Estrategias de Ingeniería Social a Partir del Análisis de Datos Residuales en la Ciudad de Tunja

Social Engineering Strategies from the Residual Data Analysis in the City of Tunja

Cristian Cusaria[1], Andrea Fagua[2]
Grupo De Investigación Muisca, Facultad de Ingeniería, Fundación Universitaria Juan de Castellanos, Tunja, Colombia.
[1]ccusaria@jdc.edu.co, [2]afagua@jdc.edu.co

Recibido / Received: 14-09-2016 – Aceptado / Accepted: 16-11-2016

Resumen

La Ingeniería Social está enfocada al engaño y persuasión que pueda llevarse a través de la tecnología o psicología, con el fin de obtener información privilegiada; esta también es utilizada mediante contactos indirectos con la víctima. *El Dumpster Diving o Trashing* es uno de estos tipos de ataques de Ingeniería Social en el que se obtiene información privada (correos electrónicos, contraseñas, números de teléfono, números de cuentas bancarias, números de cedula, etcétera) por medio de acercamientos indirectos con la víctima (revisando su basura). El problema planteado en la presente investigación radica en la falta de conocimiento y control preventivo/correctivo sobre el manejo de los datos residuales (información) expuestos en la basura generada por las distintas empresas, organizaciones y entidades de la ciudad de Tunja, ya que esto puede propiciar un ataque informático basado en información sensible o privada, obtenida mediante "Trashing". Teniendo en cuenta que lo señalado como 'basura' contiene información correcta o falsa, en esta investigación deseamos analizar y demostrar que esta técnica ("*Trashing*") es un resultante de transmisión de información importante para cualquier entidad; en efecto, las empresas no son sensatas del riesgo que parten ante este tipo de descuidos. Por ello, la necesidad de diagnosticar medidas de seguridad, capacitación y formación de los empleados en este sentido, así como la creación de protocolos de eliminación de datos, ya sea desde el ámbito de las nuevas tecnologías, o desde los métodos convencionales (destructoras de papel o contratar servicios externos), así como incluir estas opciones delictivas en las auditorías internas.

Palabras clave: Seguridad Informática, Basurología, Telemática, Ingeniería de Sistemas, Ciberseguridad.

Abstract

The Social Engineering is focused on deception and persuasion that can be through technology or psychology, in order to get inside information; this is also used by indirect contact with the victim, The Dumpster Diving or Trashing is one of these types of social engineering attacks in which private information (emails, passwords, phone numbers, numbers of bank account, numbers the identity card, etc) through indirect approaches to the victim (Looking through her trash). The problem of this research is the lack of knowledge and preventive / corrective control on handling residual data (information) displayed on the waste generated by the various companies, organizations and institutions in the city of Tunja as this can lead a computer-based attack sensitive or private information obtained by "trashing". Given that what is stated as 'waste' contains incorrect or false information, this research we want to analyze and demonstrate that this technique "Trashing" is a result of transmission of important information for any entity, in fact businesses are unaware of the risk who are against this type of oversights, so the need to diagnose security measures, training and employee training in this regard, as well as the creation of protocols for data removal, either from the field of new technologies, or from conventional methods (paper shredders or outsource) and criminal options include these internal audits.

Keywords: Security Informatic, Basurología, Telematics, Systems Engineer, Cybersecurity.

I. Introducción

La ingeniería Social es definida desde distintos tipos de visión, la psicología, el hacktivismo, la seguridad informática, la computación, entre otros, es así como se encuentran distintas definiciones para este concepto, por ejemplo, se define como "El acto de manipular a las personas para llevar a cabo acciones o divulgar información confidencial"[1]. Aunque parecido a una estafa o un simple fraude, el término se aplica normalmente a las artimañas o engaños con el propósito de obtener información, llevar a cabo un fraude o acceder a un sistema informático; en la mayoría de los casos, el atacante nunca se enfrenta cara a cara con la víctima [2].

A pesar de que se ha ganado cierto mal nombre debido al exceso de sitios web con reclamos del tipo "pizza gratis", "café gratis", entre otros; en realidad, los aspectos de la ingeniería social afectan a muchos aspectos del día a día [3].

El diccionario *Webster* define "Social" como "relativo o perteneciente a la vida, el bienestar y las relaciones de los seres humanos en una comunidad". También, define la ingeniería como "el arte o la ciencia de llevar a aplicación práctica el conocimiento de las ciencias puras como la física o la química, en la construcción de máquina, edificaciones, embarcación, minas y plantas químicas o artilugios ingeniosos; maniobrar"[4].

Combinando ambas definiciones, puede verse fácilmente que la ingeniería social es el arte o, mejor aún, la ciencia, de maniobrar hábilmente para lograr que los seres humanos actúen en algún aspecto de sus vidas [5]. Yendo un poco más allá y consultando distintas definiciones, podríamos decir que la ingeniería social es el acto de manipular a una persona para que lleve a cabo una acción que "puede ser o no" lo más conveniente para el "objetivo" [6]. Esto puede incluir obtener información, conseguir algún tipo de acceso o lograr que el objetivo realice cierta acción. Todas estas amenazas posiblemente desarrolladas digitalmente como físicamente mediante distintas técnicas, procedimientos o métodos de ingeniera social.

