Guía de recomendaciones para el uso seguro del correo electrónico

SEGURIDAD DE LA INFORMACIÓN

División de Transformación Digital

Abril 2020

Uso Público

Introducción

El correo electrónico es una herramienta de uso común en nuestra sociedad, tanto en el ámbito empresarial como en el personal. Por ello está permanentemente en el punto de mira de los delincuentes informáticos como canal para introducir malware en las organizaciones y en nuestros hogares, o simplemente para robar información de los usuarios y usuarias con la que posteriormente se comercia en internet.

EMASESA no es una excepción y todos los días se reciben multitud de correos cuyo tratamiento inadecuado podría poner en peligro el patrimonio tecnológico de la compañía y sus activos de información. Por ello, desde el área de Seguridad de la Información de EMASESA se ha elaborado esta guía con el objetivo fundamental de ayudar al personal a utilizar esta herramienta de forma adecuada y detectar este tipo de correos malintencionados.

A modo ilustrativo, se han incluido ejemplos reales de correos maliciosos recibidos en EMASESA.

En gran medida, las recomendaciones que se recogen en esta guía son aplicables a otros canales de comunicación telemática como son las aplicaciones de mensajería instantánea (WhatsApp, etc.) cuyo uso está cada vez más extendido, incluso en el ámbito profesional.

EMASESA está firmemente comprometida con la creación de una sociedad digital más segura. Con esta finalidad, el presente documento se ha adaptado a partir de la correspondiente guía interna con objeto de que pueda ser utilizado pública y libremente por cualquier persona u organización interesada.

Recomendaciones para el uso del correo electrónico

No responsas al correo no solicitado (spam) ya que puede ser una forma de aumentar la cantidad de correo basura en nuestro buzón, al indicar al remitente que el correo ha sido leído. Los mensajes no deseados deben borrarse directamente. Recuerda también vaciar la carpeta de "Elementos eliminados", ya que además así ahorrarás espacio en tu buzón.

No abras ficheros adjuntos que no esperes pues, aunque procedan aparentemente de personas conocidas, puede tratarse de malware. Ante la duda siempre puedes contactar con el remitente (por ejemplo, mediante teléfono) para comprobar la autenticidad del correo.

No difundas correo electrónico no solicitado (cadenas de mensajes, publicidad, rumores, bulos...) pues de esta forma contribuyes a aumentar el correo no solicitado entre tus conocidos.

Utiliza tu dirección de correo con moderación, no la proporciones en webs de dudosa confianza o que puedan enviarte publicidad no deseada. Es una buena idea disponer de una cuenta gratuita para uso específico si necesitas registrarte en este tipo de sitios.

Diferencia entre correo profesional y personal, para ello obtén una cuenta de correo electrónico para asuntos personales en algún sitio web de los numerosos que hay disponibles. De esta forma podrás reducir el volumen de correo de tu buzón profesional, manteniéndolo para fines adecuados.

Limita el tamaño de los mensajes y el uso de adjuntos, ya que el correo electrónico no es el mecanismo adecuado para transferir ficheros de elevado tamaño. Ten en cuenta que el destinatario puede tener problemas para leerlos, bien por su excesivo tamaño o porque el tipo de fichero (.exe, .vbs,...) puede estar prohibido en el sistema receptor. Cuando envíes un adjunto es aconsejable indicar en el texto del mensaje cual es su contenido y su propósito para evitar que el destinatario sospeche que se trata de un virus. Es preferible enviar los archivos adjuntos comprimidos para reducir su tamaño. Si los documentos están disponibles en una página web (por ejemplo, una noticia de prensa, un artículo técnico, una ley, etc.), es más conveniente enviar un enlace al mismo, en lugar del documento como fichero adjunto.

Limita el tamaño de las firmas automáticas Las firmas automáticas y otro tipo de texto de inclusión automática deben ser lo más esquemáticas posibles y sin incluir información innecesaria. Piensa si quieres que tus datos sean visibles cuando escribes a ciertas personas o a listas de distribución.

No utilices estilos ni adornos innecesarios, evita el uso de estilos con fondos de mensaje prediseñados o con colores ya que recargan (en todos los sentidos) el correo y pueden provocar problemas en el destinatario (por ejemplo, que sean bloqueados por el filtro antispam).

Incluye en el campo "Asunto" una frase descriptiva del mensaje, pues de esta forma se facilita su clasificación, recuperación y lectura, y además es una norma de cortesía.

Respeta la privacidad de tus destinatarios en envíos múltiples, añadiéndolos siempre en copia oculta (CCO) y poniendo tu propia dirección en el campo "Para". De esta forma evitas:

- Que los destinatarios de tus mensajes puedan ver y hacer uso de todas las direcciones de correo electrónico a quienes remites tu mensaje.
- Que todos tus destinatarios reciban todas las respuestas. Si alguien decide "Responder a todos", todas las direcciones en los campos "Para" o "CC" recibirán la respuesta, inundando su buzón de correos no deseados o de remitentes desconocidos para ellos.

No obstante, es aceptable dejar la lista de destinatarios visible cuando se envía un correo a personas que se conocen todas entre sí y se pretende que puedan contestar a todos los demás.

No reenvíes mensajes que vengan destinados a ti, sin el permiso del remitente, sobre todo aquellos con contenido sensible o confidencial. No divulgues la dirección de una persona a terceros sin su permiso, ni publiques direcciones de correo en una web sin permiso del titular.

Evita mantener el correo en la "Bandeja de entrada", ésta debe utilizarse principalmente para el correo pendiente de lectura, y aun así, transfiérelo cuanto antes a otra carpeta para salvaguardar el espacio de tu buzón y mejorar el rendimiento del servidor de correo.

No utilices el signo de puntuación en el nombre de los archivos que vayas a enviar como ficheros adjuntos en un correo electrónico. Los ordenadores interpretan el tipo de archivo que se trata según las tres letras que siguen al signo de puntuación en el nombre (por ejemplo ".doc" para archivos de Word, ".xls" para archivos de Excel...). Si se incluyen signos de puntuación adicionales al nombrarlos, puede ocurrir que el ordenador del destinatario no los interprete correctamente, o que su antivirus bloquee estos archivos.

