U.C. Introdução à Investigação

Phishing

Docente: Luís Rato
Discentes: André Baião 48092
Gonçalo Barradas 48402
Guilherme Grilo 48921

Março 2022

Resumo

Sendo um dos grandes problemas da atualidade o *Phishing*, é uma das formas mais eficazes e utilizadas de crimes cibernéticos, sendo utilizada contra utilizadores individuais, empresas e agências corporativas ou governamentais. O *Phishing* tem um elevado impacto económico e social, assim como psicológico.

Existem vários tipos de *Phishing*, e várias formas de o combater. As tentativas de combate têm vindo a aumentar, e o desenvolvimento de ferramentas que ajudam a diminuir o número de ataques bem como a sua eficácia também.

O objetivo deste trabalho é fazer uma revisão das metodologias que estão implementadas e as que estão a ser desenvolvidas para combater o *Phishing*.

1 Introdução

Atualmente a utilização da internet é generalizada e essencial ao nosso dia-a-dia, havendo por isso cada vez mais partilha de informação online por parte do utilizador. Como resultado desta enorme partilha de informações e transações financeiras existe uma maior vulnerabilidade ao cibercrime. O *Phishing* é uma das formas mais eficazes e utilizadas de crimes cibernéticos, sendo utilizada contra utilizadores individuais, empresas e agências corporativas ou governamentais [4].

Nos últimos tempos temos assistido a cada vez mais fraudes online, ataques a sistemas de grandes empresas, bem como acesso a informações confidenciais de empresas, bancos etc,.. existem casos bastante mediáticos tanto no nosso país como noutros que incluem este tipo de crimes, sendo por isso essencial arranjar soluções para proteger as empresas e as pessoas deste tipo de crimes.

O Phishing pode conter vários tipos de crimes/objetivos, como falsificação de documentos, falsificação de dados informáticos, acesso ilegítimo, burla etc... O impacto económico do *Phishing* pode ser avaliado no caso das burlas, mas também em todos os gastos associados à resolução do ataque bem como à prevenção. O impacto social, ou psicológico pode dar origem a desconfiança constante, medo e ansiedade por parte da população em geral. O impacto emocional resultante de um ataque *Phishing* pode ser devastador para a vida da vítima, visto que vê a sua privacidade invadida, podendo ocorrer perdas monetárias grandes ou até mesmo vir a ter problemas com a justiça devido à ocorrência de roubo de identidade [5].

2 Estado de Arte

Ao longo dos anos têm sido desenvolvidas ferramentas para combater e diminuir os ataques de *Phishing*, a Tabela 1, apresenta exemplos de algumas dessas ferramentas.

Tabela 1: Ferramentas anti-*Phishing*

Ferramenta	**Tipo de Pishing**	**Estratégia**	**Referencias**
AntiPhish	Sites *Phishing*	Histórico de correspondência/uso de perfil	[13]
BogusBiter	Sites *Phishing*	Autenticação do servidor	[27]
CANTINA+	Sites *Phishing*	Aprendizagem	[25]
Quero	Sites *Phishing*	Mineração de texto	[14]
iTrustPage	Sites *Phishing*	Listas	[20]
SpoofGuard	Sites *Phishing*	Heurísticas baseadas em regras	[6]
PhishCatch	E-mail *Phishing*	Heurísticas baseadas em regras	[26]
BayeShield	Sites *Phishing*	Teste com base no usuário	[16]
B-APT	Sites *Phishing*	Aprendizagem	[17]
AZ-protect	Sites *Phishing*	Aprendizagem	[1]
MobiFish	App Smartphone	Correspondência de perfil	[24]
PhishAri	*Phishing* Social	Aprendizagem	[3]
PhishBlock	Sites *phishing*	Abordagem Híbrida	[7]

3 Tipos de *Phishing*

3.1 Deceptive Attack

É o tipo mais comum de ataque, no qual são utilizadas técnicas de engenharia social para enganar as vítimas. Este tipo de *Phishing* pode ser utilizado através de e-mails, sites, telefone ou redes sociais.

