



# G Data Informe 1/2011

## Spam: el negocio y sus trucos

Sabrina Berkenkopf y Ralf Benzmüller  
G Data SecurityLabs



# Contenidos

<b>1</b>	<b>Introducción</b>	<b>5</b>
1.1	Correo electrónico – información general	5
1.2	¿Quién se encuentra detrás del spam?	6
1.3	Fundamento psicológico del spam	7
<b>2</b>	<b>Diferentes tipos de estafas</b>	<b>9</b>
2.1	Estafa para volver a registrarse (robo de datos, malware)	9
2.2	La estafa de prácticas irregulares (phishing)	11
2.3	Las estafas con tarjetas de felicitación (malware)	13
2.4	La estafa del envío de un paquete (malware y phishing)	15
2.5	La estafa del tipo "¡Mira esto!" (malware y publicidad)	17
2.6	La estafa de los descuentos (malware)	18
2.7	Estafas mediante títulos académicos o universitarios (phishing y timos)	19
2.8	Estafas con casinos online (phishing y timos)	20
2.9	Estafa 419 / spam nigeriano (timo)	21
2.10	Estafas de ofertas de trabajo (malware y timos)	23
2.11	Estafa de la novia rusa (timo)	25
2.12	Estafa de la lotería (timo)	26
<b>3</b>	<b>Consejos y trucos</b>	<b>27</b>
3.1	Reglas de conducta útiles	27



3.2	Medidas técnicas .....	<b>27</b>
<b>4</b>	<b>Glosario.....</b>	<b>28</b>



# 1 Introducción

## 1.1 Correo electrónico – Información general

Actualmente, el correo electrónico es un medio de comunicación de uso habitual tanto en el trabajo como en el hogar y se utiliza de una forma tan generalizada que, prácticamente, no podemos vivir sin él. El envío de correos electrónicos es extremadamente barato, rápido y de alcance mundial.


Para trabajar con el correo electrónico, los usuarios utilizan programas instalados en sus ordenadores (clientes de correo electrónico) o acceden a él a través de un navegador. Por supuesto, estas herramientas populares atraen a los estafadores, quienes se muestran siempre dispuestos a explotar las vulnerabilidades técnicas de esta herramienta de comunicación.

Los procesos para enviar y recibir correos electrónicos se realizan en un segundo plano y, lo que es mejor, el usuario no participa en ellos. El protocolo para el envío de correos electrónicos se llama Protocolo Sencillo de Transferencia de Correo (Simple Mail Transfer Protocol, SMTP). Los correos electrónicos se reciben mediante la versión 3 del protocolo de oficina de correo (Post Office Protocol version 3, POP3) o mediante el protocolo de acceso a mensajes de Internet (Internet Message Access Protocol, IMAP).

La composición del correo electrónico se parece al formato de las tarjetas postales tradicionales. Por una parte tenemos la sección de la información (cabecera), que muestra los datos del remitente y del receptor, la fecha, el asunto, etc. El segundo componente es el texto que se incluye en el mensaje.

Como no hay autenticación del texto simple cuando se envía un correo electrónico a través de SMTP, los fraudes se realizan justamente en esta etapa. De esta forma, es posible cambiar la dirección del remitente en la cabecera y, por lo tanto, engañar al receptor utilizando una falsa identidad. Asimismo, el contenido puede también manipularse con facilidad.



Sin embargo, todos los aspectos positivos del correo electrónico que ya han sido mencionados pueden tener otra perspectiva. Los buzones de entrada de correo electrónico se encuentran a rebosar, y la mayoría de mensajes recibidos son correos no solicitados que contienen ofertas publicitarias sospechosas, ofertas de trabajos de ensueño, invitaciones para establecer contactos con personas de dudosa reputación, etc. Lo que más molesta a los usuarios de ordenadores de todo el mundo a diario es el  spam<sup>1</sup>. Estos mensajes no solicitados enviados en grandes cantidades no sólo son irritantes debido al gran número de ellos que se reciben, sino que también a su capacidad para incluir ciertos peligros.

El correo electrónico fraudulento y peligroso puede ofrecerse de diferente forma- publicidad no deseada, phishing, malware en documentos adjuntos o enlaces a sitios web puestos en peligro. Antes de describir con todo detalle en la siguiente sección los procesos y las estafas específicos que utilizan los estafadores, nos gustaría aportar un poco de información sobre estas acciones.

<sup>1</sup> El glosario contiene explicaciones sobre los términos especializados marcados con el signo 

## 1.2 ¿Quién se encuentra detrás del spam?

Los ciberdelincuentes continúan utilizando en gran medida el envío de enormes cantidades de correos electrónicos para llevar a cabo sus actividades fraudulentas. La distribución de correos electrónicos no solicitados en grandes cantidades – o “spam”, que es el nombre con el que se conoce a esta actividad – es uno de los campos más habituales en la economía sumergida utilizada por los ciberdelincuentes. En el cuarto trimestre de 2010, una media del 83% de todo el tráfico del correo electrónico en el mundo era spam, lo que equivale a una media de 142.000 millones de correos electrónicos spam al día.<sup>2</sup>

Una gran parte de su popularidad puede explicarse por la atractiva proporción entre costes y beneficios. En estos momentos, los costes de envío de 1.000.000 mensajes spam se encuentran entre US\$399 y US\$800, según el proveedor de servicio que se elija, aunque también hay ofertas para enviar 2.000.000 correos electrónicos por el precio de 1.000.000 de mensajes.

General Email Marketing Campaign Prices			
# of Emails Delivered	Price	Cost p/ Thousand	
100,000	\$99	\$1.00	<a href="#">Order Now!</a>
250,000	\$199	\$.80	<a href="#">Order Now!</a>
400,000	\$249	\$.62	<a href="#">Order Now!</a>
1,000,000 <small>(Get a 2 million campaign for the price of 1 million)</small>	\$399*	\$.19	<a href="#">Order Now!</a>
3,000,000	\$549	\$.18	<a href="#">Order Now!</a>
10,000,000	\$1499	\$.15	<a href="#">Order Now!</a>
25,000,000	\$1999	\$.08	<a href="#">Order Now!</a>
50,000,000	\$2499	\$.05	<a href="#">Order Now!</a>

**Captura de pantalla 1:** lista de precios para la distribución de correos electrónicos en grandes cantidades a través de Internet. Estos son los precios para enviar correos electrónicos de manera general, sin especificar los grupos específicos a los que van dirigidos.

Asimismo, se encuentran disponibles en Internet listas de direcciones de grupos objetivo específicos, aunque también pueden adquirirse directamente a través de servicios de distribución de correos electrónicos en grandes cantidades. Además de esto, estas listas pueden incluso personalizarse si así fuera necesario. Por lo tanto, es posible adquirir direcciones clasificadas por grupos determinados – por ejemplo, listas específicas de personas que participan en juegos online, de individuos de una región en particular o muchas otras categorías.

