IV Conferencia Científica Internacional
Universidad de las Ciencias Informáticas

Temática: Aplicaciones de la Inteligencia Artificial y Ciencias de Datos a la ciberseguridad.

Principales mecanismos para el enfrentamiento al phishing en las redes de datos

Main mechanisms for dealing with phishing in data networks

Antonio Hernández Dominguez [1*], Walter Baluja García

[1] Universidad de las Ciencias Informáticas (UCI), La Habana, 19370 Cuba. ahdominguez@uci.cu
[2] Universidad de las Ciencias Informáticas (UCI), La Habana, 19370 Cuba. walterb@uci.cu

[*] Autor para correspondencia: ahdominguez@uci.cu

Resumen
En los últimos años se han utilizado diversos mecanismos para detectar ataques de phishing. El papel desempeñado por las técnicas de aprendizaje automático ha sido significativo, principalmente por los niveles de eficacia obtenidos en la detección de estos ataques. Independientemente del servicio en el que se desarrollen, siempre es posible extraer un conjunto de rasgos que permitan identificar cuándo hay o no phishing. Las características pueden extraerse de diversas fuentes como las URL, el contenido compartido a través de un sitio web, una red social o simplemente un mensaje de correo electrónico, el motor de búsqueda, el certificado digital, el tráfico de red, entre otros. La precisión de la solución AntiPhishing depende del conjunto de rasgos, los datos de entrenamiento y el algoritmo de autoaprendizaje. Este artículo presenta un análisis actualizado de los métodos de aprendizaje automático y las herramientas informáticas utilizadas para detectar ataques de phishing en redes.

Palabras clave: Phishing, detección de Phishing, Aprendizaje Automático, herramientas informáticas

Abstract
In recent years, various mechanisms have been used to detect phishing attacks. The role played by machine learning techniques has been significant, mainly because of the levels of effectiveness obtained in detecting these attacks. Regardless of the service in which they are developed, it is always possible to extract a set of features to identify when phishing is or is not taking place. The features can be extracted from various sources such as URLs, content shared through a website, a social network or simply an email message, search engine, digital certificate, network traffic, among others. The accuracy of the AntiPhishing solution depends on the feature set, training data and self-learning algorithm. This paper presents an updated analysis of machine learning methods and computational tools used to detect phishing attacks in networks.

Keywords: *Phishing, Phishing Detection, Machine Learning, computational tools*

Introducción

En la actualidad, con el desarrollo vertiginoso de las Tecnologías de la Información y Comunicación (TIC), se ha manifestado una tendencia hacia el crecimiento del desarrollo de aplicaciones, que en dependencia del tipo de negocio al que estén asociadas, se inclinan o no al procesamiento de grandes volúmenes de datos. Paralelo al desarrollo y penetración de las TIC crece la necesidad de la seguridad de la información que es generada, almacenada, intercambiada y procesada. Las tendencias mundiales revelan un crecimiento exponencial de acciones malignas encaminadas a poner en riesgo la seguridad de la información. Un ciberataque consiste en cualquier acción tomada para socavar las funciones de una red informática con fines políticos o de seguridad nacional (Salinas Macías, 2015).

El Informe de Amenaza de Seguridad de Internet, emitido por la corporación multinacional estadounidense *Symantec* (Symantec, 2019), arroja que, en los últimos años, las tácticas más sencillas y los delincuentes informáticos más innovadores consiguieron resultados sin precedentes en el panorama de las amenazas mundiales. Los ataques que se realizan utilizando las técnicas de ingeniería social (Hadnagy, 2011), estimulan un ambiente con cierta manipulación psicológica, con el fin de lograr mediante el engaño a usuarios o empleados, que estos entreguen sus credencias de acceso u otros datos confidenciales. Frecuentemente, se hace uso del correo electrónico u otro medio de comunicación que invoca la urgencia, el miedo o emociones similares en la víctima, lo que lleva a esta a revelar rápidamente información sensible, hacer clic en un enlace malicioso o abrir un archivo malicioso.

Los ataques de phishing son uno de los más comunes entre los de ingeniería social (Sumner & Yuan, 2019). Estos emplean subterfugios técnicos y de ingeniería social para robar los datos de identidad personal y las credenciales de las cuentas financieras de los consumidores (APWG, 2020a). Este tipo de ataque suele lanzarse principalmente a través de mensajes de correo electrónico, que parecen ser enviados desde una fuente acreditada, con la intención de persuadir al usuario de que abra un archivo adjunto malicioso o siga una dirección URL fraudulenta. Una variante de phishing dirigido, denominada "*spear phishing*", se basa en la investigación previa de las víctimas para que la estafa parezca más auténtica (Allodi, Chotza, Panina, & Zannone, 2019), lo que la convierte en uno de los tipos de ataque más exitosos contra los usuarios de las redes de datos. Debido a que el factor humano juega un papel determinante, el

phishing, en los últimos años, se ha enfocado hacia las redes sociales (Yassein, Aljawarneh, & Wahsheh, 2019) y también hacia la mensajería de texto o SMS (*smishing*) (Balim & Gunal, 2019). Otras variantes de este ataque incluyen, el fraude de correo electrónico dirigido a ejecutivos (*whaling*) (G. Park & Rayz, 2018), el phishing a través de la redirección de los usuarios a un sitio falso (*pharming*) (Gajera, Jangid, Mehta, & Mittal, 2019), el phishing a través del servicio de voz (*vishing*) (Moul, 2019) y el phishing basado en el Localizador de Recursos Uniforme (URL maliciosas), contenidas en códigos de respuesta rápida o QR (*QRishing*) (Chorghe & Shekokar, 2016).

Durante el 2020, los Ataques de Comprometimiento de Correo Electrónico Empresarial (BEC), variante de *spear phishing*, fueron cada vez más costosos para las víctimas en todo el mundo. La solicitud media de transferencia bancaria en los ataques BEC aumentó de 48.000 dólares (USD) en el tercer trimestre a 75.000 dólares en el cuarto (APWG, 2020b). El número de ataques de phishing observados por el Grupo de Trabajo Anti-Phishing (APWG) y sus miembros creció hasta 2020, duplicándose en el transcurso del año (APWG, 2020b) (ver Figura 1).

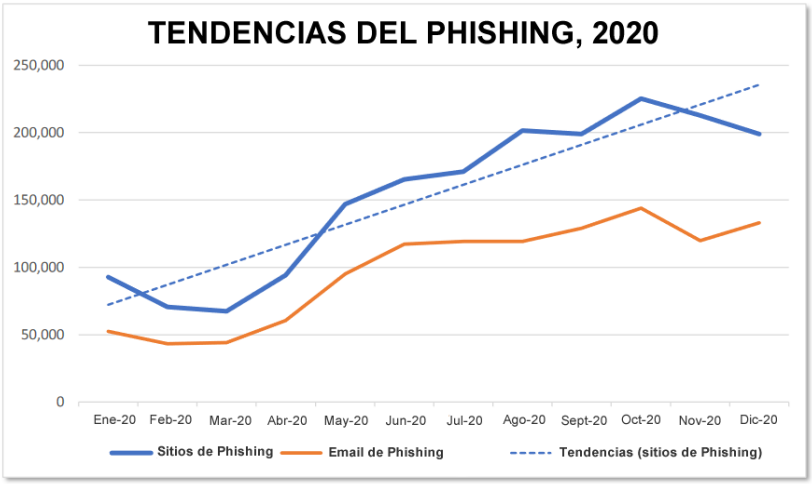

Figura 1: Tendencias de los ataques de phishing (sitios, correo electrónico) durante el 2020. Fuente: APGW (APWG, 2020b).

Otro aspecto a destacar es que los ataques de *vishing* se han detectado principalmente en el sector financiero, así como la suplantación de identidad en las redes sociales, ha aumentado considerablemente desde el 2016, debido a la utilidad que tienen los perfiles de usuario para los *phishers* (Sfakianakis, Douligeris, Marinos, Lourenço, & Raghimi, 2019).