La ingeniería social es un problema que nos embarga a todos, sus distintos métodos y técnicas, la falta de información, divulgación y capacitación en general hacen que sea difícil de controlar o evitar en dado caso. Las personas que aplican o ejecutan la ingeniería social se les llaman ingenieros sociales y de hecho existen distintos tipos de ingenieros sociales, por ejemplo, los *Hackers* (que tienen por objeto vulnerar lo que los proveedores de *software* van logrando cada vez más: "blindar" o dificultar

en acceso o copia), *Probadores De Seguridad* (profesionales que aprenden y utilizan las técnicas de los *hackers* para ayudar a garantizar la seguridad de sus clientes), *Espías* (para los espías, la ingeniería social es un modo de vida), *ladrones de identidad*, *empleados descontentos*, *artistas del timo, agentes de recursos humanos, vendedores, gobiernos*, entre otros[7].

En tal sentido, entre las diversas técnicas de ingeniería social, el "Dumpster Diving o Trashing" [8] es usada para la recopilación de información privada, sensible o importante mediante la revisión de basuras; es un potencial problema para todo tipo de entidad (empresa u organización), pero su origen radica en la falta de conocimiento y Control preventivo/correctivo con relación al manejo de los datos residuales (información) expuestos en la basura generada por las mismas, ya que esto puede propiciar a distintos ataques informáticos. Teniendo en cuenta que lo señalado como 'basura' podrá contener información verdadera o falsa, el resultante de transmisión de información es seguramente importante y sensible en dado caso; en efecto, las empresas no son conscientes del peligro que corren ante este tipo de descuidos [9], por ello, la necesidad de planificar, diseñar, desarrollar, implementar, validar y verificar distintas medidas de seguridad, capacitación y formación, protocolos de eliminación de datos, como también la inclusión del "Trashing" como delito en las auditorías internas.

Según GReAT (Global Research and AnalysisTeam) Latinoamérica, adjudicado a kasperskyLab, América Latina se ha convertido en una región no solamente basta en su territorio sino también importante desde el punto de vista del desarrollo económico, la penetración de Internet y el desarrollo industrial en la escena mundial [10]; estos tres factores han hecho que los ataques que se registraron en la región sean más complejos, mayores en sus números y hasta a veces nuevos en cuanto a las técnicas utilizadas. En uno de sus artículos de análisis, *"2014 desde la perspectiva viral en cifras en América Latina: predicciones para 2015"*, se exponen los datos estadísticos de inteligencia recopilados con la tecnología KSN (Kaspersky Security Network) durante todo el año 2014. Además, se da la proyección de los ataques venideros en el 2015 que se creían potencialmente riesgosos y ahora en 2016 se afirman muchos de ellos. Los datos estadísticos se construyeron a partir de la lista de los siguientes países: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela [11]. Analizando los resultados y pronósticos, es realmente revolucionario en cuanto a los ataques y especialmente sus tipos, sus nuevos métodos y hasta sus nuevas motivaciones y actores. Ya no podemos hablar únicamente del crimen cibernético como el único actor detrás de todo el *malware*, sino también tenemos las agencias gubernamentales y los gobiernos cuyos intereses son diferentes al robo de dinero o contraseñas de las víctimas, pero sí de la información confidencial del carácter secreto para un estado [12].

Es importante notar que los datos que han tenido lugar durante esa investigación, habían sido predichos por kaperskylab el año pasado [13]. Esto incluye los ataques dirigidos en la región y los troyanos bancarios hechos en América Latina que corren ya en los dispositivos móviles. Relata dicho artículo "**Ingeniería social para todo**: los eventos como Copa América y los juegos Olímpicos seguirán siendo explotados por los criminales locales para todo tipo de fraude. Por ejemplo, instalación de malware, ataques de phishing y hasta venta de artículos inexistentes. Todo con el fin de lucrar ilícitamente" [11]; y si hablamos de ingeniería social aplicada en nuestro país, cabe mencionar el nombre de *Jaime Alejandro Solano, bautizado como el 'rey del robo de millas'* señalado de hurtar 5 millones de millas a clientes de Diamond Avianca. Solano acudió a la persuasión y al engaño para ganarse la confianza de sus víctimas [14] (*Ingeniería Social*), en igual forma y manteniendo sus dimensiones "*dentro de los casos exitosos de ingeniería social reconocidos a nivel mundial, podemos encontrar el de la operación de rescate JAQUE"* [15].

En tal sentido, los ataques informáticos tanto digitalmente como físicamente no hubieran sido posibles sin la ingeniería social; detrás de un videojuego, un poderoso *malware* sin un *firewall* o antivirus que lo contenga y detrás de un video, un virus inmune a cualquier antivirus vigente, ¿pero

que hubiera sido de ellos si las víctimas no hubieran presionado 'clic'? [16]. Por esta razón, es de vital importancia el estudio, educación y prevención en relación con la ingeniería social, ya que "*el factor humano es el eslabón más débil de la cadena de seguridad que protege los datos en bancos y cajas"* según *la consultora en seguridad informática Deloitte en su informe 'Seguridad Global 2005'* [17], y se podría decir no solo de bancos sino también de empresas y organizaciones en general.

