poliSPAM: Análisis de la eficiencia del spam personalizado utilizando información pública de redes sociales

Enaitz Ezpeleta, Ignacio Arenaza, Roberto Uribeetxeberria y Urko Zurutuza
Depto. de Electrónica e Informática
Mondragon Goi Eskola Politeknikoa S.Coop.
Mondragon Unibertsitatea
Email: {eezpeleta, iarenaza, ru, uzurutuza}@mondragon.edu

***Resumen*—Las campañas de envío de correos electrónicos no deseados siguen siendo una de las mayores amenazas que afectan a millones de usuarios al día. Si bien los filtros anti-spam son capaces de detectar y rechazar un número elevado de mensajes, los investigadores calculan que la tasa de respuesta es de un 0.006 % [8], lo suficiente como para obtener beneficios considerables. Mientras la mayoría de investigaciones se centran en la mejora de los filtros y últimamente en la detección de spam dentro de las redes sociales, en este trabajo se demuestra que se puede llegar a obtener un ratio de click-through del 8.2 % con un modelo de spam personalizado mediante información de redes sociales. Para ello, se recopilan direcciones de correo electrónico de Internet, se completa la información de los usuarios utilizando sus datos públicos del perfil de una conocida red social, y se analizan las respuestas obtenidas en el envío de spam personalizado de acuerdo a su perfil. Finalmente se demuestra la eficiencia de estas plantillas basadas en el perfil para eludir los sistemas anti-spam.**

I. Introducción

El envío masivo de correos electrónicos no solicitados, tanto para la venta de productos en el mercado negro como para el fraude digital es una de las mayores amenazas hoy en día. Se están investigando multitud de métodos para tratar de minimizar este tipo de actividades maliciosas que reportan unos beneficios asombrosos, tratándose de un sector económico en auge conocido como economía sumergida.

Los datos hasta el momento son claros; gracias al envío masivo de mensajes se consigue alcanzar unas cuotas de mercado suficientes como para enriquecer a un sector dedicado a actividades fraudulentas, que si bien antes trabajaban por separado han visto que la unión de actividades multiplica sus beneficios: investigadores expertos en descubrir vulnerabilidades venden su conocimiento, que es procesada por creadores del código que las explota y/o sitios Web maliciosos a sueldo para propagar el malware, que a su vez se integra automáticamente en grandes redes de ordenadores manejados remotamente *botnets* controlados por organizaciones maliciosas, las cuales ofrecen servicios como:

- Pago por envío de spam
- Pago por ataques de Denegación de Servicio Distribuida (DDoS)
- Venta de números de tarjetas de crédito obtenidos mediante phishing o robo en máquinas infectadas
- Servicios de suplantación de identidad
- Venta de productos comprados mediante números de tarjetas de crédito robadas, y
- Un sinfín de actividades fraudulentas que cada vez generan mayores oportunidades de negocio.

Dentro de la problemática del spam, la mayoría de investigaciones y productos se enfocan en detectar y filtrar el correo electrónico no deseado. No en vano, las estadísticas confirman que aproximadamente el 72.9 % del correo que actualmente circula por Internet es Spam [9].

Pero con el auge de las redes sociales, y concretamente con Facebook, que cuenta con más de 800 millones de usuarios activos [4], la posibilidad de obtener información personal que los usuarios dejan a la vista en sus perfiles multiplica la posibilidad del éxito del spam. Facebook brinda una gran oportunidad a atacantes para personalizar los mensajes no deseados, por lo que con un volumen mucho más bajo de mensajes obtendría un retorno de inversión muy grande.

La aportación principal de este trabajo es la demostración experimental que se hace de la eficacia del spam personalizado con información pública de las redes sociales, tanto en el nivel de respuesta obtenida, como por la evasión de los sistemas anti-spam actuales. Primero se recogen direcciones de correo electrónico rastreando Internet. Después se comprueba que estas direcciones tienen relación con un perfil de Facebook. Una vez relacionados un número elevado de usuarios con sus direcciones, se extrae toda la información pública que contengan en el perfil y se almacenan los datos. En el siguiente paso se analiza la información guardada para obtener perfiles de usuarios relacionados con sus principales actividades de Facebook, y así poder crear diferentes plantillas de correo para cada perfil. Finalmente se realizan diferentes experimentos para demostrar la eficacia del spam personalizado.

