1), 1.

Lin, X., Zavarsky, P., Ruhl, R., & Lindskog, D. (2009, August). Threat Modeling for CSRF

Manning, R., & Aaron, G. (2016). Phishing Activity Trends Report. *Anti Phishing Work Group, Tech. Rep. 2nd Quarter*.

Milletary, J., & Center, C. C. (2005). Technical trends in phishing attacks. Retrieved December, 1(2007), 3-3.

Marcus, J. S., & Petropoulos, G. (2016). *E-commerce in Europe: parcel delivery prices in a digital single market* (No. 14632). Bruegel.

Marinos, L., & Sfakianakis, A. (2012). ENISA Threat Landscape-Responding to the Evolving Threat Environment. *ENISA (The European Network and Information Security Agency)(September 2012)*.

Marinos, L. (2014). ENISA threat landscape 2014. *European Union Agency for Network and Information Security (ENISA).*

Marinos, L. (2015). ENISA threat landscape 2015. *European Unio13n Agency for Network and Information Security (ENISA).*

Mohd Foozy, F., Ahmad, R., Abdollah, M. F., Yusof, R., & Mas' ud, M. Z. (2011). Generic taxonomy of social engineering attack.

Nohlberg, M. (2008). Securing information assets: understanding, measuring and protecting against social engineering attacks.

Ollmann, G. (2004). The Phishing Guide–Understanding & Preventing Phishing Attacks. *NGS Software Insight Security Research*.

Ollmann, G. (2007). The vishing guide. *h ttp://www. infosecwriters. com/text resources/pdf/IBM ISS vishing guide GOllmann. pdf, IBM, Tech. Rep*.

Panetta, L. (2012). Sustaining US global leadership: priorities for 21st century defense. *Washington, DC: US Department of Defense*.

Parno, B., Kuo, C., & Perrig, A. (2006, February). Phoolproof phishing prevention. In *International Conference on Financial Cryptography and Data Security* (pp. 1-19). Springer Berlin Heidelberg.

Purkait, S. (2012). Phishing counter measures and their effectiveness-literature review. *Information Management & Computer Security*, *20*(5), 382-420.

Purdy, G. (2010). ISO 31000: 2009—setting a new standard for risk management. *Risk analysis*, *30*(6), 881-886.

Rolland, C. (1998, June). A comprehensive view of process engineering. In *International Conference on Advanced Information Systems Engineering* (pp. 1-24). Springer Berlin Heidelberg.

Rolland, C., Prakash, N., & Benjamen, A. (1999). A multi-model view of process modelling. *Requirements Engineering*, *4*(4), 169-187.

Sasse, M. A., Smith, M., Herley, C., Lipford, H., & Vaniea, K. (2016). Debunking Security-Usability Tradeoff Myths. *IEEE Security & Privacy*, *14*(5), 33-39.

Schneier, B. (2000). Semantic network attacks. *Communications of the ACM*, *43*(12), 168-168.

Schultz, E. E., Proctor, R. W., Lien, M. C., & Salvendy, G. (2001). Usability and security an appraisal of usability issues in information security methods. Computers & Security, 20(7), 620-634.

Stamm, S. L. (2009). *Anticipating and hardening the web against socio-technical security attacks* (Doctoral dissertation, Indiana University).

Sheng, X. S. (2009). A policy analysis of phishing countermeasures.

Smirnov, S., Reijers, H. A., Weske, M., & Nugteren, T. (2012). Business process model abstraction: a definition, catalog, and survey. *Distributed and Parallel Databases*, *30*(1), 63-99.

Tranchard, S. (2015, May 13). The revision of ISO 31000 on risk management has started [News]. Retrieved from http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1963

Verkerke, A. T. (2015). *Towards a cyber approach for large organisations*(Doctoral dissertation, TU Delft, Delft University of Technology).

White, D., & Fortune, J. (2002). Current practice in project management—An empirical study. *International journal of project management*, *20*(1), 1-11.

Wilshusen, G. C., & Barkakati, N. (2013). Cybersecurity: National strategy, roles, and responsibilities need to be better defined and more effectively implemented. *GAO Reports*, 1-104.

Zeydan, H. Z., & Selamat, M. S. (2014). Current state of anti-phishing approaches and revealing competencies. *J. Theor. Appl. Inf. Technol*, *70*(3).

Annex A

Process Model Validation Survey

1. Design Requirements Validation

Based on the study of the problem environment a set of challenges to phishing prevention were discovered, this challenges were further investigated, resulting in a set of requirements for the design of a process model for phishing prevention. The requirements are presented in the summary of the research. The first set of questions regards the design requirements.

Q1: Which requirements do you recognize? Nominate 3 of the requirements to the '*top three most important requirements*'. Please explain your choices.

Q2: Is there other requirements you can think about, which are not (fully) identified by the research?