3.1.1 E-mail *Phishing*

Um e-mail *Phishing* é um e-mail falsificado, que tem como remetente uma pessoa ou instituição em que o destinatário confia, com o objetivo de o convencer e divulgar as suas informações confidenciais. Por vezes este tipo de e-mails são enviados para um grupo de indivíduos que estão associados a uma instituição ou que fazem parte de um mesmo grupo social de forma a que o e-mail seja mais credível, neste caso tem o nome de spear *Phishing*. No caso de os destinatários serem personalidades de relevância ou com altos cargos como CEOs por exemplo, tem o nome de whaling. No clone *Phishing*, ocorre a clonagem de um e-mail anteriormente recebido pelo destinatário, com alteração de links ou anexos do e-mail [23].

3.1.2 Sites *Phishing*

Os sites *Phishing* tem uma aparência bastante semelhante ao site legitimo. O usuário é redirecionado para este site depois de clicar num link que pode estar incorporado num e-mail ou através de um anúncio (clickjacking).

3.1.3 *Phishing* telefónico (Vishing e SMishing)

O *Phishing* telefónico é realizado através de telefonemas ou mensagens de texto. O usuário pode receber uma mensagem de alerta de segurança de um banco por exemplo, sendo coagido a efetuar uma chamada, enviar uma mensagem ou entrar num link onde partilha informações confidenciais [2].

3.1.4 *Phishing* Social

O *Phishing* social inclui o sequestro de contas, ataques de personificação, golpes e distribuição de malware [10].

3.2 Technical Subterfuge

É o ato de enganar os indivíduos para divulgar as suas informações confidenciais através do download de um código malicioso no sistema. Este tipo de *Phishing* pode ser classificado em *Phishing* baseado em malware, Phishing baseado em DNS (Pharming), *Phishing* de injeção de conteúdo, Man-in-the-middle *Phishing*, Mecanismo de pesquisa *Phishing* e Ataques URL.

3.2.1 *Phishing* baseado em malware

Este tipo de *Phishing* baseia-se na execução de um software malicioso na máquina do usuário. O malware é descarregado através de truques de engenharia social ou através de vulnerabilidades no sistema de segurança. O *Phishing* baseado em malware pode ser de vários tipos, tais como, Key Loggers and Screen Loogers, Vírus e Worms, Spyware (software de espionagem), Adware, Ransomware, Rootkits, Session Hijackers (Sequestradores de Sessão), Web Trojans, Hosts File Poisoning, Ataques de reconfiguração do sistema, Roubo de dados.

3.2.1.1 Key Loggers and Screen Loggers

São um tipo de malware geralmente instalados através de e-mail Trojans ou através de download direto. Este tipo de software monitoriza dados e regista teclas do usuário, conseguindo assim capturar informações confidenciais relacionadas às vítimas, como nomes, endereços, senhas e outros dados confidenciais.

3.2.1.1.1 Vírus e Worms

Um vírus é um pedaço de código que se espalha dentro de um aplicativo ou programa, fazendo cópias de si mesmo de forma automatizada. Os Worms são semelhantes aos vírus, mas diferem na forma de execução, pois os Worms são executados explorando a vulnerabilidade dos sistemas operativos sem a necessidade de modificar outro programa. Os vírus transferem de um computador para outro através do documento ao qual estão conectados, enquanto os Worms fazem a transferência através do arquivo de host infectado.

3.2.1.1.2 Spyware (sofware de espionagem)

O software de espionagem é um código malicioso projetado para rastrear os sites visitados pelos usuários, com o objetivo de roubar informações confidenciais. O Spyware pode ser recebido através de e-mails e após ser instalado no computador, assume o controle sobre o dispositivo e altera as suas configurações, tendo a capacidade de recolher informações como senhas e números de cartão de crédito ou registos bancários que podem ser usados para roubo de identidade.