Este trabajo se ha organizado de la siguiente forma. En la sección 2 se describen los trabajos anteriormente realizados con relación al spam personalizado y al spam en las redes sociales. La sección 3 describe los pasos realizados para la ejecución del estudio, donde se separan las fases de recogida

de información, tratamiento de datos y la personalización del spam. En la sección 4 se muestran los experimentos realizados y sus resultados. En la sección 5 se tratan los aspectos éticos de la investigació. Y por último, se recogen las conclusiones extraídas en la sección 6.

II. Trabajos relacionados

II-A. *Spam personalizado*

Durante los últimos tres años se han realizado diferentes estudios sobre la posibilidad de crear Spam personalizado o recolectar información para una futura utilización, haciendo uso de redes sociales como Facebook o Twitter.

En [3] realizado en el 2009 por investigadores de University of Cambridge y Microsoft, analizan la dificultad de extraer información de los usuarios desde Facebook para crear perfiles. Para ello primero describieron diferentes modos de recoger los datos de los usuarios, para en un segundo paso demostrar la eficiencia de dichos métodos. La conclusión a la que llegaron los investigadores, es que la protección de Facebook frente a crawlers de información es bastante baja. Además, demostraron que se podían recoger grandes volúmenes de datos. Si bien es verdad que Facebook ha mejorado su sistema desde entonces limitando el lenguaje propio para realizar consultas (FQL o Facebook Query Language), esta posibilidad sigue estando vigente.

En [2] se demostró una vulnerabilidad de los servicios de redes sociales que ofrecen a los usuarios la posibilidad de buscar los contactos mediante correo electrónico. Así, partiendo de una lista de correos consiguieron relacionarlos con usuarios de redes sociales, sobre todo Facebook, para después extraer su información. Tener acceso a esa información permitiría a un atacante lanzar ataques sofisticados, específicos, o mejorar la eficiencia de campañas de spam, pero en el trabajo no se demuestra el potencial de crear spam personalizado. Del mismo modo, Polakis recoge en [13] las posibilidades que ofrecen las diferentes redes sociales a la hora de personalizar campañas de spam.

II-B. *Spam en redes sociales*

En los últimos años, las redes sociales se han convertido en una de las principales formas para realizar un seguimiento y comunicarse con la gente. Páginas web como Facebook y Twitter se encuentran entre los 10 sitios web más vistos en Internet [15]. Por otra parte, las estadísticas muestran que de promedio, los usuarios pasan más tiempo en las redes sociales que en cualquier otro sitio [1]. El enorme aumento de la popularidad de las redes sociales [11] les permite recoger una gran cantidad de información personal de los usuarios. Desafortunadamente, esta riqueza de información, así como la facilidad con que se puede llegar a muchos usuarios, también atrae el interés de personas que quieren hacer negocio con ello.

Se han realizado estudios relacionados con el spam y las redes sociales. Por ejemplo, en el [15] del equipo de Stringhini, se demuestra que el spam es ya un problema dentro de las redes sociales. Para ello crearon centenares de perfiles trampa en las tres mayores redes sociales del momento como Facebook, Twitter y MySpace y observaron el tráfico recibido. Después desarrollaron técnicas para identificar robots de envío de spam, así como campañas a gran escala. También mostraron como sus técnicas ayudan a detectar los perfiles spam, incluso no teniendo contacto con los perfiles trampa, demostrando que estas técnicas pueden ayudar a las redes sociales a mejorar su seguridad y detectar usuarios maliciosos. De hecho, desarrollaron una herramienta para detectar spam en Twitter, herramienta que sirvió para cerrar miles de cuentas de spammers.