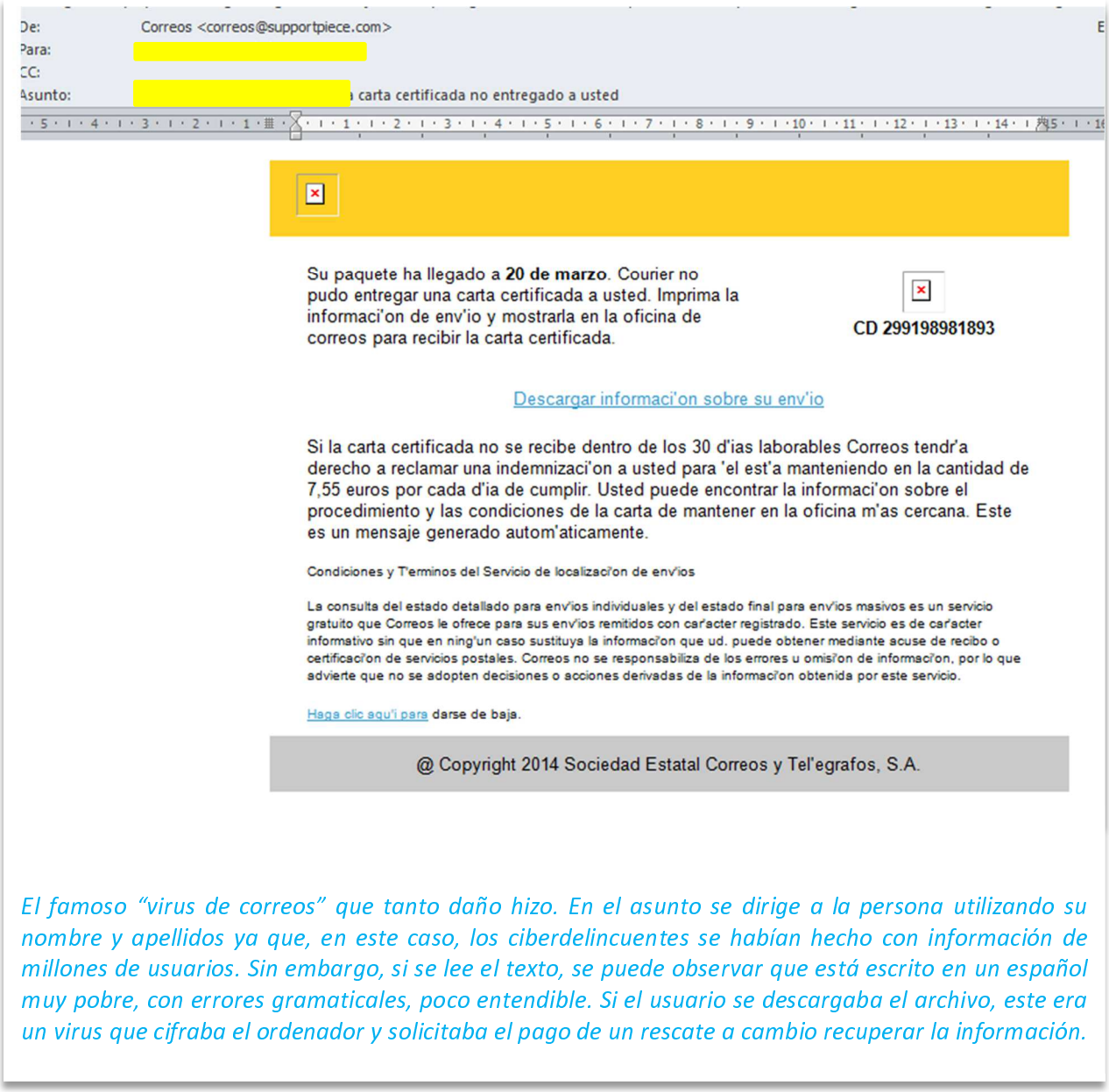
Consejos para identificar correos malintencionados.

Las direcciones de correo electrónico se obtienen de muchas formas: de páginas web, de otros correos, mediante malware,..... Luego, estas direcciones se compran y venden por internet entre los delincuentes informáticos. Cuanta más exposición pública tiene una cuenta, más fácil es que nuestra dirección circule en esas listas.

Es conveniente seguir las recomendaciones de uso que figuran en esta guía y aprender, en la medida de lo posible, a identificar y evitar los correos malintencionados. A continuación, se incluyen algunas recomendaciones que nos pueden ayudar.

- El contenido del correo puede parecer real, los delincuentes informáticos incluyen logotipos, datos de contacto, información de copyright y estilo, de forma idéntica a los de un original. En algunas ocasiones, uno o dos enlaces incluidos en el correo pudieran llevarte a páginas legítimas; sin embargo, siempre traen al menos un enlace a descargas de malware o páginas falsas para capturar tu información. En ocasiones están escritos en un español con faltas de ortografía o

errores gramaticales, y en muchos casos en inglés u otros idiomas, ya que estas bandas de delincuentes informáticos suelen ser internacionales.



De: Correos <correos@supportpiece.com>
Para:
CC:
Asunto: carta certificada no entregado a usted

Su paquete ha llegado a **20 de marzo**. Courier no pudo entregar una carta certificada a usted. Imprima la informaci'on de env'io y mostrarla en la oficina de correos para recibir la carta certificada.

CD 299198981893

Descargar informaci'on sobre su env'io

Si la carta certificada no se recibe dentro de los 30 d'ias laborables Correos tendr'a derecho a reclamar una indemnizaci'on a usted para 'el est'a manteniendo en la cantidad de 7,55 euros por cada d'ia de cumplir. Usted puede encontrar la informaci'on sobre el procedimiento y las condiciones de la carta de mantener en la oficina m'as cercana. Este es un mensaje generado autom'aticamente.

