



COMO DETECTAR SPAM Y COMO ACTUAR PARA PROTEGERTE

En la actualidad, el robo, secuestro de nuestros datos y contraseñas, junto a la llamada “suplantación de identidad” o PISHING en su denominación en inglés, es posiblemente la mayor amenaza que sufrimos los usuarios con acceso a tecnología conectada.

“Conectada” a internet, a redes sociales, a plataformas de mensajería y comunicación, siendo estas últimas, la mayor fuente de accesibilidad para los delincuentes informáticos y sus trampas.

El virus con mayor capacidad destructiva y de propagación es de formato **Ransomware**: El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales después de encriptarlos y que exige el pago de un rescate para poder acceder de nuevo a ellos. Hoy en día los creadores de ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito. Su última mutación conocida, no solo encripta los datos, sino que además modifica el registro del sistema y los vectores de los discos duros físicos, volúmenes virtuales y lógicos destruyéndolos, dejando inútil la opción de recuperar los datos mediante backups o reconstrucción de los discos o volúmenes.

¿Cómo podemos infectarnos?

De los mil y un medios o formas vamos a mencionar las más comunes:

- Por correo electrónico (Spam)
- Por introducir dispositivos USB que no son de confianza
- Por abrir enlaces fraudulentos desde los dispositivos móviles

¿Cómo detectar el spam?

Remitente no corresponde con el servicio que envía el correo

Nada más abrir un mensaje, lo primero que debemos observar es la dirección desde la que se ha enviado el mensaje. En la mayoría de las ocasiones, los ciberdelincuentes utilizan la imagen de un servicio conocido para engañar a los usuarios. Hay que cerciorarse de que esta dirección corresponde con la legítima del servicio. Sin embargo, en muchas ocasiones nos podemos encontrar con que esto no es así. Por ejemplo, en un mensaje cuya imagen es de CORREOS DE ESPAÑA, nos encontramos una dirección del tipo **soporte.correos@correos.es**. Ese sería un ejemplo de dirección falsa.

Adjuntamos imagen de un correo fraudulento.



mantenimiento informático



ju. 19/12/2019 11:42

CorreosPaq <[redacted]@correos.es>

Recepción de paquete PM427V07001554401080265

Para [redacted]

En caso de que no veas correctamente este email [pulsa aquí](#)



Hola,

Gracias por utilizar CorreosPaq, le informamos que ha recibido su paquete con identificador **PM427V*****080265**.

Le pedimos que confirme su pago de: 1.17 euros para la validación de su paquet

[haga clic aquí](#)

* Puedes utilizar el código promocional tanto en el ordenador como en la app. Válido hasta el 31 de agosto de 2019 a las 23:59 h. Solo un código por usuario. Promoción limitada a 5.000 cupones. Código promocional de 4\$ de descuento con cantidad mínima compra de 20\$.

correos.es

El responsable de este tratamiento es Sociedad Estatal Correos y Telégrafos, S.A., S.M.E ("Correos"). El envío de esta comunicación se produce por haber solicitado previamente su envío o haber prestado su consentimiento en el proceso de contratación de alguno de nuestros servicios. No obstante, si en adelante no quiere recibir nuevas comunicaciones comerciales le rogamos envíe un correo electrónico con el Asunto "Baja" a la dirección derechos_protected@correos.com o envíe una notificación postal a la dirección Vía Dublín no 7 (Campo de las Naciones) 28070 Madrid (España). También puede utilizar estas direcciones para ejercitar el resto de derechos reconocidos en nuestra normativa.

Para dar de recibir comunicaciones de correo haga clic [aquí](#)

CORREOS | Calle Vía de Dublín, 7 | Madrid | 28042

Hay que tomar en cuenta 3 reglas básicas del hacking ético, para identificar estos correos:

1. Si no estamos esperando ningún tipo de información, datos, o paquetería, debemos sospechar. NI CORREOS, NI LAS EMPRESAS ELCTRICAS, NI BANCOS, NI NINGUNA INSTITUCIÓN SERIA envía nada sin informar al destinatario.
2. Hay que revisar el nombre del remitente y verificar que cuenta es la que envía el mail. Por ejemplo:

De: Banco Santander <KE.RO15468745@KE.LEO.COM>
Para: info@netkia.es



Hola,
Deseamos informarle de que tiene una nueva actualización.
Verifique su cuenta haciendo clic el siguiente enlace:

[Revisa tu cuenta aquí](#)

Gracias a no responder a este mensaje, usted no tendrá que responde
Por favor, use nuestra sección "Contacto" en nuestra página web

Atentamente,
Banco Santander



mantenimiento informático



Your photo has been rated

Facebook Updates (fong.leong.lim@cannadal.es) [Agregar a contactos](#) 04/05/2013
 Para: [redacted]@hotmail.com

De: Facebook Updates (fong.leong.lim@cannadal.es)
 Enviado: sábado, 04 de mayo de 2013 1:14:34
 Para: [redacted]@hotmail.com

facebook

You have new notifications.