Otro interesante trabajo es [5]. En el mismo se describen el trabajo realizado en detectar y caracterizar las campañas de spam realizado por medio de mensajes asíncronos en el muro de la red social Facebook. Para ello analizaron más de 187 millones de mensajes de muro, de más de 3.5 millones de usuarios de Facebook. Gracias al estudio de los mensajes mediante diferentes técnicas de análisis de datos, se convierte en el primer estudio en cuantificar el grado de contenido malicioso y cuentas comprometidas en una gran red social online. Si bien no se puede determinar la eficacia de estos posts a la hora de atraer a los usuarios para propagar el malware, los resultados muestran claramente que las redes sociales se utilizan como plataformas de entrega de spam y malware. Además, demuestra que las técnicas automáticas de detección y heurísticas pueden ser utilizados para detectar spam social.

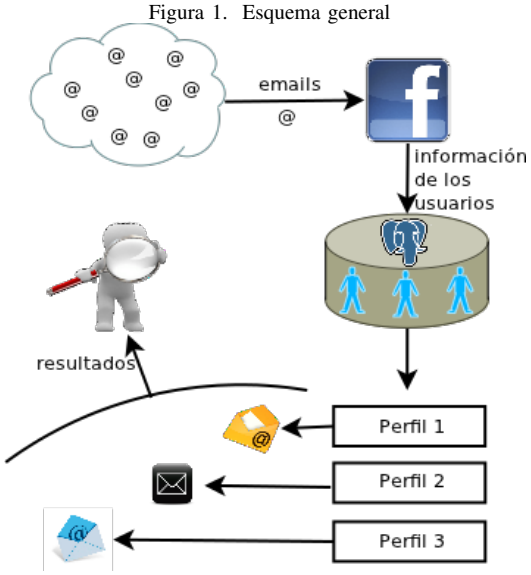
Mientras que la mayoría de los estudios se centran en las campañas de spam que aparecen dentro de las mismas redes sociales, este articulo se centra en la posibilidad de combinar el modelo de spam habitual con las redes sociales, y el riesgo que ello supone para el usuario.

III. Diseño y ejecución del experimento

III-A. *Esquema general*

Tal y como se puede ver en la figura 1, el estudio realizado cuenta con diferentes fases:

Figura 1. Esquema general



En la primera fase se ha recogido la mayor cantidad posible de información desde Facebook. Para ello, primero se recopilan direcciones de correo electrónico rastreando Internet mediante el uso de expresiones regulares, para después relacionar estas direcciones con cuentas válidas de Facebook y así poder extraer y almacenar la información pública de estas cuentas. En la segunda fase se han tratado estos datos para obtener diferentes estadísticos y con ellos crear perfiles de usuarios y plantillas para cada perfil. Una vez creadas las plantillas, en una nueva fase se ha procedido a ejecutar los experimentos, enviando spam personalizado, y finalmente se han analizado los datos obtenidos.

III-B. Recogida de información

El objetivo principal de esta fase ha sido recoger la información necesaria para el estudio y almacenarlo de un modo estructurado. Estos han sido los pasos seguidos:

III-B1. Recogida de direcciones de correo electrónico: Para realizar este trabajo se han barajado dos posibilidades: conseguir las direcciones siguiendo los pasos de [13], donde combinan la información de perfiles de diferentes redes sociales del mismo usuario; o utilizar una aplicación para rastrear Internet en busca de direcciones. Finalmente, se ha optado por la segunda opción, donde se configura una aplicación con expresiones regulares, que rastrea y extrae las direcciones de correo electrónico.