Condiciones y T'erminos del Servicio de localizaci'on de env'ios

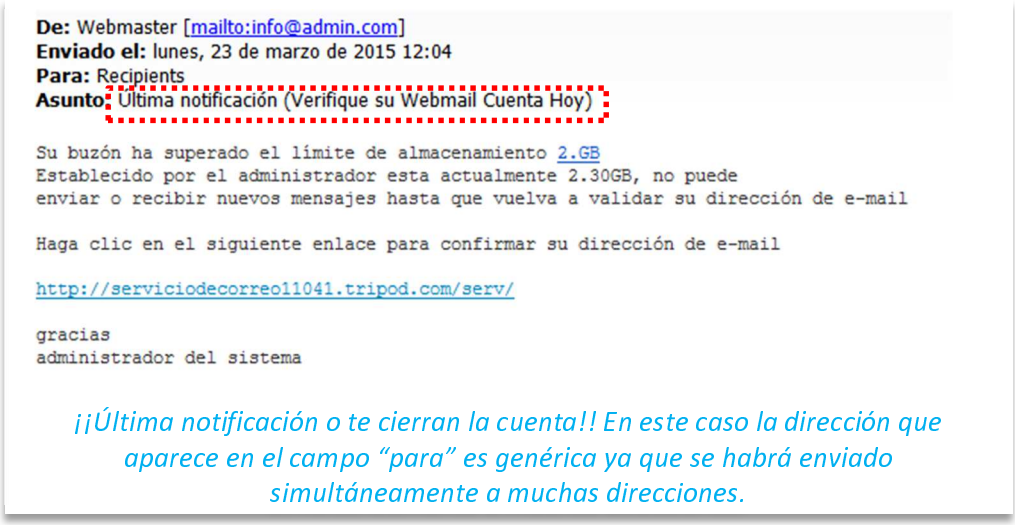
La consulta del estado detallado para env'ios individuales y del estado final para env'ios masivos es un servicio gratuito que Correos le ofrece para sus env'ios remitidos con car'acter registrado. Este servicio es de car'acter informativo sin que en ning'un caso sustituya la informaci'on que ud. puede obtener mediante acuse de recibo o certificaci'on de servicios postales. Correos no se responsabiliza de los errores u omisi'on de informaci'on, por lo que advierte que no se adopten decisiones o acciones derivadas de la informaci'on obtenida por este servicio.

Haga clic aqu'i para darse de baja.

@ Copyright 2014 Sociedad Estatal Correos y Tel'egrafos, S.A.

El famoso "virus de correos" que tanto daño hizo. En el asunto se dirige a la persona utilizando su nombre y apellidos ya que, en este caso, los ciberdelincuentes se habían hecho con información de millones de usuarios. Sin embargo, si se lee el texto, se puede observar que está escrito en un español muy pobre, con errores gramaticales, poco entendible. Si el usuario se descargaba el archivo, este era un virus que cifraba el ordenador y solicitaba el pago de un rescate a cambio recuperar la información.

- Te apremian para que actúes y que hagas clic en alguno de los enlaces o imágenes que incluyen, o a abrir algún fichero adjunto. Frases comunes*: tu cuenta debe ser actualizada, tu cuenta está a punto de ser eliminada, se detectó actividad sospechosa en tu cuenta, procedimientos rutinarios que requieren tu verificación, te han realizado un cargo en cuenta, has realizado un pago*, entre otros.



De: Webmaster [mailto:info@admin.com]
Enviado el: lunes, 23 de marzo de 2015 12:04
Para: Recipients
Asunto: Última notificación (Verifique su Webmail Cuenta Hoy)

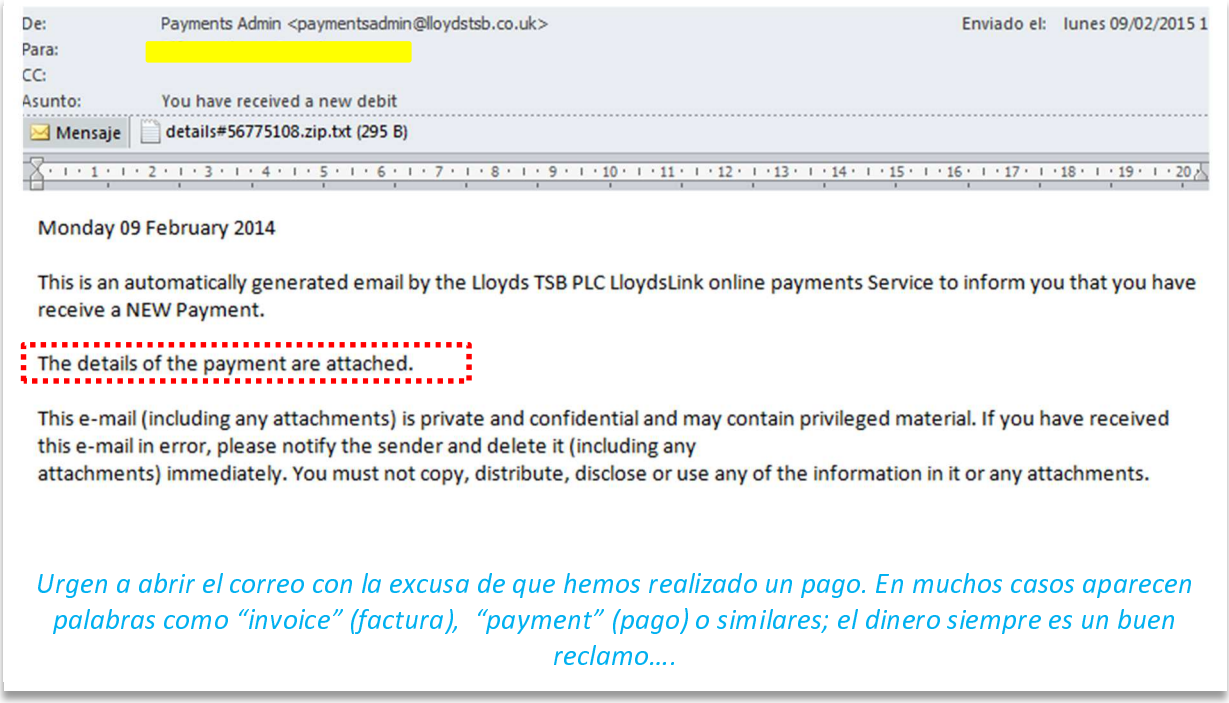
Su buzón ha superado el límite de almacenamiento 2.GB
Establecido por el administrador esta actualmente 2.30GB, no puede
enviar o recibir nuevos mensajes hasta que vuelva a validar su dirección de e-mail

