Phishing within E-Commerce: *A Trust and Confidence Game*

Greg Megaw
Department of Information Systems
University of Fort Hare
East London, South Africa
gmegaw@gmail.com

Stephen V. Flowerday
Department of Information Systems
University of Fort Hare
East London, South Africa
sflowerday@ufh.ac.za

Abstract—**E-Commerce has been plagued with problems since its inception and this paper examines one of these problems: The lack of user trust in E-commerce created by the risk of phishing. Phishing has grown exponentially together with the expansion of the Internet. This growth and the advancement of technology has not only benefitted honest Internet users, but has enabled criminals to increase their effectiveness which has caused considerable damage to this budding area of commerce. Moreover, it has negatively impacted on both the user and online business, breaking down the trust relationship between them. In an attempt to explore this problem, the following was considered; firstly, e-commerce's vulnerability to phishing attacks. By referring to the Common Criteria Security Model, various critical security areas within e-commerce are identified, and with that, the areas of vulnerability and weakness. Secondly, the methods and techniques used in phishing such as phishing emails, phishing websites and addresses, distributed attacks and redirected attacks as well as the data that phishers seek to obtain, is examined. Furthermore, the way to reduce the risk of phishing and in turn increase the trust between users and websites is explored. Here the importance of Trust and the Uncertainty Reduction Theory plus the fine balance between trust and control is explored. Finally, the paper presents Critical Success Factors that aid in phishing prevention and control, these being: User Authentication, Website Authentication, Email Authentication, Data Cryptography, Communication, and Active Risk Mitigation.**

*Keywords: **E-Commerce, Phishing, Trust, Risk***

I. Introduction

Electronic Commerce is defined as "the buying and selling of products or services over electronic systems such as the Internet and other computer networks" [1]. This largely occurs between two businesses (called B2B) or between a business and a consumer (B2C). Commerce and business transactions conducted over the Internet make use of supporting technologies such as the World Wide Web, Electronic Data Interchange, and E-mail. However, there are a number of threats which exploit these technologies thereby increasing the risk of conducting business online. Along with the significant growth in e-commerce and Internet usage, threats such as phishing have also drastically increased. Criminals have become smarter, using highly sophisticated technologies and social engineering techniques to commit information theft. This threat has resulted in Internet users having less trust in websites, generating a lack of confidence in online businesses, and forming a significant barrier to the development of e-commerce. The severity of this problem can be seen with the significant rise in phishing staring over the period January 2005 to September 2006 [2], to the latest statistics obtained from the Anti Phishing Working Group (the leading, worldwide, anti-phishing law enforcement association) below which illustrates the true extent of the phishing threat as it presently stands:

- In August 2009, the number of unique phishing websites detected by the Anti Phishing Working Group reached an all-time high of 56,362, this being a 1.3 percent increase on the previous record of 55,643 in April, 2007 [3].
- Also, unique phishing reports submitted to the Anti Phishing Working Group in the third quarter of 2009 reached a record number of 40,621 in August, being approximately 5.5 percent higher than the previous reported record high of 38,514 in September 2007 [3].

Consequently, reflecting on these statistics and the numerous occurrences in which record breaking numbers occur, one notes that there has been an aggressive increase in phishing over the 2009 period alone. Thus, it is vital that ways are found to increase the sense of trust within the e-commerce environment by reducing the risk created from the threat of phishing.

The remainder of this paper is organised as follows: Section 2 investigates the areas in which e-commerce is specifically vulnerable to phishing attacks, and reasons why those vulnerabilities exist. Section 3 presents an overview of the common methods and techniques used by phishers to carry out their attacks in order to understand how they work and operate within the world of e-commerce. Section 4 addresses how the sense of trust and confidence can be increased by managing phishing and spoofed websites. An overview of tools used to aid in detecting and preventing phishing is also provided, along with a critical comparison of these tools. Next, Section 5 provides a list of critical success factors to help in successfully reducing the risk created by the threat of phishing, and in turn, increase trust between websites and online users. Finally,

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

Section 6 contains a table which maps CSFs to e-commerce vulnerabilities.

II. E-Commerce Vulnerability to Phishing Attacks

In order to help understand the vulnerabilities found in the online environment, and the impact they have on e-commerce, the Common Criteria Security Model (CCSM) will be used. The CCSM is an effective, diagrammatical representation of the critical areas of security and the relationships between them.