III-B2. Comprobación de las direcciones de correo electrónico: El siguiente paso ha sido el de comprobar cuáles de las direcciones obtenidas estaban relacionadas con cuentas de Facebook. Facebook ofrece la posibilidad de buscar a los usuarios mediante correo electrónico sin necesidad de autentificarse, pero para evitar el uso de robots, después de realizar un número definido de consultas es necesario realizar la autenticación. Es por ello que se ha desarrollado una aplicación capaz de entrar en Facebook y realizar las búsquedas automáticamente, mediante la siguiente URL (donde en lugar de 'EMAIL', se introduce la dirección deseada):

```
http://www.facebook.com/search.php?init=s%3A
        email&q=EMAIL&type=users
```

III-B3. Recogida de información: Facebook como otras muchas páginas web, tiene una estructura HTML, lo cual permite extraer información sobre los usuarios analizando el código fuente. Para ello, se accede directamente a la página de información de cada usuario del modo en el que se muestra a continuación y se extrae una por una la información de cada usuario (donde aparece 'USERUID', se debe introducir la ID de usuario de Facebook, que se ha extraído y almacenado en el paso anterior).

```
http://www.facebook.com/profile.php?
        id=USERUID&v=info
```

III-B4. Resultados: A continuación se muestran los datos obtenidos en esta fase. Se puede observar que el 19 % de las direcciones de correo extraídas de Internet tienen una cuenta de Facebook relacionada.

Cuadro I
PORCENTAJE DE CUENTAS

Nº de direcciones de correo	Nº de cuentas de Facebook	Porcentaje
119.012	22.654	%19

III-C. Tratamiento de datos

El objetivo de esta fase ha sido tratar los datos para conseguir sacar el máximo provecho de la información que se ha conseguido en la fase anterior. Para ello se han realizado dos tareas principales. Primero, se ha creado una nueva tabla en la base de datos, donde se realiza un resumen de la información obtenida, para facilitar el análisis de los datos. Y segundo, se han creado diversas estadísticas utilizando las tablas de la base de datos para extraer el mayor conocimiento posible sobre los usuarios.

III-C1. Resultados: En esta fase, con las estadísticas obtenidas, se han extraído las siguientes conclusiones:

- La mayoría de los usuarios de Facebook eligen su grupo musical favorito y lo dejan público.
- El 30 % de los usuarios que tienen introducido algún dato en Facebook y lo dejan público, tienen relación al menos con una empresa.
- El número de hombres es 12 puntos porcentuales mayor que el número de mujeres en este estudio.

III-D. Spam personalizado

El objetivo de esta fase ha sido utilizar todo el conocimiento previo obtenido en el estudio, para conseguir crear spam personalizado y eficiente. Para ello, primero se han creado plantillas para los correos electrónicos con las cuales se mandan los correos a los usuarios, y después se ha creado un sistema de monitorización de las respuestas mediante una página web. Los usuarios acceden a dicha página desde una URL incluida en los mensajes, que lleva un *token* que identifica al usuario y tipo de mensaje al que responde.

III-D1. Plantillas de correo: El primer paso de esta fase ha sido analizar los datos extraídos en la fase anterior para así poder definir los perfiles de los usuarios y las plantillas relacionadas con cada perfil. Haciendo uso de las estadísticas obtenidas en los pasos anteriores se analiza la cantidad de personas que tienen introducido cada una de las variables de Facebook. En la siguiente tabla II se muestran las cinco variables más destacadas.

Cuadro II
Nº DE USUARIOS QUE TIENEN CADA UNA DE LAS VARIABLES

Variable	Cantidad	Porcentaje
hombre	8.786	39 %
mujer	6.189	27 %
música	5.788	26 %
títulos	5.612	25 %
empresa	5.149	23 %

Como se puede observar las variables más destacadas son las que representan el género de los usuarios, dato que no es suficiente para crear plantillas personalizadas, aunque sí para

realizar un saludo educado al principio del mensaje. Por el contrario las siguientes tres variables han sido las utilizadas para crear las plantillas. Así, si el usuario tiene un grupo musical introducido, se les ha enviado la **plantilla de música**. Sin embargo, si no tiene grupo musical pero sí los estudios que ha cursado, se les ha enviado la **plantilla académica**. Y por último, a aquellos usuarios sin ninguna de las variables anteriores especificadas, pero que hayan introducido su compañía o empresa en la que trabajan, se les ha enviado la **plantilla de empresa**.