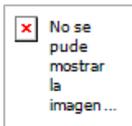
Your photo has been rated.

[See All Notifications](#) [Go to Facebook](#)

This message was sent to ruth_soleada@hotmail.com. If you don't want to receive these emails from Facebook in the future, please click: [unsubscribe](#).
 Facebook, Inc. Attention: Department 415 P.O Box 10005 Palo Alto CA 94303

3. Ninguna empresa o plataforma debería pedir que valides tus claves o datos mediante enlace por correo electrónico. Un ejemplo de este tipo de trampas por mail sería este.

De: Servicio Clientes Apple <noreply6100587@credem.it>
 Fecha: 15 de diciembre de 2015, 11:03:01 CET
 Para: [redacted]
 Asunto: COMUNICACION URGENTE 6100587



Estimado cliente de iCloud, [\[redacted\]@icloud.com](#)

Este es un mensaje automatico enviado por nuestro sistema de seguridad para hacerle saber que usted tiene 48 horas para confirmar su informacion de cuenta
 Su cuenta de iCloud se ha congelado temporalmente para validar su informacion . .
 Una vez que haya actualizado sus registros de cuentas, vamos a tratar de nuevo para validar la informacion y la suspension de su cuenta sera levantado. .
 Esto ayudara a proteger su cuenta en el futuro. Este proceso no toma mas de 3 minutos.
 Para proceder a confirmar los datos de su cuenta, por favor haz clic en el enlace a continuacion y siga las instrucciones..

[Haga clic aqui validar su cuenta](#)





mantenimiento
informático



Gramática con fallos

Muchos ciberdelincuentes buscan maximizar las estafas. Por este motivo, reaprovechan el mensaje para diferentes localizaciones. Teniendo en cuenta para estas tareas se utilizan traductores, o que el ciberdelincuente confíe en su pericia traduciendo el texto, lo más probable es que nos encontremos con faltas de ortografía, incoherencias gramaticales, ... Este sería un buen momento para proceder al borrado el mensaje si la dirección no ha servido como criba.

De: [REDACTED]@yahoo.com>

Enviado: viernes, 7 de diciembre de 2018 13:28

Para: [REDACTED]

Asunto: id k37jLidln

Saludos Codriales mi rico bandido.

Somos bosses del gueco grave que tu antes visitaste. Esto pasa! Usted no es ni unico ni mas pendejo! Vacilando en nuestro pagina su computadora se prendio el nuestro virus.

Que barbaridad... El troyan guarda toditito que se produces en systema igual con los cookies.

Pero mas trampa es que mi malware se abre su web cam y transpasa toditos los personas de su mail. Ahoritita yo tengo puerta a su mail tambien con absolutamente todos paginas tuyos.

Hoy dia!!! Nosotros tenemos los datos donde tu estas desnudo y estas haciendo la paja.

Si vos no quiere que yo paso estos cosas sucias a su familia, chamos, colegas del estudio y colegas del trabajo, aparecen en internet, en paginas mas populares y buenos de la red como un meme yo trato propuestar el mi resolucion y salida salida de su problema.

Tu pasas 499 eur a mi crypto billetera btc 19Uu4Qm1pZNGCesgQtJGjwWZAKY4dzoWiz Despues de ahorrar su btc y en mismo momento quemamos todos los files contra de su personalidad y tu nunca mas escucharas de los datos alguna vez. En el reverse, si yo no confirmo su crypto monedas terminando un dia del momento que esta letra esta leida yo derijo todititos sus interesantes datos compromatos a sus familiares, compas, colegas de la escuela y colegas laborales. Ademas de esto yo voy elaborar un meme gif de su foto y voy llenar el internet con su rostro. No contesta a esta correo.

Si necesita 48 horas sólo responder a esta carta con+.

Esto mail nunca mas sera usado una vez mas.



mantenimiento
informático



URLs falsas camufladas en hipervínculos

Se trata de una práctica habitual. Se informa al usuario de un problema con la cuenta de un servicio y se le invita a acceder a la página web para iniciar sesión. En estos casos, los ciberdelincuentes nunca dejan al descubierto la dirección URL de la página, ya que no se encuentra en el dominio del servicio cuya imagen ha sido utilizada en el mensaje spam. Si el usuario se siente tentado de acceder, debe confirmar que la URL pertenece al servicio. De no ser así, no se debe introducir nunca información en el formulario. La finalidad de este no es otra que recopilar la información, enviada a servidores propiedad de los ciberdelincuentes.

