Definitions

Table 3 lists the 113 definitions of the phenomenon ‘phishing’ that were found with the literature search.

Table 3: An overview of the found articles that define phishing.

Author	Definition
Adida (2007)	Attackers provide a spoofed web page, where the user is fooled into entering her credentials.
Ahamid et al. (2013)	Phishing is a type of semantic attack in which victims are sent emails that deceive them into providing sensitive information such as account numbers, passwords, or other personal to phisher.
Al-Hamar et al. (2011)	(...) a technique of obtaining private information fraudulently and thereafter obtaining money illegally (...)
Ali and Rajamani (2012)	Phishing a fraudulent trick of stealing victim's personal information by sending spoofed messages, through Instant Messengers via socially engineered messages.
ALmomani et al. (2012)	Such a type of threats, phishing e-mails, is used to steal sensitive and personal data or user's' account information from their computers.
ALmomani et al. (2013)	Phishing is a kind of attack in which criminals use spoofed emails and fraudulent web sites to trick financial organization and customers. Criminals try to lure online users by convincing them to reveal the username, passwords, credit card number and updating account information or fill billing information.
Amin et al. (2012)	email soliciting personal information
Anderson and Moore (2009)	(...) in which crooks send emails pretending to be from a bank or service provider and inviting its customers to log on at its website.
Bainbridge (2007)	Obtaining information such as a person's bank account details by sending an e-mail purporting to be from that person's bank.
Baker et al. (2006)	(...) the fraudulent and increasingly authentic looking e-mail attempts aimed to lure unsuspecting recipients into sharing sensitive financial and personal information.
Barraclough et al. (2013)	Phishing is an instance of social engineering techniques used to deceive users into giving their sensitive information using an illegitimate website that looks and feels exactly like the target organization website.
Basnet et al. (2008)	Phishing is a form of identity theft that occurs when a malicious Web site impersonates a legitimate one in order to acquire sensitive information such as passwords, account details, or credit card numbers.

Continued on next page

Table 3: *(continued.)*

Author	Definition
Beatty et al. (2011)	In a typical phishing scam, the consumer receives an email purportedly from a trusted online vendor (a bank is a typical example). This email contains a call to action, a request to undertake some action that requires the user to disclose their authentication credentials. A hyperlink to the vendor's (supposed) site is provided. Consumers fall prey to this scam when they follow the link and provide their credentials.
Beliakov et al. (2012)	Phishing usually involves acts of social engineering attempting to extract confidential details by sending emails with false explanations urging users to provide private information that will be used for identity theft.
Bergholz et al. (2010)	Phishing emails usually contain a message from a credible looking source requesting a user to click a link to a website where she/he is asked to enter a password or other confidential information.
Biddle et al. (2012)	Phishing is a type of social engineering in which users are tricked into entering their credentials at a fraudulent website recording user input.
Brainard et al. (2006)	the fraudulent use of e-mail to capture user passwords (and other information)
Butler (2007)	Phishing represents an online method of identity theft employed by phishers to steal attributes (like passwords or account numbers) used by online consumers.
Cao et al. (2008)	The attacker tricks the user into submitting his/her confidential information (such as password) into a fraudulent web site that has high visual similarities as the genuine one.
Chen et al. (2009)	Phishing is a form of online identity theft associated with both social engineering and technical subterfuge. Specifically, phishers attempt to trick Internet users into revealing sensitive or private information, such as their bank account and credit-card numbers.
Cranor (2008)	Phish e-mails are constructed by con artists to look like legitimate communications, often from familiar and reputable companies, and usually ask victims to take urgent action to avoid a consequence or receive a reward. The desired response typically involves logging in to a Web site or calling a phone number to provide personal information. Sometimes victims need only click on links or open e-mail attachments for their computers to become infected by malicious software –known as malware– that allows phishers to retrieve the data they want or take control of the victim's computer to launch future attacks.