Para una mejor personalización de las plantillas, también se han utilizado otras variables que se han considerado interesantes, como por ejemplo los idiomas. Así, se han utilizado tres idiomas en las plantillas: Euskara, Castellano e Inglés. Además del idioma, también se le ha añadido el nombre de cada usuario en todos los correos, y el genero de cada uno en alguna plantilla. Por último, en la plantilla de música también se ha introducido la ciudad de los usuarios que lo tienen establecido, para atraer aún más su atención. Cabe mencionar también que todas las plantillas llevan una URL que da acceso a la página web del experimento.

III-D2. Página web: Para realizar la monitorización del experimento se ha desarrollado una página web en PHP. En la misma ofrecemos nuestras disculpas a la vez que explicamos la investigación con sus fines científicos, ofreciendo a su vez al usuario la posibilidad de darse de baja del estudio, así como de dejar un comentario libre. La web debe ofrecer la total seguridad de que solamente se pueda acceder desde los correos electrónicos enviados en el proyecto, para poder asegurar unos resultados reales. Además, analiza la URL con la que se accede con el fin de procesar la información de qué usuario y mediante qué plantilla ha accedido a la página. Tomando en cuenta estas características, se ha decidido insertar todos los parámetros necesarios, tanto de seguridad, como de personalización en la URL que llevan los correos personalizados. De este modo, cuando un usuario accede al enlace, y su petición llega a la web, todos los parámetros quedarán almacenados en la base de datos.

IV. Resultados obtenidos

En esta sección se muestran los resultados obtenidos durante la investigación. En ella se han realizado dos experimentos bien diferenciados. En el primero de los experimentos, se ha enviado spam típico a algunos de los usuarios almacenados previamente, y se ha podido comprobar que apenas se han obtenido respuestas. La causa de este resultado podría ser: que los correos han sido detectados y filtrados por los servidores de correo electrónico, por sistemas del propio proveedor de servicios de Internet, por software instalado en clientes de correo, o finalmente que han sido ignorados o borrados por el propio usuario. Tras el envío del spam típico, se ha mandado spam personalizado a esas mismas personas. Finalmente, el segundo experimento se ha centrado en el envío masivo de correos electrónicos personalizados.

IV-A. Primer experimento

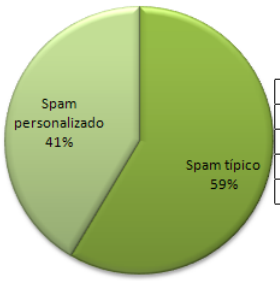
Usando diferentes direcciones de correo electrónico, se han enviado correos electrónicos no deseados a una parte de los usuarios almacenados en la base de datos. Primero, se ha enviado el contenido de un spam típico que usan los atacantes para atraer la atención de usuarios y dirigirlos hasta una página web concreta. Después, se ha enviado spam personalizado a las mismas personas desde otra dirección de correo electrónico. No ha sido posible personalizar los correos de todos los usuarios que habían recibido el spam típico debido a la insuficiente información pública de algunas de estas personas. La siguiente tabla muestra el número de correos electrónicos enviados.

Cuadro III
Número de emails enviados

	Cantidad
Spam típico enviado:	972
Imposible personalizar:	283
Spam personalizado:	689
Spam total enviado:	1.661

Los correos enviados se pueden clasificar en las siguientes plantillas, conteniendo cada una de ellas una URL personalizada para realizar el seguimiento de cada uno de los emails enviados.

Figura 2. Tipos de correos enviados



Tipo	Cantidad	Porcentaje
Típico	972	59 %
Música	462	28 %
Académico	182	11 %
Laboral	45	2 %

Finalmente, se analizarán las respuestas obtenidas. Hay que mencionar que en la página web a la que llegan los usuarios, se piden disculpas de las posibles molestias causadas por el experimento, y se da la opción de darse de baja del mismo o dejar un comentario. Relacionado con esto último, hay que destacar que los aspectos éticos del proyecto se tratan en la sección 5. Cabe destacar también que tanto los comentarios de este experimento, como del segundo no aportan ninguna información u opinión relevante para el proyecto.