En atención a la técnica del "Dumpster Diving o Trashing", este método no es muy conocido en Colombia, pero sí empleado por *hackers*, probadores de seguridad, espías y, sobre todo, por el espionaje empresarial [18]. En consecuencia, la pertinencia de esta investigación hacia la falta de conocimiento, control preventivo y correctivo para este tipo de ataque informático es vital e imprescindible dentro y fuera de cualquier organización.

Para concluir esta sección, se plantea la siguiente pregunta: ¿De qué manera podemos prepararnos para ataques de ingeniería social y específicamente mediante la técnica de "Dumpster Diving o Trashing"?

II. Metodología

Dentro de la investigación realizada de los documentos bibliográficos, se utilizaron varias fuentes documentales. ScienceDirect (acceso privado JDC), TDR (Tesis Doctorales en Red), CornellUniversity Library, Dialnet, Universidad de la Rioja Directory of Open Access Journals (DOAJ), Science.gov, BDCOL (Biblioteca digital Colombiana), CHEMEDIA, entre otras; así mismo, se ejecutó una búsqueda bibliográfica en julio y agosto del 2016 en la biblioteca de la Fundación Universitaria Juan de Castellanos, utilizando los descriptores: *Dumpster Diving*, *Trashing*, Basurología, técnicas de ingeniería social, ingeniería social. Los registros obtenidos promedian entre 2 y 5 registros tras la combinación de las diferentes palabras clave. También, se realizó una búsqueda directamente en el buscador "Google académico" con los mismos términos, de allí se seleccionaron tan solo dos documentos que muy levemente hablaban sobre los aspectos formales que debía contener tan grande red de información. En dado caso, se entrelazan con la revisión y compilación de publicaciones encontradas en revistas, periódicos, blogs, libros de ingeniería social tanto digitalmente como físicamente, todos estos analizados a profundidad buscando su parte formal y verídica.

Al indagar en estas fuentes confiables y trascendentes en sus publicaciones, se desprende y sintetiza que el 'Dumpster Diving o Trashing' es la acción de recolectar información a partir de material descartado o comúnmente llamado 'Basura', con objetivo de obtener datos que sirvan como información para cometer fraudes [19]. Cabe resaltar que la información que se quiere revisar, husmear o examinar, se recolecta de las canecas, cestos o recipientes contenedores de notas, papeles, facturas, ordenadores, cartas, dispositivos de almacenamiento de datos fijos o portables y muchos más artilugios e informes que realmente pueden proporcionar increíbles cantidades de datos, a esto se le ha de considerar *Trashing físico* pero cuando el atacante procura conseguir información revisando los archivos que puedan estar en la computadora (papelera de reciclaje, historial de navegación, o los archivos que almacenan *cookies*), se denomina *Trashing Lógico* [20].

Esta acción '*Trashing'*, recientemente, es considerada un delito informático a nivel internacional [21]. No obstante, en Colombia la ley no lo estipula de una forma puntual, pero podría considerarse ya que un delito informático es toda aquella actividad criminal que está encuadrada en atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos [22], más específicamente, el Artículo 269F de la ley 1273 de 2009 lo abarcaría, *"*Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga,…intercepte... o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes" [23]; ya que apunta a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una empresa u otra entidad, con el fin de utilizarla en actividades delictivas, estas actividades

pueden tener como objetivo la realización de espionaje, coerción o simplemente el lucro mediante el uso ilegítimo de códigos de ingreso a sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada, suplantación de identidades, entre otras más [24]. Esta minuciosa distinción de sujetos, según su actuar, no son útiles para tipificar el delito puesto que son sujetos indeterminados, no requieren condición especial; más vale realizar dicha diferenciación para ubicarnos en el marco en que se desenvuelven y las características de su actuar, favoreciendo con ello el procedimiento penal que se deberá llevar a cabo luego de producirse el delito [25].

En Colombia es evidente, y no hablo de empresas en especial o entidades particulares; se desconoce la técnica del *Trashing* "Recoger o Buscar en la basura", ya que no existen casos de mayor importancia o un aumento en la práctica de esta técnica de ingeniería social comparativamente con Estados Unidos o países europeos donde es noticia diaria[26]; el origen de esta técnica no se puntualiza en ningún libro, pero posiblemente se le asigne al *hacker* norteamericano Kevin Mitnick, el cual comparte y describe con mayor profundidad estas técnicas en su libro *The Art of Deception*, allí expone todo lo que constituye la ingeniería social y al *Trashing* [27].

A. Modelo de Ejecución Ingeniería Social – Técnica Trashing o Dumpster Diving

Para que un ataque de tipo informático al momento de ser aplicado o ejecutado a una empresa se defina como exitoso, se requiere de 5 fases, pero en la que más se detallará es la fase de reconocimiento porque es aquí donde la ingeniería social se enfatiza.

TABLA 1. FASES ADAPTABLES PARA UN MODELO DE TRASHING – BASADO EN LAS FASES DE EJECUCIÓN ATAQUE INFORMÁTICO

FASES	CARACTERÍSTICAS
Fase 1: *Footprinting* (Reconocimiento)	Nivel básico: poca información, lugar y sitio de los botes de basura.
Fase 2: *Fingerprinting* (Exploración)	Nivel inicial: bolsas de basura y lugar apto para la posible exploración.
Fase 3: *Gaining Access* (Obtener acceso)	Nivel medio: verificación de la información encontrada.
Fase 4: *Maintaining Access* (Mantener el acceso)	Nivel avanzado: pruebas.
Fase 5: *Covering Tracks* (Borrar huellas)	Nivel superior: acceso al sistema por parte del atacante.