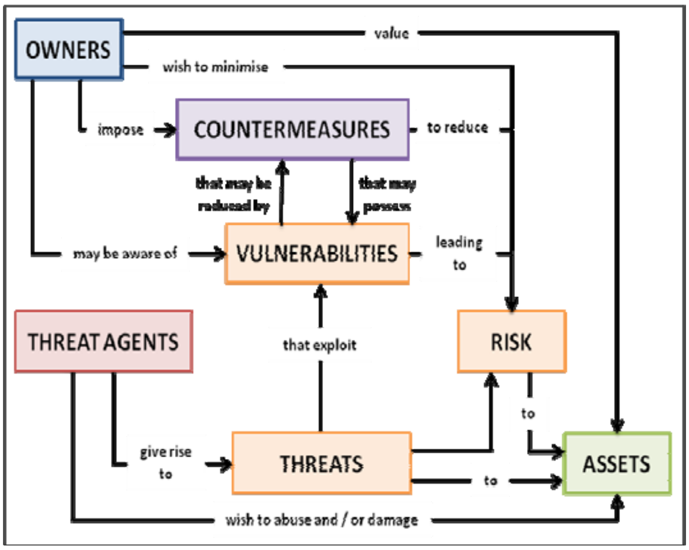

Figure 1. The Common Criteria Security Model [4]

When applying this model in context, one notes that ‘Threat Agents’ (which in this case are the phishers) give rise to threats, or the presence of the ability to commit a phishing crime. These threat agents will essentially have an underlying desire to abuse, or damage valuable assets such as confidential and personal information, online identities, or credit card details held by owners (online users and websites). The phishing threat will always exist, but it is the phishing risk that can be influenced (increased or reduced); therefore the objective is to target and reduce the phishing risk by lowering owner vulnerability, and not the threat itself. To do this, one needs to consider the ‘Owner’ side of the model. Owners (users and websites), whether they are aware of their vulnerability or not, require countermeasures (anti-phishing methods and tools) to be imposed so as to effectively reduce their vulnerability to phishing threats, and in turn, reduce the phishing risk, thus protecting the assets they value.

E-commerce activities and online transactions require trust and confidence by the user in the e-commerce website and its security. Thus, e-commerce is especially vulnerable to phishing attacks because phishing is “nothing more than a confidence game” [5], creating a false sense of confidence and tricking users into falling prey to a scam. This false confidence is created and maintained, beginning with the phishing email, and continues to highly believable phishing websites that have been designed with the same look and feel as legitimate sites. Victims are lured into trusting a fraudulent website and thereby willingly provide their confidential information which they would not normally have done if they had been aware that the website had been created by a phisher. This is an “erosion of trust” [5], which is also supported by the following statement: “Victims perceive that phishing emails are associated with a trusted brand, but in reality they are the work of con artists” [6]. In addition, the Internet is playing an increasingly significant role in online commerce activities, and due to a lack of Internet security, attackers are able to easily target online users involved in e-commerce [7]. Consequently, it is users who have very little understanding of web browser and Internet security that are targeted. Based on this, the following vulnerabilities within e-commerce were found:

TABLE I. Identified Vulnerabilities

NAME	DESCRIPTION
VUL01 - High required level of trust providing an easy target for exploitation	E-commerce, and its activities, requires high levels of trust and confidence between users and websites, and because phishing is specifically designed to target and to exploit that very trust and confidence, these two issues are not only seen as its strength, but also its greatest weakness [15] [16] [17].
VUL02 - Weaknesses in the medium across which business occurs	E-businesses rely heavily on the Internet (which lacks security) and websites (which can be easily compromised) to perform critical business activities, making them highly vulnerable to attack [18] [19].
VUL03 - Weak control of information exchange over the web	The openness and free exchange of confidential information across the web lends itself to abuse [20] [21].
VUL04 - Increasing levels of internet usage not followed by equal levels of security	Internet availability, popularity, and usage of e-commerce are increasing, but it lacks effective security [7].
VUL05 - Lack of understanding and knowledge about Internet Security	Users have very little understanding or knowledge of web browser and Internet security, leaving them open to exploitation and attack [7].
VUL06 - Ease of access through the web to phishing tools	The ease of access to and availability of tools allows criminals to easily mimic websites and create believable, spoofed emails [22] [23].
VUL07 - Mass implementation and use of email	The ubiquitous use of email has spawned mass spamming attacks which affect a vast number of users [24] [25].

Based on this, it can be seen that e-commerce, and the online nature in which e-commerce activities are conducted, are vulnerable and open to phishing attacks. The reason for this is because phishing attacks directly target, via tools provided through the Internet, websites and users, and the weaknesses they may have.