Una de las plataformas más usadas para el engaño es Apple, pero también podemos encontrarnos encabezados de DROPBOX, GMAIL, BANCOS, ETC.

Re: [Security Patch] [e-Mail Receipt] Statement was submitted to reset your password [Attention] - 1 November 2019. Ticket ID: 71180264.

Apple ID Locked

Your Apple ID has been Locked
for security reasons. November, 2 2019 PDT , To unlock it, you
must verify your identity.

You cannot access your account and any Apple Services, Before
completing verification, and you have to completing verification
before 12 hours or your account will be permanently Locked.

Unlock Account



mantenimiento informático

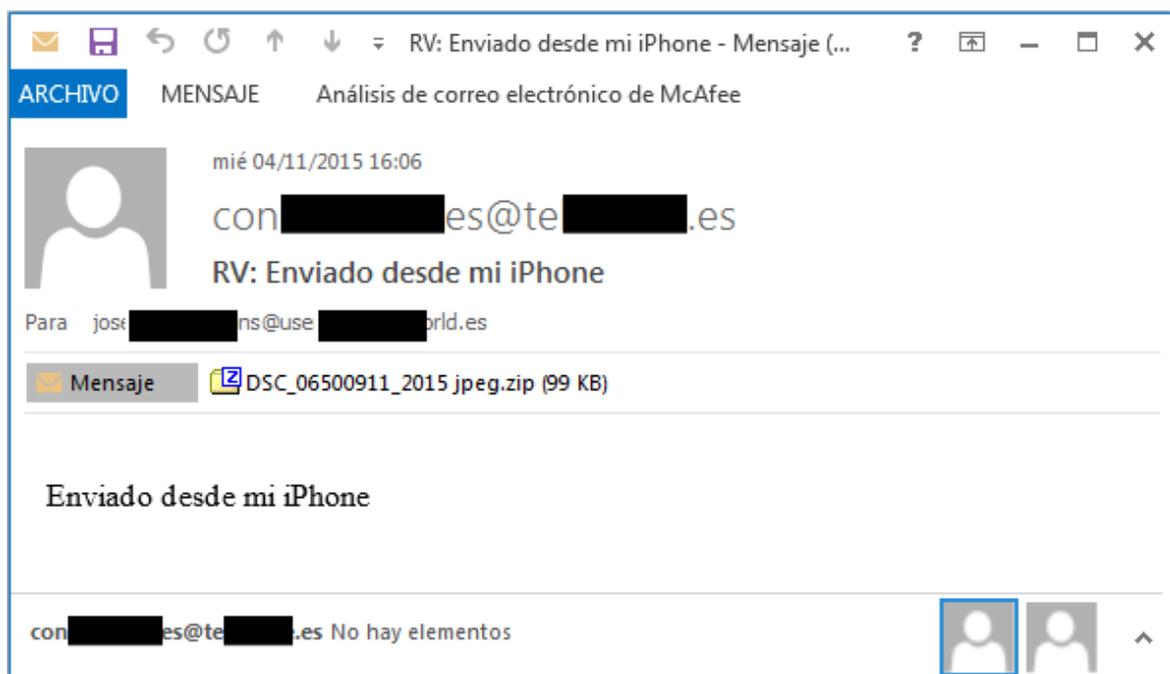


Archivos adjuntos que no son lo que parecen

En muchas ocasiones, sobre todo si se quiere instalar malware en el equipo del usuario, los ciberdelincuentes adjuntan documentos que a priori son Word o PDF comprimidos. Si cuando realicemos la descompresión del archivo lo que aparece es un .exe, la acción siguiente a realizar será el borrado de este y del correo. Además, hay que fijarnos en el nombre del adjunto, en la gran mayoría de ocasiones, los nombres de estos archivos llevan símbolos raros o nombres que nada tienen que ver con el asunto del mail.

Pero esta no es la única vía, si es cierto y se descarga un Word o un Libro de Excel, hay que prestar atención a las macros. Por defecto no están activadas. Si se solicita su activación para visualizar de forma correcta el documento, se debe pensar mal y cancelar su apertura y borrado inmediato.

Un ejemplo de esto, puede ser el que se muestra a continuación:





mantenimiento
informático



Correo de un servicio que no has utilizado o no contratado

Es el más evidente. Si recibes un mensaje reclamando una cantidad o adjuntando un documento de un servicio que no utilizas, existen dos opciones: que una persona se haya equivocado de correo y haya ofrecido por error tu dirección (algo que no acostumbra a ser lo habitual) o se trata de una estafa enviada de forma masiva. Es probable que, de entre todos los usuarios a los que se les ha enviado el mensaje, un porcentaje no sea cliente de ese servicio. En ese caso, el borrado debería ser automático.