Haga clic en el siguiente enlace para confirmar su dirección de e-mail

http://serviciodecorreo11041.tripod.com/serv/

gracias
administrador del sistema

¡¡Última notificación o te cierran la cuenta!! En este caso la dirección que aparece en el campo "para" es genérica ya que se habrá enviado simultáneamente a muchas direcciones.



De: Payments Admin <paymentsadmin@lloydstsb.co.uk> Enviado el: lunes 09/02/2015 1
Para:
CC:
Asunto: You have received a new debit
Mensaje details#56775108.zip.txt (295 B)

Monday 09 February 2014

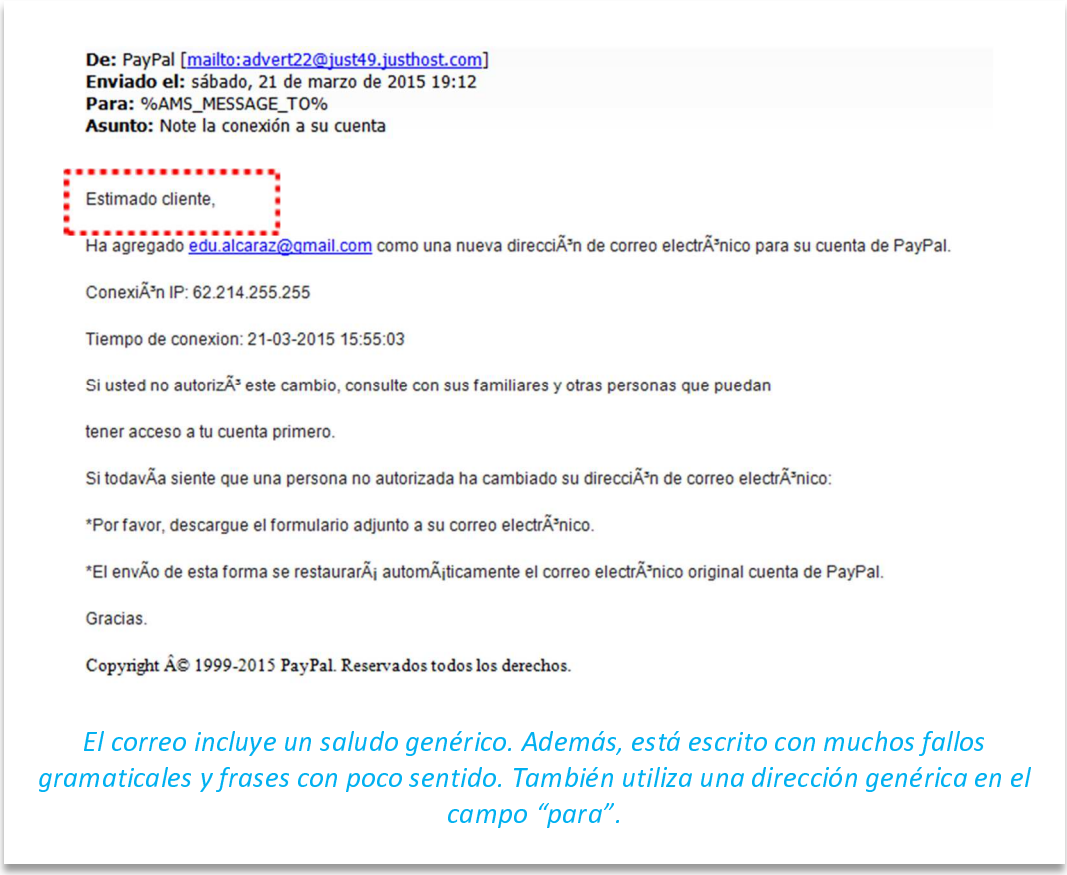
This is an automatically generated email by the Lloyds TSB PLC LloydsLink online payments Service to inform you that you have receive a NEW Payment.

The details of the payment are attached.

This e-mail (including any attachments) is private and confidential and may contain privileged material. If you have received this e-mail in error, please notify the sender and delete it (including any attachments) immediately. You must not copy, distribute, disclose or use any of the information in it or any attachments.

Urgen a abrir el correo con la excusa de que hemos realizado un pago. En muchos casos aparecen palabras como "invoice" (factura), "payment" (pago) o similares; el dinero siempre es un buen reclamo….

- Incluyen saludos genéricos, ya que están diseñados para ser enviados a muchos destinatarios, de los cuales usualmente los delincuentes informáticos sólo conocen una dirección de correo electrónico. De ahí que su saludo sea algo similar a *"Estimado cliente"* o sus equivalentes en inglés. Cualquier compañía u organismo que se precie se dirige al cliente utilizando su nombre.



De: PayPal [mailto:advert22@just49.justhost.com]
Enviado el: sábado, 21 de marzo de 2015 19:12
Para: %AMS_MESSAGE_TO%
Asunto: Note la conexión a su cuenta

Estimado cliente,

Ha agregado edu.alcaraz@gmail.com como una nueva direcciÃ³n de correo electrÃ³nico para su cuenta de PayPal.

ConexiÃ³n IP: 62.214.255.255

Tiempo de conexion: 21-03-2015 15:55:03

Si usted no autorizÃ³ este cambio, consulte con sus familiares y otras personas que puedan

tener acceso a tu cuenta primero.

Si todavÃa siente que una persona no autorizada ha cambiado su direcciÃ³n de correo electrÃ³nico:

*Por favor, descargue el formulario adjunto a su correo electrÃ³nico.