Dada la vigencia e impacto de estos ataques, se han realizado numerosas investigaciones sobre los enfoques de detección. Los trabajos de revisión precedentes (Adil, Khan, & Ghani, 2020; Althobaiti, Rummani, & Vaniea, 2019; Chorghe & Shekokar, 2016; Qabajeh, Thabtah, & Chiclana, 2018; Shaikh, Shabut, & Hossain, 2016; Yassein et al., 2019; Zuraiq & Alkasassbeh, 2019) se han centrado en el estudio y clasificación de las técnicas de detección más significativas en cada servicio. Sin embargo, esta investigación proporcionará un análisis integral, amplio y actualizado de los métodos y herramientas informáticas existentes que han demostrado ser más efectivos en los últimos años.

Materiales y métodos

A nivel internacional se han utilizado diversos métodos para la detección de los ataques de phishing. Según se aprecia en la Figura 2, el estudio de trabajos precedentes permite agrupar estas soluciones en dos grandes grupos: convencionales y automatizados (Hernández Dominguez & Baluja García, 2021).

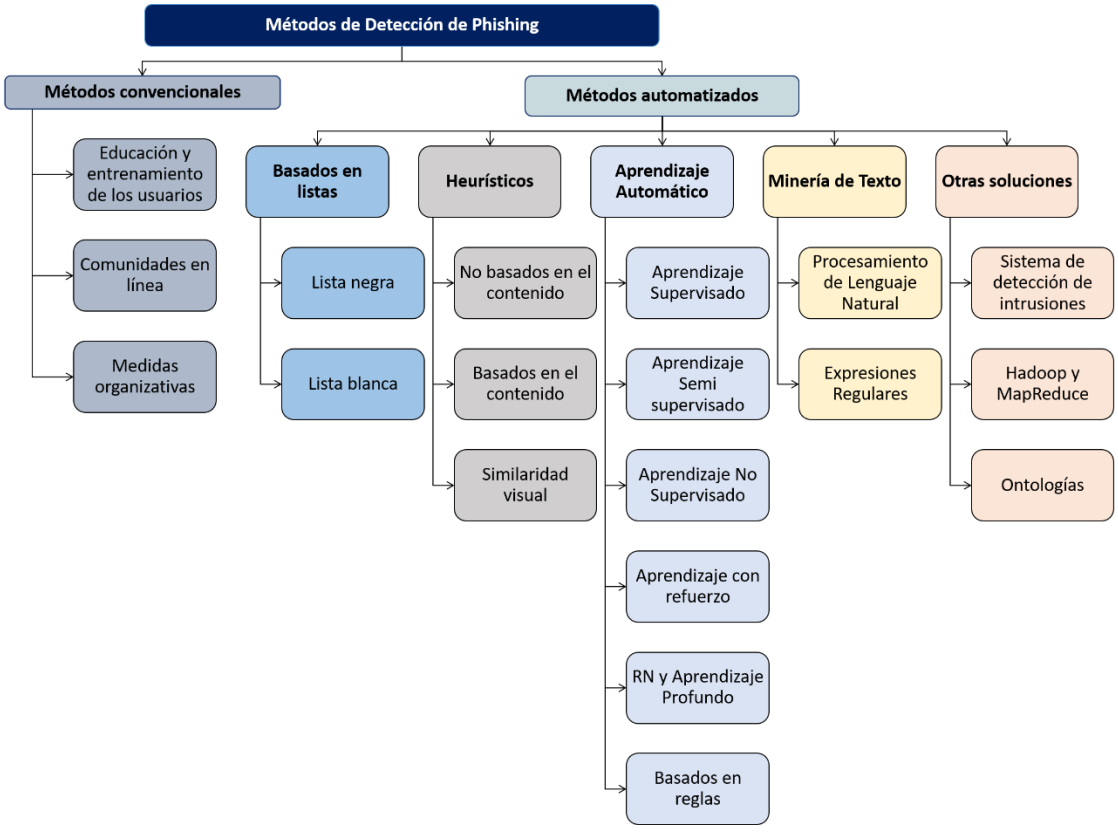

Figura 2: Métodos más utilizados en la detección de ataques de phishing. Fuente: (Hernández Dominguez & Baluja García, 2021)

Métodos convencionales

Según la literatura existen soluciones encaminadas a la formación de los usuarios, para detectar este tipo de ataques, utilizando para ello un entorno de entrenamiento integrado (Dixon, Arachchilage, & Nicholson, 2019) con situaciones reales. Otras soluciones son basadas en la experiencia del usuario, lo que ha permitido la creación de comunidades en línea como Anti-Phishing (APWG[1], *PhishTank*[2], *Millersmiles*[3], *Symantec*[4], entre otros), las cuales tienen como función general monitorizar y denunciar las actividades de phishing recientes a los diferentes grupos de interés (Baadel, Thabtah, & Majeed, 2018).

Soluciones para la educación y entrenamiento de los usuarios

A continuación, se describen brevemente las herramientas AntiPhishing (Aassal & Verma, 2019) para la formación de usuarios:

- ***SecurityIQ-PhishSim*:** Plataforma basada en la web, desarrollada por el Instituto Infosec con el fin de formar en materia de AntiPhishing y concienciar a los usuarios en materia de seguridad. Entre las múltiples funcionalidades se encuentran la creación de correos electrónicos de phishing personalizados o el uso de plantillas ya disponibles, la simulación de ataques, las funciones de seguimiento y la posibilidad de enviar distintos tipos de correos electrónicos a diferentes usuarios como parte de un mismo ataque.
- ***Gophish*:** Plataforma de código abierto desarrollada por Jordan Wright, en noviembre de 2013. Está diseñada para permitir a los probadores de penetración simular ataques de phishing de forma rápida y eficiente. Ofrece múltiples rasgos, como la importación del formato de correo electrónico y la clonación de sitios web, para utilizarlos como plantillas en una simulación determinada.
- **Software de phishing LUCY:** Herramienta basada en la web que permite concienciar a los empleados sobre el phishing. A través de la plataforma en línea, los usuarios tienen acceso a un panel de control personal donde pueden hacer un seguimiento de todas las simulaciones realizadas, o crear otras nuevas, en vista de utilizarlas para futuros programas de entrenamiento. Además, se pueden configurar listas de destinatarios para

[1] https://apwg.org/
[2] https://www.phishtank.com/
[3] http://www.millersmiles.co.uk/
[4] https://securitycloud.symantec.com/

utilizarlas en ataques de phishing. LUCY ofrece múltiples plantillas de correo electrónico, cada una de las cuales puede utilizarse en varios idiomas.

- ***KingPhisher*:** Solución de código abierto desarrollada por *SecureStare*. *King Phisher* es una herramienta para probar y promover la sensibilización de los usuarios mediante la simulación de ataques de phishing. Cuenta con una arquitectura sencilla y flexible, que permite un control total sobre los correos electrónicos y el contenido del servidor. *King Phisher* puede ser utilizada para ejecutar las simulaciones que van desde la formación y concienciación simple hasta los escenarios más complicados en los que se sirven contenidos al usuario para recopilar credenciales.
- ***SpeedPhish Framework*:** Herramienta en *Python* desarrollada por *Adam Compton*. Esta herramienta puede ser utilizada para entrenar a los usuarios acerca de los principales conceptos relacionados con phishing. Esta herramienta sólo está disponible en sistemas Linux. Uno de los rasgos útiles de esta herramienta es la función de reconocimiento que permite buscar en motores de búsqueda objetivos potenciales. También contiene desplegado un servidor web integrado basado en la biblioteca *Twisted Python*, mediante el cual se ofrecen funciones de clonación de sitios web.
- ***Phishing Frenzy*:** Aplicación de código abierto para que un probador de penetración simule correos electrónicos de phishing. Desarrollada en 2013 por *Brandon McCann*, facilita la gestión de ataques de phishing de phishing. Entre sus funcionalidades destacan la disponibilidad de plantillas, la clonación de sitios web, la gestión de credenciales, emisión de estadísticas asociadas a un ataque y la exportación de los resultados en formatos XML o PDF.
- ***Wombat Security – ThreatSim*:** Plataforma web para desarrollar ataques de phishing integrada con varios módulos de formación, adquirida por la empresa *Wombat Security Technologies*, hoy día *Proofpoint Security Awareness Training*, el 14 de octubre de 2015. Es una herramienta totalmente comercial que ofrece más de 130 plantillas actualizadas casi semanalmente, en más de 25 idiomas. Tiene soporte para distintos tipos de ataques de phishing. También ofrece múltiples funciones, incluyendo la clonación de sitios web y la edición de código HTML para el caso de las plantillas de correo electrónico y sitios web.