III. Phishing – Methods and Techniques

Phishing is defined as “…the use of ‘spoofed’ emails and fraudulent websites designed to fool recipients into divulging personal and financial data” [8]. A more comprehensive definition sees phishing as “…a social engineering attack in which an adversary lures an unsuspecting Internet user to a web site posing as a trustworthy business with which the user has a relationship”, and continues to state that “the broad goal is identity theft; phishers try to fool web visitors into revealing their login credentials, sensitive personal information, or credit

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

card numbers with the intent of impersonating their victims for financial gain” [9].

Essentially phishing can be seen as a ‘phishing attack process’ (as illustrated in Figure 2), and usually comprise of a delivery component (the spoofed phishing email), and a mimicry component i.e. presenting information in a way that is believable causing people to provide their credentials. This is usually in the form of a fraudulent phishing website that has been so designed so as to ‘mimic’ a legitimate website [5].

Internet users will firstly be sent a spoofed email (called the ‘lure’ as it is aimed at fooling, or luring users redirecting them to a phishing website) [5]. These emails are difficult to detect by visual checks and spam filters, and are designed to be highly believable and trustworthy. Various online tools make them easy to spoof, and because they can be sent to vast numbers of people at one time, it is the most used and preferred method of attack [25]. They will often also be characterised as an urgent call to action, encouraging users to follow a link telling them that they will receive a reward for complying, or suffer a penalty for failing to comply, thus directing them to the phisher’s website.

The user will then be led (believing that the email and website encountered, are true) to a fraudulent phishing website, which has been designed to imitate the appearance of a legitimate website such as a bank. Imitating a real site enables phishers to make users believe they are using the legitimate site, and therefore continue the ‘confidence game’ [5]. Once on the website, the victim will be asked to divulge sensitive and confidential information. This information can include personal data, financial data, login credentials such as usernames and passwords, bank account information, credit card details, and online identities.

The goal of the phisher is to trick the victim into supplying as many credentials as possible, so the phisher can then sell the information to ‘cashers’ i.e. the “consumers of financial institution credentials” [10], who will then use the information to commit other criminal acts. Cashers’, being ultimately the ‘customers’ of, and the finishing point for phishers, main role is to monetise phished information. This will involve using the phished credentials and obtaining currency straight from the accounts linked to those credentials [5] [10].

Generally, phishers will often use either the distributed attack or the redirection attack in order to do this. It is explained that phishers trying to evade detection will often use these two particular types of attacks [11]. In explanation, the distribution attack does not route users directly to the phishing website, but rather makes use of many different domains and IP addresses. In the redirection attack, the phisher directs all victims to a single URL, and then redirects each victim to a different address in order to be phished. Generally attacks on computer security are classified in three types namely, physical (attacks that target physical system infrastructure and networks), syntactic (attacks that target the software), and semantic, which are aimed at people [6]. Phishing is a form of semantic attack because it exploits how people interact with computers, how they understand and act on messages,