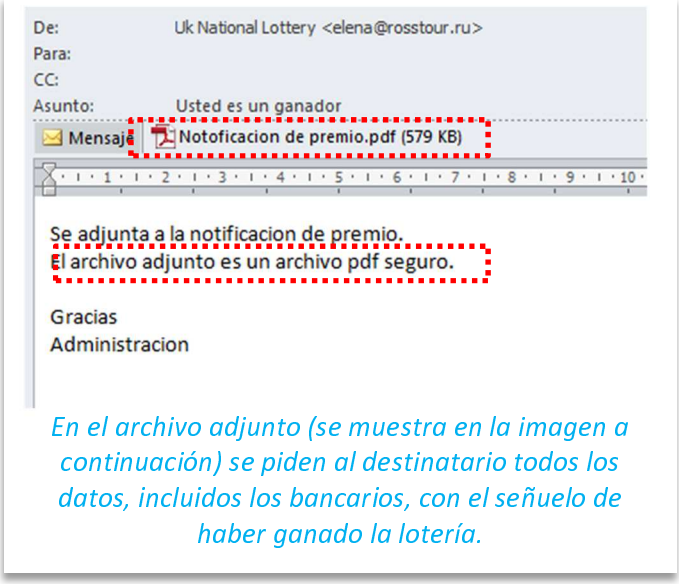
*El envÃo de esta forma se restaurarÃ¡ automÃ¡ticamente el correo electrÃ³nico original cuenta de PayPal.

Gracias.

Copyright Â© 1999-2015 PayPal. Reservados todos los derechos.

El correo incluye un saludo genérico. Además, está escrito con muchos fallos gramaticales y frases con poco sentido. También utiliza una dirección genérica en el campo "para".

- Solicitan información confidencial. Como regla general ninguna compañía u organismo te enviará un correo electrónico no solicitado por ti (como consecuencia de una solicitud tuya o un proceso que tu iniciaste), pidiéndote información confidencial.



De: Uk National Lottery <elena@rosstour.ru>
Para:
CC:
Asunto: Usted es un ganador
Mensaje | Notoficacion de premio.pdf (579 KB)

Se adjunta a la notificacion de premio.
El archivo adjunto es un archivo pdf seguro.

Gracias
Administracion

En el archivo adjunto (se muestra en la imagen a continuación) se piden al destinatario todos los datos, incluidos los bancarios, con el señuelo de haber ganado la lotería.

PO Box 251WatfordWD18 9BR
London, United Kingdom.

The National Lottery

From: International Award Dept.
Reference Number: GTC1/2551256003/09
Batch Number: BC-00067/5808 31-03- 2015

PREMIO ASEGURADO

Tenemos el inmenso placer de informarle hoy día 30 Marzo de Diciembre. 2015, el resultado de las promociones de loterías "Uk National Lottery llevado a cabo el día 31 de Marzo 2015. Su nombre con su email ha sido premiado adjunto al boleto: 026-9-2 con número de serie: 7-8 mostró el número afortunado De Remesa: 1-8-3. En consecuencia, ganador de la lotería en tercera categoría. Por lo tanto, a usted le ha correspondido un premio de €915.000,00 euros (Novecientos QUINCE MIL EUROS) en efectivo. El número de referencia de archivo para reclamar su premio es: GTC1/2551256003/09. El premio total en efectivo es €19.733.910 euros (DIECINUEVE MILLONES SETECIENTOS TREINTA Y TRES MIL NOVECIENTOS DIEZ EUROS). Compartido entre varios ganadores a diferente escala internacional en esta categoría 3. Felicitaciones!

Todos los participantes han sido seleccionados a través de un sistema informático, llevado a cabo anualmente. En este momento, su dinero se encuentra depositado en una cuenta provisoria a su nombre, bajo un seguro que nuestra empresa ha puesto a su dinero para tenerlo asegurado. Para mayor seguridad, le pedimos guarde bien esta documentación, ya que aquí figura su número de referencia y cualquier persona que posea estos datos podría reclamar el dinero en su nombre.

Para comenzar su demanda, debe ponerse en contacto con el número de teléfono que aquí le indicamos, y su agente le informara el procedimiento para el cobro correspondiente a su dinero. Teléfono: +44-708-7625569 Fax: +44-203-163-8652 Email: birminghamlawyers@legislator.com (BIRMIGHAM LAW FIRM LLP) Persona responsable de asesoramiento: MR ADAMS WRIGHT

NOTA: Todo premio debe ser reclamado antes de 07 de Junio de 2015. Después de esta fecha, los fondos serán devueltos al MINISTERIO DE ECONOMIA como no reclamado.

RELLENE EL FORMULARIO Y ENVIARLO POR EMAIL AL TU AGENCIAS JUNTO CON TU PHOTOCOPIA DE TU DNI. ENVIALO A birminghamlawyers@legislator.com

NOMBRE DE BENEFICIARO.....FETCH DE NASCIMIENTO.....Importe obtenido:.....

DIRECION.....REFERENCE NO.....BATCH NO.....

PAIS:.....CUIDA:.....CODIGO POSTAL:.....

TELEFONO:.....NUMERO DE FAX:.....MOBILE:.....

EMAIL:.....OCUPACION:.....

Opciones de pago

(1) Transferencia bancaria ☐ (2) Talon ☐

NOMBRE DE BANCO:.....NUMERO DE CUENTA:.....

SWIFT CODE:..... DIRECION DEL BANNCO:.....

TEL DEL BANCO:.....FAX:.....

También quede informado que el 5% (cinco por ciento) del premio que obtiene pertenece BIRMIGHAM LAW FIRM LLP Porcentaje que será remitido después de que usted haya recibido su correspondiente cantidad, en un plazo máximo de siete días.