Métodos automatizados para la detección de phishing

- **Métodos basados en listas:** Una práctica común es la utilización de bases de datos (lista negra y lista blanca), los cuales reflejan una efectividad de detección de ataques de phishing en el intervalo de un 47% a un 83%,

como promedio (Dong, Kapadia, Blythe, & Camp, 2015). Algunos ejemplos son: *MXToolBox Blacklist Check* (Bikov, Iliev, Mihaylov, & Stoyanov, 2019), *Barracuda Blacklist* (Chin, Xiong, & Hu, 2018), *Spamhaus Whitelist*, las listas negras de *PhishTank*, *Microsoft*, *Google* (Dong et al., 2015), entre otros. Estas soluciones pueden ser utilizadas en diversos servicios telemáticos.

- **Métodos heurísticos:** Existen varias estrategias heurísticas contra el phishing que han sido debatidas en la literatura. Los enfoques se dividen comúnmente en tres tipos (Silva, Feitosa, & Garcia, 2020): el enfoque no basado en contenido (Jayan & Dija, 2015), el enfoque basado en contenido (Nathezhtha, Sangeetha, & Vaidehi, 2019) y el enfoque basado en similitud visual (Huang, Yang, Qin, & Wen, 2019), siendo este último el más utilizado. Para la extracción de los rasgos utilizados durante la clasificación, en el caso de la similitud visual, se utiliza generalmente la técnica de Reconocimiento Óptico de Caracteres (OCR) (Wang & Duncan, 2019).
- **Métodos de Aprendizaje Automático (ML):** Teniendo en cuenta que el phishing es un problema típico de clasificación (Qabajeh et al., 2018), las técnicas de ML y la Minería de Datos (DM) resultan apropiadas para obtener conocimiento. Algunos de los métodos de la Inteligencia Artificial (IA) más referenciados en la literatura (Mishra & Soni, 2019), para la detección de phishing, son: los Árboles de Decisión (DT), los Métodos de Conjunto (Bosques Aleatorios (RF)), los Modelos Probabilísticos (Clasificador Bayesiano Ingenuo (NB) y Redes Bayesianas), la Máquina de Soporte Vectorial (SVM), la Lógica Difusa, las Redes Neuronales (NN) y los algoritmos de Aprendizaje Profundo (DL). De cada uno de los métodos de Aprendizaje Automático se derivan diversos enfoques que son aplicados en los sistemas Anti-Phishing, por lo que uno de los factores analizados siempre es el nivel de efectividad que estos tienen.
- **Minería de Texto (TM) y Procesamiento del Lenguaje Natural (NLP):** Utilizando estos métodos es posible identificar los intentos de phishing, a través del análisis de patrones sospechosos que incluyen, entre otros, el contenido de correos electrónicos, sitios web, URL, mensajes instantáneos, entre otros. Se han aplicado cuatro tipos de técnicas de TM y NLP en la detección de phishing: la Frecuencia de Término - Frecuencia Inversa de Documento (TF-IDF) (Dou, Khalil, Khreishah, Al-Fuqaha, & Guizani, 2017), las Expresiones Regulares (RE) (Abahussain & Harrath, 2019), el Modelado de Temas usando Análisis Semántico Latente (LSA) (Jain & Gupta, 2016) y el Modelo de Memoria Distribuida de Vectores de Párrafo (PV-DM) (Douzi, Amar, & Ouahidi, 2017).
- **Otras Soluciones:** Se identificaron varias técnicas emergentes contra el phishing, incluidas ontologías (G. Park & Rayz, 2018) y los Sistemas de Detección de Intrusos (Lam & Kettani, 2019). Además, en la literatura revisada (Vieira, Koch, Sobral, Westphall, & Leão, 2019) se propone Hadoop y se utilizan las principales ventajas que

proporciona la técnica de MapReduce para el procesamiento de los datos y la selección de rasgos que serán utilizados en la detección de phishing.

Rasgos más utilizados en la detección de phishing

A continuación, se resumen los rasgos más utilizados por los métodos automatizados de detección de phishing. En el caso de la web, se extraen mediante el análisis de las imágenes, los textos, y de los enlaces de los textos, de los documentos HTML y CSS del sitio web. Además, en este contexto también se tienen en cuenta los rasgos de JavaScript, los objetos ActiveX y los formularios, de ahí que se puedan agrupar de la siguiente manera:

Rasgos basados en la URL

- **Léxicos:** Las URL presentan numerosos rasgos léxicos que se utilizan en la detección de phishing, que incluyen: dirección IP y número de puerto contenidos en la URL, longitud, cantidad de parámetros, frecuencia de palabras claves, existencia de caracteres especiales ('/', '=', '@', '&' y '_') frecuencia de palabras en la lista negra, relación entre dígitos y caracteres, uso del Protocolo Seguro de Transferencia de Hipertexto (HTTPS), cantidad de puntos (Korkmaz, Sahingoz, & Diri, 2020), complejidad de *Kolmogorov* (Cuzzocrea, Martinelli, & Mercaldo, 2018), *Ngrams* de caracteres (Vazhayil, Vinayakumar, & Soman, 2018), entropía de URL (Aung & Yamana, 2019).
- **servicios de terceros:** Rasgos obtenidos a partir de los servicios WHOIS (Fang, Bailing, Junheng, Yushan, & Yuliang, 2015) y *Alexa Rank* (Shirazi, Bezawada, & Ray, 2018) (información de registro de nombre de dominio, edad del dominio, información geográfica y la similitud de nombre de dominio en función de la distancia de *Levenshtein* (Nathezhtha et al., 2019)), rasgos del dominio de nivel superior (TLD) (Tyagi, Shad, Sharma, Gaur, & Kaur, 2018), y el manejador de formularios del servidor (SFH) (Korkmaz et al., 2020).

Rasgos basados en el contenido

- **HTML:** cantidad de etiquetas, atributos de etiqueta HTML, Frecuencia de Término (TF-IDF), cantidad de elementos fuera de lugar, cantidad de elementos pequeños/ocultos, cantidad de elementos sospechosos, cantidad de enlaces internos/externos, enlaces nulos en el sitio y pie de página, existencia de más de una etiqueta de HEAD/BODY, marcos invisibles, cantidad de tipo de archivo específico, cantidad de *iframes*, árbol del Modelo de Objeto de Documento (DOM) (G. Sonowal & Kuppusamy, 2016), función ActiveX (Satam, Kelly, & Hariri,

2016), clic derecho deshabilitado, administrador de formularios del servidor, e identidad de formulario de inicio de sesión (Korkmaz et al., 2020).