3.2.1.1.3 Adware

O adware é um tipo de malware que mostra ao usuário uma janela pop-up sem fim com anúncios que podem prejudicar o desempenho do dispositivo. Alguns dos adwares podem ser usados para rastrear os sites da internet que o usuário visita ou até mesmo gravar as teclas do usuário.

3.2.1.1.4 Ransomware

Ransomware é um tipo de malware que criptografa os dados do usuário depois de executar um programa malicioso no dispositivo. Neste tipo de ataque, a chave de descriptografia é mantida até que o usuário pague um resgate. O Ransomware geralmente é recebido pelo usuário através de um e-mail.

3.2.1.1.5 Rootkits

Um rootkit é uma coleção de programas, que permitem o acesso a uma rede de computadores. Estes conjuntos de ferramentas são utilizados para ocultar ações dos administradores do sistema. Normalmente este género de software é utilizado com o intuito de alertar as ferramentas existentes do sistema para escapar à detecção.

3.2.1.2 Session Hijackers (Sequestradores de Sessão)

O sequestrador de sessão permite que o invasor monitorize as atividades do usuário, incorporando um software no navegador, ou na rede. A monotorização tem como objetivo permitir ao invasor realizar ações não autorizadas tais como transferências financeiras e/ou de dados.

3.2.1.3 Web Trojans

Os Web Trojans são programas maliciosos que coletam as credenciais do usuário, aparecendo de forma oculta sobre a tela de login.

3.2.1.4 Hosts File Poisoning

Quando o usuário digita um endereço específico, o URL é traduzido num IP antes de aceder ao site, sendo o DNS alterado o que leva o usuário a um site específico de *Phishing*.

3.2.1.5 Ataques de reconfiguração do sistema

Neste caso as configurações do computador são alteradas utilizando diferentes métodos, como por exemplo reconfiguração do sistema operativo ou alteração do DNS. Esta reconfiguração permite a monitorização do usuário.

3.2.1.6 Roubo de dados

O roubo de dados pode ser realizado através de um e-mail de *Phishing* que leva a um download, que, por sua vez, rouba informações confidenciais que estão armazenadas diretamente nesse computador. As informações roubadas podem ser senhas, números de segurança social, informações de cartão de crédito ou e-mails confidenciais.

3.2.2 *Phishing* baseado em DNS (Pharming)

Inclui todas as formas de *Phishing* que interferem com o DNS para que o usuário seja redirecionado para o site malicioso, sobrecarregando a cache do DNS do usuário com informações erradas. Embora o arquivo do host não faça parte do DNS, a infeção por arquivos do host é outra forma de *Phishing* deste tipo. Por outro lado, os endereços IP genuínos são modificados, comprometendo assim o DNS. O usuário pode ser vítima de pharming mesmo clicando num link legítimo porque o DNS do site pode ser sequestrado por cibercriminosos [12].

3.2.3 *Phishing* de injeção de conteúdo

Phishing de injeção de conteúdo refere-se à inserção de conteúdo falso num site legítimo. O conteúdo pode ser colocado num site de três maneiras:

- através de uma vulnerabilidade de segurança e comprometimento de um servidor web;
- através de uma vulnerabilidade de Scripting cross-site (XSS), que é uma falha de programação permitindo aos invasores inserir scripts do lado do cliente em páginas Web, que serão visualizados pelos visitantes no site alvo;
- através de uma vulnerabilidade de injeção de Linguagem de Consulta Estruturada (SQL), que permite que hackers roubem informações da base de dados do site, executando comandos num servidor remoto [22].

3.2.4 Man-in-the-middle *Phishing*

O ataque Man-In-The-Middle (MITM) é uma forma de *Phishing*, no qual são inseridas comunicações entre duas partes (ou seja, entre usuário e site) e tentam obter as informações de ambas as partes interceptando as comunicações da vítima, de tal forma que a mensagem é encaminhada para o invasor ao invés dos destinatários legítimos. O ataque do MITM ocorre através de várias técnicas, como envenenamento pelo Address Resolution Protocol Poisoning, falsificação de DNS, Trojan Key Loggers e URL Obfuscation.