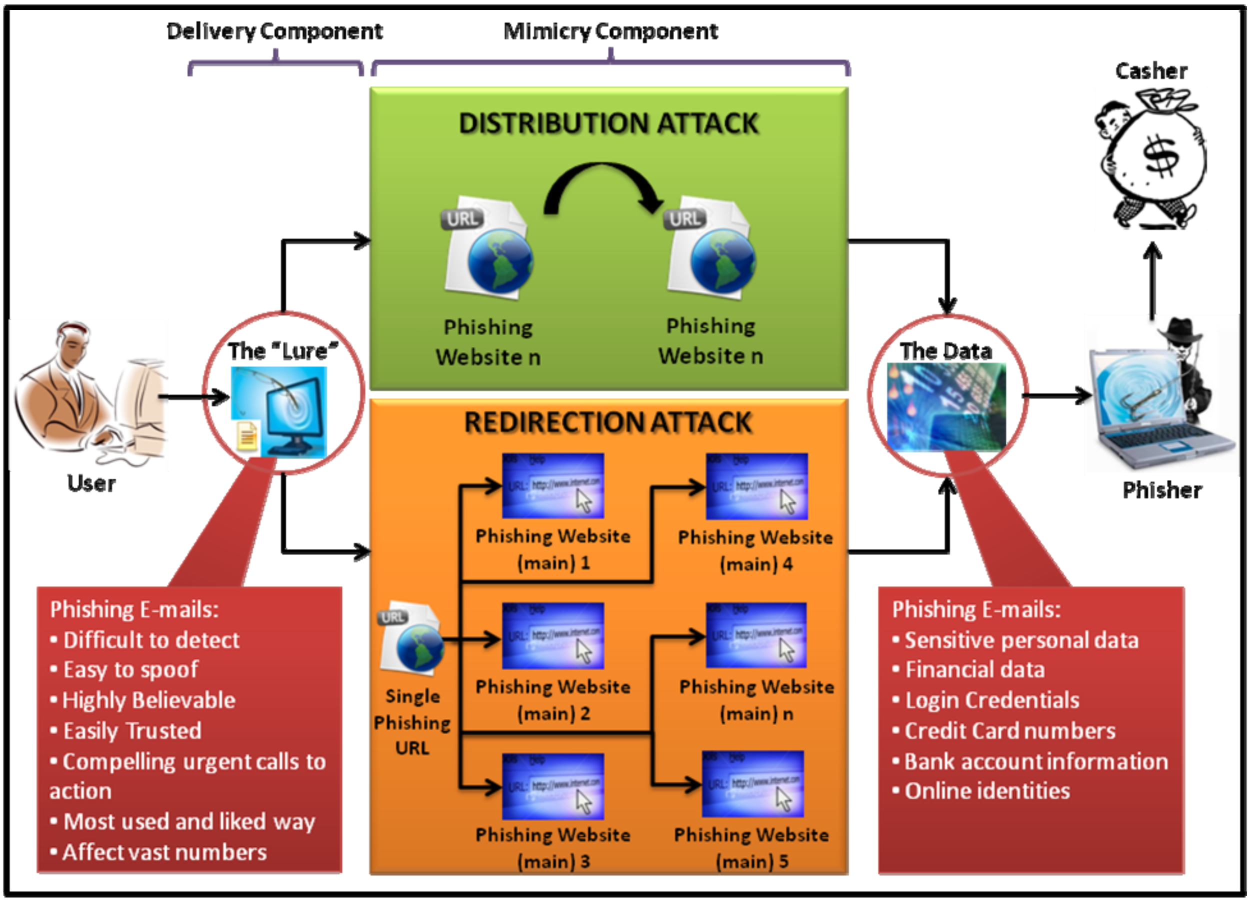

Figure 2. The Phishing Attack Process Diagram (Own Compilation)

furthermore they place their trust and confidence in the online e-commerce environment.

Phishing techniques have evolved and become increasingly sophisticated, damaging, and elusive, making use of multiple methods and new technologies in order to obtain the valuable assets that belong to online users. In light of this, identifying phishing methods is crucial.

IV. Reducing the Risk, Increasing the Trust

In order to determine how to reduce the phishing risk and increase trust (and similarly confidence), the importance of building trust needs to be addressed at the outset. This forms the basis on which to discover ways that a sense of trust and confidence can be increased, as well as an understanding of how controls are required to manage and reduce the risks created by this threat of phishing.

A. The Importance of Increasing Trust

Trust, can be defined as a "psychological state comprising the intention to accept vulnerability, based upon positive expectations of the intentions or behaviour of another" and involves two parties taking risks based on the belief that each party is dependable and trustworthy [12]. When a user intends to conduct online e-commerce activities, it requires a trusting relationship to exist between the user and the website in order for a successful exchange of information and transactional funds to occur. The risk involved here is that the user is providing personal and financial details to a website that is supposedly trustworthy, and the website is accepting and trusting that the user of the website is who they claim to be. Therefore, before any e-commerce activities can take place, trust is a prerequisite for reducing uncertainty. Trust essentially builds a relationship of safety and security, protecting both parties and allowing them the freedom to safely exchange confidential information. Whilst in the exchange, risks associated with online transacting are knowingly undertaken (in this case the risk created by the threat of phishing attacks), they are mitigated by trust, along with the use of controls.

B. Trust and the Uncertainty Reduction Theory

In order to understand the link between uncertainty reduction and its affect on building trust, a trust theory called the Uncertainty Reduction Theory will be used. The basic premise of the Uncertainty Reduction Theory states that when two parties meet each other for the first time, they undergo a series of stages in order to reduce uncertainty about each other, this forms part of an evaluation process that attempts to determine whether the two parties like or dislike each other and whether each of them can trust and be trusted. The theory describes how, through communication and the motivation of uncertainty avoidance (the fact that uncertainty is unpleasant and people will be motivated to reduce it), uncertainty reduction takes place and trust is developed.