Continued on next page

Table 3: *(continued.)*

Author	Definition
Dhamija and Tygar (2005)	In a phishing attack, the attacker spoofs a website (e.g., a financial services website). The attacker draws a victim to the rogue website, sometimes by embedding a link in email and encouraging the user to click on the link. The rogue website usually looks exactly like a known website, sharing logos and images, but the rogue website serves only to capture the user's personal information. Many phishing attacks seek to gain credit card information, account numbers, usernames and passwords that enable the attacker to perpetrate fraud and identity theft.
Dhamija et al. (2006)	The practice of directing users to fraudulent web sites.
Dong et al. (2010)	Phishing attacks are well-organised and financially motivated crimes which steal users' confidential information and authentication credentials.
Downs et al. (2006)	Phishing emails are semantic attacks that con people into divulging sensitive information using techniques to make the user believe that information is being requested by a legitimate source.
Downs et al. (2009)	Attempts to criminally obtain sensitive information (e.g., social security numbers and credit cards) by pretending to be a legitimate businesses.
Drake et al. (2004)	"Phishing" is an email scam that attempts to defraud people of their personal information including credit card number, bank account information, social security number, and their mother's maiden name.
Egelman et al. (2008)	a scam to collect personal information by mimicking trusted websites
Elmaleh (2007)	This type of unsolicited correspondence has the intention of directing users to a fake web site, facilitating the unauthorised retrieval of personal financial information which can then be used to fraudulently access a user's bank account.
Emm (2006)	It involves tricking computer users into disclosing their personal details (username, password, PIN number or any other access information) and using these details to obtain money under false pretences.
Fernandez et al. (2005)	(...) in which a perpetrator sends an e-mail purporting to be from the victim's Internet service provider, bank, or other company with whom the victim does business. The e-mail asks the victim to update his account information. When the victim complies with the request, he will have unwittingly sent his personal information to a criminal.
Fette et al. (2007)	(...) attacks are launched with the aim of making web users believe that they are communicating with a trusted entity for the purpose of stealing account information, logon credentials, and identity information in general.

Continued on next page

Table 3: *(continued.)*

Author	Definition
Florêncio and Herley (2007)	(...) a victim is lured into submitting her password to a malicious site masquerading as a trusted institution (...)
Forte (2009)	(...) the objective of which is to trick us into revealing sensitive information.
Fumera et al. (2006)	(...) they try to convince them to surrender personal information like passwords and account numbers, through the use of spoof messages which are masqueraded as coming from reputable on-line businesses such as financial institutions.
Garera et al. (2007)	Phishing is form of identity theft that combines social engineering techniques and sophisticated attack vectors to harvest financial information from unsuspecting consumers.
Gastellier-Prevost and Laurent (2011)	By spoofing the identity of a company that proposes financial services, phishing attacks steal confidential information (e.g. login, password, credit card number) to the Internet users
Geer (2005)	(...) phishing, in which e-mails lure unsuspecting victims into giving up user names, passwords, Social Security numbers, and account information after linking to counterfeit bank, credit card, and e-commerce Web sites.
Gouda et al. (2007)	In this type of attack, an attacker sends fraudulent emails to users, pretending to be the system administrator of a benign website such as an online banking website, and fools users to take login actions on a malicious website, which looks very similar to the benign website, but is set up by the attacker. Once a user tries to login on such a malicious website, his user name and password will be recorded and possibly later will be used by the attacker to login on the benign website.
Gross and Rosson (2007)	Phishing involves an attacker, posing as bank, vendor, or other trusted source, who sends an email asking the recipient to confirm personally identifying information by entering it on a website. This information is then used in identity theft.
Guan et al. (2012)	(...) the malicious mail, which mostly contains a URL to convince the victims to visit a fraudulent website where sensitive information like credit card numbers and passwords are requested.
Gupta and Pieprzyk (2011)	Phishing is the process of covertly and illicitly obtaining user credentials for future gains.
Halevi et al. (2013)	Phishing is an attack that uses fraudulent electronic mail (email) that claims to be from a trustworthy source. The goal of phishing emails is to get personal information from the users, such as user ID and passwords. The attacker can then use this information to impersonate a user and access the user account for financial gain.

Continued on next page

Table 3: *(continued.)*

Author	Definition
Han et al. (2012)	Phishing employs social engineering to trick a user into revealing his or her web digital identities to a fraudulent web site.
He et al. (2011)	Phishing usually takes a form of a fake webpage whose appearance is similar to the page of a real website in order to steal user credentials and identities.
Herzberg (2009)	Password theft via fake websites.
Hinson (2010)	using spam e-mails,targeted e-mails,short message service (SMS) text messages, phone calls, and even leaflets on the windscreen to fool victims into visiting fake websites and disclosing their login credentials or other personal information
Hodgson (2005)	Phishing attacks simulate established and reputable organisation's Web sites and trick the user into providing personal information that is then used by the criminal to either steal from the victim or use the victim's identity to commit further crimes.
Hong (2012)	Phishing is a kind of social-engineering attack in which criminals use spoofed email messages to trick people into sharing sensitive information or installing malware on their computers.
Huber et al. (2011)	An attacker tries to lure victims into entering sensitive information, such as a password or credit-card number, into a fake website that the attacker controls.
Ilchev and Ilchev (2012)	(...) a popular approach used by criminals to acquire sensitive client data such as personal identification numbers (PINs), transaction authentication numbers (TANs), bank account numbers, credit card numbers and passwords.
Jagatic et al. (2007)	Phishing is a form of deception in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity.
Jahankhani (2009)	This is a technique used to gain personal information for the purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers and Social Security numbers.
Jakobsson and Ratkiewicz (2006)	persuades a user to release sensitive personal or financial information, such as login credentials or credit card numbers.
Jakobsson and Stamm (2007)	Phishing combines the deceitful techniques of con artists with the Internet's scalability to commit identity theft by stealing credentials.