Geographic Email List Options	Price	
1 Country or 1 State or 1 City or 1 US Zip Code	\$298	<a href="#">Order Now!</a>
2 Countries or 2 States or 2 Cities or 3 US Zip Codes	\$398	<a href="#">Order Now!</a>
3 Countries or 4 States or 4 Cities or 6 US Zip Codes	\$498	<a href="#">Order Now!</a>
6 Countries or 8 States or 8 Cities or 15 US Zip Codes	\$798	<a href="#">Order Now!</a>
12 Countries or 14 States or 14 Cities or 25 US Zip Codes	\$1198	<a href="#">Order Now!</a>
Larger List Packages	Inquire	<a href="#">Order Now!</a>

**Captura de pantalla 2:** Recargo adicional por distribución de correo electrónico a grupos específicos –en este

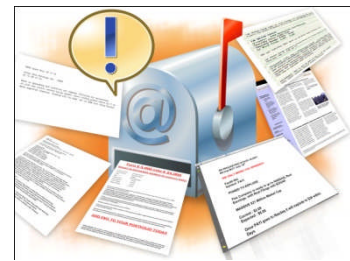
<sup>2</sup> Commtouch, Informe del cuarto trimestre de 2010 sobre Tendencias de las Amenazas en Internet, basado en flujo de datos sin filtrar, excluyendo el tráfico interno corporativo

*caso, a grupos objetivo localizados*

El correo electrónico spam se envía principalmente a través de botnets. Por ejemplo, un operador de botnet con una pequeña red de unos 20.000 ordenadores zombis y una tasa de 2 correos electrónicos al segundo por cada bot activo, puede precisar tan sólo 25 segundos para enviar 1.000.000 de correos electrónicos. Por lo tanto, basándonos únicamente en estas cifras, el operador de un botnet relativamente pequeño puede ganar hasta US\$ 115.200 cada hora.

### 1.3 Fundamento psicológico del spam

Independientemente de la vía que utilice el correo electrónico para llegar a su buzón de entrada, la mayoría de los trucos que usan los estafadores mediante el envío de correos electrónicos se basan en mecanismos de ingeniería social. Estos métodos incluyen la explotación de sentimientos, opiniones, actitudes y patrones de conducta para, de esta manera, tratar de engañar a los receptores de los mensajes. Dichos intentos usan técnicas de manipulación social para acceder a datos confidenciales y explotan un tipo de "agujero en la seguridad del ser humano".



Para aprovechar al máximo las técnicas de ingeniería social, los estafadores utilizan nombres de remitentes, asuntos o contenidos de mensajes falsos. Sin embargo, también se utilizan para encubrir un intento de fraude nombres de archivos adjuntos, extensiones de archivos duplicadas e iconos populares o nombres de dominio con enlaces. En un informe de 2005, Jordan y Goudey<sup>3</sup> indicaron los siguientes 12 factores psicológicos como los más utilizados para favorecer la distribución de gusanos entre 2001 y 2004:

- Inexperiencia
- Curiosidad
- Avaricia
- Inseguridad
- Cortesía
- Vanidad
- Credulidad
- Deseo
- Lujuria
- Temor
- Reciprocidad
- Amabilidad

Un año después, M. Braverman<sup>4</sup> amplió este listado para incluir:

- Conversación genérica: afirmaciones breves (como "cool", etc.)
- Advertencias sobre virus y parches de software
- Malware descubierto en el PC
- Informes de detección de virus al final de un correo electrónico
- Información o mensajes sobre cuentas (por ejemplo, el troyano de telecomunicaciones que se identifica como una factura de teléfono desproporcionada)
- Mensajes de error en la entrega de un correo electrónico

<sup>3</sup> Ver Jordan, M., Goudey, H. (2005) "The Signs, Signifiers and Semiotics of the Successful Semantic Attack". En: Proceedings of the EICAR 2005 Conference, pp.344 - 364.

<sup>4</sup> Ver Braverman (2006) "Behavioural Modelling of Social Engineering-based Malicious Software". En: Proceedings of Virus Bulletin Conference 2006, pp.15-22.



- Atracción física
- Acusaciones (por ejemplo, el troyano BKA que afirma haber encontrado archivos ilegales)
- Noticias de actualidad
- Artículos gratuitos: algunas personas pierden el control cuando se menciona algo gratuito

## 2 Diferentes tipos de estafas

### 2.1 Estafa para volver a registrarse (robo de datos, malware)

Este tipo de correo electrónico sugiere que un sistema o programa online ha sido actualizado y que los datos del cliente deben de ser actualizados inmediatamente para poder seguir utilizando sin problema las prestaciones del servicio. El enlace al supuesto sitio web para la actualización se ofrece directamente en el correo electrónico. A veces sólo es necesaria una rápida comprobación a la dirección que se incluye en el enlace para ver que no se trata de la dirección correcta. De hecho, el sitio web al que se conecta el enlace es, a menudo, una réplica del original y – según el cuidado con el haya sido diseñado – puede resultar difícil de identificar como un sitio falso.

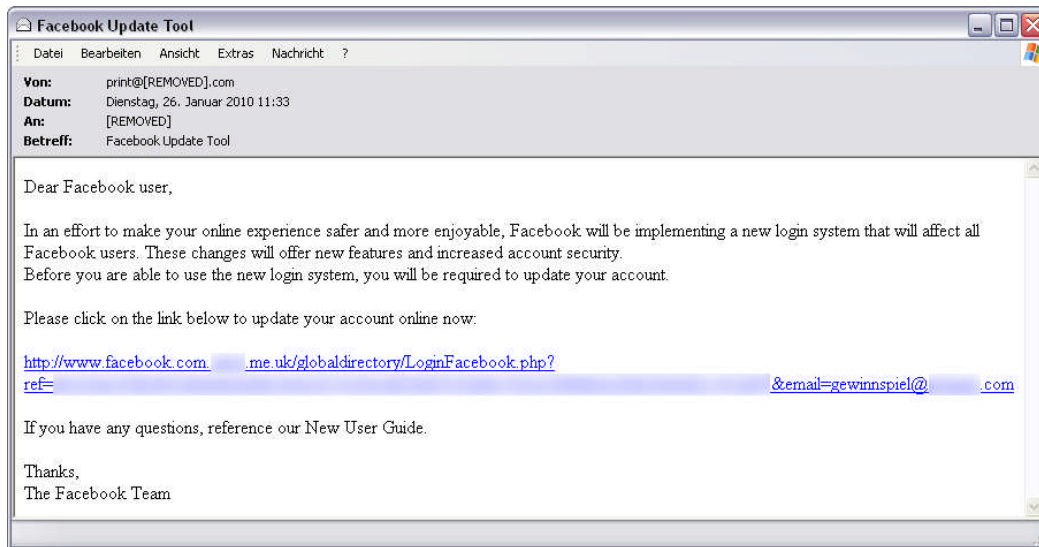
**Grupo objetivo:** cualquier usuario de Internet – pero, especialmente, los clientes de una amplia serie de bancos y de servicios de pago, además de los usuarios de los programas de software más populares, redes sociales, juegos online, servicios de correo electrónico gratuitos y aplicaciones web.

**Punto de partida psicológico:** inexperiencia, credulidad, conocimiento de la seguridad

**Riesgos:** los estafadores adquieren una información valiosa sobre los individuos cuando las personas confiadas visitan el sitio web falso facilitado a través del enlace y, posteriormente, proporcionan los datos solicitados. Dependiendo del tipo y la presentación del sitio web, esta información puede abarcar desde su nombre y dirección al número de su tarjeta de crédito y el número PIN. A partir de ahí, estos datos pueden utilizarse para realizar actividades ilegales.

La autoridad tiene un papel de gran importancia en este tipo de estafas, ya que los usuarios menos experimentados pueden ser engañados con facilidad para hacer clic en los enlaces y seguir las instrucciones de los remitentes falsos y de supuestas agencias conocidas.