Cuadro IV
Datos de la página web

	Cantidad	% del total de envíos
Usuarios que han accedido a la web	43	2,59 %
Usuarios que se han dado de baja	17	2,1 %
Usuarios que han comentado	2	0,12 %

La tabla V recoge el ratio de respuesta obtenido por cada tipo de spam en el experimento. Si se analizan los datos

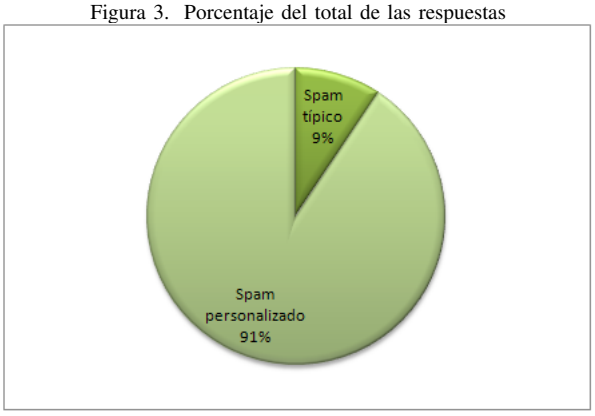
obtenidos en profundidad, se puede observar que solamente 4 personas han accedido a la web desde spam típicos, frente a las 39 personas que lo han hecho desde sus correos personalizados. Es decir un 0,41 % del spam típico frente al 5,66 % del spam personalizado.

Cuadro V
RESULTADOS

	Enviados	Respuestas	Porcentaje	% del total de envíos
Spam típico	972	4	0,41	0,24 %
Spam personalizado	689	39	5,66	2,35 %
Total	1.661	43	2,59	2,59 %

Si se observa el número total de respuestas recibidas, se puede ver que solamente el 9 % de las respuestas provienen de un spam típico, un porcentaje muy inferior al total de spam típico enviado que se sitúa en el 59 % del total de correos enviados.

Figura 3. Porcentaje del total de las respuestas



También se puede analizar el spam personalizado, dividiéndolo en las diferentes plantillas utilizadas durante el envío, tal y como se puede observar en la tabla VI.

Cuadro VI
ACCESO A LA WEB SEGÚN LA PLANTILLA

Tipo	Cantidad	% del total de las respuestas
Música	18	42 %
Académico	16	37 %
Laboral	5	12 %

IV-B. Segundo experimento

Una vez extraídos los datos que aparecen en el experimento anterior, de los que se muestran las conclusiones en el apartado correspondiente, se ha llevado a cabo un segundo experimento que se detalla a continuación.

En este caso, en lugar de enviar un spam típico al inicio, se envían directamente correos electrónicos personalizados a 2.200 usuarios de Facebook a través de las plantillas de perfil de usuario.

Cuadro VII
NÚMERO DE CORREOS ENVIADOS

Tipo	Cantidad	Porcentaje
Música	1.325	60,23 %
Académico	661	30,05 %
Laboral	214	9,73 %

Los resultados de estos nuevos envíos se muestran a continuación siguiendo el mismo formato que en el primer experimento.

Cuadro VIII
DATOS DE LA PÁGINA WEB

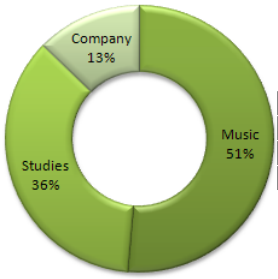
	Cantidad	% del total de envíos
Usuarios que han accedido a la web	181	8,23 %
Usuarios que se han dado de baja	23	1,05 %
Usuarios que han comentado	9	0,41 %

Cuadro IX
RESULTADOS

	Enviados	Respuestas	Porcentaje
Spam personalizado	2.200	181	8,23 %

Los usuarios acceden a la página web desde distintas plantillas tal y como se muestra en la tabla 4. En la misma se puede observar que tal y como sucedía en el primer experimento, la plantilla por la que más usuarios acceden, es la de música.