- **JavaScript:** cantidad de cadenas sospechosas, cantidad de cadenas de caracteres largos (>40, >51), rutinas de decodificación, detección de *shellcode* (Moustafa, Misra, & Slay, 2018), cantidad de cadenas de *iframe* (Tahir, Asghar, Zafar, & Gillani, 2016), cantidad de objetos sospechosos, cantidad de *scripts* y cantidad de funciones (*eval*, *setInterval*, *OnMouseOver*) (Zhu et al., 2018).
- **Similitud visual del sitio web:** Texto, imágenes y similitud general (captura de pantalla), color dominante y su coordenada centroide (Futai, Yuxiang, Bei, Li, & Linsen, 2016), logo (A. J. Park, Quadari, & Tsang, 2017) y el ícono de página (*favicon*) (Hasan, Hasan, & Zahan, 2019).
- **URL acortadas:** Frecuencia de caracteres especiales ('/', '=', '@', '&' y '_'), ofuscación de la dirección IP, codificación de la URL, suplantación de la ruta, no coincidencia en el origen y destino de la URL, dirección IP del nombre de dominio, ofuscación de nombre de dominio, frecuencia de punto de entrada de la URL, cantidad de nombres de dominio y direcciones IP (Patil, Rane, & Bhalekar, 2017).
- **motor de búsqueda:** Se obtienen a partir de consultas de las componentes de la URL (URL completa, nombre de dominio, y otros) en los motores de búsqueda. (Althobaiti et al., 2019).
- **basados en redireccionamiento:** cantidad de dominios diferentes, direcciones IP en la cadena de redirecciones, cantidad de redirecciones (Althobaiti et al., 2019).

Rasgos basados en certificados

- **certificado TLS/SSL** (seguridad en la capa de transporte/capa de sockets seguros): nivel de validación, la ubicación del emisor, si es de pago o gratuito, las fechas de inicio y finalización del certificado (Althobaiti et al., 2019).

Por otro lado, los diferentes campos del mensaje del correo electrónico (Lam & Kettani, 2019) son utilizados como rasgos para detectar los ataques de phishing que habitualmente afectan este servicio. Existen variantes que incluyen el análisis de rasgos genéricos obtenidos a partir del encabezado y del propio contenido del mensaje. Resulta muy útil el resumen que se encuentra en (Han & Shen, 2016), en el que se agrupan los rasgos en cuatro categorías: de origen, de texto, de adjunto y de destinatario, pero solo es efectivo para el caso específico de los ataques de *spear phishing*.

Teniendo en cuenta esta clasificación y las presentadas en la literatura (Iyer, Atrey, Varshney, & Misra, 2017) se identificaron los siguientes rasgos:

- **genéricos:** tamaño, identificador del mensaje, fecha de envío del mensaje, cantidad de partes del cuerpo del mensaje (Han & Shen, 2016).
- **remitente:** dominio, dirección IP, Número de Sistema Autónomo (ASN), país, organización (Iyer et al., 2017).
- **destinatario:** dominio y organización (Verma & Aassal, 2017).
- **contenido**
  - **asunto:** longitud, cantidad de palabras, cantidad de caracteres, palabras en lista negra (Rathod & Pattewar, 2015).
  - **texto:** longitud promedio de las palabras, longitud el texto del mensaje, cantidad de palabras funcionales, expresiones regulares, cantidad de palabras complejas y simples, cantidad de caracteres, métricas de estilo, índices de legibilidad (Egozi & Verma, 2018), análisis de redes semánticas (Bhakta & Harris, 2015), urgencia, recompensa, lenguaje de amenazas en el contenido, saludo, firma, despedida en el mensaje, presencia de "De:" y "Para:" en el contenido del correo electrónico, cantidad de dominios vinculados, palabras del mensaje en la lista negra, cantidad de eventos *onClick*() en el contenido del correo electrónico (Zhang, He, & Wang, 2017), Indexación Semántica Latente (Chin et al., 2018), y las métricas (índice de niebla, índice inverso de niebla, índice SMOG, Índice de *Flesch-Kincaid* (FKRI)), utilizadas por Han (Han & Shen, 2016).
- **Rasgos de archivos adjuntos:** tamaño, tipo de archivo (Han & Shen, 2016).

En el caso de las redes sociales, según (Yassein et al., 2019) los principales rasgos utilizados para detectar phishing se obtienen del contenido, la información de la red social y la reputación de los enlaces. Los rasgos identificados para el caso de los ataques basados en URL se pueden aplicar aquí, puesto que un texto compartido por un usuario puede contener direcciones electrónicas, según plantea (Al-Janabi, Quincey, & Andras, 2017). De igual manera, este autor plantea el uso de los siguientes rasgos específicos del perfil del usuario:

- antigüedad de la cuenta,
- cantidad de seguidores,
- cantidad de perfiles seguidos,
- cantidad de elementos favoritos del usuario,
- imagen predeterminada del perfil,

- longitud del nombre de usuario,
- habilitación de la geolocalización de la cuenta,
- cantidad de contenido compartido.

Según (Amrutkar, Kim, & Traynor, 2017) los principales rasgos utilizados para detectar este tipo de phishing en la mensajería corta e instantánea son el contenido y la URL que pueda formar parte del contenido del mensaje enviado. En la Figura 3 se muestra un resumen de los principales rasgos según el servicio que se utilizan.

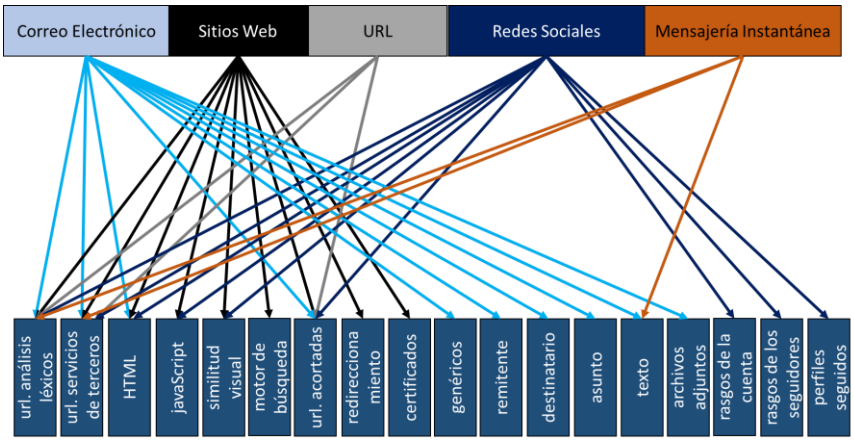

Figura 3: Relación de rasgos por servicios.

Herramientas que implementan la detección automatizada de phishing

Según la literatura se han encontrado varias herramientas informáticas para la detección de phishing, las mismas se clasifican en: herramientas puras de detección de phishing y aquellas dedicadas a la formación y concienciación de los usuarios. Con respecto al primer caso, en la Tabla 2 se muestra la efectividad de cinco herramientas antivirus que presentan módulos para la detección de phishing.

Tabla 1: Detección de Phishing a través de herramientas antivirus. Fuente: (Aassal & Verma, 2019)

Antivirus	**Avast**	**Kaspersky**	**AVG**	**Norton Antivirus**	**ESET**
Phishing Correos electrónicos Detectado	92.3%	87.7%	91.8%	37.4%	7.3%
Phishing Correos electrónicos no	7.7%	12.3%	8.2%	62.6%	92%7

Detectado					
Enlaces detectados en Navegador	80%	81.08%	60%	98%	98%

Cabe mencionar además las siguientes herramientas que pueden ser utilizadas para este fin:

- ***Netcraft*:** Constituye una barra de herramientas que utiliza varios métodos para determinar la autenticidad de un sitio web. Detecta, fundamentalmente, los sitios con direcciones URL que contienen caracteres sin significado. Proporciona la ubicación donde se encuentra alojado el sitio web. Además, realiza advertencias emergentes a los usuarios sobre los sitios sospechosos de phishing (Devi & Kumar, 2020).
- **AntiPhishing:** Complemento del navegador Mozilla Firefox cuyo objetivo es proteger a los usuarios inexpertos contra los ataques de phishing basados en sitios web. Esta barra de herramientas registra regularmente la información sensible del usuario y evita que esta información se transmita hacia un sitio web que no se considere "de confianza". Comprueba si el sitio web tiene una conexión segura con certificado SSL o no (Sharma, Meenakshi, & Bhatia, 2017).
- **Barra de información *URLcheck*:** Esta herramienta comprueba direcciones URL, así como los dominios y las direcciones IP asociadas. Permite generar informes personalizados a partir de las URL que contienen caracteres alfanuméricos o especiales (Sharma et al., 2017). La detección se realiza sobre la base de si la URL ya ha sido clasificada en otras plataformas AntiPhishing como *PhishTank*, APWG, entre otros.
- ***BitDefender*:** Utiliza la combinación de métodos heurísticos y listas negras. La herramienta presenta tres modos de alerta: verde, rojo y amarillo, con los cuales el usuario puede identificar en tiempo real los intentos de phishing. Esta permite bloquear los sitios web de phishing detectados anteriormente. También detecta si un sitio web tiene rastreadores y su ubicación (G. Sonowal, Kuppusamy, & Kumar, 2017).
- ***Spoofguard*:** Solución AntiPhishing desarrollada en la Universidad de *Stanford*. La barra de herramientas contiene varias reglas para identificar los sitios web de phishing. Inicialmente realiza un chequeo del nombre de dominio. Luego, se inspecciona la URL para detectar los números de puertos que no son estándares. *SpoofGuard* establece, a través de mecanismos heurísticos, advertencias a los usuarios de que el sitio es un sitio de phishing (Boneh, Mitchell, Ledesma, Chou, & Teraguchi, 2021).
- ***PhishDetector*:** Es una extensión de Google Chrome para detectar sitios bancarios fraudulentos. Es un sistema basado en reglas que analiza el contenido de la página web para identificar los ataques de phishing. La barra de herramientas detecta las estafas bancarias en línea y con un valor bajo de falsos negativos. Para

proteger al usuario del acceso a sitios web bancarios fraudulentos es muy recomendable instalar esta extensión en el navegador. Detecta un sitio de phishing en función de la revisión del contenido de la página web (Sharma et al., 2017).

- ***SafePreview*:** Extensión para el navegador Google Chrome que permite la comprobación de seguridad de sitios web, manteniendo el control de los enlaces sospechosos con servicios antivirus como *Norton Safe Web*, *McAfee WOT*, entre otros. Permite comprobar directamente un enlace recibido en un correo electrónico. La herramienta ofrece la posibilidad de añadir y eliminar sitios web de confianza para un sistema concreto (Roopak, Vijayaraghavan, & Thomas, 2019).
- ***Of-the-Hook*:** Complemento del navegador que permite detectar en tiempo real sitios web de phishing. La implementación se basa únicamente en la información extraída del navegador web, por lo tanto, se preserva la privacidad de los usuarios (Marchal et al., 2017). Mediante la combinación de una lista negra, un método de aprendizaje automático y 210 rasgos, este modelo puede detectar varios ataques de phishing (Zhu, Chen, Ye, Li, & Liu, 2019).
- ***Optimal Feature Selection* (OFS-NN):** Modelo eficaz de detección de sitios web de phishing basado en el método de selección óptima de rasgos y en la teoría de las redes neuronales. Mediante los rasgos sensibles seleccionados y un gran número de análisis experimentales, se entrena la estructura óptima de la red neuronal y se construye el clasificador final. Este modelo es capaz de detectar con precisión muchos tipos de ataques de phishing. Gracias a las potentes capacidades de aprendizaje y ajuste de la red neuronal, OFS-NN muestra un mejor rendimiento que muchos sistemas existentes en la detección de sitios web de phishing (Marchal et al., 2017).
- **S-Detector:** Modelo AntiPhishing que utiliza una combinación de técnicas basadas en el contenido y en la URL para detectar y bloquear los mensajes de *smishing*. Se divide en cuatro componentes: monitor de SMS, detector de SMS, analizador de SMS y base de datos. El contenido de los SMS se analiza comprobando la presencia de URL y palabras clave de *smishing* en el mensaje de texto. Las palabras clave de los SMS se analizan y clasifican mediante un clasificador bayesiano ingenuo (Mishra & Soni, 2019).
- **SmiDCA:** Presenta un modelo de detección de *smishing* que utiliza una combinación de métodos heurísticos, extracción de rasgos basados en el contenido y algoritmos de aprendizaje automático para diferenciar los mensajes de phishing de los legítimos (Gunikhan Sonowal & Kuppusamy, 2018).

Resultados y discusión

En cuanto a las herramientas utilizadas para el entrenamiento de los usuarios, todas las analizadas tienen documentación disponible y dan al usuario cierta libertad en cuanto a la creación de plantillas para simular ataques de Phishing. *PhishSim*, por ejemplo, tiene una opción de edición limitada, ya que no es posible eliminar el pie de página del correo electrónico que se genera y que indica, que este forma parte de un entrenamiento y no constituye una amenaza real. Mientras que *Gophish* da libertad absoluta a la creación de correos electrónicos, pero no ofrece plantillas predeterminadas. Casi todas las herramientas permiten a los usuarios elegir un servidor SMTP específico para retransmitir los correos electrónicos. Esta funcionalidad puede ser peligrosa, ya que les permite a los usuarios elegir cualquier plantilla abierta y crear un mensaje de phishing, que luego puede ser utilizado por los *phisher* para enviar ataques reales, especialmente si el usuario tiene la mencionada libertad de edición de plantillas.

Métodos automatizados con mayor efectividad en la detección de phishing

La efectividad de estos métodos (algoritmos, modelos, marcos de trabajo, entre otros), se comparó en términos de **EXACTITUD** de la detección (relación entre las predicciones correctas y las predicciones totales (Tyagi et al., 2018)). Tras la revisión de la literatura se ha determinado que los Árboles de Decisión y la Máquina de Soporte Vectorial son los métodos que ofrecen mayor efectividad y que se han utilizados para detectar phishing en todos los servicios analizados. Como se puede apreciar en la Tabla 1 y en la Figura 4, las Redes Neuronales Convolucionales, el Clasificador Bayesiano Ingenuo y los Bosques Aleatorios también destacan por su frecuencia de uso y efectividad.

Tabla 2: Comparación de la efectividad máxima en las propuestas de detección de phishing, según la literatura, por tipo de servicio

Método propuesto	Web	URL	Email	Redes Sociales	SMS/IM
DT	99,87	99,14	99,69	99,10	70,60
Boosting	97,49	99,60	99,84	No	No
NB	99,55	99,80	98,85	95,00	No
LR	98,19	99,56	99,69	97,00%	No
RF	98,86	99,50	99,99	95,40%	99,47
SVM	99,55	96,78	99,69	99,00%	78,1

k-NN	99,10	99,29	99,79	92,00%	98,61
CNN	99,00	99,63	99,42	83,30	No
RCNN	93,28	98,99	99,85	No	No

Métodos de Aprendizaje Automático; DT = árboles de decisión, NB = Clasificador Bayesiano Ingenuo, LR = Regresión Logística; RF = Bosques Aleatorios, SVM = Máquina de Soporte Vectorial, k-NN = Métodos de los k vecinos más cercanos, CNN = Redes Neuronales Convolucionales, RCNN = Redes Neuronales Convolucionales Recurrentes

En la literatura se encontraron pocas soluciones integradas las que, como parte de su funcionamiento, permitan detectar Phishing en más de un servicio, con el objetivo de optimizar los niveles de efectividad. Al diseñar soluciones integradas, los métodos de Aprendizaje Automático deben constituir un mecanismo esencial, debido a los niveles de eficacia que se logran cuando se aplican a problemas más específicos. Las redes neuronales artificiales están entre las más precisas. Del mismo modo, cuando se combinan algunos métodos de Aprendizaje Automático, los valores de exactitud se incrementan aún más. Por tanto, como parte del diseño de nuevas propuestas híbridas se deben seleccionar aquellas combinaciones de métodos que ofrezcan mejores resultados. Por otra parte, los rasgos más comunes utilizados para detectar el phishing se basan en el contenido, especialmente en el cuerpo de los mensajes y las URL.