Fuente: Referencia [28]

1) Fase 1: Footprinting (Reconocimiento)

Con el reconocimiento de las basuras, se proyecta recolectar todo dato y toda la información posible, que sea representativa de las organizaciones en objeto. Para hacer esto, los ingenieros sociales y atacantes informáticos utilizan varias herramientas:

Lo primero que hacen de todo lo que tienen planteado, es el salto al contenedor (*Dumpster Diving*), con este se procura recoger la mayor información posible (*Trashing*) en el momento de tomar una bolsa o de hurgar en contenedores de basura; si se realiza una previa visita al lugar, se podría saber más específicamente lo que se busca o lo que se puede encontrar; para una mayor certeza en la exploración, se hurga o busca dentro de la basura: información financiera, listas de contraseñas (bancarias, correo electrónico), listas de números de seguridad social, notas y documentos de investigación, redes sociales, claves

de acceso (telefónicos, servidores, computadores) y fotocopias de documentos (números de cédula, de cuentas bancarias), organigramas, unidades de almacenamiento masivo (CD's, USB's, etc.) [29].

También, en la ejecución 'Trashing Digital', se persiste en la exploración de historiales de navegación, papeleras de reciclaje, bloc de notas con nombres poco comunes. En dados casos, se aplican técnicas de peritaje forense, como recuperación de archivos borrados en los discos duros, USB's, disco extraíbles y hasta técnicas forense a equipos de cómputo [30].

3) Fase 2: Fingerprinting (Exploración)

En este espacio se usa toda la información conseguida en la fase 1; la fase 2 se caracteriza por apoderarse de toda la información inicialmente importante: información financiera, listas de contraseñas bancarias, correos electrónicos, listas de números de seguridad social, notas y documentos de investigación de redes sociales, claves de acceso, números telefónicos, nombres de servidores, nombres de computadores y fotocopias de documentos como números de cédula, de cuentas bancarias, organigramas, cartas, direcciones y servicios que prestan; su primordial diferencia con la fase de *Footprinting* (Reconocimiento) está en que hace la búsqueda de información de una manera más directa sobre el objetivo, por lo cual, la fase anterior se concentra solo en la información contenida en lugares de desecho de información digital y en recoger una bolsa de basura o de hurgar en contenedores físicos [28][31].

Fase 3: Gaining Access (Obtener acceso)

En esta instancia, se logra probar muchos de los datos e información, para esto, el atacante comienza a materializar toda la exploración y reconocimiento realizado en las fases 1 y 2 [28].

4) Fase 4: Maintaining Access (Mantener el acceso)

Una vez ha ingresado el atacante al sistema, buscará instalar herramientas que le permitan volver a acceder en un futuro, algunos de los programas que son utilizados, son *Sniffers* [32] que le admitan capturar contraseñas del sistema, sesiones FTP [33] y telnet [34], también recurren a instalar *backdoors*, *rootkits* y *troyanos* [35] que le ayudarán a ingresar posteriormente sin ningún inconveniente.

5) Fase 5: CoveringTracks (Borrar huellas)

En esta fase, el atacante ha logrado obtener y mantener el acceso al sistema; hace todo lo más viable por destruir toda evidencia de lo cometido con el fin de ocultarse, y así poder tener control por más tiempo en el sistema sin ser sorprendido por el encargado de la seguridad de la empresa [28].

Sin embargo, muchos de nosotros creemos que no es necesario tener precaución y cuidado a la hora de desechar las distintas facturaciones que generan el poseer cuentas bancarias, correo físico, líneas móviles, inscripciones a periódicos, entre otros servicios en nuestro lugar de residencia, pero realmente es algo muy serio y grave en su descuido, pensemos ¿Qué tan grave puede ser arrojar a la basura un papelito con un usuario y contraseña de una cuenta? ¿O una simple factura con número de cédula y cuenta bancaria? ¿O peor aún, arrojar a la caneca nuestra *laptop* dañada con un sinfín de información potencialmente sensible?, Entonces, ¿qué podría decir una empresa, que arroja cientos de bolsas con información privada a la basura? ¿Alguien se ha puesto a analizar qué información contiene un extracto bancario? [36]. Si lo han pensado y lo han analizado, podrán observar que es muy posible un robo de identidad debido que los extractos bancarios, recibos de las líneas móviles, contienen datos tan básicos que un delincuente informático logrará estudiar la identidad de cualquier víctima y, posteriormente, procederá a: suplantarlo ya sea por medios telefónicos o suplantarlo personalmente, aunque la segunda sea la más difícil pero quizá es la más eficaz para este tipo de ataques [37].