2. Risk Management in Phishing Prevention

The study of the problem environment and the resulting identified challenges suggested similarities between risk management and phishing prevention. The argument for adaptation of risk management process to phishing prevention is central to the research. This following questions are about risk management and phishing prevention.

Q4: Do you agree with the argument for adaptation of risk management to phishing prevention? Why? Is there something else you would like to add?

Q5: What elements from the risk management process would you select to recycle into a phishing prevention process? Why?

Q6: Do you think the risk management process is an useful basis for creating a phishing prevention process? Why?

3. A Process Model for Phishing Prevention

Q7: Is the process model presented, in your opinion, complete? Why? Is there something else missing? Would you like to modify, add or erase anything from it?

Q8: Is the process model useful to you? Why? Is there anything overlooked or overdone in it?

Q9: Do you think the Process Model can implemented? Why?

Q10: Is there something you would leave out of the process model?

4. Open questions

Q11: Is there anything you would like to comment?

Q12: Do you have something to add regarding the summary of the research or the questionnaire or something else?

Annex B

Research summary

1. Introduction

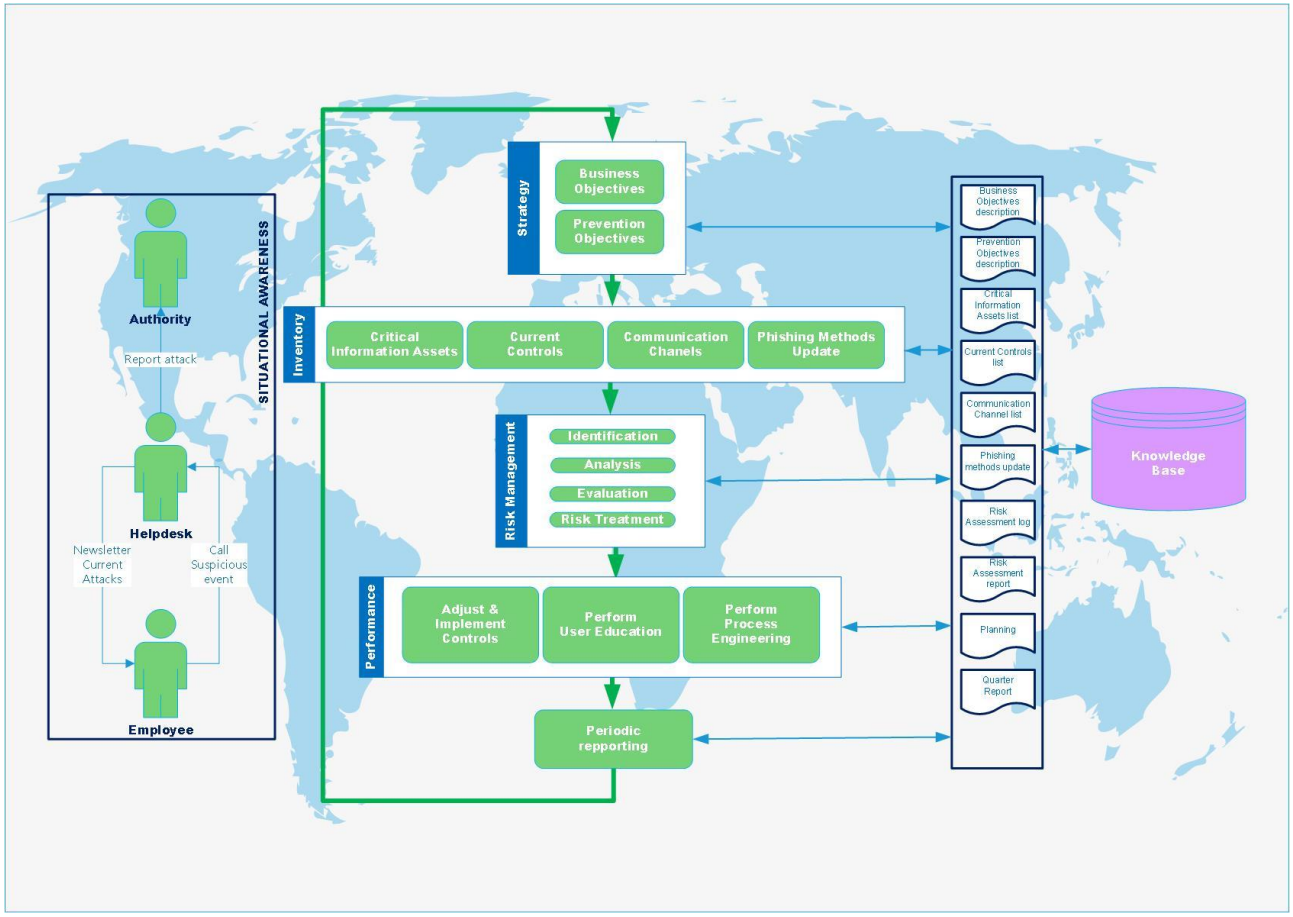
With the widespread of Internet connection throughout the globe, e-commerce became big. Many businesses seized the opportunity to sell their products and services online. Unfortunately, not only businesses and governments expanded their presence in cyberspace; All sorts of criminals extended their activities into cyberspace too. Phishing is a kind cyber security threat that hits individuals, businesses and government alike. Phishing is also a growing problem, both in volume of phishing attacks but also in sophistication. Some sources estimate the damage caused by phishing attacks to be approximately $8.5 billion annually. Organisations trying to keep themselves and their clients safe in cyberspace face difficult challenges when it comes to phishing prevention: Phishing is a complex phenomenon, emerging in many different forms from many different channels, targeting the interaction between people and computers, exploiting technical vulnerabilities and human emotions to perpetrate, among other things, the theft of login credentials for online financial services like credit cards and online banking. The best-known kind of phishing attack is through e-mail messages where the target is lured to click on a link, apparently from an official source. As the target unsuspectingly visits a counterfeit website to perform the action solicited by the attacker (like providing login credentials to online banking account), the victim unwittingly hands over the keys to the content of his bank savings to internet criminals.