Continued on next page

Table 3: *(continued.)*

Author	Definition
Jo et al. (2013)	Phishing is an attack where fraudulent websites impersonate legitimate counterparts to steal users confidential information.
Khonji et al. (2013)	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.
Khot et al. (2012)	(...) attacker tricks the user into divulging the password information through fraudulent websites and emails.
Kim et al. (2012)	(...) attempts to steal confidential user information such as credit card numbers or passwords and social engineering and spoofing techniques are frequently used.
Kirda and Kruegel (2005)	Phishing is a form of online identity theft that aims to steal sensitive information from users such as online banking passwords and credit card information.
Kirlappos and Sasse (2012)	Tricking computer users to disclose personal information, credit card details, user names, and passwords.
Knight (2005)	The practice is known as phishing, and uses social engineering and technical subterfuge to steal consumers' personal data and bank account details.
Kumaraguru et al. (2007)	Criminals lure Internet users to websites that impersonate legitimate sites
Kumaraguru et al. (2010)	(...) phishing, in which victims get conned by spoofed emails and fraudulent websites.
Larcom and Elbirt (2006)	Phishing is the act of convincing users to provide personal identification information such as credit card numbers, social security numbers and bank account information for explicit illegal use.
Lenton (2005)	(...) rogue emails usually purporting to be from a bank that direct them to a bogus website or attempt to identify their personal details
Levy (2004)	Phishing (the act of conning a person into divulging sensitive information) commonly uses legitimate-looking Web sites that mimic the online interface of the institution the attacker is misrepresenting (usually a bank, merchant, or ISP)
Li et al. (2012)	Phishing is one type of identity theft, where the aim is to steal confidential information, e.g. credit card number, credentials and social security ID numbers, and the list can go on.

Continued on next page

Table 3: *(continued.)*

Author	Definition
Liu et al. (2005)	Phishing is a criminal trick of stealing victims' personal information by sending them spoofed emails urging them to visit a forged webpage that looks like a true one of a legitimate company and asks the recipients to enter personal information such as credit card number, password and etc.
Liu et al. (2010)	Phishing is a kind of online attack widely used by phishers to steal users' accounts and passwords, and other personal information for illegal appropriation.
Ludl et al. (2007)	Phishing is a form of electronic identity theft in which a combination of social engineering and web site spoofing techniques are used to trick a user into revealing confidential information with economic value.
Maurer and Höfer (2012)	(...) the act of stealing personal data of Internet users for misuse (...)
McFedries (2006)	"Phishing" refers to creating a replica of an existing Web page to fool users into submitting personal, financial, or password data to what they think is their bank or a reputable online retailer.
McNealy (2008)	The sender creates e-mails, resembling those from a well-known companies, requesting that the recipient click on a URL provided, which links to a dummy company Web site where the recipient is asked to input personal information. The e-mail sender may then use the information for illegal purposes.
Mills and Byun (2006)	Stealing personal information by requesting it via fraudulent email messages or Web pages
Mohebzada et al. (2012)	Phishing is a type of social engineering where a potential victim is sent a message that impersonates a legitimate source or organization. Phishing attacks typically lure the targets into revealing confidential information such as password, credit card details, bank account numbers, or any other sensitive information.
Moore (2007)	Phishing is the process of enticing people into visiting fraudulent websites and persuading them to enter identity information such as usernames and passwords. This information is then used to impersonate the victim (...)
Moore and Clayton (2007)	Phishing is the process of enticing people into visiting fraudulent websites and persuading them to enter identity information such as usernames, passwords, addresses, social security numbers, personal identification numbers (PINs) and anything else that can be made to appear to be plausible.
Moran and Moore (2010)	Phishing is the criminal activity of enticing people to visit websites that impersonate genuine bank websites and dupe visitors into revealing passwords and other credentials.