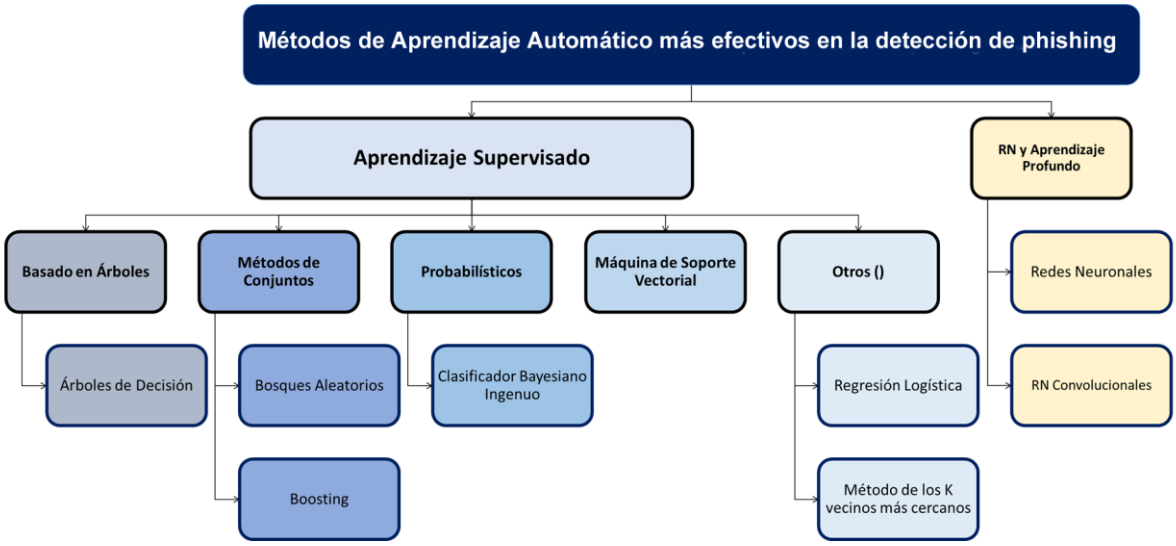

Figura 4: Métodos más efectivos en la detección de ataques de phishing.

En cuanto a las herramientas para la detección, en la Figura 3 se muestra una comparación de la efectividad de cada herramienta según la experimentación realizada en la literatura por (Sharma et al., 2017), (Mishra & Soni, 2019) y (Vijayalakshmi, Shalinie, Yang, & U, 2020). Las propuestas de Firefox, *BitDefender*, así como *Of-the-Hook*, *SmiDCA* y *Optimal Feature Selection* resultan las que más destacan con valores superiores al 90%. Por otra parte, se puede observar, como los métodos heurísticos y los basados en listas negras resultan ser ampliamente utilizados en la actualidad por las herramientas analizadas, aunque estos no sean precisamente los que mayor efectividad ofrezcan. Las siete primeras herramientas presentan un esquema comercial basado en el navegador o plataforma para la cual fueron desarrolladas. En el caso de los sitios web predomina la implementación de herramientas AntiPhishing de tipo complemento o extensión del navegador. Para el caso de la mensajería instantánea a partir del 2017 comienzan a surgir mode los híbridos que a futuro se incluirán en nuevas herramientas informáticas para la detección de phishing.

Tabla 3: Comparación de las herramientas para la detección automatizada de phishing.

Herramienta AntiPhishing	**Método de Detección**	**Servicio**	**Efectividad**
Netcraft (Devi & Kumar, 2020)	- Técnica de *sniffing* - Lista negra - Métodos heurísticos	Sitios web	73.90%
AntiPhishing Firefox (Sharma et al., 2017)	- Lista negra	Sitios web	96.75%
URLcheck (Sharma et al., 2017)	- Lista negra	URL	88.15%
BitDefender (G. Sonowal et al., 2017)	- Lista negra - Métodos heurísticos	Sitios web	94.85%
Spoofguard (Boneh et al., 2021)	- Lista negra - Métodos heurísticos	URL	84.35%
PhishDetector (Sharma et al., 2017)	- Sistema basado en reglas Máquina de Soporte Vectorial	Sitios web	59.15%
SafePreview (Roopak et al., 2019)	-Lista blanca -Lista negra -Métodos heurísticos	URL Correo electrónico	65.20%
Of-the-Hook (Marchal et al., 2017)	-Lista negra -Métodos heurísticos	Sitios web	97.50%

	-Aprendizaje Automático: *Boosting*		
Optimal Feature Selection (OFS-NN) (Zhu et al., 2019)	-Métodos heurísticos -Aprendizaje Automático: Redes Neuronales	Sitios web	99.30%
S-Detector (Mishra & Soni, 2019)	-Aprendizaje Automático: Clasificador Bayesiano ingenuo	SMS/IM	No se especifica
SmiDCA (Gunikhan Sonowal & Kuppusamy, 2018)	-Aprendizaje Automático: Bosques aleatorios, árboles de decisión, *boosting*, máquina de soporte vectorial	SMS/IM	96.40%

Conclusiones

En este artículo se presenta una revisión de los principales métodos, modelos y herramientas informáticas para la detección y la educación de los usuarios en cuanto al phishing en redes de datos. Aunque la educación de los usuarios, ya sea utilizando o no herramientas informáticas, puede influir positivamente en los esfuerzos globales para detectar estos ataques, este enfoque exige altos costos. Dado que las técnicas de phishing continúan evolucionando, no todas las organizaciones tienen los recursos necesarios para invertir en este enfoque. Esto hace que los usuarios comunes sean vulnerables, incluso si poseen conocimientos básicos sobre phishing (Qabajeh et al., 2018). Además, esta solución requiere conocimientos básicos de seguridad informática entre los usuarios formados (Alkhalil, Hewage, Nawaf, & Khan, 2021).

Los métodos de Aprendizaje Automático (Bosques Aleatorios, Árboles de Decisión y la Máquina de Soporte Vectorial) resaltan por su efectividad y frecuencia de utilización en las propuestas científicas existentes. Las herramientas de detección analizadas utilizan en su mayoría la combinación de varios métodos, entre ellos las listas negras, los métodos heurísticos y en casos limitados las técnicas de aprendizaje automático, de ahí que estas en su mayoría no han implementado aún los métodos más exitosos de la literatura científica.

Las técnicas de Aprendizaje Profundo no se han explotado lo suficiente en las herramientas para la detección de phishing, por lo que constituyen un método novedoso a explorar en investigaciones y desarrollos futuros. Por otra parte, no existen soluciones que permitan detectar el phishing en diversos escenarios/servicios, ni en la literatura ni entre las herramientas, resaltando la necesidad de trabajar en el desarrollo de un método que permita obtener una

solución integral para ser utilizada en escenarios con diversos servicios telemáticos, desde un enfoque sistémico y de gestión, que permita mejorar la detección de los ataques de phishing en las redes de datos.