In order to reduce this uncertainty, both parties enter into an uncertainty reduction development process made of up three phases, the Entry Phase, the Personal Phase, and the Exit Phase. As the parties move through the phases, communication increases, along with their level of involvement. Essentially, the parties in communication look to increase their predictability of the other in terms of their behaviour in various situations, thus reducing uncertainty and increasing trust between them. The theory goes on to explain that, uncertainty exists due to the presence of risk and threats and through communication and information exchange, a reduction in uncertainty takes place. In reducing uncertainty, increased predictability about behaviour occurs, which leads to an increased knowledge of future trusting behaviour, therefore increasing trust and minimising vulnerability.

Hence, by applying this theory to relationships found in online environments, uncertainty definitely exists due to the presence of typical online risks and threats such as phishing. The two communicators in the online world of e-commerce are the user and the e-commerce website. When a user encounters a website, it is essential for both parties to be certain of each other (i.e. uncertainty needs to be reduced and trust needs to be built) in order to facilitate interaction. Both the user and the website need to be authenticated in real-time reassuring each other that they are 'who they claim to be'. Another factor to be considered in the interaction between the user and the website is the means of communication which is email. Email is widely used as the main form of communication, and whilst it is easy to use and has a vast number of advantages, email is also used as part of the phisher's attack (i.e. known as the 'lure'). Thus emails also need to be taken into account, identified, verified, and authenticated in order to protect both parties as well as maintain a trusting relationship.

C. The Balance of Trust and Control

The confidence that users have in an e-commerce website, and vice versa, is determined by two factors: the level of trust, and the presence and adequacy of controls. To achieve a good trusting relationship there needs to be the right balance between trust and controls. The following diagram illustrates this balance:

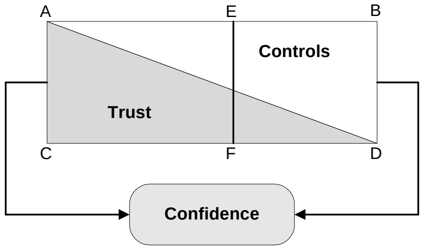

Figure 3. The Relationship between Trust, Controls and Confidence [12]

Figure 3 illustrates how trust and controls will interact together to provide security and confidence in a specific business process or transaction area.

TABLE II. Trust and Control Diagram Narrative

POSITION	DESCRIPTION
Triangle ABD	This is the control area (protected by controls)
Triangle ADC	This is the trust area (protected by trust)
Line EF	The risk appetite (i.e. the desire or willingness to take on various levels of risk)
Rectangle ABDC	This is the business process or transaction area

The position of the Risk Appetite Line will be dependent on how much the two parties trust each other. If the two parties trust each other more, the focus will be more on trust (trust area) and less on controls (controls area), and the risk appetite line will be to the left. If the two parties do not trust each other, the focus will be more on controls and less on trust, and the risk appetite line will be more to the right. Having complete trust and no controls (due to motivation from large reductions in costs), or complete controls and no trust (due to motivation from being able to have complete power and control) are impractical extremes and are not feasible when trying to provide a sense of confidence and security. Therefore, a balance between trust and controls is required.

D. Controls to Govern Trust and Manage the Risks of Phishing

An investigation was performed to identify effective tools that govern trust and manage the phishing risk. In this investigation, a comparison of these tools was conducted and the findings presented in Table 3.

In order for the e-commerce industry to continue to grow, trust between the website and the user needs to be established because when conducting e-commerce activities, risks are undertaken by both parties. By reducing uncertainty between the two parties via information sharing through communication, and implementing controls that focus on identification as well as authentication, both parties and their trust relationship can be effectively protected and increased over time.