3.2.5 Mecanismo de pesquisa *Phishing*

São criado sites maliciosos com ofertas atraentes que utiliza técnicas de otimização de mecanismos de pesquisa para que eles sejam indexados legitimamente, de modo a que os mesmos apareçam ao usuário, de forma sugestiva, ao procurar produtos ou serviços.

3.2.6 Ataques URL

Na maioria dos ataques de *Phishing*, os phishers visam convencer um usuário a clicar num determinado link que conecta a vítima a um servidor de *Phishing* malicioso em vez do servidor de destino. Esta é a técnica mais popular usada pelos phishers atualmente. Este tipo de ataque é realizado recorrendo à técnica de URL Obfuscation, no site ao qual usuário se pretende conectar.

4 Medidas contra o *Phishing*

Existem 3 estratégias base para combater o *Phishing*:

- a consciencialização do utilizador para que este seja capaz de identificar e reagir de forma adequada, quando confrontado com uma ameaça;
- utilização da lei como medida de dissuasão;
- soluções técnicas de deteção automática dos ataques em estágios iniciais.

Dentro das soluções técnicas para deteção automática de *Phishing* existem essencialmente 3 categorias, tais como, ativação baseada em endereços Web, ativação baseada em conteúdos/similaridade da página web e abordagem híbrida.

4.1 Ativação baseada em endereços da web

A URL é um endereço de rede constituído por protocolo, nome e extensão do domínio, caminho e nome do arquivo. A ativação baseada em endereços web, tem como finalidade a avaliação de cada uma destas estruturas. Os esquemas de avaliação podem ser realizados com diferentes metodologias: técnicas de deteção baseadas em listas, técnicas heurísticas de deteção baseadas em regras e técnicas de deteção baseadas em aprendizagem [8].

4.1.1 Técnicas de deteção baseadas em listas

Neste tipo de técnica existe uma lista com URLs que pode ser uma lista branca que contém URLs que são considerados fidedignos, ou uma lista negra com URLs que são considerados maliciosos. No caso de listas brancas, o acesso é fornecido apenas para os URLs que estão presentes na lista, enquanto na abordagem de lista negra o acesso é fornecido a qualquer URL diferente dos que estão presentes na lista, sendo que esta tem que ser constantemente atualizada. [19].

4.1.2 Técnicas heurísticas de deteção baseadas em regras

As técnicas heurísticas de avaliação de endereços web baseados em regras aplicam heurísticas com base nas normas de estrutura de um URL, para verificar a autenticidade do mesmo. [11].

4.1.3 Técnicas de deteção baseadas em aprendizagem

Algoritmos de aprendizagem como machine learning e deep learning são usados para detetar os ataques com base nos recursos extraídos do URL. Os recursos estatísticos e recursos de NLP dos URLs são extraídos e alimentados em algoritmos de machine learning, como máquina vetorial de suporte (SVM), árvore de decisão, algoritmo ingénuo de Bayes, floresta aleatória etc. para classificação posterior. O classificador cria um modelo baseado na inferência extraída das amostras experimentais. A URL suspeita é avaliada com base no modelo construído pelo classificador. [21].

4.2 Ativação baseada em conteúdos/similaridade da página Web

A falsificação de páginas web implica a cópia das fontes, layout, imagens e logótipos de forma a que o site se assemelhe o mais possível com o original. Para detetar estes sites, é realizada a extração de vários recursos da página e avaliada a semelhança com o site original. Esta avaliação pode ser com base em esquemas de seleção baseada em conteúdos ou esquemas de deteção baseados em layout. No caso dos esquemas de detecção baseados em conteúdo, o conteúdo da página Web serve como o principal parâmetro para classificar sites de *Phishing*, e são extraídas palavras-chave suspeitas, que são utilizadas como parâmetros de pesquisa para medir a acessibilidade da página web. [28].