Continued on next page

Table 3: *(continued.)*

Author	Definition
Nykodym et al. (2010)	Phishing is a scam to steal valuable information by sending out fake emails, or spam, written to appear as if they have been sent by banks or other reputable organizations with the intent of luring the recipient into revealing sensitive information such as usernames, passwords, social security numbers, account IDs, ATM PIN's or credit card details.
Olurin et al. (2012)	Fraudsters can create fake websites to lure users for the purpose of collecting their data. (...) Phishing attacks can steal personal identity information such as username, passwords, and credit card details from unsuspecting users by masquerading as trusted entities, such as PayPal sites.
Parno et al. (2006)	In phishing, an automated form of social engineering, criminals use the Internet to fraudulently extract sensitive information from businesses and individuals, often by impersonating legitimate web sites.
Paulson (2010)	Phishers typically create webpages that look like those belonging to banks, e-commerce operations, or other businesses on which users might enter financial or accountaccess information. When a user enters such data on a fake page, the phisher captures the information and utilizes it to defraud the victim.
Piper (2007)	Phishing is an attempt provided by vendors using email or Internet social spaces such as MySpace to obtain sensitive personal information such as usernames and passwords, social Security Numbers, credit-card numbers, and others.
Ranganayakulu et al. (2011)	Phishing is the combination of social engineering and technical exploits which has adverse effects aiming at the monetary gain of the attacker (phisher). (...) Phishing attacks use spoofed e- mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.
Ray and Schultz (2007)	Phishing is a technique that many attackers use to trick computer users into revealing personal or financial information through specially worded email messages or websites.
Ross (2006)	(...) in which con artists send e-mails purporting to be from legitimate organizations, such as banks, in order to inveigle recipients into revealing personal information.
Ross (2009)	Phishing e-mails deceive individuals into giving out personal information which may then be utilized for identity theft.
De Ryck et al. (2013)	(...) the process that involves an attacker tricking users into willingly surrendering their credentials (...)
Saberi et al. (2007)	Phishing attack is a kind of identity theft which tries to steal confidential data like on-line bank account information.

Continued on next page

Table 3: *(continued.)*

Author	Definition
Shahriar and Zulkernine (2012)	Phishing is a web-based attack that allures end users to visit fraudulent websites and give away personal information (e.g., user id, password)
Emilin Shyni and Swamynathan (2013)	A phishing attack is a criminal activity which mimics a certain legitimate webpage using a fake webpage with an intention of luring end-users to visit the fake website thereby stealing their personal information such as usernames, passwords and other personal details such as credit card information.
Sood et al. (2011)	Phishing is an online identity theft that combines social engineering and web site spoofing techniques to cheat the user by redirecting his confidential information to an untrusted destination.
Stabek et al. (2010)	(...) which are also synonymous with identity theft and credit/debit card fraud.
Sweeney (2006)	Phishing, which is the act of sending an email message impersonating a respected organization in an attempt to get the reader to click on the provided link and give personal information.
Thiyagarajan et al. (2012)	In this attack, the attacker tries to mimic as legitimate site and gather critical information from the user which in turn will be used to make control of the users valuable and critical information.
Vamosi (2009)	Phishing refers to an attempt to collect usernames, passwords, and credit card data by posing as a legitimate, trusted party.
Varshney et al. (2012)	Phishing is a deception technique used by attackers for gaining personal information from end users, with the help of fraudulent and spoofed emails, Phished Websites and various deception techniques. The aim of the phisher lies in obtaining personal information or credentials from an end user such as bank account numbers their passwords, credit card details etc.
Verma et al. (2012)	Phishing is a social engineering threat aimed at gleaning sensitive information such as user names, passwords and financial information from unsuspecting victims. Attacks are typically carried out via communication channels such as email or instant messaging by attackers masquerading as legitimate and trustworthy entities.
Vitaliev (2010)	fraudulent messages that attempt to withdraw personal and financial information from the reader.
Wang et al. (2012)	Email-based deception where a perpetrator (phisher) camouflages emails to appear as a legitimate request for personal and sensitive information is known as phishing.

Continued on next page

Table 3: *(continued.)*

Author	Definition
Wenyin et al. (2012)	Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as user names, passwords, and creditcard details from a victim by pretending to be a trustworthy entity in an electronic communication.
Whittaker et al. (2010)	We define a phishing page as any web page that, without permission, alleges to act on behalf of a third party with the intention of confusing viewers into performing an action with which the viewer would only trust a true agent of the third party.
Workman (2008)	Phishing is a ruse designed to gain sensitive information from an intended victim by way of e-mail and Web pages or letters that appear to be from genuine businesses, that command the potential victim to supply information to prevent an account from being closed, or as part of a promotion or give-away called a gimmie.
Wu et al. (2006a)	Phishing attacks typically use legitimate-looking but fake emails and websites to deceive users into disclosing personal or financial information to the attacker. Users can also be tricked into downloading and installing hostile software, which searches the user's computer or monitors online activities to steal private information.
Wu et al. (2006b)	Phishing attacks typically use legitimate-looking but fake emails and websites to deceive users into disclosing private information to the attacker.
Xiang and Hong (2009)	Phishing is a form of identity theft, where criminals create fake web sites that masquerade as trustworthy organizations. The goal of phishing is to trick people into giving sensitive information, such as passwords, personal identification numbers, and so on.
Xiang et al. (2011)	Phishing is a form of identity theft, in which criminals build replicas of target Web sites and lure unsuspecting victims to disclose their sensitive information like passwords, personal identification numbers (PINs), etc.
Yearwood et al. (2009)	Phishing can be defined as a scam by which an email user is duped into revealing personal or confidential information which the scammer can use illicitly. Phishing attacks use both social engineering and technical subterfuge to steal personal identity data and financial account credentials.
Yee and Sitaker (2006)	(...) phishing attacks, in which the user is fooled into entering a password at an imitation site.
Zhang et al. (2007)	A kind of attack in which victims are tricked by spoofed emails and fraudulent web sites into giving up personal information.
Zhang et al. (2012)	By masquerading as a trustworthy entity, phishing is a criminally fraudulent process of attempting to acquire sensitive information.