III. Discusión

1) *Frente la pregunta planteada en un principio*: *¿De qué manera podemos prepararnos para ataques de ingeniería social y específicamente mediante la técnica de "Dumpster Diving o Trashing"?,* podemos evidenciar y relacionar con todo lo anteriormente relatado que, en primera medida,

no estamos preparados y conscientes de este tipo de ingeniería social en nuestro país (Colombia) y mucho menos en nuestra ciudad (Tunja); en segunda medida, las pocas personas que conocen del tema, no demuestran su sentido de convivencia informando a las personas de ello; en igual forma, se presentan muy pocos casos de denuncia, por ende podríamos asegurar que muchas empresas y organizaciones en general están siendo vulneradas mediante diversas técnicas de ingeniería [38] y, por qué no, de *Trashing* sin que ellas se den cuenta, así como personas naturales en dados casos. En las peores circunstancias, este método de robar información ('Trashing') puede generar problemas caóticos, y nos referimos a caóticos por tanto es evidente que controlar este tipo de eventos no solo corresponde al área de informática o sistemas de las organizaciones, sino específicamente a las personas en general [39]; para nosotros, es normal ver a una persona de la calle explorando nuestra basura, pero si un ingeniero social quisiera disfrazarse, bien podría hacerlo sin que nosotros nos inquietáramos en lo absoluto. Hay rumores, y solo rumores, de que muchas organizaciones colombianas pagan por realizar *Trashing* a la competencia, pero es evidente que se realiza por muchas de las cosas que vemos a diario [40].

2) *Cómo prepararnos:* a manera de colofón, podemos prepararnos de muchas maneras y preparar al personal desde el ingreso muchas organizaciones para corresponder a precauciones y medidas de control correctivo y preventivo, pero reiterativamente todo descansa en los hombros del eslabón más débil de la cadena de seguridad, "El recurso Humano" [41].

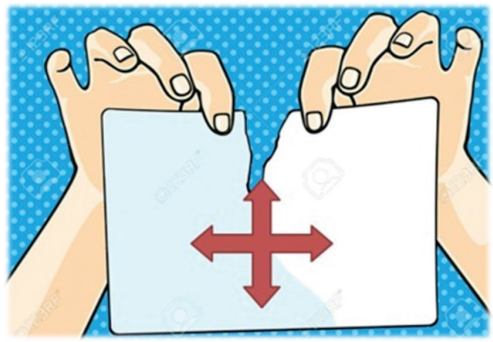
Actividades preventivas y correctivas que se definen así:

a) *Crear protocolos de eliminación de datos y desarrollar políticas de seguridad:* [42] indiscutiblemente, estamos en la era de las actualizaciones, y en el tema de seguridad informática aún más; en cuanto políticas de seguridad, existen muchos modelos, normas [43] también; pero, siempre es aconsejable adaptar más de uno.

b) *Evitar arrojar a nuestra basura documentación relevante:* al deshacerse de cualquier tipo de documento sin previa revisión de su contenido a la basura, abrirá la puerta de entrada más grande para los ciberdelincuentes e ingenieros sociales, ya que tienen datos veraces de las personas, por lo tanto, tener cuidado con lo que depositamos en nuestra basura sería uno de los pasos esenciales en nuestro compromiso de evitar Ingeniería Social [44].

c) *Debido depósito de basura:* algunos documentos después de ser rotos o triturados, pueden permitir una legible lectura de palabras completas y hasta textos enteros, como muestra la Fig. 1. Un poco de tiempo, paciencia y cinta adhesiva bastarán para recomponer aunque sea parcialmente y así revelar información realmente desbastadora, por ello, romper la documentación posiblemente sensible en las dos direcciones, como lo muestra la Fig. 2 sería dificultarles el trabajo y hasta impedírselo a un ingeniero social. [45]

Fuente: http://blogthinkbig.com/crear-contrasenas-seguras/
Fig. 1. Unir los jirones largos permite que se pueda leer algunas palabras



Fuente: http://es.123rf.com/photo_21524508_manos-romper-el-papel.html
Fig. 2. Romper en ambas direcciones toda información que esté en papel.

Una cortadora es una herramienta, como lo muestra la Fig. 3, muchas veces eficiente para deshacerse, de una manera definitiva, de papelería o archivos (documentos en físico) ya impresos, solo si esta máquina tritura en ambas direcciones, ya que al reutilizar o en muchos casos apachurrar y botar a la cesta de la basura documentos rotos en un solo sentido quedarán expuestos a todo aquel delincuente informático para un posible ataque [3], [47].

Fuente: http://es.aliexpress.com/w/wholesale-manual-paper-shredder.html
Fig. 3. Trituradoras mecánicas y digitales [48].

d) *Usar variedad de contraseñas:* lo común es tener al menos una cuenta de correo electrónico, ya que si se utilizan varias cuentas en diferentes correos o redes sociales y para estas mismas se utiliza la misma contraseña, este sería el gran error y problema, ya que al momento en que si un delincuente informático obtiene mediante '*Trashing*' el acceso a una de las cuentas tendrá, por lo tanto, el acceso a todas las demás, las contraseñas se deberán cambiar al menos cada 3 meses, o menos [49].

e) *Uso de contraseñas fuertes y seguras:*

Para crear contraseñas fuertes y muy seguras, hay que hacer lo siguiente: no pensar en nada que tenga que ver en lo personal ni mucho menos familiar, ya que no debe tener nombres propios, nombres de familiares, de las mascotas, ni fechas especiales. Una contraseña segura debe incluir caracteres alfanuméricos, caracteres especiales y más de 10 caracteres, por lo tanto, las empresas deben asignarles una única contraseña a sus empleados y que solo el responsable de la seguridad sea quien la cambie [50].