Nos esquemas de deteção baseados em similaridade, o layout do site é levado em consideração, podendo ser aplicada heurística ou algoritmos de machine learning.

4.2.1 Cálculo de similaridade de páginas Web baseado em regras heurísticas

No cálculo de similaridade de páginas Web baseado em heurística, são extraídos da página suspeita palavras-chave e recursos, que são verificados na página Web alvo utilizando métodos de pesquisa. Os recursos extraídos incluem recursos HTML, como número de links internos e externos, links vazios, formulários de login, comprimento de conteúdo HTML, janela de alarme, redirecionamento, informações ocultas/restritas, consistência entre marca de título e marca URL, consistência entre marca de link mais frequente e marca URL, recursos internos e externos, número da marca URL que aparece em HTML e assim por diante [15] e recursos CSS, como cor de propriedade, preenchimento em relação ao elemento no parágrafo, tamanho da fonte, borda, família de fontes e margens. [18].

4.2.2 Avaliação de similaridade de páginas web baseada em algoritmos de machine learning

Os recursos HTML, linguagem de marcação extensível, JavaScript (JS) e CSS são extraídos do código-fonte da página web e são alimentados em algoritmos de machine learning para sua classificação. [28].

4.3 Abordagem híbrida

As abordagens híbridas para deteção de *Phishing* na Web são uma combinação dos esquemas de deteção de ativação baseada em endereços Web e ativação baseada em conteúdos/similaridade da página Web. [9].

5 Problema

Tendo como base todas as ferramentas apresentadas na secção 2, vamos aprofundar a metodologia utilizada na PhishBlock, pois apresenta uma abordagem híbrida, que é descrita na bibliografia como sendo uma das formas mais eficazes de combate ao *Phishing* até ao momento.

O PhishBlock é uma ferramenta para deteção dinâmica e proativa de sites falsificados, que junta sistemas de pesquisa e classificação num simples aplicativo independente do navegador. O PhishBlock usa um código-fonte aberto.

No PhishBlock são utilizadas três listas locais (lista preta, branca e suspeita) nas quais verifica a presença do URL em questão. Se for encontrado em qualquer uma delas, é apresentada uma mensagem ao usuário (Falso, Seguro ou Suspeito), caso contrário, o URL é enviado para os servidores globais a serem testados pelo SVM.

No PhishBlock são utilizados três servidores (Phishtank, Google e Escrow Fraud). O URL em questão passa pelo Phishtank, onde é detetado como um site falso ou desconhecido, se for considerado desconhecido passa para o Escrow Fraud, caso contrário é adicionado à lista negra do PhishBlock. O mesmo procedimento ocorre no Escrow Fraud, onde o URL é transferido para o Google se não for desconhecido, caso contrário é adicionado à lista negra do PhishBlock. O sistema de classificação PhishBlock é implementado utilizando redes neurais, que são utilizadas para extrair padrões e detetar tendências muito complexas. A rede neuronal utilizada é a máquina vetorial de suporte (SVM). Os SVMs são um conjunto de métodos de aprendizagem supervisionados relacionados, utilizados para classificação. Dado um conjunto de exemplos de treino, cada um marcado como pertencente a uma das duas categorias, um algoritmo de treino SVM constrói um modelo que prevê se um novo exemplo se encaixa numa categoria ou noutra.

A ferramenta de anti-*Phishing* PhishBlock apresentou uma precisão de 95% e uma taxa de falsos positivos muito baixa (0,1%). Este estudo sugere que sistemas que dependem apenas de mecanismos de pesquisa ou sistemas de classificação que utilizam um pequeno conjunto de recursos são ineficazes no combate ao *Phishing*.