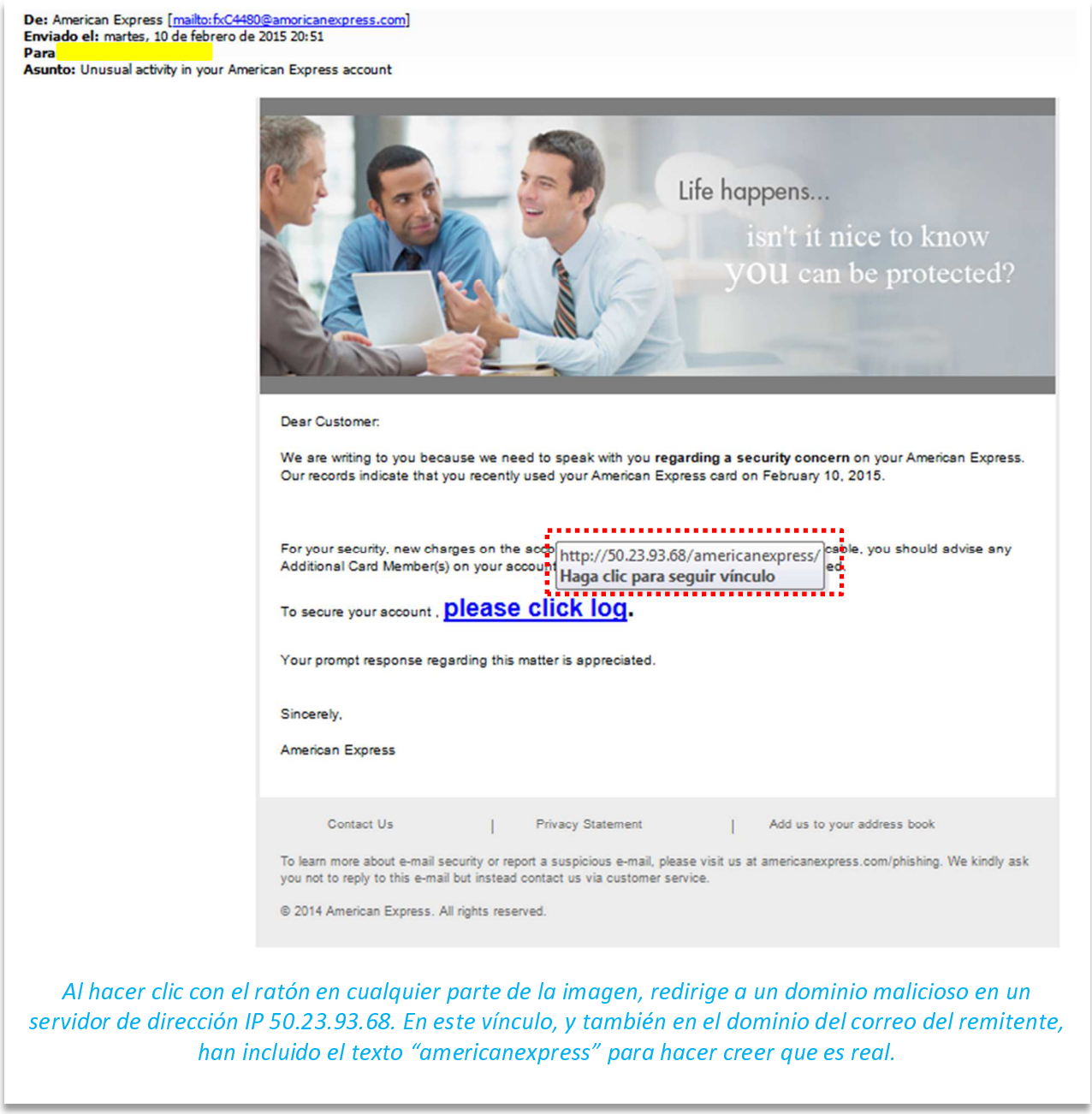
Dr.DouglasPeterside
Presidente

BIRMIGHAM LAW FRIM LLP
EL BUFETE DE ABOGADOS
UNITED KINGDOM

- El dominio del remitente del correo electrónico no se corresponde con el dominio esperado. El dominio de una dirección de correo electrónico es la parte que aparece a continuación del símbolo @. Por ejemplo, en el caso de una dirección de correo electrónico de EMASESA sería "emasesa.com". Si este dominio no se corresponde con la compañía que en teoría está enviando el correo, debemos sospechar que se trata de un fraude.

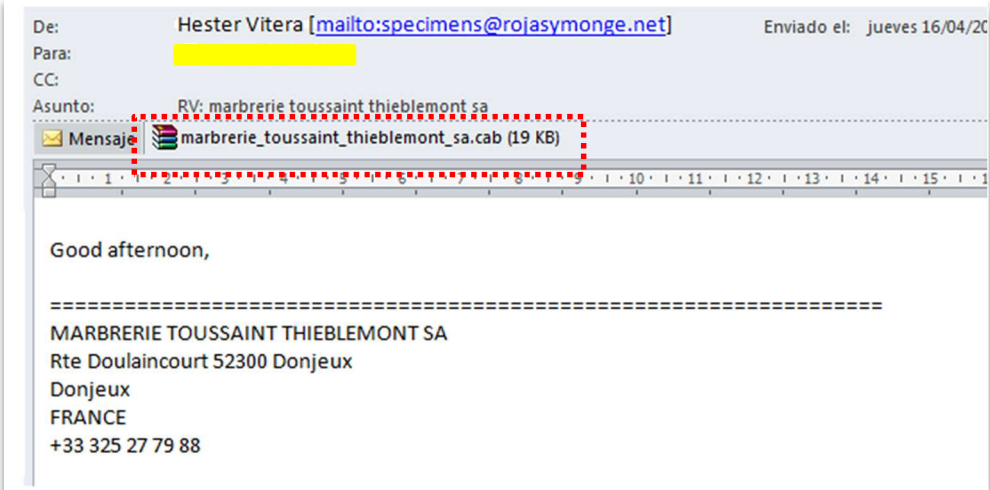
Con el señuelo de un vale para Mercadona, al pasar el ratón sobre el enlace sin hacer clic en él, se puede observar que redirige a una web maliciosa de dominio "bestcareeradvise.com"

- Otra técnica también utilizada y aún más peligrosa, consiste en incluir imágenes con enlaces; en este caso, **el correo es en su totalidad es una imagen y si haces clic sobre ella** (en cualquier parte del cuerpo del correo), voluntaria o involuntariamente, **se abre un enlace fraudulento**. Si esto te ocurriera, cierra inmediatamente la ventana o pestaña que se abra en el navegador.