TABLE III. ANTI-PHISHING TOOLS AND CONTROLS SUMMARY

ANTI-PHISHING TOOL	STRENGTHS	WEAKNESSES
iTrustPage A free downloadable extension for Firefox which seeks to prevent users from entering information into phishing websites.	• Has a basic automatic validation system that keeps a memory cache (white list) of previously validated websites. • Relies on user input and search engines for validation. • Prevents users from entering information into phishing sites. • False positives are rare and less likely to irritate. • Easy to use.	• Experiences ambiguity determining website legitimacy. • It does not deal with embedded objects (e.g. ActiveX) • Relies on visual hints and user awareness.
Delayed Password Disclosure A username and password authentication protocol providing users with dynamic feedback while username and password entry occurs.	• A user interface that provides visual, dynamic, character by character, feedback as passwords are being entered. • Feedback also remains flexible via a double checking system in case users fail to recognise incorrect visual feedback.	• Expensive to implement. • Consists of complex algorithms making it impractical.
Password Re-Use Client A browser plug-in client (that reports password reuse events at unfamiliar sites) and a server (that collects these reports and detects an attack).	• Accurate detection of attacks. • Mitigation of compromised accounts. • Aims at detecting phishing attacks globally. • Implements actionable procedures against phishing websites (e.g. technical or legal takedowns).	• Requires large scale deployment of the solution.
Strong Authentication System A dual factor authentication system consisting of a knowledge factor (usernames and passwords) and an ownership factor (e.g. One time passwords).	• Combines two methods of authentication. • Provides a high degree of security. • Can be customised to suit the needs of users / organisations. • Can integrate existing directory services (Microsoft active directory) into the system.	• Expensive to implement. • High time needs.
Anti-Phishing Toolbars (Trustbar) A free and downloadable plug-in toolbar for Firefox that authenticates both the website visited and the certificate authority.	• Automatic. • Effectively alerts users once a phishing website is identified. • Flexibility i.e. allows user input and interpretation. • User friendly.	• Requires an accurate, dynamic, and up-to-date blacklist of phishing sites. • Uses pop-ups and warnings which are usually ignored. • Requires user input where users can make mistakes.
NMA ZSentry Complete protection using a four pillar architecture – Authorisation, Spoof Prevention, Authentication, and Access Control.	• Is an all-in-one package. • Simple to use, with no training required. • Two factor authentication (Unique User Code + visual authentication of Return Code). • Passwords are not accessed, copied, or stored anywhere.	• Security breaches can result in significant damage, loss and costs.
PHONEY An anti-phishing framework for automatic detection and analysis of phishing attacks.	• Automatic. • User friendly. • Detects a wide range of different types of attacks. • Maintains a list of all tested and authenticated websites.	• Open to evasion of defence mechanisms through replaying responses of legitimate websites for phoney inputs. • Vulnerable to robot detecting schemes. • Possible legal ramifications due to the large consumption of bandwidth.

V. CRITICAL SUCCESS FACTORS

Critical Success Factors are "the critical factors or activities required for ensuring success", and are the key activities or focus areas required for achieving success in any area [13]. This research project identified that the following critical success factors need to be considered to effectively ensure success in reducing the risk of phishing and increasing the trust between users and websites.

A. User Authentication

User authentication is essentially the ability to identify and authenticate the user who is trying to gain access to a particular website. It should be considered a critical factor to success and be implemented using the various tools discussed, but as a minimum requirement, should include:

- Non-static usernames and passwords that provide a dynamic feedback checking system at the point of login. When users enter their login details, visual, character-by-character feedback should occur allowing them to check if anything unusual arises. This system needs to be relatively inexpensive to implement and easy to use. Also, to ensure that confidential information is indeed, secure, Authentication System's should not access, copy, or store usernames and passwords anywhere or in any format.
- A dual factor authentication system also needs to be put in place. Such a system authenticates the usernames and passwords, as well as, the one-time passwords, security tokens or digital certificates of a user, thus providing a higher degree of security. The systems need to be highly customizable (suiting the needs of users), integrate into existing directory services, and allow users to switch between security methods.
- Public key infrastructures that facilitate and support the use of digital certificates.
- Tools that link together, but should not come combined with each other in a single package.

B. Website Authentication

The tools need to have the ability to identify and authenticate a website to prevent users from entering confidential information into a phishing site that is posing as legitimate, and should have characteristics present in them, as follows:

- Should alert users to phishing using meaningful and helpful warnings, and be effective in preventing users from entering information into phishing websites. They should also guide users to legitimate sites if a phishing site is indeed found.
- Must have a validation system that must not be completely automated, but must include user assistance so as to add the human factor in authentication i.e. they must remain flexible to human interpretation and intervention, and allow users to verify websites through visual comparison.
- Should include memory caches that keep a white list of visited sites, and make use of external information repositories.
- Must, as a minimum acceptable requirement, minimise false positives, be user friendly and easy to implement.
- Should report password reuse at unfamiliar sites, and have a server that collects these reports and detects an attack and at the same time provide mitigation of any compromised accounts. They should also implement actionable procedures against phishing websites.
- Must operate on a global scale.
- Provide fake information to websites, analysing its behaviour until the site has been authenticated.

C. Email Authentication

This is the ability to identify and authenticate emails, checking them for signs of phishing. Phishing generally begins with the lure or the email, so it is critical that anti-phishing efforts start at the source of a phishing attack. Anti spam and phishing tools and filters need to be able to detect a wide range of attacks, including various phishing email formats, analyse sender domains and block phishing emails.