IV. Recomendaciones y Conclusiones

La seguridad de la información no solo debe verse, entenderse y aplicarse como un conjunto de elementos técnicos y físicos, sino como un proceso cultural de personas y organizaciones, es decir, de aprendizaje en el que todos tenemos parte y contraparte, está en nosotros dejarnos como comúnmente se dice '*hackear*'; es evidente que el usuario es el eslabón más débil y que deben existir controles que ayuden a disminuir el riesgo que este pueda representar. Sin embargo, solo es cuestión de estar alertas, educarnos e informarnos. Lo más importante de todo esto, es que no debemos ser extremistas o sobresalirnos de nuestros cabales a la hora de usar un equipo o sistema informático. Reiterativamente, existen peligros reales, y por eso debemos compartir y denunciar cualquiera de ellos, para que se tomen las medidas necesarias por los entes encargados. Las premisas de seguridad que se aplican en la vida cotidiana, no están de

menos, tener cuidado dónde anoto, guardo y arrojo mi basura, pero, sobre todo, quién la recoge. Kevin Mitnick, el *hacker* más reconocido a nivel mundial y experto en Ingeniería Social, concluye uno de sus libros diciendo: "Puedes gastar una fortuna en tecnología y servicios… y como sea, tu infraestructura de red podría estar vulnerable a la forma más vieja de manipulación" ¿por medio de qué o quién? 'El eslabón más frágil de la cadena'. Ahora que conocemos más sobre la ingeniería social y la seguridad de la información, la próxima vez que pensemos que nuestra información está completamente segura, recordemos que no todas las intrusiones son siempre tan obvias, hay otras menos obvias, como: el *Dumpster Divi*ng o *Trashing* ¿a quién se le podría ocurrir que me estén espiando por medio de lo que arrojo a mi basura? A nadie. ¿Debería preocuparme? Evidentemente.

Referencias

[1] R. Shimonski and J. Zenir, "Chapter 3 – Social Engineering", in Cyber Reconnaissance, Surveillance and Defense Ingeniería social, Vol. 1, USA: Edit. Allison Bishop. pp. 85-112. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128034057000060

[2] L. Romero, "Tema: Nada es lo que parece: en materia de seguridad, la prevención es indispensable", Underc0de, ítem N° 5-9, p. 1, Seguridad Informática y Seguridad de la Información, 2013 [Online], Available: https://underc0de.org/foro/seguridad/nada-es-lo-que-parece-en-materia-de-seguridad-la-prevencion-es-indispensable/ Accessed on: 06, Agosto, 2016.

[3] C. Hadnagy, Ingeniería Social el Arte del Hacking Personal, USA, Multimedia-Anaya Interactiva, 2011, pp. 39-41.

[4] Anonimo. Definición 'Social', in Diccionario Web, USA: Dictionary W, 2014, pp. 3900 [Online], Available: http://webstersdictionary1828.com/Dictionary/social.

[5] Logo BSC Consultores, "La Ingeniería Social: El Arte del Engaño", BSC, Septiembre, 2011. [Online] Available: http://www.bsc-consultores.cl/descargas/B.1%20La%20Ingeniera%20Social.pdf Accessed on: 07, Agosto, 2016.

[6] F. Moutona, L. Leenena and H.S. Venterb, "Social engineering attack examples, templates and scenarios", in Computers & Security, Vol. 59, Pretoria, South Africa, Elseiver: 2016, pp. 186-209. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404816300268.

[7] Mr Ian Man, "Social Engineering", in Hacking the Human, Vol. 1, England: Gower Publishing Limited, 2008. pp. 01-252. [Online]. Available: https://books.google.com.co/books?id=U1IihJpdrGwC&printsec=frontcover&dq=social+engineering&hl=es-419&sa=X&ved=0ahUKEwiu2JrD4cbPAhVKWx4KHRjDAnkQ6AEILjAC#v=onepage&q=social%20engineering&f=false.

[8] E. J. Sandoval Castellanos, "Defensa Digital e Ingeniería Social: Corrompiendo la mente humana", Revista Seguridad, Tomo 1, no. 10, pp. 23-25. May, 2011. [Online]. Available: http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana Accessed on: 08, Agosto, 2016.

[9] Anónimo. "Delito de trashing, búsqueda de información confidencial en la basura", DelitosInformaticos, Abr., 2014. [Online] Available: http://www.delitosinformaticos.com/04/2014/noticias/delito-de-trashing-busqueda-de-informacion-confidencial-en-la-basura Accessed on: 09, Agosto, 2016.

[10] Anónimo, Kaspersky about. Disponible en: http://www.kaspersky.com/about/security_experts Security Experts

[11] Experts Security Kaspersky, "2014 desde la perspectiva viral en cifras en América Lati-

na: predicciones para 2015", GReAT (Global Research and AnalysisTeam) Latinoamérica. Dic., 2014. [Online]. Available: http://www.kaspersky.co.in/about/security_experts Accessed on: Agosto, 02, 2016.

[12] Anónimo. "Penalizan Espionaje Informático", Casa editorial El Tiempo, Jun., 2002. [Online]. Available: http://www.eltiempo.com/archivo/documento/MAM-1355295 Accessed on: Agosto, 16, 2016.