Continued on next page

Table 3: *(continued.)*

Author	Definition
Zhou et al. (2009)	Phishing is a form of social engineering attack, which exploits human vulnerabilities rather than software vulnerabilities.

References

Adida, B. (2007). Beamauth: Two-factor web authentication with a bookmark. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 48–57.

Ahamid, I., Abawajy, J., and Kim, T.-H. (2013). Using feature selection and classification scheme for automating phishing email detection. *Studies in Informatics and Control*, 22(1):61–70.

Al-Hamar, M., Dawson, R., and Al-Hamar, J. (2011). The need for education on phishing: A survey comparison of the uk and qatar. *Campus-Wide Information Systems*, 28(5):308–319.

Ali, M. and Rajamani, L. (2012). Deceptive phishing detection system: From audio and text messages in instant messengers using data mining approach. In *Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME)*, pages 458–465.

ALmomani, A., Gupta, B., Wan, T.-C., Altaher, A., and Manickam, S. (2013). Phishing dynamic evolving neural fuzzy framework for online detection "zero-day" phishing email phishing email. *Indian Journal of Science and Technology*, 6(1):3960–3964.

ALmomani, A., Wan, T.-C., Altaher, A., Manasrah, A., ALmomani, E., Anbar, M., ALomari, E., and Ramadass, S. (2012). Evolving fuzzy neural network for phishing emails detection. *Journal of Computer Science*, 8(7):1099–1107.

Amin, R., Ryan, J., and van Dorp, J. (2012). Detecting targeted malicious email. *IEEE Security and Privacy*, 10(3):64–71.

Anderson, R. and Moore, T. (2009). Information security: Where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 367(1898):2717–2727.

Bainbridge, D. (2007). Criminal law tackles computer fraud and misuse. *Computer Law and Security Report*, 23(3):276–281.

Baker, E., Tedesco, J., and Baker, W. (2006). Consumer privacy and trust online: An experimental analysis of anti-phishing promotional effects. *Journal of Website Promotion*, 2(1-2):89–113.

Barraclough, P., Hossain, M., Tahir, M., Sexton, G., and Aslam, N. (2013). Intelligent phishing detection and protection scheme for online transactions. *Expert Systems with Applications*, 40(11):4697–4706.

Basnet, R., Mukkamala, S., and Sung, A. (2008). Detection of phishing attacks: A machine learning approach. *Studies in Fuzziness and Soft Computing*, 226:373–383.

Beatty, P., Reay, I., Dick, S., and Miller, J. (2011). Consumer trust in e-commerce web sites: A meta-study. *ACM Computing Surveys*, 43(3):14:1–14:46.

Beliakov, G., Yearwood, J., and Kelarev, A. (2012). Application of rank correlation, clustering and classification in information security. *Journal of Networks*, 7(6):935–945.

Bergholz, A., De Beer, J., Glahn, S., Moens, M.-F., Paaß, G., and Strobel, S. (2010). New filtering approaches for phishing email. *Journal of Computer Security*, 18(1):7–35.

Biddle, R., Chiasson, S., and Van Oorschot, P. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, 44(4):19:1–19:41.

Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., and Yung, M. (2006). Fourth-factor authentication: somebody you know. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pages 168–178.

Butler, R. (2007). A framework of anti-phishing measures aimed at protecting the online consumer's identity. *Electronic Library*, 25(5):517–533.

Cao, Y., Han, W., and Le, Y. (2008). Anti-phishing based on automated individual white-list. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 51–60.

Chen, K.-T., Chen, J.-Y., Huang, C.-R., and Chen, C.-S. (2009). Fighting phishing with discriminative keypoint features. *IEEE Internet Computing*, 13(3):56–63.

Cranor, L. (2008). Can phishing be foiled? *Scientific American*, 299(6):104–110.

De Ryck, P., Nikiforakis, N., Desmet, L., and Joosen, W. (2013). Tabshots: Client-side detection of tabnabbing attacks. In *Proceedings of the 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, pages 447–455.

Dhamija, R. and Tygar, J. D. (2005). The battle against phishing: Dynamic security skins. In *Proceedings of the symposium on Usable privacy and security (SOUPS)*, pages 77–88.

Dhamija, R., Tygar, J. D., and Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 581–590.