D. Data Cryptography

This is the process of "transforming clear, meaningful information into an enciphered, unintelligible form using an algorithm and a key" [14]. It involves encrypting data (converting data into some scrambled form and locking it, making the data secure over the Internet) and decrypting data (unlocks encrypted data and converts it back in the original form). Data cryptography methods and techniques are critical to the online e-commerce environment, as they are needed in protecting confidential information used during information exchange that occurs when making transactions via a website.

E. Communication

This is the communication that should take place between websites and users. Websites should communicate to users the risk of phishing, about the legitimacy of their websites, the preventive controls in place and other details relating to phishing and Internet security. Communicating this to users will result in an increased awareness of phishing.

F. Active Risk Mitigation

Websites need to have an active risk mitigation plan in place in order to inform their users and protect themselves. This is essentially a step by step action plan for the website company and users to follow if they are caught in a phishing attack. If websites have an action plan to handle the phishing risk, they can be well prepared in advance and effectively mitigate this risk, minimise the impact, and have procedures in place to efficiently deal with the effects. If users can see and know what to do if a phishing attack occurs, they will have increased confidence in the website and will know that the site is actively trying to protect them.

VI. CSF to vulnerability Relationship Mappings

To link back to the vulnerabilities in e-commerce previously identified, a mapping of how each critical success factor (from section 5) covers a specific vulnerability (section 2) is provided in Table 4, this being the main contribution of the paper.

TABLE IV. CSF to E-Commerce Vulnerability Elements Map

CRITICAL SUCCESS FACTOR		VULNERABILITES IN E-COMMERCE	
CSF01	**User Authentication** The ability to identify and authenticate the user who is trying to gain access to a particular website	VUL01	High required level of trust providing an easy target for exploitation
		VUL04	Increasing levels of internet usage not followed by equal levels of security
		VUL07	Mass implementation and use of email
CSF02	**Website Authentication** The ability to identify and authenticate a website to prevent users from entering confidential information into a phishing site that is posing as legitimate.	VUL01	High required level of trust providing an easy target for exploitation
		VUL02	Weaknesses in the medium across which business occurs
		VUL04	Increasing levels of internet usage not followed by equal levels of security
		VUL06	Ease of access through the web to phishing tools
CSF03	**Email Authentication** The ability to identify and authenticate emails, checking them for signs of phishing	VUL01	High required level of trust providing an easy target for exploitation
		VUL02	Weaknesses in the medium across which business occurs
		VUL04	Increasing levels of internet usage not followed by equal levels of security
		VUL06	Ease of access through the web to phishing tools
		VUL07	Mass implementation and use of email
CSF04	**Data Cryptography** The process of “transforming clear, meaningful information into an enciphered, unintelligible form using an algorithm and a key”	VUL01	High required level of trust providing an easy target for exploitation
		VUL02	Weaknesses in the medium across which business occurs
		VUL03	Weak control of information exchange over the web
		VUL04	Increasing levels of internet usage not followed by equal levels of security
CSF05	**Communication** The communication that should take place between websites and users in order to create a security awareness of phishing	VUL01	High required level of trust providing an easy target for exploitation
		VUL05	Lack of understanding and knowledge about Internet Security
CSF06	**Active Risk Mitigation** A step by step action plan for the website company and users to follow if they are caught in a phishing attack	VUL01	High required level of trust providing an easy target for exploitation
		VUL05	Lack of understanding and knowledge about Internet Security

By ensuring that these critical success factors are adopted into an anti-phishing strategy, the risk of phishing will be reduced and the trust between users and websites will be increased.

VII. Conclusion

In conclusion, e-commerce has been found to be highly vulnerable to phishing attacks in their various shapes and forms. These attacks have been specifically designed to target vulnerabilities in the system and take advantage of both users and websites. Phishing has damaged the crucial ingredients for e-commerce: Trust and Confidence. In order to increase and build trust, it is essential that the risk of phishing, created from the phishing threat, be reduced. In order to address this problem one needs to reduce uncertainty through information sharing and communication and have a good balance between trust and controls. The critical success factors will effectively aid in increasing trust within the e-commerce environment by reducing the risk created from the threat of phishing.

References

[1] Xun, L., and Lixia, Y. (2009). The Study of E-Commerce System Integration Based on PDM, In the proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA’09). Nanchang, China, 306-308.