[13] F. Assolini, Robo a bancos y cajeros automáticos al estilo APT: las nuevas amenazas Financieras en AL, presented at Cumbre Latinoamericana de Analistas de Seguridad NOI. [Online]. Available: http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/cumbre-latinoamericana-de-analistas-de-seguridad

[14] É. Medina, "Ingeniería social, la razón del éxito de los ladrones digitales", Redacción Tecnósfera. Jul., 2015. [Online]. Available: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/de-que-se-trata-la-ingenieria-social/16020156 Accessed on: 02, Agosto, 2016.

[15] A. Arbelaez, "Ingeniería Social: El Hackeo Silencioso". Mar., 2013. [Online]. Available: http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/ Accessed on: 01, Agosto, 2016.

[16] M. G. Kelman, Trashing, Critical Legal Studies Symposium. Stanford. USA. Stanford Law Review. 1984. pp. 293-348. Page Count: 56. [Online]. Available: http://www.jstor.org/stable/1228685

[17] Redacción Revista el Pais, "El factor humano es la mayor amenaza para la seguridad informática de los bancos", Elpais.es, no. 12, p. 16, Jun., 2005. [Online]. Available: http://tecnologia.elpais.com/tecnologia/2005/06/23/actualidad/1119515280_850215.html Accessed on: 16, Agosto, 2016.

[18] Sala de Redacción Caracol Radio, "Ingeniería Social: el Hackeo humano". Caracol Radio. Ago., 2011. [Online] Available: http://caracol.com.co/radio/2011/08/26/tecnologia/1314366240_538059.html Accessed on: 06, Agosto, 2016.

[19] G. Watson, "Chapter 11 – The Physical Attack Vector", in Social Engineering Penetration Testing, Utah, USA: RandomStorm Limited, 2014, pp. 255-270. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780124201248000119.

[20] J. Long and S. Pinzon, CISSP, Technical Editor, Jack Wiles, Kevin D. Mitnick, "Chapter 1 – Dumpster Diving", in No Tech Hacking, USA: CISSP, 2008, pp. 1-12. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9781597492157000019.

[21] S. L. Arregoitia López, "Posibles sujetos de los delitos informáticos". Informática Jurídica, no. 12, pp. 01-015, Ene., 2014. [Online]. Available: http://www.informatica-juridica.com/trabajos/posibles-sujetos-de-los-delitos-informaticos/ Accessed on: 02, Agosto, 2016.

[22] H.J. Van Peenen, "Surviving by dumpster Diving", The American Journal of Medicine, Vol. 101, pp. 118-119, Nov., 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0002934397894235.

[23] Congreso de la República de Colombia, Ley de Delitos Informáticos en Colombia. In Ley 1273 del 2009. Bogotá, Colombia: 2009, Artículos 001- 004, Diario Oficial 47.223. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

[24] M. Reguant i Fosas, "Nuevas tecnologías: ética y confidencialidad de datos", in FMC - Formación Médica Continuada en Atención Primaria, Barcelona. España: ElSeiver, 2013, Vol. 20, pp 458–463. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1134207213706297.

[25] D. Littlejohn Shinder, Prevención y Detección De Delitos Informáticos, 1 ed. USA: Anaya Multimedia, 2003, p. 829.

[26] Parlamento Americano. "Legislación Delitos Informáticos", in Código Penal USA. NY, USA, 2012. [Online]. Available: http://catherinpacheco01.blogspot.com.co/2014/11/legislacion-informatica-de-estado-unidos.html.

[27] K. Mitnick and S. Wozniak. The Art of Deception. 1 ed. Ciudad, USA: Editorial John Wiley & Sons, 2003. 368 p.

[28] J. Scott Giboneya, J. Gainer Proudfootb, Sanjay Goela and J. S. Valacichc, "The Security Expertise Assessment Measure (SEAM): Developing a scale for hacker expertise", Computers & Security, Vol. 60, NY 12222, USA: CrossMark, 2016, pp. 37-51. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404816300323.

[29] F. G. Pacheco y H. Jara, "Hackers al descubierto, entienda sus vulnerabilidades evite que lo sorprendan". in Users Manuales, p. 24. [Online] Available: https://books.google.com.co/books?id=q8j4UCoBQlkC&pg=PA24&dq=Fase+1:+Footprinting+(Reconocimiento)&hl=es-419&sa=X&ved=0ahUKEwi7w4mf0LzOAhWEOSYKHchbBOgQ6AEIGjAA#v=onepage&q=Fase%201%3A%20Footprinting%20(Reconocimiento)&f=false

[30] Olmus Redacción, "Buscando en la basura... Trashing", Nas/servicios/net, Vol. 1, Oct., 2015. [Online]. Available: http://www.olmus.es/?p=1585 Accessed on: 16, Agosto, 2016.

[31] V. Thomas, "Chapter 7 – Social Engineering", in Building an Information Security Awareness Program, VA, USA: Securicon, Lorton, 2014, pp 45-63. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780124199675000077.

[32] DragonJAR, L. C, "Conceptos y Definiciones Básicas", DragonJAR Actualidad, Vol. 1, Abr., 2013. [Online]. Available: http://www.dragonjar.org/conceptos-y-definiciones-basicas-relacionadas-con-la-certificacion-ceh-iv.xhtml. Accessed on: 20, Agosto, 2016.