**Ejemplos de líneas de asuntos:** Confirmación de restablecimiento de contraseña de Facebook (Facebook Password Reset Confirmation). Mensaje al cliente (Customer Message). Advertencia de Yahoo (Verifique su cuenta ahora para evitar la cancelación del servicio - (Yahoo Warning!!! (Verify Your Account Now To Avoid Service Suspension)  
Aviso Urgente: Paypal Limited – (Urgent Notice: Paypal Limited)  
Su cuenta tiene problemas -(Your account has open issues !!!)  
Herramienta para actualizar Facebook – (Facebook Update Tool)  
Cuenta de World of Warcraft - Aviso de cambio de subscription – (World of Warcraft Account - Subscription Change Notice)



**Captura de pantalla 3:** correo electrónico con solicitud para acceder a una actualización mediante un enlace. Este enlace no lleva a Facebook, sino a un sitio con el dominio de segundo nivel .me.uk

## 2.2 La estafa de prácticas irregulares (phishing)

Esta estafa lleva a las víctimas potenciales a creer que ha habido un problema con sus cuentas y que, por lo tanto, se bloquearán instantáneamente. Para evitar este bloqueo, el usuario debe registrar inmediatamente (!) los datos de su cuenta en un sitio web del que se ofrece un enlace.

**Grupo objetivo:** cualquier usuario de Internet, especialmente los usuarios de una amplia serie de bancos y de servicios de pago, servicios de correo electrónico, etc.

Los usuarios de los servicios cuyo control de acceso consiste en un nombre de autenticación y una contraseña, son unos objetivos especialmente lucrativos – especialmente si pueden transferir dinero a través de los servicios o si estos datos tienen valor en el mercado negro (para lavar dinero, envío de spam, envío de artículos robados, etc).

**Puntos de partida psicológicos:** inexperiencia, inseguridad y temor

**Riesgos:** al igual que sucede con las estafas para volver a registrarse, los ataques de phishing se dirigen específicamente a los datos personales de contenido valioso, centrándose especialmente en cualquier tipo de datos bancarios. En este caso, como ocurre con las estafas para las actualizaciones, la aceptación de una autoridad falsa resulta fundamental para el éxito de estos ataques.

**Ejemplos de líneas de asunto:** ¡Atención! ¡Alguien ha accedido a su cuenta de PayPal! (Attention!

Your PayPal account has been violated!)

Su cuenta de PayPal puede estar en peligro- (Your Pay PalAccount May Be Compromised)

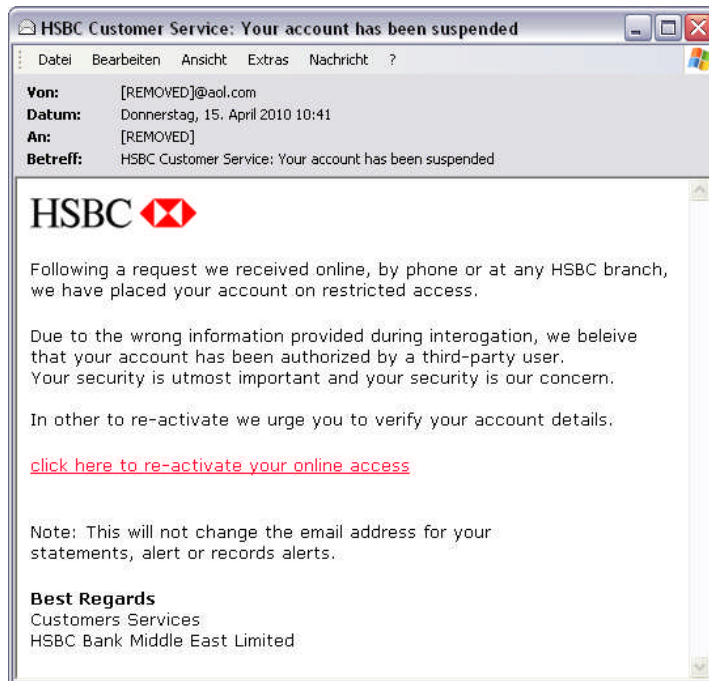
Múltiples errores de acceso en su cuenta – (Multiple Logon Errors on your Account).

Aviso de acceso de cuenta limitado RXI034 – (Notification of Limited Account Access RXI034)

Mensaje urgente e importante sobre la fusión del Santander – (Santander Merger Important Urgent Message)

MENSAJE IMPORTANTE DEL CENTRO DE SEGURIDAD (<<< IMPORTANT MESSAGE FROM SECURITY CENTER >>>)

A la atención de todos los usuarios de Webmail- (Attn. All Webmail Users)



**Captura de pantalla 4:** una captura de correo de phishing que imita la correspondencia oficial de un banco



## 2.3 Las estafas con tarjetas de felicitación (malware)

Las falsas tarjetas de felicitación se distribuyen durante todo el año aunque, sin embargo, reciben una atención especial por parte de los estafadores y de las víctimas en fechas clave y en períodos vacacionales importantes. Todos nos vemos muy tentados a ver una supuesta felicitación enviada por “un amigo” y esa curiosidad es, justamente, la base de esta clase de estafas.

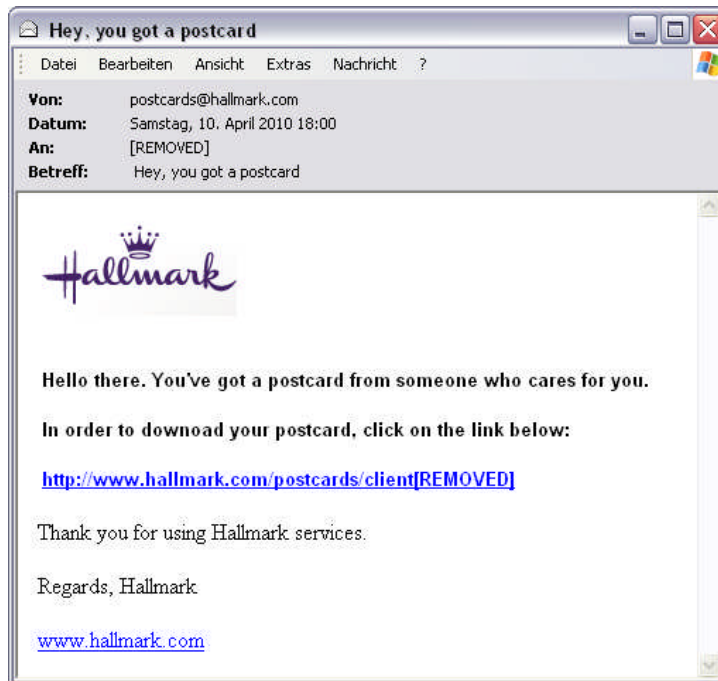
Existen numerosos tipos de correo electrónico de este tipo: por una parte, hay correos con adjuntos que dicen ser tarjetas de felicitaciones electrónicas (eCards) pero que lanzan su ataque en cuanto se abren. También hay correos electrónicos que invitan al usuario a visitar un sitio web para instalar un supuesto códec o un reproductor de multimedia para ver la eCard. Y, por último, están los correos electrónicos que lanzan una infección de paso e inadvertida cuando se visita un supuesto sitio de tarjetas de felicitación.

**Grupo objetivo:** cualquier usuario de Internet

**Puntos de partida psicológicos:** curiosidad, amabilidad

**Riesgos:** al igual que ocurre con la estafa de tipo “¡Mira esto!”, el usuario se expone al código malicioso en cuanto visita un sitio, abre un adjunto o instala el programa ejecutable camuflado. De esta manera, se ofrece una oportunidad al malware para apropiarse de datos personales y/o causar más caos.

**Ejemplos de líneas de asunto:** ¡Te doy un beso, amor mío! ¡Feliz Día de San Valentín – (Kiss You My Love! Happy Valentine's Day!)  
 Ha recibido una tarjeta de felicitación navideña – (You have received a Christmas Greeting Card!)  
 Despina le envía una tarjeta de regalo – (Despina sended you a giftcard!)  
 Tiene una tarjeta de dGreetings enviada por un amigo –(You dGreetings card from a friend)  
 Ha recibido una felicitación de alguien que se preocupa por usted – (You have received a greeting from somebody who cares for you !!!)  
 ¡Hey! Tiene una nueva felicitación – (Hey, you have a new Greeting !!!)