[2] APACS (2007). New research reveals that people are still unaware of basic security measures when banking online. Retrieved December 2007 from http://www.apacs.org.uk/

[3] APWG (2009). Phishing Activity Trends Report, 3rd Quarter, 2009. Retrieved February 1, 2009, from http://www.antiphishing.org/

[4] The CCRA (2009). Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3 Final, Part 1. Retrieved February 14, 2009, from http://www.commoncriteriaportal.org/

[5] Jakobsson, M., and Myers, S. (2007). Delayed Password Disclosure. In the ‘Distributed computing’ column of the ACM SIGACT News (2007). ACM Press, New York, NY, 38, 3, 56-75.

[6] Downs, J., Holbrook, M., and Cranor, L. (2006). Decision Strategies and Susceptibility to Phishing. In the proceedings of the second symposium on Usable privacy and security (Pittsburgh, Pennsylvania, 2006). ACM Press, New York, NY, 149, 79-90.

[7] Chandrasekaran, M., Chinchani, R., and Upadhyaya, S. (2006). PHONEY: Mimicking User Response to Detect Phishing Attacks. In the proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks (2006). ACM Press, New York, NY, 668-672.

[8] Martin, S., Sewani, A., Nelson, B., Chen, K., and Joseph, A.D. (2005). Analyzing Behavioural Features for Email Classification. Retrieved May 17, 2008, from http://www-static.cc.gatech.edu/

[9] Karlof, C., Tygar, J.D., Wagner, D., and Shankar, U. (2007). Dynamic Pharming Attacks and Locked Same-origin Policies for Web Browsers. In the proceedings of the 14th ACM conference on Computer and Communications Security (Alexandria, Virginia, USA, 2007). ACM Press, New York, NY, 58-71.

[10] Abad, C., (2006). The Economy of Phishing: A Survey of the Operations of the Phishing Market. Retrieved February 14, 2009, from http://www.cloudmark.com/

[11] Florêncio, D., and Herly, C. (2007). Evaluating a Trial Deployment of Password Re-Use for Phishing Prevention. Retrieved May 17, 2008, from http://www.apwg.com/ecrimeresearch/2007/

[12] Flowerday, S., and von Solms, R. (2006). Trust: an Element of Information Security. IFIP International Federation for Information Processing, 201, 87-98.

[13] Critical Success Factors (2008). Retrieved September 29, 2008, from http://www.rapidbi.com/created/criticalsuccessfactors.html

[14] Glossary of Common PKI Terms (2008). Retrieved September 29, 2008, from http://www.tbs-sct.gc.ca/pki-icp/beginners/glossary/glossary-eng.asp

[15] Salehi-Abari, A. (2009). The Exploitation-Resistant Trust (Ert) Model for Open Distributed Systems. Retrieved February 14, 2009, from http://sikaman.dyndns.org/

[16] Corritore, C., Kracher, B., and Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. International Journal of Human-Computer Studies, Vol 58, pp. 737–758.

[17] Lewicki, R., McAllister, D., and Bies, R. (1998). Trust and Distrust: New Relationships and Realities. The Academy of Management Review, Vol. 23, No. 3, pp. 438-458.

[18] Ferrer, C. (2009). State of the Internet 2009: A Report on the Ever-Changing Threat Landscape. Retrieved February 14, 2009, from http://ca.com/files/SecurityAdvisorNews/

[19] Atkinson, R. (1995). Security for the Internet Protocol. Retrieved February 14, 2009, from http://www.dtic.mil/cgi-bin/

[20] Malhotra, N., Kim, S., and Agarwal, J. (2004). Internet User's Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research, Vol 15, 4, pp. 336-355.

[21] Olivero, N., and Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. Journal of Economic Psychology, Vol 25, 2, pp. 243-262.

[22] Ronda, T., Saroiu, S., and Wolman, A. (2008). iTrustPage: A User-Assisted Anti-Phishing Tool. In the proceedings of the 3rd ACM SIGOPS/EuroSys European Conference on Computer Systems (Glasgow, Scotland, UK, 2008). ACM Press, New York, NY, 261-272.

[23] Ramzan, Z., and Wuest, C. (2007). Phishing Attacks: Analyzing Trends in 2006. In the proceedings of the Fourth Conference on Email and AntiSpam, Mountain View, California, USA.

[24] Garera, S., Provos, N., Rubin, A.D., and Chew, M. (2007). A Framework for Detection and Measurement of Phishing Attacks. In the proceedings of the ACM workshop on Recurring malcode (Alexandria, Virginia, USA, 2007). ACM Press, New York, NY, 1 – 8.

[25] Abu-Nimeh, S., Nappa, D., Wang, X., and Nair, S. (2007). A Comparison of Machine Learning Techniques for Phishing Detection. In the proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit (Pittsburgh, Pennsylvania, 2007). ACM Press, New York, NY, 269, 60-69.