[33] D. Kampitaki, Simulation Study of MANET Routing Protocols Under FTP Traffic. 1 ed. Vol. 17, Macedonia, Greece: Anastasios A. Economides, 2014, Anastasios A. Economides. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2212017314004691

[34] R. Cameron and N. R. Wyler, "Chapter 9 – Web/File/Telnet/SSH", in Juniper® Networks Secure Access SSL VPN Configuration Guide. Salt Lake City, Utah, USA: Juniper, 2007, pp 335-399. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9781597492003000094.

[35] PandaLabs. "Qué es un Troyano", Panda Mediacenter, Dic., 2013. [Online]. Available: http://www.pandasecurity.com/spain/mediacenter/consejos/que-es-un-troyano/ Accessed on: 05, Agosto, 2016.

[36] Naciones Unidas, Embajada Británica Bogotá, Riesgo de Lavado de Activos en Instrumentos Financieros UNODC. Presented at Programa de Asistencia Legal para América Latina y el Caribe LAPLAC. [Online]. Available: https://www.unodc.org/documents/colombia/2013/diciembre/Riesgo_de_Lavado_de_activos_version_I.pdf.

[37] C. Bettischmid, "Cuidado con la suplantación de su identidad en Redes Sociales", Edicion ElColombiano, Jun., 2013. [Online]. Available: http://www.elcolombiano.com/historico/cuidado_con_la_suplantacion_de_su_identidad_en_redes_sociales-GBEC_248493 Accessed on: 05, Agosto, 2016.

[38] Redacción el tiempo, "Espías Rondan las Empresas", El Tiempo, Vol. 2, no. 9, Sep., 2013. [Online]. Available: http://www.eltiempo.com/archivo/documento/MAM-1002471 Accessed on: 09, Agosto, 2016.

[39] L. Vanegas Loor y J. Murillo Rosado, "Auditoria de sistemas de información", in Auditoria de Sistemas: Estandar Cobit 4.1, USA, Dreams Magnet: 2014, pp, 92 [Online]. Available: https://books.google.com.co/books?id=GJZirgEACAAJ&dq=auditoria+de+sistemas+2014&hl=es-419&sa=X-&ved=0ahUKEwiJkbTd1cbPAhUEKx4KHZ-vMA-UQ6AEIIzAA.

[40] Sala de Redacción revista Semana, "Espías S.A." Revista Semana. Oct., 2010. [Online]. Available: http://www.semana.com/economia/articulo/espias-sa/43741-3 Accessed on: 16, Agosto, 2016.

[41] H. Herrera. "El eslabón más débil de la cadena: factor humano", Activos TI. Agos., 2014. [Online]. Available: http://www.activosti.com/el-eslabon-mas-debil-de-la-cadena-factor-humano/ Accessed on: 10, Agosto, 2016.

[42] Anónimo, "¿Qué es el trashing?", Confirma Sistemas (Canal Basics). Abril, 2014. [Online]. Available: http://www.confirmasistemas.es/es/contenidos/canal-basics/que-es-el-trashing Accessed on: 10, Agosto, 2016.

[43] Estándar Internacional ISO. ISO 27000. Barcelona, España: Iso ORG, 2006 Seguridad de la Información. [Online]. Available: http://www.iso27000.es/

[44] K. Krombholz, H. Hobel, M. Huber y E. Weippl, "¿Qué es la ingeniería social? En qué consiste y cómo evitar", Journal of Information Security and Applications, Vol. 22, pp. 113-122, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214212614001343

[45] Redacción Normadat, "Cómo hacer destrucción segura de documentos y cumplir la LOPD". Normadat, Julio, 2015. [Online]. Available: http://www.normadat.es/noticias/3-como-hacer-destruccion-segura-de-documentos-y-cumplir-la-lopd Accessed on: 10, Agosto, 2016.

[46] G. Mckeon, "Identity Theft and Fraud", Ezinearticles, Sept., 2010. [Online]. Available: http://ezinearticles.com/?Identity-Theft-and-Fraud&id=5016429 Robo de Identidad y Accessed on: 10, Agosto, 2016.

[47] K. Mitnick and D. S. William L, Ghost In The Wires: My Adventures as the World's Most Wanted Hacker. USA. Little, Brown, 2014, pp. 301 p. [Online]. Available: https://books.google.com.co/books?op=lookup&id=lVXcoQEACAAJ&continue=https://books.google.com.co/books/about/Ghost_in_the_Wires.html%3Fid%3DlVXcoQEACAAJ%26source%3Dkp_cover%26redir_esc%3Dy%26hl%3Des-419

[48] Trituradoras mecánicas y digitales. Available:http://es.aliexpress.com/w/wholesale-manual-paper-shredder.html

[49] B. Wimmer, Business Espionage, 5 ed. USA: Risk, Threats, and Countermeasures, 2015, pp. 59-73. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B978012420054800005X.

[50] Anonimo. "¿Cómo crear contraseñas seguras?", Eduteca, Vol. 2, pp. 01-10, Jul., 2013. [Online]. Available: http://www.seguridad.unam.mx/usuario casero/eduteca/main.dsc?id=185. Accessed on: 01, Septiembre, 2016.