**Captura de pantalla 5:** el correo electrónico que parece legítimo lleva a un archivo .exe ejecutable, en vez de conectarse a la página de inicio de la empresa de tarjetas de felicitación

## 2.4 La estafa del envío de un paquete (malware y phishing)

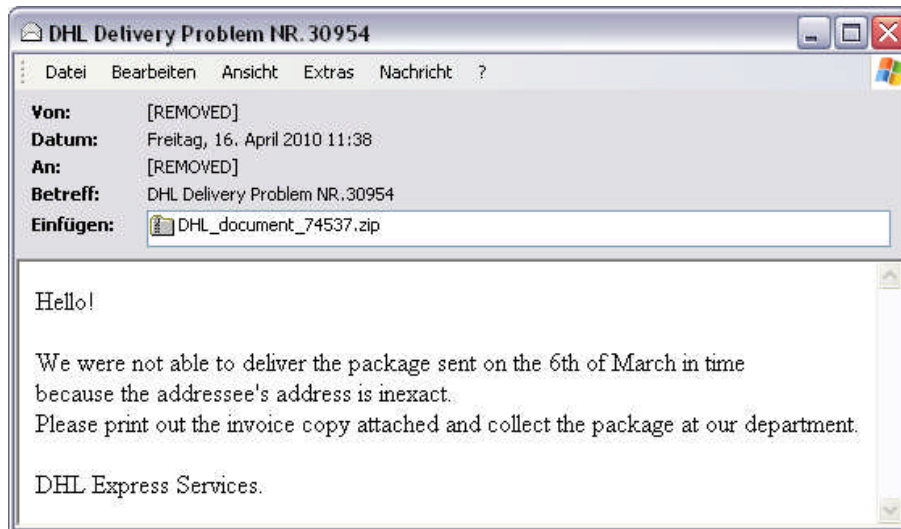
El receptor recibe un correo electrónico con un mensaje relacionado con un supuesto problema con el envío de un paquete. Para resolver el problema o para recibir más información, el receptor debe abrir un archivo adjunto o hacer clic en un enlace que se proporciona. Los delincuentes se dirigen a menudo a los clientes de compañías de reparto de paquetería en las que los envíos pueden recogerse en un punto de recogida en cualquier momento, utilizando para ello un PIN. Muy frecuentemente se utilizan los nombres de servicios de reparto de mensajería conocidos en todo el mundo como anzuelo para este tipo de campañas de phishing.

**Grupo objetivo:** cualquier usuario de Internet pero, especialmente, los clientes de servicios populares de reparto de mercancías.

**Puntos de partida psicológicos:** curiosidad, avaricia, vigilancia

**Riesgos:** si el usuario abre sin darse cuenta el archivo adjunto en el correo electrónico – que se camufla a menudo como un aviso de entrega – se instala malware en su ordenador (en forma de, por ejemplo, un programa que captura las contraseñas, un programa para copiar las teclas pulsadas, etc) para, de esta manera, apoderarse de los datos personales y reenviarlos a otra persona. Los usuarios caen en la trampa del phishing en cuanto registran, por ejemplo, datos personales relacionados con el punto de entrega de un paquete en un sitio web falso y camuflado pero con una apariencia legítima de una supuesta empresa de reparto de mercancías. De esta manera, los ciberdelincuentes pueden hacerse con los datos de acceso, apoderarse de paquetes entregados en los puntos de recogida y usar el punto de entrega para el envío de bienes adquiridos de forma ilegítima. Las cuentas para estos puntos de entrega se usan en el mercado negro para enviar artículos adquiridos con datos de bancos o tarjetas de créditos robados. Por último, también pueden utilizarse para el lavado de capital y, por eso, son muy buscados. Debido a todo lo anteriormente explicado, cualquier persona que revele sus datos proporcionándolos en una página de acceso falsa, puede sufrir daños generalizados.

**Ejemplos de líneas de asunto:** Servicios de DHL. Por favor, recoja su paquete NR.0841 (DHL Services. Please get your parcel NR.0841)  
Oficina de DHL. Recoja su paquete NR.1572 (DHL Office. Get your parcel NR.1572)  
DHL Express. Recoja su paquete NR.3029 (DHL Express. Get your parcel NR.3029)  
Problema de entrega de UPD NR 68522 (UPS Delivery Problem NR 68522)  
Gracias por el envío N° 538532 (Thank you for setting the order No.538532)



**Captura de pantalla 6:** un correo electrónico con un adjunto infectado, camuflado como un documento oficial

## 2.5 La estafa del tipo "¡Mira esto!" (malware y publicidad)

En esta variante, los estafadores se basan principalmente en técnicas de ingeniería social e incitan la curiosidad del receptor del correo electrónico sobre supuestas ofertas de última hora en Internet, imágenes aparentemente comprometidas de la persona que recibe el mensaje u otros temas de interés.

En este caso, el malware puede camuflarse directamente en el adjunto infectado que se incluye en el correo electrónico o en el sitio web al que lleva un enlace que se muestra en el correo. En numerosas ocasiones, el enlace conduce a una solicitud para instalar un códec o un nuevo programa ejecutable que, cuando se ejecuta, instala malware en el ordenador.

**Grupo objetivo:** cualquier usuario de Internet pero, especialmente, los usuarios de redes sociales

**Puntos de partida psicológicos:** curiosidad, lujuria

**Riesgos:** en esta variante, la víctima es atacada con malware y puede ver su ordenador infectado con varios programas maliciosos. Estos programas pueden leer contraseñas, apoderarse de datos de tarjetas de crédito, incorporar el PC a un botnet y muchas otras acciones más.

**Ejemplos de líneas de asunto:** ¡ Escándalo! Britney Spears ha fallecido (Scandal Britney Spears dead)

Un volcán de Islandia causa problemas en vuelos, etc .... (Iceland volcano disrupts flights accumulable

200,000 flood Shanghai Expo preview acetabular)

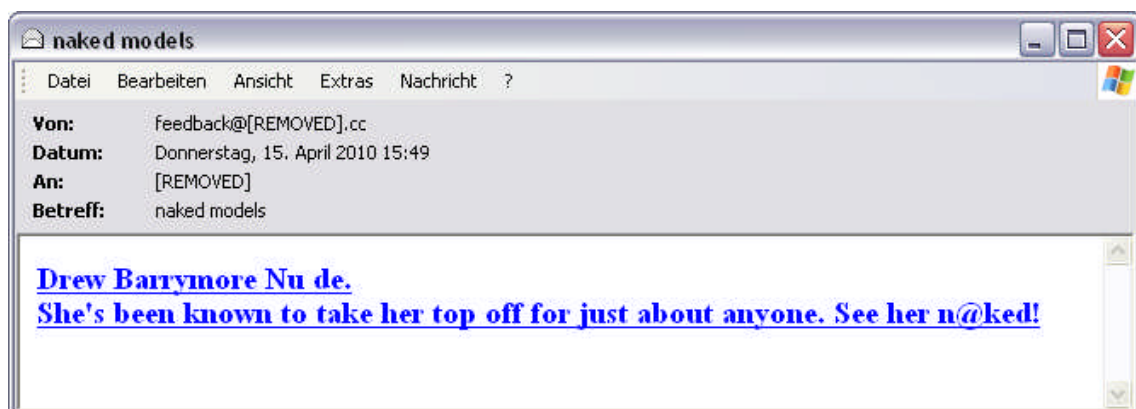
UN VÍDEO DE UN NUEVO ESCÁNDALO (NEW SCANDAL VIDEO)

¿Es usted el profesor que aparece en la imagen? (are you a teacher in the picture?)