Referencias

- Aassal, A. E., & Verma, R. (2019). *Spears Against Shields: Are Defenders Winning the Phishing War?* Paper presented at the Proceedings of the ACM International Workshop on Security and Privacy Analytics, Richardson, Texas, USA.
- Abahussain, O., & Harrath, Y. (2019, 22-23 Sept. 2019). *Detection of Malicious Emails through Regular Expressions and Databases.* Paper presented at the 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT).
- Adil, M., Khan, R., & Ghani, M. A. N. U. (2020, 17-19 Feb. 2020). *Preventive Techniques of Phishing Attacks in Networks.* Paper presented at the 2020 3rd International Conference on Advancements in Computational Sciences (ICACS).
- Al-Janabi, M., Quincey, E. d., & Andras, P. (2017). *Using supervised machine learning algorithms to detect suspicious URLs in online social networks.* Paper presented at the Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017, Sydney, Australia.
- Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *3*(6). doi:10.3389/fcomp.2021.563060
- Allodi, L., Chotza, T., Panina, E., & Zannone, N. (2019). On the Need for New Antphishing Measures Against Spear Phishing Attacks. *IEEE Security & Privacy*, 0-0. doi:10.1109/MSEC.2019.2940952
- Althobaiti, K., Rummani, G., & Vaniea, K. (2019, 17-19 June 2019). *A Review of Human- and Computer-Facing URL Phishing Features.* Paper presented at the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).
- Amrutkar, C., Kim, Y. S., & Traynor, P. (2017). Detecting Mobile Malicious Webpages in Real Time. *IEEE Transactions on Mobile Computing, 16*(8), 2184-2197. doi:https://doi.org/10.1109/TMC.2016.2575828
- APWG. (2020a). *Phishing Activity Trends Report - 2nd Quarter 2020*. Retrieved from USA. San Francisco: https://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf
- APWG. (2020b). *Phishing Activity Trends Report - 4th Quarter 2020*. Retrieved from USA. San Francisco: https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf
- Aung, E. S., & Yamana, H. (2019). *URL-based Phishing Detection using the Entropy of Non-Alphanumeric Characters.* Paper presented at the Proceedings of the 21st International Conference on Information Integration and Web-based Applications & Services, Munich, Germany.
- Baadel, S., Thabtah, F., & Majeed, A. (2018, 1-3/11/2018). *Avoiding the Phishing Bait: The Need for Conventional Countermeasures for Mobile Users*. Paper presented at the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON).
- Balim, C., & Gunal, E. S. (2019, 6-7 Nov. 2019). *Automatic Detection of Smishing Attacks by Machine Learning Methods.* Paper presented at the 2019 1st International Informatics and Software Engineering Conference (UBMYK).
- Bhakta, R., & Harris, I. G. (2015, 7-9 Feb. 2015). *Semantic analysis of dialogs to detect social engineering attacks.* Paper presented at the Proceedings of the 2015 IEEE 9th International Conference on Semantic Computing (IEEE ICSC 2015).

- Bikov, T. D., Iliev, T. B., Mihaylov, G. Y., & Stoyanov, I. S. (2019, 20-24/05/2019). *Phishing in Depth – Modern Methods of Detection and Risk Mitigation.* Paper presented at the 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).
- Boneh, D., Mitchell, J., Ledesma, R., Chou, N., & Teraguchi, Y. (2021). Portal Web oficial de Spoofguard. Retrieved from https://crypto.stanford.edu/SpoofGuard/
- Chin, T., Xiong, K., & Hu, C. (2018). Phishlimiter: A phishing detection and mitigation approach using Software-Defined networking. *IEEE Access, 6*, 42516-42531. doi:10.1109/ACCESS.2018.2837889
- Chorghe, S. P., & Shekokar, N. (2016, 26-27 Aug. 2016). *A survey on anti-phishing techniques in mobile phones.* Paper presented at the 2016 International Conference on Inventive Computation Technologies (ICICT).
- Cuzzocrea, A., Martinelli, F., & Mercaldo, F. (2018). *Applying Machine Learning Techniques to Detect and Analyze Web Phishing Attacks.* Paper presented at the Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services, Yogyakarta, Indonesia.
- Devi, R. S., & Kumar, M. M. (2020, 15-17 June 2020). *Testing for Security Weakness of Web Applications using Ethical Hacking.* Paper presented at the 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184).
- Dixon, M., Arachchilage, N. A. G., & Nicholson, J. (2019). *Engaging Users with Educational Games: The Case of Phishing.* Paper presented at the Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, Scotland Uk.
- Dong, Z., Kapadia, A., Blythe, J., & Camp, L. J. (2015, 26-29 May 2015). *Beyond the lock icon: real-time detection of phishing websites using public key certificates.* Paper presented at the 2015 APWG Symposium on Electronic Crime Research (eCrime).
- Dou, Z., Khalil, I., Khreishah, A., Al-Fuqaha, A., & Guizani, M. (2017). Systematization of Knowledge (SoK): A Systematic Review of Software-Based Web Phishing Detection. *IEEE Communications Surveys & Tutorials, 19*(4), 2797-2819. doi:10.1109/COMST.2017.2752087
- Douzi, S., Amar, M., & Ouahidi, B. E. (2017). *Advanced Phishing Filter Using Autoencoder and Denoising Autoencoder*. Paper presented at the Proceedings of the International Conference on Big Data and Internet of Thing, London, United Kingdom.
- Egozi, G., & Verma, R. (2018, 17-20 Nov. 2018). *Phishing Email Detection Using Robust NLP Techniques.* Paper presented at the 2018 IEEE International Conference on Data Mining Workshops (ICDMW).
- Fang, L., Bailing, W., Junheng, H., Yushan, S., & Yuliang, W. (2015, 29 Oct.-1 Nov. 2015). *A proactive discovery and filtering solution on phishing websites.* Paper presented at the 2015 IEEE International Conference on Big Data (Big Data).
- Futai, Z., Yuxiang, G., Bei, P., Li, P., & Linsen, L. (2016, 14-17 Oct. 2016). *Web Phishing detection based on graph mining.* Paper presented at the 2016 2nd IEEE International Conference on Computer and Communications (ICCC).
- Gajera, K., Jangid, M., Mehta, P., & Mittal, J. (2019, 12-14 June 2019). *A Novel Approach to Detect Phishing Attack Using Artificial Neural Networks Combined with Pharming Detection.* Paper presented at the 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA).
- Hadnagy, C. (2011). *Ingeniería social: el arte del hacking personal*: Ediciones Anaya Multimedia.
- Han, Y., & Shen, Y. (2016). *Accurate spear phishing campaign attribution and early detection.* Paper presented at the Proceedings of the 31st Annual ACM Symposium on Applied Computing, Pisa, Italy.

- Hasan, K. M. Z., Hasan, M. Z., & Zahan, N. (2019, 11-12 July 2019). *Automated Prediction of Phishing Websites Using Deep Convolutional Neural Network.* Paper presented at the 2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2).
- Hernández Dominguez, A., & Baluja García, W. (2021, 2021//). *Updated Analysis of Detection Methods for Phishing Attacks.* Paper presented at the Futuristic Trends in Network and Communication Technologies, Singapore.
- Huang, Y., Yang, Q., Qin, J., & Wen, W. (2019, 5-8 Aug. 2019). *Phishing URL Detection via CNN and Attention-Based Hierarchical RNN.* Paper presented at the 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).
- Iyer, R. P., Atrey, P. K., Varshney, G., & Misra, M. (2017, 9-11 Oct. 2017). *Email spoofing detection using volatile memory forensics.* Paper presented at the 2017 IEEE Conference on Communications and Network Security (CNS).
- Jain, A. K., & Gupta, B. B. (2016, 16-18 March 2016). *Comparative analysis of features based machine learning approaches for phishing detection.* Paper presented at the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom).
- Jayan, A., & Dija, S. (2015, 10-12 Dec. 2015). *Detection of spoofed mails.* Paper presented at the 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC).
- Korkmaz, M., Sahingoz, O. K., & Diri, B. (2020, 26-28 June 2020). *Feature Selections for the Classification of Webpages to Detect Phishing Attacks: A Survey.* Paper presented at the 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA).
- Lam, T., & Kettani, H. (2019). *PhAttApp: A Phishing Attack Detection Application.* Paper presented at the Proceedings of the 2019 3rd International Conference on Information System and Data Mining, Houston, TX, USA.
- Marchal, S., Armano, G., Gröndahl, T., Saari, K., Singh, N., & Asokan, N. (2017). Off-the-Hook: An Efficient and Usable Client-Side Phishing Prevention Application. *IEEE Transactions on Computers, 66*(10), 1717-1733. doi:10.1109/TC.2017.2703808
- Mishra, S., & Soni, D. (2019, 8-10 Aug. 2019). *SMS Phishing and Mitigation Approaches.* Paper presented at the 2019 Twelfth International Conference on Contemporary Computing (IC3).
- Moul, K. A. (2019). *Avoid Phishing Traps.* Paper presented at the Proceedings of the 2019 ACM SIGUCCS Annual Conference, New Orleans, LA, USA.
- Moustafa, N., Misra, G., & Slay, J. (2018). Generalized Outlier Gaussian Mixture technique based on Automated Association Features for Simulating and Detecting Web Application Attacks. *Intelligent phishing website detection using random forest classifier*, 1-1. doi:10.1109/TSUSC.2018.2808430
- Nathezhtha, T., Sangeetha, D., & Vaidehi, V. (2019, 1-3 Oct. 2019). *WC-PAD: Web Crawling based Phishing Attack Detection.* Paper presented at the 2019 International Carnahan Conference on Security Technology (ICCST).
- Park, A. J., Quadari, R. N., & Tsang, H. H. (2017, 3-5 Oct. 2017). *Phishing website detection framework through web scraping and data mining.* Paper presented at the 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON).
- Park, G., & Rayz, J. (2018, 7-10/10/2018). *Ontological Detection of Phishing Emails.* Paper presented at the 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC).