Figura 4. Acceso a la página web según la plantilla



Tipo	Cantidad	Porcentaje
Música	93	51,38 %
Académico	65	35,91 %
Laboral	23	12,71 %

V. CONSIDERACIONES ÉTICAS

Algunas medidas adoptadas en este trabajo se podrían considerar sensibles desde el punto de vista ético, e inaceptables desde el punto de vista legal. La recopilación de información a partir de redes sociales está mal considerada aun tratándose de información pública, y el envío de spam incumple multitud de términos legales. Pero tal y como se justifica en [6], [7] y más recientemente en [2], la mejor forma de realizar una investigación es que esta sea lo más real posible. El único modo de demostrar que el spam personalizado es efectivo y entraña un riesgo para el usuario final, es realizando un envío real y analizando los resultados obtenidos, por eso se ha escogido esta vía. Este trabajo se apoya en algunas de las consideraciones realizadas en los trabajos anteriores:

Primero, hay que tener claro que en este estudio se trabaja con el fin de mejorar la seguridad del usuario final, demostrando los riesgos que tiene dejar información personal en Internet accesible. Segundo, únicamente se usa información pública de usuarios de las redes sociales. No se ha realizado ningún ataque a ninguna cuenta, contraseña, ni área privada del usuario. Tercero, los atacantes podrían usar esta misma información para realizar ataques. Si se actúa como ellos, más facil será entender y proponer métodos para la protección de los usuarios. Finalmente, se ha recibido el visto bueno del consejo de dirección de Mondragon Unibertsitatea para realizar los experimentos.

VI. Conclusiones

Este trabajo muestra el problema que podría existir si los creadores de las campañas de spam introdujeran textos personalizados basados en información públicamente accesible de redes sociales, sobre los millones de direcciones que poseen.

Por un lado, se ha demostrado que el 19 % de las direcciones de correo de Internet tienen asociada su correspondiente cuenta de Facebook. Por otra parte, es posible extraer la información básica pública de los usuarios, para poder personalizar tanto el asunto como el contenido del correo electrónico. Estos emails pueden tener un ratio de respuesta mayor que el 8,2 % lo cual es 1.000 veces superior al ratio de una campaña de spam típica. Es por ello que junto a la investigación de nuevas técnicas para la detección del spam dentro de las redes sociales, es necesario la investigación más allá del clásico filtrado de spam, teniendo en cuenta el éxito de las campañas de spam personalizado.

En cuanto al comportamiento de los usuarios de la red social analizada, se ha podido observar que la mayoría de los usuarios de Facebook eligen su grupo de música favorito y dejan dicha información pública. También se ha podido ver que el 30 % de los usuarios que tienen algún dato de forma pública, tienen relación con al menos una empresa.

Otro dato interesante que se ha extraído ha sido la diferencia del género de los usuarios, donde el número de hombres es 12 puntos mayor que el de mujeres. Esto puede deberse a que tradicionalmente los hombres están más relacionados con las TICs (dejando su dirección de correo en Internet), o también a que éstos tienen una mayor confianza en la Red.

La conclusión principal que se puede extraer de este trabajo es que se ha logrado el objetivo principal del proyecto, demostrando que es posible desarrollar técnicas avanzadas de generación de correo electrónico personalizado que eluden los sistemas de detección de spam. Clara muestra de ello son los datos que se analizan en la sección 4, donde se puede observar como en el primer experimento el porcentaje de personas que 'muerden el anzuelo' con el spam personalizado es del 5,66 %. Frente al 0,41 % que lo hacen con el spam típico. Además, en el segundo experimento, en el que solo se envían correos personalizados, la tasa de respuesta llega hasta el 8,2 %.