¿Por qué usted? (Why You?)

Foto reenviada (Fwd: Photo)

Un usuario de Windows Live ha compartido una foto con usted (Windows Live User has shared photos with you)



**Captura de pantalla 7:** un correo electrónico que intenta engañar a las personas curiosas para que visiten un sitio web infectado. Un ejemplo muy conocido de este tipo de mensajes es el anuncio de fotografías desnudas de Anna Kournikova en 2001.

## 2.6 La estafa de los descuentos (malware)

Los filtros de spam se encuentran saturados por anuncios publicitarios no solicitados de pequeñas pastillas azules, el software más barato del mundo, descuentos fantásticos y promesas de dietas milagrosas. Con todos estos mensajes, la regla es muy sencilla: si parece demasiado bueno como para ser verdad, no debemos creer lo que afirman.

**Grupo objetivo:** cualquier usuario de Internet

**Puntos de partida psicológicos:** avaricia

**Riesgos:** cuando se hace clic en el enlace, se lleva al usuario a tiendas online sospechosas. Los ciberdelincuentes están al acecho esperando que el usuario registre en un impreso electrónico sus datos personales valiosos, información bancaria o los números de su tarjeta de crédito. También es muy probable que el ordenador se vea infectado por una descarga de malware de paso cuando se visita el sitio web al que lleva el enlace. Las consecuencias de todo esto son consecuencia del malware utilizado, que causará todo tipo de problemas en el ordenador de la víctima.

**Ejemplos de líneas de asunto:** rder And Save 40%, For March Only

Software Offers You Will Love!

Dear [...], 15-22 March 2010 +4833 78% OFF.

Save thousands of dollars on original D&G accessories.

Bvlgari jewelry would look great on your girlfriend.

Cheaper Than Ever - Expensive Watches

Descuentos

Worlds only herball pill that corrects erectile dysfunction,  
strengthens erections and enhances libido

Productos farmacéuticos

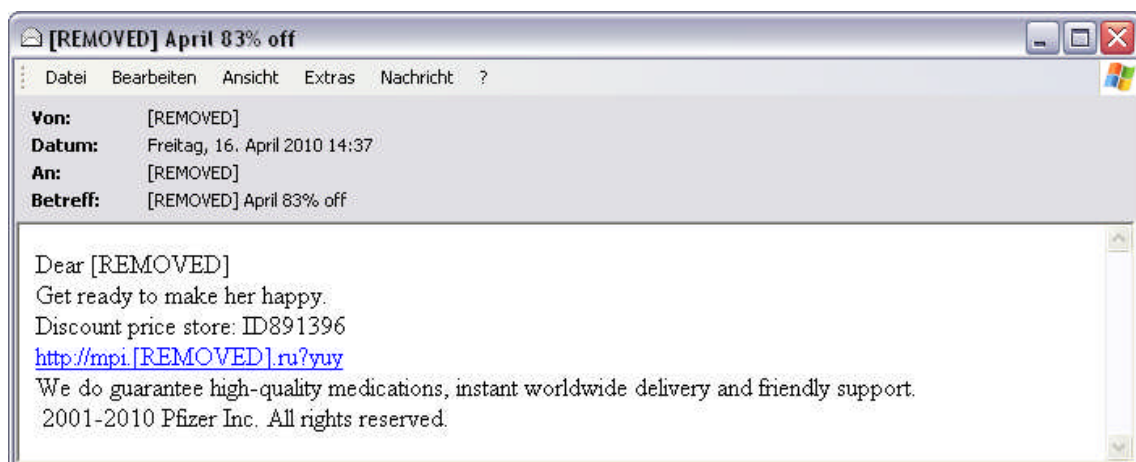
You can be another on the long lish of Quick Slim Success stories.

This Is How Mado#nn^a Lost Weight

Sport is Murder

Too Fat? Lose Weight!

Dietas



**Captura de pantalla 8:** este correo electrónico promete grandes descuentos para seducir al usuario

## 2.7 Estafas mediante títulos académicos o universitarios (phishing y timos)

El texto publicitario intenta atraer a las personas prometiéndoles la obtención rápida y sencilla de un título académico o universitario – sin necesidad de estudiar y, normalmente, sin exámenes finales.

**Grupo objetivo:** cualquier usuario de Internet

**Puntos de partida psicológicos:** deseo, credulidad

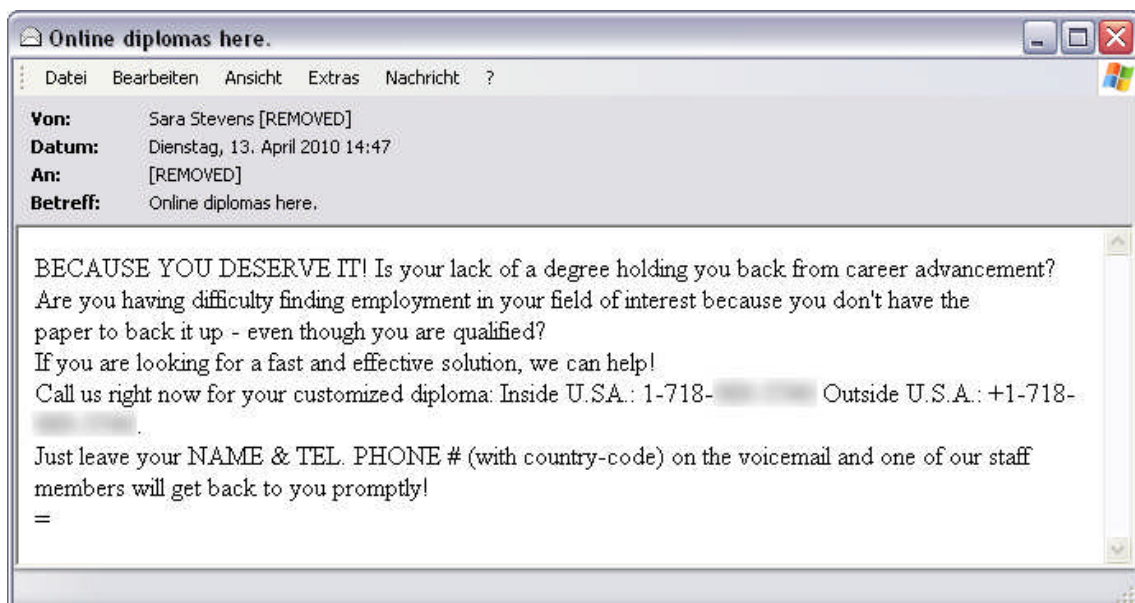
**Riesgos:** cualquier persona a la que el usuario contacte a través de los números de teléfono o direcciones de correo electrónicos facilitados solicitará a la víctima una gran cantidad de datos personales, haciendo que el usuario le comunique una información confidencial valiosa. La persona que adquiera un título académico mediante estos canales perderá por completo el dinero abonado. Por otra parte, cualquier persona que utilice las calificaciones de una universidad de dudosa reputación y que utilice un título académico comprado puede ser perseguida por la ley alemana, siguiendo el artículo § 132a del Código Penal de Alemania.