A continuación algunos ejemplos que podemos ver a diario.



Estimado cliente:

Ante las noticias surgidas en los últimos días relativas al incremento de los precios de la luz, queremos informarle de que un cliente medio en el PVPC, Precio Voluntario para el Pequeño Consumidor (modalidad que tiene usted contratada), tendrá una factura de enero 3,3€ mayor que la que resultaría con precios de diciembre.

Consulte [aquí](#) para conocer todos los detalles relacionados con el PVPC.

Si necesita cualquier aclaración puede contactar con nosotros en [@Tulberdrola](#), en [Facebook.com/IberdrolaClientes](#), en el Teléfono **900 225 235** o en cualquiera de nuestros **Puntos de Atención**.

Un cordial saludo.

Iberdrola

Fwd: Importante



SANTANDER <sales-santander@xtra.co.nz>
Hoy, 19:44
santander2018@gmail.com

Responder | v



Estimado cliente,

Lamentamos informarle que hemos bloqueado su tarjeta de crédito para su propia protección. Este procedimiento de seguridad entró en vigencia porque aún no ha confirmado su tarjeta de crédito.

Para que podamos continuar proporcionándole un servicio de pago seguro, se requiere la verificación de su tarjeta de crédito. Inicie la confirmación a través del botón de abajo, no habrá ningún cargo por usted. De lo contrario, tendremos que confirmar la entrega por correo postal dentro de los 14 días hábiles. Esto está asociado con una tarifa de procesamiento de 8.40 EUR, que luego se deduce de su cuenta

[Continuar con la actualización.](#)



mantenimiento
informático

Recomendaciones de seguridad.



Algunas de las formas de prevención, las hemos enumerado en cada apartado anteriormente mencionado.

Sin embargo, os dejamos un breve resumen de acciones simples y sencillas que pueden ayudarnos a diario a evitar ser víctimas de ataques informáticos.

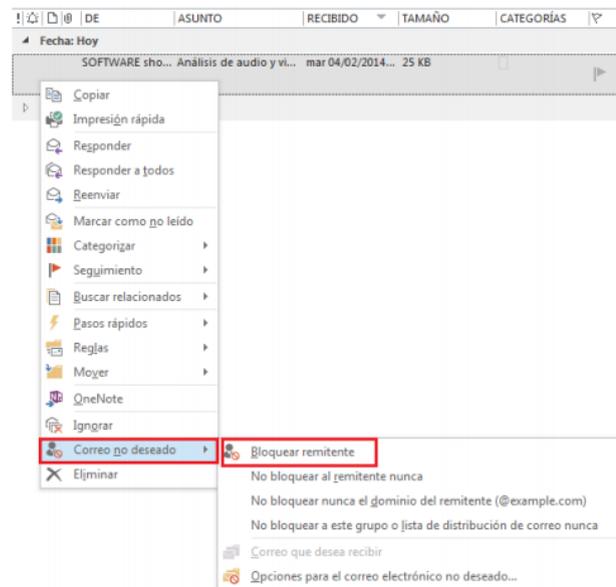
1. Si se duda del nombre o contenido de un correo. Marcarlo como Spam y eliminarlo.

Abre la bandeja.

Pasa el puntero sobre el correo que quieras marcar como spam.

Marca la casilla que aparece a su izquierda.

En la zona superior, selecciona Correo no deseado.



2. NUNCA ENVIES USUARIO O CONTRASEÑAS DE TUS ACCESOS POR MAIL
3. Recuerda que nunca debes actualizar, o recuperar tus datos bancarios o de tus cuentas de correo mediante enlaces incrustados en tu mail.
4. Recuerda que si no usas un producto o servicio es siempre falso.
5. Recuerda que muchos correos fraudulentos son prácticamente idénticos a los originales, pero fíjate en su dirección, en su dominio y sobre todo verificar su autenticidad por otros medios. Por ejemplo, mediante una llamada.
6. Si tienes un departamento informático, no dudes en pasarles la consulta inmediatamente, para que verifiquen su peligrosidad y realicen acciones de prevención.
7. Nunca abras enlaces de los que no estas seguro su procedencia o contenido.
8. Recuerda nadie te va a regalar nada por mail, Ni eres el afortunado ganador de un iPhone o un Ferrari.
9. Los correos que contienen texto con traducciones erróneas son directamente sospechosos.
10. SI NO USAS UN SERVICIO O PRODUCTO NO ENTRES A VERIFICAR TUS FACTURAS, NO LOS USAS POR LO TANTO ES FALSO.