6 Conclusão

O *Phishing* tem vindo a aumentar nos últimos anos, o que leva a um impacto bastante negativo tanto a nível económico como a nível social. Cada vez mais empresas têm vindo a ser vítimas de ataques, aumentando assim a preocupação, bem como a urgência em encontrar métodos eficazes que impeçam futuros ataques. Várias ferramentas têm sido desenvolvidas com o objetivo de diminuir o número de ataques e a suscetibilidade das pessoas aos mesmos. Até ao momento os métodos que se mostram mais eficazes são os que utilizam uma abordagem híbrida, visto que o processo de análise é feito em várias etapas e sujeito a várias verificações, tornando mais difícil qualquer erro passar despercebido. No entanto, ainda temos um longo caminho a percorrer, pois os métodos de ataque estão em constante mudança, sendo estes cada vez mais sofisticados e difíceis de detetar.

Referências

[1] Ahmed Abbasi, Zhu Zhang, David Zimbra, Hsinchun Chen, and Jay F. Nunamaker. Detecting fake websites: The contribution of statistical learning theory. *MIS Quarterly*, 34(3):435–461, 2010. **https://doi.org/10.2307/25750686.**

[2] Maher Aburrous, M. A. Hossain, Fadi Thabatah, and Keshav Dahal. Intelligent phishing website detection system using fuzzy techniques. In *2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications*, pages 1–6, 2008. **https://doi.org/10.1109/ICTTA.2008.4530019**.

[3] Anupama Aggarwal, Ashwin Rajadesingan, and Ponnurangam Kumaraguru. Phishari: Automatic realtime phishing detection on twitter. In *2012 eCrime Researchers Summit*, pages 1–12, 2012. **https://doi.org/10.1109/eCrime.2012.6489521**.

[4] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, 2021. **https://doi.org/10.3389/fcomp.2021.563060**.

[5] APAV. Folha informativa phishing, 2013.

[6] Neil Chou, Robert Ledesma, Teraguchi Yuka, and John C Mitchell. Client-side defense against web-based identity theft. *Computer Science Department, Stanford University. Available:* ***http://crypto. stanford. edu/SpoofGuard/webspoof. pdf***, 2004.

[7] Hossam M.A. Fahmy and Salma A. Ghoneim. Phishblock: A hybrid anti-phishing tool. In *2011 International Conference on Communications, Computing and Control Applications (CCCA)*, pages 1–5, 2011. **https://doi.org/10.1109/CCCA.2011.6031523**.

[8] Varshney Gaurav, Misra Manoj, and K Atrey Pradeep. A survey and classification of web phishing detection schemes. *Security and Communication Networks*, 9(18):6266–6284, 2016. **https://doi.org/10.1002/sec.1674**.

[9] R. Gowtham and Ilango Krishnamurthi. A comprehensive and efficacious architecture for detecting phishing webpages. *Computers Security*, 40:23–37, 2014. **https://doi.org/10.1016/j.cose.2013.10.004**.

[10] Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. Social phishing. *Commun. ACM*, 50(10):94–100, oct 2007. **https://doi.org/10.1145/1290958.1290968**.

[11] S. Carolin Jeeva and Elijah Blessing Rajsingh. Intelligent phishing url detection using association rule mining. *Human-centric Computing and Information Sciences*, 6(1):10, Jul 2016. **https://doi.org/10.1186/s13673-016-0064-3**.

[12] Latika Kharb. What is pharming? 01 2017.

[13] Engin Kirda and Christopher Kruegel. Protecting Users against Phishing Attacks. *The Computer Journal*, 49(5):554–561, 01 2006. **https://doi.org/10.1093/comjnl/bxh169**.

[14] Viktor Krammer. Phishing defense against idn address spoofing attacks. PST '06, New York, NY, USA, 2006. Association for Computing Machinery. **https://doi.org/10.1145/1501434.1501473**.

[15] Yukun Li, Zhenguo Yang, Xu Chen, Huaping Yuan, and Wenyin Liu. A stacking model using url and html features for phishing webpage detection. *Future Generation Computer Systems*, 94:27–39, 2019. **https://doi.org/10.1016/j.future.2018.11.004**.