Dong, X., Clark, J., and Jacob, J. (2010). Defending the weakest link: Phishing websites detection by analysing user behaviours. *Telecommunication Systems*, 45(2-3):215–226.

Downs, D., Ademaj, I., and Schuck, A. (2009). Internet security: Who is leaving the 'virtual door' open and why? *First Monday*, 14(1).

Downs, J. S., Holbrook, M. B., and Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security (SOUPS)*, pages 79–90.

Drake, C., Oliver, J., and Koontz, E. (2004). Anatomy of a phishing email. In *Proceedings of the 2004 Conference on Email and Anti-Spam*.

Egelman, S., Cranor, L., and Hong, J. (2008). You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1065–1074.

Elmaleh, D. (2007). Phishing forbidden. *Card Technology Today*, 19(9):12–13.

Emilin Shyni, C. and Swamynathan, S. (2013). Protecting the online user's information against phishing attacks using dynamic encryption techniques. *Journal of Computer Science*, 9(4):526–533.

Emm, D. (2006). Phishing update, and how to avoid getting hooked. *Network Security*, 2006(8):13–15.

Fernandez, J. D., Smith, S., Garcia, M., and Kar, D. (2005). Computer forensics: a critical need in computer science programs. *Journal of Computer Sciences in Colleges*, 20(4):315–322.

Fette, I., Sadeh, N., and Tomasic, A. (2007). Learning to detect phishing emails. In *Proceedings of the 16th international conference on World Wide Web*, pages 649–656.

Florêncio, D. and Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, pages 657–666.

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

Fumera, G., Pillai, I., and Roli, F. (2006). Spam filtering based on the analysis of text information embedded into images. *Journal of Machine Learning Research*, 7:2699–2720.

Garera, S., Provos, N., Chew, M., and Rubin, A. (2007). A framework for detection and measurement of phishing attacks. In *Proceedings of the 2007 ACM Workshop on Recurring Malcode (WORM)*, pages 1–8.

Gastellier-Prevost, S. and Laurent, M. (2011). Defeating pharming attacks at the client-side. In *Proceedings of the 5th International Conference on Network and System Security (NSS)*, pages 33–40.

Geer, D. (2005). Technology news: Security technologies go phishing. *Computer*, 38(6):18–21.

Gouda, M., Liu, A., Leung, L., and Alam, M. (2007). Spp: An anti-phishing single password protocol. *Computer Networks*, 51(13):3715–3726.

Gross, J. B. and Rosson, M. B. (2007). Looking for trouble: understanding end-user security management. In *Proceedings of the 2007 symposium on Computer human interaction for the management of information technology.*

Guan, B., Wu, Y., and Wang, Y. (2012). A novel security scheme for online banking based on virtual machine. In *IEEE Sixth International Conference on Software Security and Reliability Companion (SERE-C)*, pages 12–17.

Gupta, G. and Pieprzyk, J. (2011). Socio-technological phishing prevention. *Information Security Technical Report*, 16(2):67–73.

Halevi, T., Lewis, J., and Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd international conference on World Wide Web companion (WWW)*, pages 737–744, Republic and Canton of Geneva, Switzerland. International World Wide Web Conferences Steering Committee.

Han, W., Cao, Y., Bertino, E., and Yong, J. (2012). Using automated individual white-list to protect web digital identities. *Expert Systems with Applications*, 39(15):11861–11869.

He, M., Horng, S.-J., Fan, P., Khan, M., Run, R.-S., Lai, J.-L., Chen, R.-J., and Sutanto, A. (2011). An efficient phishing webpage detector. *Expert Systems with Applications*, 38(10):12018–12027.

Herzberg, A. (2009). Why johnny can't surf (safely)? attacks and defenses for web users. *Computers and Security*, 28(1-2):63–71.

Hinson, G. (2010). There must be thirty ways to steal your id. *The EDP Audit, Control, and Security Newsletter*, 41(5):1–15.

Hodgson, P. (2005). The threat to identity from new and unknown malware. *BT Technology Journal*, 23(4):107–112.

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

Huber, M., Mulazzani, M., Weippl, E., Kitzler, G., and Goluch, S. (2011). Friend-in-the-middle attacks: Exploiting social networking sites for spam. *IEEE Internet Computing*, 15(3):28–34.

Ilchev, S. and Ilchev, V. (2012). Modular data hiding for improved web-portal security. In *Proceedings of the 13th International Conference on Computer Systems and Technologies*, pages 187–194.

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

Jahankhani, H. (2009). The behaviour and perceptions of on-line consumers: Risk, risk perception and trust. *International Journal of Information Science and Management*, 7(1):79–90.

Jakobsson, M. and Ratkiewicz, J. (2006). Designing ethical phishing experiments: A study of (rot13) ronl query features. In *Proceedings of the 15th International Conference on World Wide Web*, pages 513–522.