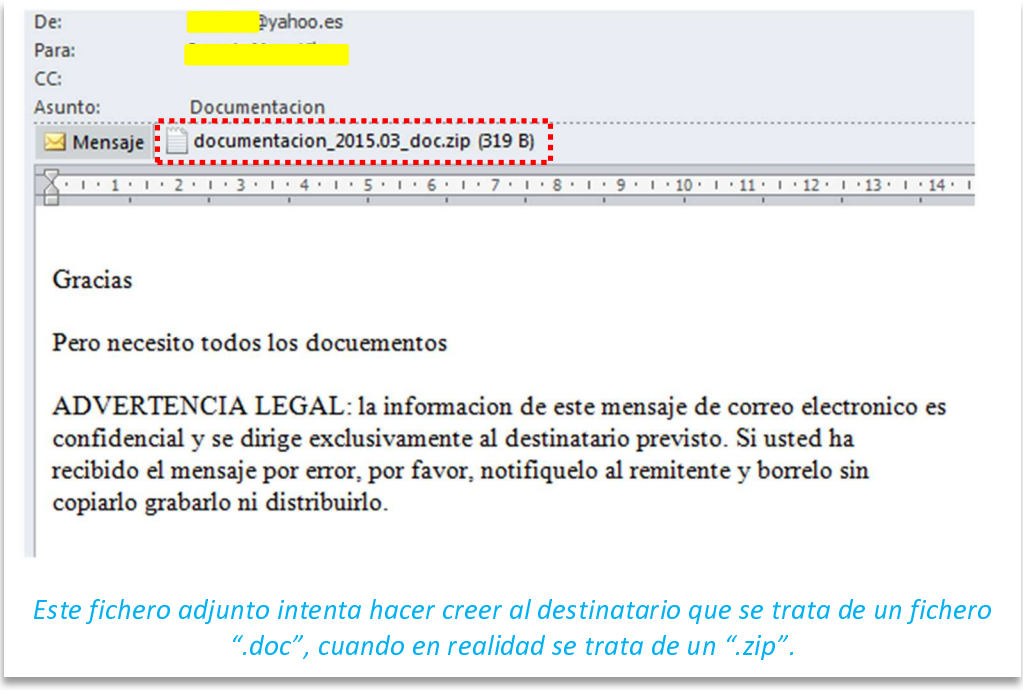
Al hacer clic con el ratón en cualquier parte de la imagen, redirige a un dominio malicioso en un servidor de dirección IP 50.23.93.68. En este vínculo, y también en el dominio del correo del remitente, han incluido el texto "americanexpress" para hacer creer que es real.

- Incluye archivos adjuntos que pueden ejecutarse como por ejemplo extensiones del tipo ".bat", ".cmd", ".exe", ".lnk", ".cab", ".msi", ".html" y otras muchas. Como norma general, **cualquier adjunto que venga de un remitente desconocido o que no esperamos, no debe abrirse**. Siempre cabe la opción, en caso de duda, de consultar al remitente para comprobar la veracidad del envío, por ejemplo mediante teléfono.



Se trata de un fichero con malware en un formato "cab". Viene en inglés, de un destinatario desconocido…

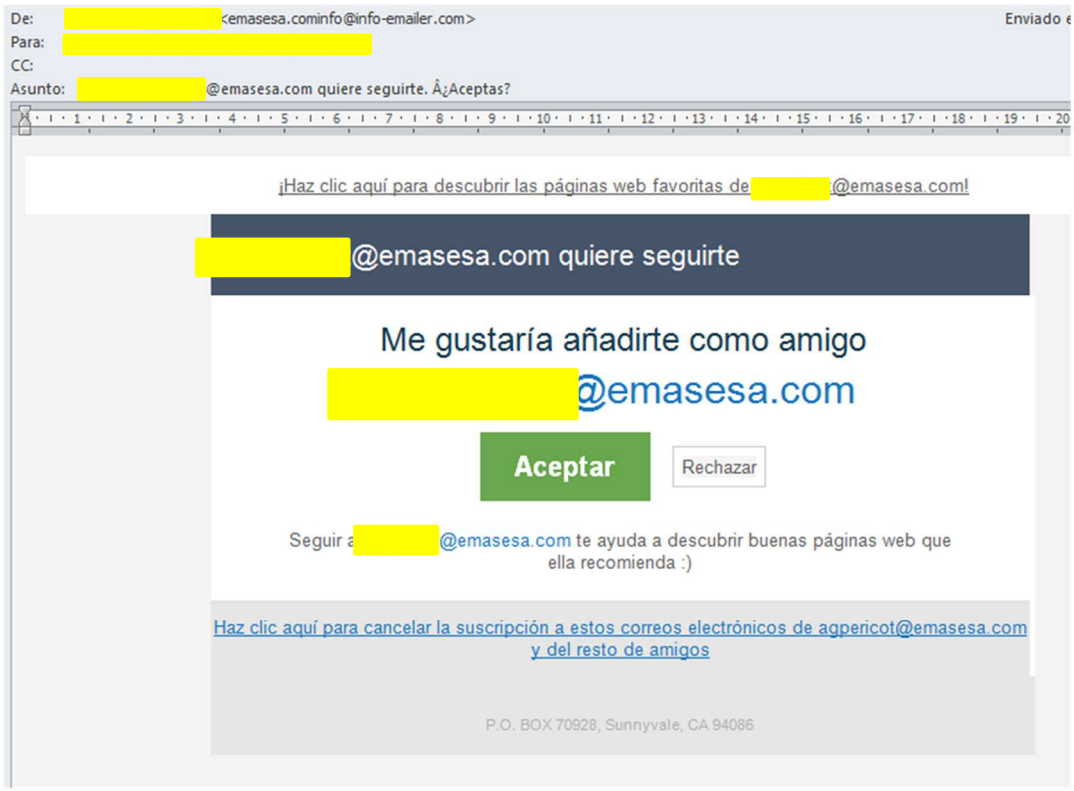
- Una técnica habitualmente utilizada es incluir ficheros adjuntos con doble extensión, o que en el propio nombre del archivo incluya una extensión para tratar de engañarnos.