- Patil, P., Rane, R., & Bhalekar, M. (2017, 19-20 Jan. 2017). *Detecting spam and phishing mails using SVM and obfuscation URL detection algorithm.* Paper presented at the 2017 International Conference on Inventive Systems and Control (ICISC).
- Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review, 29*, 44-55. doi:10.1016/j.cosrev.2018.05.003
- Rathod, S. B., & Pattewar, T. M. (2015, 2-3 Nov. 2015). *A comparative performance evaluation of content based spam and malicious URL detection in E-mail.* Paper presented at the 2015 IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS).
- Roopak, S., Vijayaraghavan, A. P., & Thomas, T. (2019, 19-20 March 2019). *On Effectiveness of Source Code and SSL Based Features for Phishing Website Detection.* Paper presented at the 2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE).
- Salinas Macías, J. A. (2015). El uso de la fuerza en el ciberespacio. *Perspectiva Jurídica. Facultad de Derecho. Universidad Panamericana. México, 3*(5), 229.
- Satam, P., Kelly, D., & Hariri, S. (2016, 29 Nov.-2 Dec. 2016). *Anomaly behavior analysis of website vulnerability and security.* Paper presented at the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA).
- Sfakianakis, A., Douligeris, C., Marinos, L., Lourenço, M., & Raghimi, O. (2019). ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends. *10*, 622757.
- Shaikh, A. N., Shabut, A. M., & Hossain, M. A. (2016, 15-17 Dec. 2016). *A literature review on phishing crime, prevention review and investigation of gaps.* Paper presented at the 2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA).
- Sharma, H., Meenakshi, E., & Bhatia, S. K. (2017, 19-20 May 2017). *A comparative analysis and awareness survey of phishing detection tools.* Paper presented at the 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT).
- Shirazi, H., Bezawada, B., & Ray, I. (2018). *Know Thy Domain Name: Unbiased Phishing Detection Using Domain Name Based Features.* Paper presented at the Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies, Indianapolis, Indiana, USA.
- Silva, C. M. R. d., Feitosa, E. L., & Garcia, V. C. (2020). Heuristic-based strategy for Phishing prediction: A survey of URL-based approach. *Computers & Security, 88*, 101613. doi:10.1016/j.cose.2019.101613
- Sonowal, G., & Kuppusamy, K. S. (2016). *MASPHID: A Model to Assist Screen Reader Users for Detecting Phishing Sites Using Aural and Visual Similarity Measures.* Paper presented at the Proceedings of the International Conference on Informatics and Analytics, Pondicherry, India.
- Sonowal, G., & Kuppusamy, K. S. (2018). SmiDCA: An Anti-Smishing Model with Machine Learning Approach. *The Computer Journal, 61*(8), 1143-1157. doi:10.1093/comjnl/bxy039
- Sonowal, G., Kuppusamy, K. S., & Kumar, A. (2017, 6-7 Jan. 2017). *Usability evaluation of active anti-phishing browser extensions for persons with visual impairments.* Paper presented at the 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS).
- Sumner, A., & Yuan, X. (2019). *Mitigating Phishing Attacks: An Overview.* Paper presented at the Proceedings of the 2019 ACM Southeast Conference, Kennesaw, GA, USA.
- Symantec. (2019). Internet Security Threat Report 2019. *24*. https://docs.broadcom.com/doc/istr-24-2019-en

- Tahir, M. A. U. H., Asghar, S., Zafar, A., & Gillani, S. (2016, 15-17 Dec. 2016). *A Hybrid Model to Detect Phishing-Sites Using Supervised Learning Algorithms.* Paper presented at the 2016 International Conference on Computational Science and Computational Intelligence (CSCI).
- Tyagi, I., Shad, J., Sharma, S., Gaur, S., & Kaur, G. (2018, 22-23 Feb. 2018). *A Novel Machine Learning Approach to Detect Phishing Websites.* Paper presented at the 2018 5th International Conference on Signal Processing and Integrated Networks (SPIN).
- Vazhayil, A., Vinayakumar, R., & Soman, K. (2018, 10-12 July 2018). *Comparative Study of the Detection of Malicious URLs Using Shallow and Deep Networks.* Paper presented at the 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT).
- Verma, R., & Aassal, A. E. (2017). *Comprehensive Method for Detecting Phishing EmailsUsing Correlation-based Analysis and User Participation.* Paper presented at the Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, Scottsdale, Arizona, USA.
- Vieira, K., Koch, F. L., Sobral, J. B. M., Westphall, C. B., & Leão, J. L. d. S. (2019). Autonomic Intrusion Detection and Response Using Big Data. *IEEE Systems Journal*, 1-8. doi:10.1109/JSYST.2019.2945555
- Vijayalakshmi, M., Shalinie, S. M., Yang, M. H., & U, R. M. (2020). Web phishing detection techniques: a survey on the state-of-the-art, taxonomy and future directions. *IET Networks, 9*(5), 235-246. doi:10.1049/iet-net.2020.0078
- Wang, Y., & Duncan, I. (2019, 3-4 June 2019). *A Novel Method to Prevent Phishing by using OCR Technology.* Paper presented at the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security).
- Yassein, M. B., Aljawarneh, S., & Wahsheh, Y. A. (2019, 9-11 April 2019). *Survey of Online Social Networks Threats and Solutions.* Paper presented at the 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT).
- Zhang, Z., He, Q., & Wang, B. (2017). *A Novel Multi-Layer Heuristic Model for Anti-Phishing.* Paper presented at the Proceedings of the 6th International Conference on Information Engineering, Dalian Liaoning, China.
- Zhu, E., Chen, Y., Ye, C., Li, X., & Liu, F. (2019). OFS-NN: An Effective Phishing Websites Detection Model Based on Optimal Feature Selection and Neural Network. *IEEE Access, 7*, 73271-73284. doi:10.1109/ACCESS.2019.2920655
- Zhu, E., Ye, C., Liu, D., Liu, F., Wang, F., & Li, X. (2018, 11-13 Dec. 2018). *An Effective Neural Network Phishing Detection Model Based on Optimal Feature Selection.* Paper presented at the 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom).
- Zuraiq, A. A., & Alkasassbeh, M. (2019, 9-11 Oct. 2019). *Review: Phishing Detection Approaches.* Paper presented at the 2019 2nd International Conference on new Trends in Computing Sciences (ICTCS).