**Ejemplos de líneas de asunto:** Un título de Doctorado puede ser suyo (Doctorate degree can be yours)

Diplomas online aquí (Online diplomas here)

Títulos y premios de MBA (Re: MBA- qualification & award)

Obtenga un diploma para conseguir un mejor trabajo (Get a diploma for a better job)



**Captura de pantalla 9:** este correo electrónico vende títulos universitarios para mejorar una carrera profesional

## 2.8 Estafas con casinos online (phishing y timos)

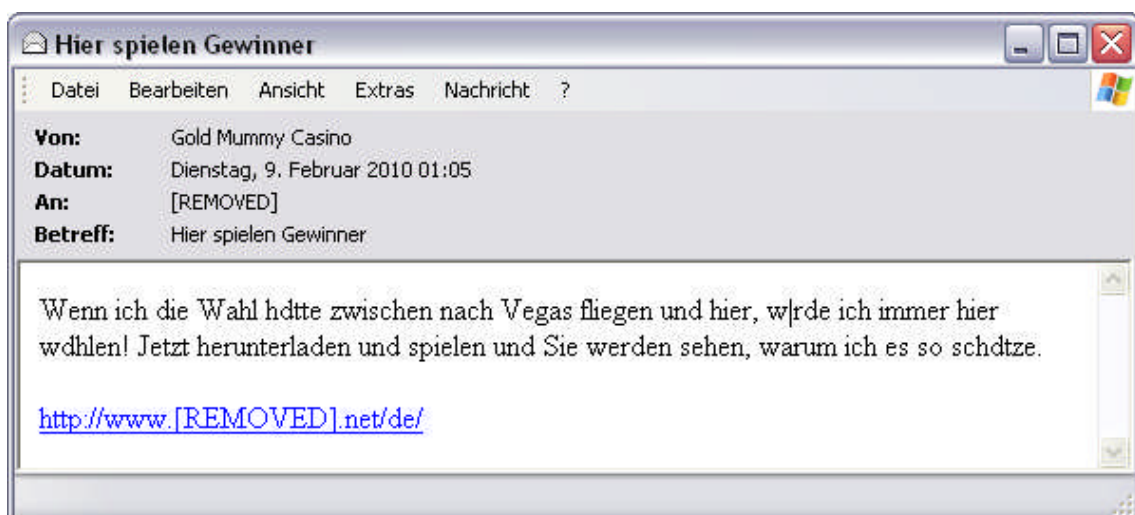
Los juegos online de cualquier tipo se están haciendo cada vez más populares. Desde hace mucho tiempo, el póker online se encuentra entre los juegos más utilizados. El correo electrónico spam de este tipo sugiere que se puede ganar una gran cantidad de dinero con una pequeña apuesta. Como incentivo, se prometen bonificaciones con el primer pago, o se ofrecen créditos ya disponibles.

**Grupo objetivo:** cualquier usuario de Internet

**Puntos de partida psicológicos:** deseo, avaricia, curiosidad, instinto de juego

**Riesgos:** los casinos online que, por motivos legales, no pueden encontrarse en Alemania, exigen un pago inicial a los jugadores potenciales. Al hacer esto, los usuarios a menudo ofrecen de forma inadvertida datos bancarios valiosos o incluso los números de sus tarjetas de crédito a sitios de juegos online de dudosa reputación. Un peligro más se presenta a la hora de recibir dinero cuando se gana una partida porque, a menudo, se deniegan dichos pagos por varias razones por lo que se pierde tanto el dinero ganado como el pagado. En estos casos no hay ningún recurso legal disponible, ya que tanto la participación como los pagos en juegos online se encuentran prohibidos en Alemania desde enero de 2009.

**Ejemplos de líneas de asunto:** Obtenga sus premios con esta fantástica oferta (Take your winnings after experiencing this fantastic offer)  
Disfrute de nuestros juegos con nuestra fantástica bonificación de inicio (Enjoy playing our games with our fantastic start bonus)  
Una generosa bonificación de bienvenida (Generous welcome bonus)  
Último recordatorio (Final reminder)



**Captura de pantalla 10:** un correo electrónico que intenta seducir a una persona para que juegue en un casino online



## 2.9 Estafa 419 / spam nigeriano (timo)

Este término se refiere a las estafas mediante correo electrónico con pagos anticipados. El receptor del correo electrónico puede llegar a pensar que tiene derecho a recibir una gran cantidad de dinero por alguna razón como, por ejemplo, una herencia, como agradecimiento por ocuparse de varias transacciones o como ganancias por haber participado en un supuesto concurso. Otros escenarios pueden incluir la participación del usuario en buenas acciones o la ayuda a una persona sin hogar / a un animal abandonado (recibiendo dinero a cambio, por supuesto). La única acción necesaria para recibir el dinero / ofrecer ayuda es ponerse en contacto con la persona nombrada en el correo electrónico.

El nombre "estafa 419" para este tipo de actividad proviene del código penal nigeriano, ya que en la sección 38 del artículo 419<sup>5</sup> se explica las circunstancias y las penas para fraudes y estafas.

Los daños causados por la estafa 419 y por sus consecuencias en 2009 alcanza unas pérdidas de, como mínimo, US\$ 522 millones en Alemania y de US\$ 2.110 millones en EE.UU.<sup>6</sup>.

**Grupo objetivo:** cualquier usuario de Internet

**Puntos de partida psicológicos:** avaricia, credulidad

**Riesgos:** cuando se realiza el contacto inicial, se hace que la gran cantidad de dinero ofrecida parezca incluso más atractiva a la víctima. Sin embargo, para transferir el dinero a la cuenta de la víctima, se precisa que el usuario transfiera una cantidad X a una cuenta de Western Union en el extranjero. A continuación siguen una serie de costes adicionales ficticios para abogados, visitas a las autoridades, certificados, etc. El dinero enviado por la víctima (en varias etapas) se pierde por completo y la cantidad de dinero prometido nunca se recibe.

**Ejemplos de líneas de asunto:** ¡Urgente! (URGENT!)

Se necesita un socio de confianza (Reliable Partnership needed)

SE NECESITA CONFIRMACIÓN DE ACEPTACIÓN (NEED CONFIRMATION OF ACCEPTANCE)

¡Su carta de aviso! (Your Notification Letter !!!)

<sup>5</sup> <http://www.nigeria-law.org/>

<sup>6</sup> Ultrascan Advanced Global Investigations (2010), „419 Advance Fee Fraud Statistics 2009“ S. 29



**Captura de pantalla 11:** grandes promesas sin referencia reconocible a una persona real, utilizando una pésima redacción del texto



## 2.10 Estafas de ofertas de trabajo (malware y timos)

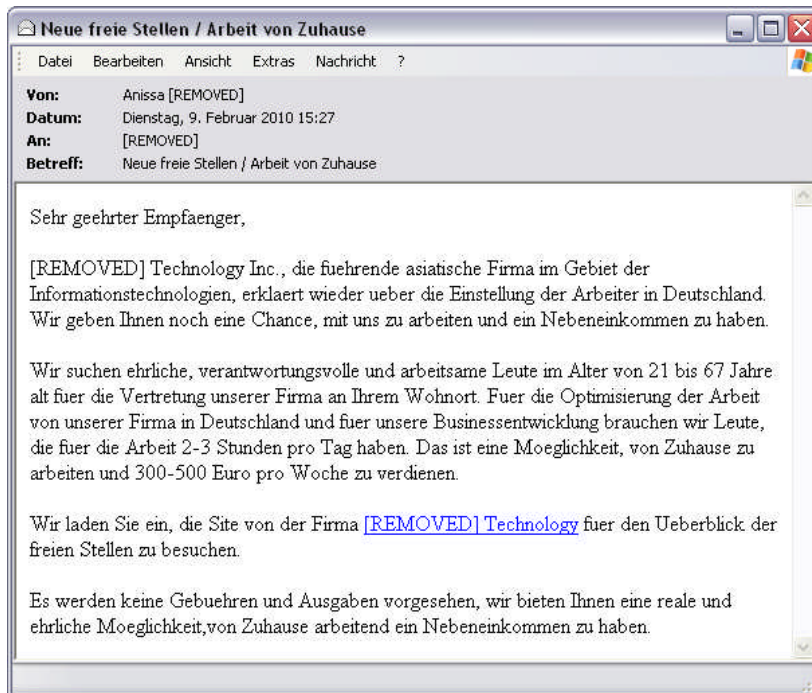
Las promesas de correos electrónicos ofrecen puestos bien remunerados (en compañías conocidas) por realizar poco trabajo. Los salarios son altos, las horas de trabajo escasas y, a menudo, no resulta necesario desplazarse de la sala de estar. Estas propuestas son verdaderamente atractivas en estos tiempos económicamente complicados. Esta estafa puede formar parte de un ataque del tipo estafa 419.