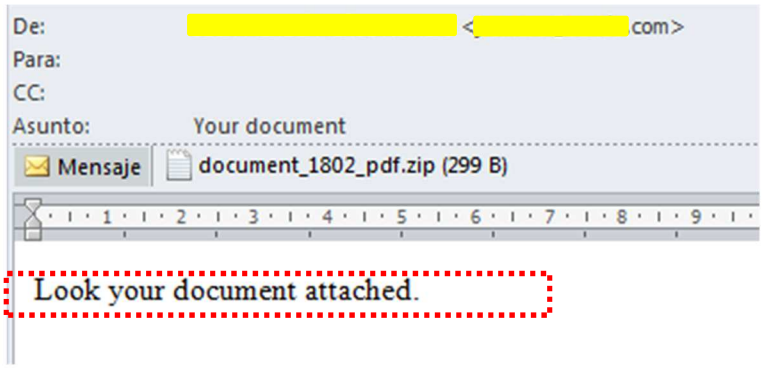
Este fichero adjunto intenta hacer creer al destinatario que se trata de un fichero ".doc", cuando en realidad se trata de un ".zip".

- En ocasiones se incluyen direcciones de correo de personas conocidas, para ganar nuestra confianza, pero normalmente no su nombre y apellidos ya que es más complicado que los delincuentes informáticos se hayan hecho con esta

información (aunque no imposible, como vimos anteriormente con el ejemplo del "virus de correos"). En muchas ocasiones aparecen en correos de petición de amistad o incorporación a redes sociales que normalmente se utilizan para robar la lista de contactos y seguir obteniendo información o distribuyendo malware entre éstos. Es conveniente avisar al remitente de que está enviando este tipo de correos.



¡¡Cada recuadro amarillo oculta el correo electrónico de un remitente conocido por le destinatario!!. Cualquier enlace sobre el que se haga clic ("Aceptar", "Rechazar", "Haz click aquí..", etc.) provoca el robo de la lista de contactos de este.

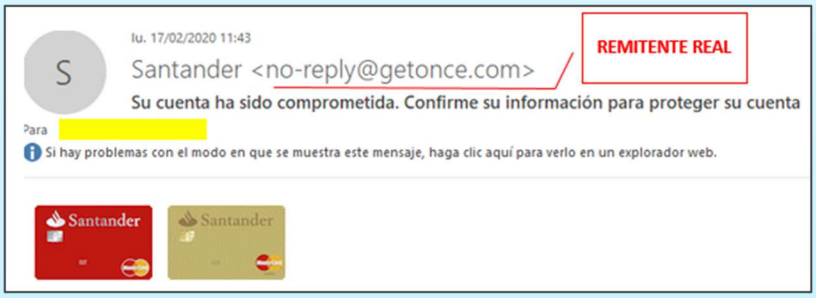


En este caso, un remitente conocido que es español, … y que escribe en inglés… invitándo a abrir el fichero adjunto

Y por último recuerda...

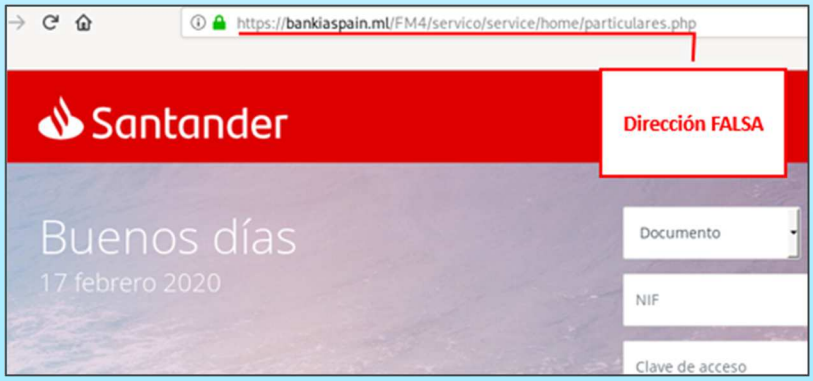
- **Evita abrir correos** de usuarios **desconocidos** y tampoco los contestes.

- Antes de abrir cualquier fichero adjunto a un correo o acceder a un enlace, **aunque aparentemente sea de un remitente conocido**, asegúrate de quién es el REMITENTE REAL, y que **este es de confianza**. Comprueba si el asunto del correo se corresponde con lo que esperarías de ese remitente, si estás esperando recibir ese correo o si el remitente se dirige a ti en los términos habituales. Si tienes dudas, ponte en contacto telefónico con el remitente para comprobar la veracidad del correo o consúltanos.



- **Sospecha siempre de los correos de remitentes que te apremian o urgen a hacer algo**; en muchas ocasiones los ciberdelincuentes tratan de engañar utilizando como señuelo el envío de facturas, notificaciones, premios, requerimientos legales, etc.

- Si crees que un remitente es fiable y llegas a **abrir un enlace** del correo electrónico recibido, **fíjate bien en la dirección de la página web a la que te redirige** y asegúrate de que: **1.- es correcta, 2.- está bien escrita y 3.- es de confianza**. Ten presente que el **"candado verde" o "candado cerrado"** que aparece en el navegador, es una **condición necesaria**, pero **no es suficiente** para garantizar la fiabilidad de una página web.



- **Nunca facilites información personal sensible a través de correo electrónico** (datos personales, credenciales, número de cuenta bancaria, etc.); ninguna entidad seria te solicitará este tipo de información mediante un correo electrónico.