Por último, se proponen tres modos para evitar el spam personalizado:

- *Limitando la información pública de los usuarios:* Las redes sociales pueden limitar la cantidad de información que cada usuario deja público, esto dificultaría extraer dicha información. Esta es una medida muy controvertida, porque la visibilidad es uno de los aspectos fundamentales de las redes sociales.
- *Cambiando el código de las páginas:* A día de hoy es posible recoger la información desde el código fuente de las páginas de Facebook. Si cambian el modo de desarrollo de las páginas impidiendo la posibilidad de extraer la información de una forma legible, dificultarían la extracción a los atacantes.
- *Concienciación:* Sin lugar a dudas el método más efectivo de hacer frente a los ataques personalizados, es mediante la concienciación de los usuarios de las redes del peligro que supone mostrar información personal de forma pública en las diferentes redes sociales. Si los usuarios disminuyen la cantidad de información que tienen de forma pública en sus perfiles, será más difícil conseguir una buena personalización.

Referencias

[1] I. Alexa Internet. Alexa top 500 global sites. http://www.alexa.com/topsites, 2012.

[2] M. Balduzzi, C. Platzer, T. Holz, E. Kirda, D. Balzarotti, y C. Kruegel. Abusing social networks for automated user profiling. En actas de *13th international conference on Recent advances in intrusion detection*, RAID'10, páginas 422–441, Berlin, Heidelberg, 2010. Springer-Verlag.

[3] J. Bonneau, J. Anderson, y G. Danezis. Prying data out of a social network. *Social Network Analysis and Mining, International Conference on Advances in*, 0:249–254, 2009.

[4] Facebook. Facebook: Timeline. http://www.facebook.com/press/info.php?timeline, 2012.

[5] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, y B. Y. Zhao. Detecting and characterizing social spam campaigns. En actas de *17th ACM conference on Computer and communications security*, CCS '10, páginas 681–683, New York, NY, USA, 2010. ACM.

[6] M. Jakobsson, N. Johnson, y P. Finn. Why and how to perform fraud experiments. *IEEE Security and Privacy*, 6(2):66–68, 2008.

[7] M. Jakobsson y J. Ratkiewicz. Designing ethical phishing experiments: a study of (ROT13) rOnl query features. En *WWW '06: Actas de 15th international conference on World Wide Web*, páginas 513–522, New York, NY, USA, 2006. ACM.

[8] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, y S. Savage. Spamalytics: an empirical analysis of spam marketing conversion. En actas de *15th ACM conference on Computer and communications security*, CCS '08, páginas 3–14, New York, NY, USA, 2008. ACM.

[9] M. Ltd. Symantec cloud messagelabs. http://www.symanteccloud.com/es/es/globalthreats/overview/r_mli_reports, 2011.

[10] J. Méndez, F. Fdez-Riverola, F. Díaz, y J. Corchado. Sistemas inteligentes para la detección y filtrado de correo spam: una revisión. *Inteligencia Artificial, Revista Iberoamericana de Inteligencia Artificial*, 34:63–81, 2007.

[11] D. Novillo Ortiz. davidnovillo.es(o no es): Redes sociales en españa 2011, algunos datos... http://www.davidnovillo.es/2011/01/02/tecnologia/redes-sociales-en-espana-2011-algunos-datos/, enero 2011.

[12] F. Ortega, J. Troyano, F. Cruz, y F. Enrıquez. Detección de spam en la web mediante el análisis de texto y de grafos. *IV Jornadas TIMM Tratamiento de la Información Multilingüe y Multimodal 7 y 8 de abril de 2011*, página 13.

[13] I. Polakis, G. Kontaxis, S. Antonatos, E. Gessiou, T. Petsas, y E. P. Markatos. Using social networks to harvest email addresses. En actas de *9th annual ACM workshop on Privacy in the electronic society*, WPES '10, páginas 11–20, New York, NY, USA, 2010. ACM.

[14] E. P. Sanz, J. M. G. Hidalgo, y J. C. Cortizo. Email spam filtering. *Advances in Computers*, páginas 45–114, 2008.

[15] G. Stringhini, C. Kruegel, y G. Vigna. Detecting spammers on social networks. En actas de *26th Annual Computer Security Applications Conference*, ACSAC '10, páginas 1–9, New York, NY, USA, 2010. ACM.