**Grupo objetivo:** cualquier usuario de Internet

**Puntos de partida psicológicos:** deseo, vanidad

**Riesgos:** a veces, estos correos electrónicos se envían con unos adjuntos que, cuando se abren, infectan al ordenador con gusanos y que se utilizan para seguir distribuyendo mensajes spam con esta oferta de trabajo. Sin embargo, existe otro riesgo camuflado detrás del riesgo técnico: los trabajos que se ofrecen ocultan a menudo una propuesta para lavar dinero o para el reenvío de bienes adquiridos de manera ilegal. Frecuentemente, el uso de una cuenta privada es uno de los principales criterios que se especifican en la descripción del trabajo y, también a menudo, los buscadores de trabajo demasiados crédulos se ven envueltos en prácticas para lavado de dinero o compraventa de bienes robados cuando entablan relaciones con estos estafadores. El robo de la identidad es otra posibilidad, cuando se entregan a los estafadores todo tipo de datos personales (para, por ejemplo, realizar un supuesto contrato).

**Ejemplos de líneas de asunto:** Oferta de trabajo. Trabajo a tiempo parcial/completo. 8 años de experiencia (Job offer. Contract. Part-time/Full-time. 8 years in business)  
Servicio al cliente/oferta de trabajo/UPS/MBE (Consumer service/Job offer/UPS/MBE)  
Pluriempleo (Sideline)  
Trabaje para nosotros (Work for us)  
Usted puede ser contratado (You can be hired)  
Una organización busca compañeros de trabajo (Organisation seeks colleagues)  
El equipo directivo busca compañeros de trabajo (Management seeking work colleagues)



**Captura de pantalla 12:** un intento para engañar a usuarios mediante un correo electrónico con una supuesta oferta de trabajo para que los usuarios confiados caigan en la trampa

## 2.11 Estafa de la novia rusa (timo)

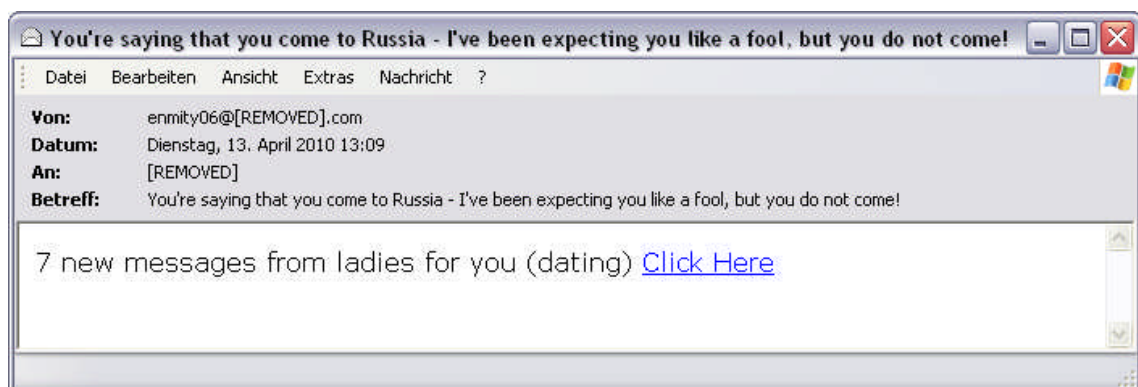
Estos correos electrónicos prometen el amor verdadero o tan sólo un romance pasajero, frecuentemente con una típica y rubia joven rusa. Supuestamente, las mujeres han estado esperando una respuesta durante mucho tiempo y desean conocer o casarse con su amado. Estas citas también se utilizan para lavar dinero, cuando el “cariñito” ruso pide a su “amado” que le que le envíe regalos y dinero para que ella pueda ir a verle. Las estafas 419 a menudo también usan esta técnica.

**Grupo objetivo:** cualquier usuario de Internet pero, especialmente, los hombres solteros de Europa Occidental

**Puntos de partida psicológicos:** lujuria, reciprocidad

**Riesgos:** cualquier persona que responda al correo electrónico e inicie contacto con la supuesta mujer soltera encontrará pronto que la conversación pasa rápidamente al envío de dinero, visas y propuestas de matrimonio. La señorita necesitará dinero para viajar, para sus gastos, para sobornar a los oficiales y, por lo tanto, exigirá que se le transfiera más fondos a una cuenta corriente anónima. Si el hombre crédulo envía dinero, no lo verá de nuevo y, muy probablemente, jamás vuelva a tener noticias de su “amorcito”.

**Ejemplos de líneas de asunto:** Tiene un nuevo correo de Olga, de 26 años. Cita con una rusa (You have new mail from Olga 26 y.o. Russia, dating)  
Conozca a mujeres rusas aquí (Meet Russian women here)  
¿Aún soltero? Mira mi perfil. Olga, de Rusia (Still single?look at my profile, Olga from Russia)  
¿Quiere saber lo que realmente les encanta a las mujeres rusas? (Want to know what the real Russian girls love and warmth?)  
Las bellezas rusas le están esperando (Russian beauties are waiting)



**Captura de pantalla 13:** uno de los muchos mensajes anzuelo basados en citas para buscar pareja

## 2.12 Estafa de la lotería (timo)

Se comunica al receptor de este tipo de correo electrónico que ha ganado una gran cantidad de dinero en euros, dólares o en otra moneda. Todo lo que necesita hacer es ofrecer sus datos personales a la persona XY. Las loterías son realizadas supuestamente por unas compañías de gran reputación y los bancos involucrados son conocidos en todo el mundo. Esta estafa también puede ser parte de un ataque de tipo spam nigeriano.