2. Research validation

The main goal of the research is to produce a process model for phishing prevention. The purpose of the process model is to help cyber security professionals in the development of a phishing prevention process for their organisations. The main goal is pursued through the achievement of the following milestone: 1. Understanding of what phishing is and what it's not, 2. Understanding the current practice in phishing prevention, 3. Determining the requirements for the design of a process model, 4. Design the process model and 5. Validate the process model. In milestone 1 and 2, a set of challenges to phishing prevention were identified. In milestone 3 the following requirements for the design of a process model for phishing prevention were collected:

#	Requirement description
R1:	Phishing prevention must be adaptive, incremental and continuous.
R2:	Phishing prevention should be embodied in the organisation improvement cycle.
R3:	Phishing prevention must be based on Risk Management.
R4:	Risk assessment should be the core activity within the phishing prevention process.
R5:	The organisation knowledge of emerging phishing methods, techniques and attack vectors, is up-to-date and its impact in the organisation can be quickly assessed.
R6:	Employees are educated about emerging social-engineering methods, techniques and vector attacks, and quickly informed in case of a confirmed attacks against the organisation.
R7:	Access to Critical Information Assets (CIA) is restricted to the employees who 'need-to-know'.
R8:	The organisation implements current proven (technical) solutions as soon as possible.
R9:	Security controls are adopted only if no considerable impact in usability is evident.
R10:	The Phishing prevention improvement cycle should be short, preferably a Quarter of year.
R11:	Every presumption of a phishing attack is investigated, every confirmed attack is communicated to all employees, to the authorities and, if possible, the attacker(s) prosecuted
R12:	Technical measures, users education and process engineering approaches must be aligned, based on a risk assessment, with the phishing prevention process.

In line with the requirements presented above, in milestone 4 the process model was designed, see figure below.



In the next page each component of the process model for phishing prevention is briefly described:

3. Strategy: Business and Prevention Objectives

In the two initial steps, the general business objectives and the goals of the organisation regarding prevention are summarized. Some organisations require distinct protection level than others. These steps are intended as a preliminary investigation into the feasibility of the project. In these steps, it's important to determine which approach to quality, risk management and cyber security are adopted in the organisation.

4. Inventory: Critical Information Assets, Current Controls, Communication Channels and Phishing update

In the next four process steps, an inventory of the critical information assets, cyber security current controls, communication channels and phishing methods, are made. These lists are important, they help to direct the priority to right place, the "Crown jewels" of the organisation. The currently deployed cyber security controls are listed too, together with the inventory of the communication channels which can be used by cyber criminals to launch phishing attacks. Finally, the actual cutting-edge information on phishing attacks is collected. All this information will be used as input to the core element in the process model: Risk Assessment.

5. Risk Management

In this step the actual execution of a risk assessment takes place. The risk assessment steps of Identification, Analysis and Evaluation, follow each other in this sequence, each component adding a deeper level of understanding of the risks, it's possible causes, impact and consequences. The risk assessment results in a risk log that is catalogued, analysed and prioritized, necessary as input for the decision-making process regarding the adoption of security controls.

6. Implementation and reporting

In the next four steps, the selected controls are implemented in the organisation. Activities related to user education and process engineering – the fine-tuning of business process in order to diminish the risk of a successful phishing attack – are performed. Before the cycle is complete, a periodic report needs to be made and distributed in the organisation, in order to inform management and employees about the status of phishing prevention. The end of the cycle announces the beginning of the next cycle.

7. Situational awareness

Situational Awareness is a part of the phishing prevention process that is continuously active or in stand-by, handling external and internal communication. The external communication includes the reporting of phishing attacks to authorities, as well as the gathering of insights from cyber security forums regarding phishing trends. Internal communication includes employees reporting suspected phishing attacks – suspicious e-mails, phone calls, websites etc. – as well as newsletters informing employees about phishing attacks.