Jakobsson, M. and Stamm, S. (2007). Web camouflage: Protecting your clients from browser-sniffing attacks. *IEEE Security and Privacy*, 5(6):16 –24.

Jo, I., Jung, E., and Yeom, H. (2013). Interactive website filter for safe web browsing. *Journal of Information Science and Engineering*, 29(1):115–131.

Khonji, M., Iraqi, Y., and Jones, A. (2013). Phishing detection: A literature survey.

Khot, R. A., Kumaraguru, P., and Srinathan, K. (2012). Wyswye: shoulder surfing defense for recognition based graphical passwords. In *Proceedings of the 24th Australian Computer-Human Interaction Conference (OzCHI)*, pages 285–294.

Kim, Y.-G., Lee, M., Cho, S., and Cha, S. (2012). A quantitative approach to estimate a website security risk using whitelist. *Security and Communication Networks*, 5(10):1181–1192.

Kirda, E. and Kruegel, C. (2005). Protecting users against phishing attacks with antiphish. In *Proceedings of the International Computer Software and Applications Conference*, volume 1, pages 517–524.

Kirlappos, I. and Sasse, M. (2012). Security education against phishing: A modest proposal for a major rethink. *IEEE Security and Privacy*, 10(2):24–32.

Knight, W. (2005). Caught in the net. *IEE Review*, 51(7):26–30.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J., and Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. In *Proceedings of the Conference on Human Factors in Computing Systems*, pages 905–914.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L., and Hong, J. (2010). Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10(2).

Larcom, G. and Elbirt, A. (2006). Gone phishing. *IEEE Technology and Society Magazine*, 25(3):52–55.

Lenton, D. (2005). Bigger phish to fry. *IEE Review*, 51(10):26–27.

Levy, E. (2004). Interface illusions. *IEEE Security and Privacy*, 2(6):66–69.

Li, L., Helenius, M., and Berki, E. (2012). A usability test of whitelist and blacklist-based anti-phishing application. In *Proceedings of the 16th International Academic MindTrek Conference*, pages 195–202.

Liu, G., Qiu, B., and Wenyin, L. (2010). Automatic detection of phishing target from phishing webpage. In *Proceedings of the 20th International Conference on Pattern Recognition (ICPR)*, pages 4153–4156.

Liu, W., Guanglin, H., Liu, X., Xiaotie, D., and Zhang, M. (2005). Phishing webpage detection. In *Proceedings of the International Conference on Document Analysis and Recognition (ICDAR)*, pages 560–564.

Ludl, C., McAllister, S., Kirda, E., and Kruegel, C. (2007). On the effectiveness of techniques to detect phishing sites. In *Proceedings of the 4th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, volume 4579, pages 20–39.

Maurer, M.-E. and Höfer, L. (2012). Sophisticated phishers make more spelling mistakes: Using url similarity against phishing. In *Proceedings of the 4th International Symposium on Cyberspace Safety and Security*, volume 7672, pages 414–426.

McFedries, P. (2006). Technically speaking: Gone phishin'. *IEEE Spectrum*, 43(4):80.

McNealy, J. (2008). Angling for phishers: Legislative responses to deceptive e-mail. *Communication Law and Policy*, 13(2):275–300.

Mills, J. and Byun, S. (2006). Cybercrimes against consumers: Could biometric technology be the solution? *IEEE Internet Computing*, 10(4):64–71.

Mohebzada, J., El Zarka, A., Bhojani, A., and Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. In *Proceedings of the International Conference on Innovations in Information Technology (IIT)*, pages 249–254.

Moore, T. (2007). Phishing and the economics of e-crime. *Infosecurity*, 4(6):34–37.

Moore, T. and Clayton, R. (2007). Examining the impact of website take-down on phishing. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, pages 1–13.

Moran, T. and Moore, T. (2010). The phish-market protocol: Secure sharing between competitors. *IEEE Security and Privacy*, 8(4):40–45.

Nykodym, N., Kahle-Piasecki, L., Ariss, S., and Toussaint, T. (2010). Cybercrime and business: How to not get caught by the online phisherman. *Journal of International Commercial Law and Technology*, 5(4):252–259.

Olurin, M., Adams, C., and Logrippo, L. (2012). Platform for privacy preferences (p3p): Current status and future directions. In *Proceedings on the 10th Annual International Conference on Privacy, Security and Trust (PST)*, pages 217–220.

Parno, B., Kuo, C., and Perrig, A. (2006). Phoolproof phishing prevention. In *Proceedings of the 10th International Conference on Financial Cryptography and Data Security*, pages 1–19.

Paulson, L. D. (2010). New technique provides energy wirelessly. *Computer*, 43(4):16–19.

Piper, P. (2007). A newer, more profitable aquaculture. *Searcher: Magazine for Database Professionals*, 15(9):40–47.