[16] Peter Likarish, Donald E Dunbar, Juan Pablo Hourcade, and Eunjin Jung. Bayeshield: conversational anti-phishing user interface. In *SOUPS*, volume 9, page 1, 2009.

[17] Peter Likarish, Eunjin Jung, Don Dunbar, Thomas E Hansen, and Juan Pablo Hourcade. B-apt: Bayesian anti-phishing toolbar. In *2008 IEEE International Conference on Communications*, pages 1745–1749. IEEE, 2008. **https://doi.org/10.1109/ICC.2008.335**.

[18] Jian Mao, Wenqian Tian, Pei Li, Tao Wei, and Zhenkai Liang. Phishing-alarm: Robust and efficient phishing detection via page component similarity. *IEEE Access*, 5:17020–17030, 2017. **https://doi.org/10.1109/ACCESS.2017.2743528**.

[19] Issa Qabajeh, Fadi Thabtah, and Francisco Chiclana. A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review*, 29:44–55, 2018. **https://doi.org/10.1016/j.cosrev.2018.05.003**.

[20] Troy Ronda, Stefan Saroiu, and Alec Wolman. Itrustpage: A user-assisted anti-phishing tool. In *Proceedings of the 3rd ACM SIGOPS/EuroSys European Conference on Computer Systems 2008*, Eurosys '08, page 261–272, New York, NY, USA, 2008. Association for Computing Machinery. **https://doi.org/10.1145/1352592.1352620**.

[21] Ozgur Koray Sahingoz, Ebubekir Buber, Onder Demir, and Banu Diri. Machine learning based phishing detection from urls. *Expert Systems with Applications*, 117:345–357, 2019. **https://doi.org/10.1016/j.eswa.2018.09.029**.

[22] Marcelo Invert Salas Palma, Paulo Licio De Geus, and Eliane Martins. Security testing methodology for evaluation of web services robustness - case: Xml injection. In *2015 IEEE World Congress on Services*, pages 303–310, 2015. **https://doi.org/10.1109/SERVICES.2015.53**.

[23] Xinyuan Wang, Ruishan Zhang, Xiaohui Yang, Xuxian Jiang, and Duminda Wijesekera. Voice pharming attack and the trust of voip. SecureComm '08, New York, NY, USA, 2008. Association for Computing Machinery. **https://doi.org/10.1145/1460877.1460908**.

[24] Longfei Wu, Xiaojiang Du, and Jie Wu. Mobifish: A lightweight anti-phishing scheme for mobile phones. In *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*, pages 1–8, 2014. **https://doi.org/10.1109/ICCCN.2014.6911743**.

[25] Guang Xiang, Jason Hong, Carolyn P. Rose, and Lorrie Cranor. Cantina+: A feature-rich machine learning framework for detecting phishing web sites. *ACM Trans. Inf. Syst. Secur.*, 14(2), sep 2011. **https://doi.org/10.1145/2019599.2019606**.

[26] Weider D. Yu, Shruti Nargundkar, and Nagapriya Tiruthani. Phishcatch - a phishing detection tool. In *2009 33rd Annual IEEE International Computer Software and Applications Conference*, volume 2, pages 451–456, 2009. **https://doi.org/10.1109/COMPSAC.2009.175**.

[27] Chuan Yue and Haining Wang. Bogusbiter: A transparent protection against phishing attacks. 10(2), jun 2010. **https://doi.org/10.1145/1754393.1754395**.

[28] Yue Zhang, Jason I. Hong, and Lorrie F. Cranor. Cantina: A content-based approach to detecting phishing web sites. In *Proceedings of the 16th International Conference on World Wide Web*, WWW '07, page 639–648, New York, NY, USA, 2007. Association for Computing Machinery. **https://doi.org/10.1145/1242572.1242659**.