**Grupo objetivo:** cualquier usuario de Internet

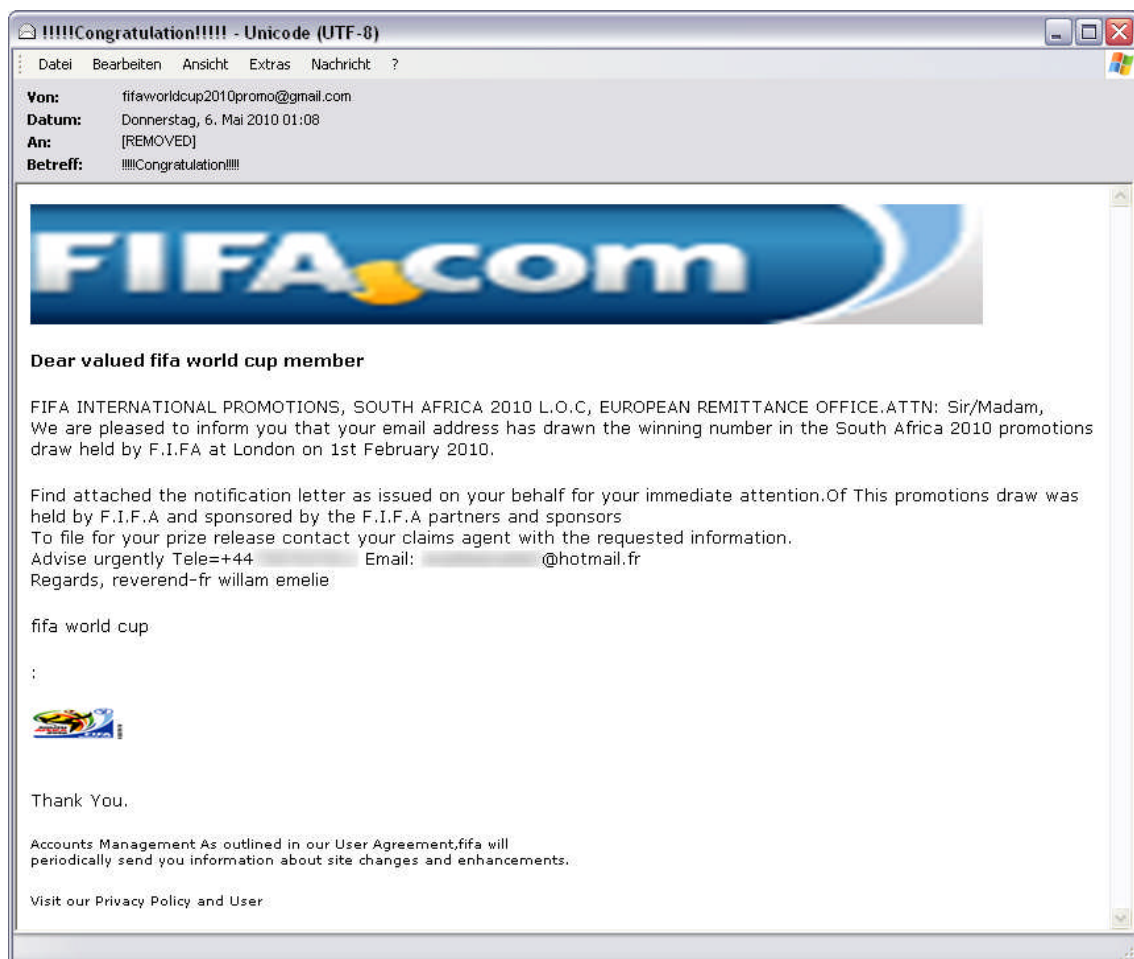
**Puntos de partida psicológicos:** avaricia, deseo

**Riesgos:** para recibir este dinero, el supuesto ganador debe, en primer lugar, transferir fondos a los estafadores – normalmente a una cuenta bancaria extranjera y/o anónima. Una cantidad sigue a la otra, y la víctima seguirá pagando sin ver nada de las ganancias o de las cantidades ya abonadas.

**Ejemplos de líneas de asunto:** REF NR. GOOGLE-0293856-2009

Su dirección de correo electrónico ha obtenido un premio (Your E-mail Address Won)

AVISO DE UN GRAN PREMIO (Felicidades. Usted ha resultado ser ganador)  
(NOTICE OF GRANT AWARD (Congratulations you are a winner))



**Captura de pantalla 14:** un aviso de un supuesto premio



## 3 Consejos y trucos

Para evitar ser víctima de una de las estafas anteriormente descritas, los internautas deberían tener en cuenta los siguientes puntos.

### 3.1 Reglas de conducta útiles

- Trate siempre con precaución cualquier correo electrónico enviado por remitentes desconocidos. Si un correo electrónico parece muy extraño, esto es lo que debe hacer: ignorarlo o borrarlo pero, bajo ningún concepto, debería abrir un adjunto o hacer clic en direcciones URL incluidas en el mensaje.
- Nunca responda a correo electrónico spam, porque lo que indica dicha respuesta al estafador es que la dirección a la que envía el mensaje es una dirección válida.
- Nunca dé a conocer información personal y/o datos bancarios – ya sea a través de correo electrónico o mediante sitios web de dudosa reputación.
- Nunca realice transferencias de dinero a personas desconocidas.
- Nunca publique irreflexivamente su dirección de correo electrónico principal en Internet (en foros o libros de visita) ya que los estafadores podrían utilizarla. En estas ocasiones resulta recomendable utilizar una dirección secundaria.

### 3.2 Medidas técnicas

- Una solución de seguridad para el ordenador con una función de spam integrada utilizará un filtro para proteger el PC contra la entrada de correo electrónico no deseado o peligroso.
- Abrir archivos adjuntos – especialmente los enviados por desconocidos – puede acarrear ciertos riesgos. Los adjuntos deberían ser primeramente analizados con un programa antivirus y, si fuera necesario, deberían ser borrados antes de abrirlos.
- Nunca haga clic en los enlaces incluidos en los correos electrónicos sin pensárselo antes. Compruebe antes la dirección URL. Muchos programas de correo electrónico permiten ver el objetivo real del enlace con tan sólo desplazar el ratón sobre el enlace visible, sin necesidad de hacer clic sobre él – lo que se conoce como la función “ratón por encima” (mouse-over).



## 4 Glosario

**Bot:** los bots son pequeños programas que, normalmente, se ejecutan sin que el usuario lo perciba en un segundo plano en el ordenador de la víctima. Dependiendo de las funciones que realice, puede llevar a cabo varias tareas, desde ataques distribuidos de denegación de servicio a correos electrónicos spam, registro de teclas pulsadas, etc. La gama de funciones depende esencialmente de la cantidad que se pague por un bot. Por esa razón, los bots que realizan una gran cantidad de funciones son más caros que los bots más sencillos con funciones limitadas. Estos programas pueden adquirirse en foros del mercado negro.

**Botnets:** un botnet es una red de (los así llamados) PC zombi. Los servidores de comando y control (Command and Control Servers, C&C Servers) se utilizan para administrar un botnet. Entre otras cosas, los botnets se utilizan para lanzar ataques para sobrecargar la capacidad de los servidores web (ataques de denegación de servicio y ataques distribuidos de denegación de servicio) y para enviar spam.

**Ingeniería social:** se entiende por ingeniería social aquellas tácticas de persuasión utilizadas por un hacker con el objetivo de seducir a un usuario para que le ofrezca la información que precisa para causar daño al usuario y/o a su organización. Para conseguir este fin, el hacker se camufla a menudo con un papel de autoridad para, de esta forma, obtener acceso a los datos o a las contraseñas de la víctima.

**Spam:** a mediados de los años 90, se utilizó el término spam para describir la distribución excesiva del mismo mensaje en los foros de Usenet. Esta palabra proviene de un sketch de Monty Python. Actualmente, entendemos por spam varias cosas. De forma genérica, spam es la distribución en grandes cantidades de correos electrónicos no solicitados. En un sentido más estricto, el término 'spam' se limita a los correos electrónicos publicitarios, por lo que los gusanos, los bulos, los mensajes de phishing y los autorrespondedores no se incluyen en esta acepción.

**PC zombi:** un PC zombi es un equipo controlado a través de una puerta trasera, utilizando para ello un ordenador remoto que se encarga de gestionar sus acciones. Igual que ocurre en las películas de terror de muertos vivientes, el PC zombi sólo obedece a un maestro oculto y se encarga de llevar a cabo las órdenes que se le da (que, a menudo, constituyen objeto de delito). Normalmente, los PC zombis se combinan para formar botnets.