Ranganayakulu, D., Kavisankar, L., and Chellappan, C. (2011). Enhanced e-mail authentication against spoofing attacks to mitigate phishing. *European Journal of Scientific Research*, 54(1):165–175.

Ray, E. and Schultz, E. (2007). An early look at windows vista security. *Computer Fraud and Security*, 2007(1):4–7.

Ross, D. (2009). Ars dictaminis perverted: The personal solicitation e-mail as a genre. *Journal of Technical Writing and Communication*, 39(1):25–41.

Ross, P. (2006). Microsoft to spammers: go phish. *IEEE Spectrum*, 43(1):48–49.

Saberi, A., Vahidi, M., and Bidgoli, B. (2007). Learn to detect phishing scams using learning and ensemble methods. In *Proceedings of the International Conference on Web Intelligence and Intelligent Agent Technology*, pages 311–314.

Shahriar, H. and Zulkernine, M. (2012). Trustworthiness testing of phishing websites: A behavior model-based approach. *Future Generation Computer Systems*, 28(8):1258–1271.

Sood, S., Sarje, A., and Singh, K. (2011). Dynamic identity-based single password anti-phishing protocol. *Security and Communication Networks*, 4(4):418–427.

Stabek, A., Watters, P., and Layton, R. (2010). The seven scam types: Mapping the terrain of cybercrime. In *Proceedings of the Second Cybercrime and Trustworthy Computing Workshop (CTC)*, pages 41 –51.

Sweeney, L. (2006). Protecting job seekers from identity theft. *IEEE Internet Computing*, 10(2):74–78.

Thiyagarajan, P., Aghila Prof., G., and Prasanna Venkatesan, V. (2012). Pixastic: Steganography based anti-phishing browser plug-in. *Journal of Internet Banking and Commerce*, 17(1).

Vamosi, R. (2009). Security alert: Phishers dangle some brand-new bait. *PC World*, 27(12):37–38.

Varshney, G., Joshi, R., and Sardana, A. (2012). Personal secret information based authentication towards preventing phishing attacks. *Advances in Intelligent Systems and Computing*, 176:31–42.

Verma, R., Shashidhar, N., and Hossain, N. (2012). Two-pronged phish snagging. In *Proceedings on the 7th International Conference on Availability, Reliability and Security (ARES)*, pages 174–179.

Vitaliev, D. (2010). The shadownet. *Engineering Technology*, 5(16):19–22.

Wang, J., Herath, T., Chen, R., Vishwanath, A., and Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *Professional Communication, IEEE Transactions on*, 55(4):345–362.

Wenyin, L., Liu, G., Qiu, B., and Quan, X. (2012). Antiphishing through phishing target discovery. *IEEE Internet Computing*, 16(2):52–60.

Whittaker, C., Ryner, B., and Nazif, M. (2010). Large-scale automatic classification of phishing pages. In *Proceedings of the 17th Annual Network and Distributed System Security Symposium (NDSS)*.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4):662–674.

Wu, M., Miller, R., and Garfinkel, S. (2006a). Do security toolbars actually prevent phishing attacks? In *Proceedings on the Conference on Human Factors in Computing Systems*, pages 601–610.

Wu, M., Miller, R., and Little, G. (2006b). Web wallet: preventing phishing attacks by revealing user intentions. In *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS)*, pages 102–113.

Xiang, G. and Hong, J. (2009). A hybrid phish detection approach by identity discovery and keywords retrieval. In *Proceedings of the 18th International World Wide Web Conference (WWW)*, pages 571–580.

Xiang, G., Hong, J., Rose, C., and Cranor, L. (2011). Cantina+: A feature-rich machine learning framework for detecting phishing web sites. *ACM Transactions on Information and System Security*, 14(2).

Yearwood, J., Webb, D., Ma, L., Vamplew, P., Ofoghi, B., and Kelarev, A. (2009). Applying clustering and ensemble clustering approaches to phishing profiling. In *Proceedings of the Eighth Australasian Data Mining Conference*, pages 25–34.

Yee, K.-P. and Sitaker, K. (2006). Passpet: convenient password management and phishing protection. In *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS)*, pages 32–43.

Zhang, J., Wu, C., Li, D., Jia, Z., Ouyang, X., and Xin, Y. (2012). An empirical analysis of the effectiveness of browser-based antiphishing solutions. *International Journal of Digital Content Technology and its Applications*, 6(7):216–224.

Zhang, Y., Hong, J., and Cranor, L. (2007). Cantina: A content-based approach to detecting phishing web sites. In *Proceedings of the 16th International World Wide Web Conference (WWW)*, pages 639–648.

Zhou, C., Leckie, C., and Karunasekera, S. (2009). Collaborative detection of fast flux phishing domains. *Journal of Networks*, 4(1):75–84.