No abras ese correo: qué hacer ante un mail sospechoso

Hay correos electrónicos que pueden infectar y secuestrar tu PC. Otros intentan robar información confidencial a través del engaño. Y unos cuantos intentan usar tu buzón para multiplicarse y dañar otros ordenadores. Y es que la tentación de abrir cualquier correo es muy alta, especialmente si parece misterioso o importante. Asociamos el correo a personas de confianza, a mensajes urgentes que no suelen ir a través de otros canales menos “serios”. Para evitar infecciones dañinas y de consecuencias desastrosas para tu bolsillo, conviene que resistas el impulso de abrir todo lo que entre en tu buzón de correo. Sigue los consejos que enumero a continuación.

1. ¡Si no has solicitado nada, no hagas clic!

Es una regla de oro: si no has solicitado nada a una persona o una empresa, esta no tiene por qué enviarte instrucciones de ningún tipo, ni mucho menos archivos adjuntos. ¿Por qué debería hacerlo? Empresas e instituciones usan el correo solo para informar, a menos que tú pidas algo, como una nueva clave, o hayas iniciado una gestión que contempla el envío de un correo de confirmación o una copia de alguna transacción Cuando te llega un mensaje y no consigas reconducirlo a una conversación previa con la persona o empresa indicada en el correo, empieza a desconfiar. Hazte estas preguntas:

¿Qué tengo que ver yo con este mensaje?

¿Por qué me han enviado este correo ahora?

¿Tiene razón de ser lo que me están pidiendo?

Si no consigues contestar esas preguntas, **no hagas clic** en ningún enlace ni archivo adjunto del correo en cuestión, al menos no hasta haber recabado más información sobre el mismo. Lo que nos lleva a los siguientes puntos.

2. ¿Texto sospechoso? Búscalo en Google

Los mails con estafas o malware **suelen tener siempre el mismo texto**, a veces con ligeras variaciones. Sus características son fáciles de reconocer, sobre todo si las comparas con las comunicaciones de una empresa real:

- **Frases incomprensibles y palabras extranjeras,** debidas al uso de un traductor automático: muchos hackers operan desde países donde la ley no puede actuar

- **Errores ortográficos e incoherencias en el texto**, como si fuera un corta-y-pega apresurado: la mayoría de criminales informáticos tienen prisa y saben generalmente poco de diseño y ortografía
- **Imágenes mal encajadas o en baja resolución**: han intentado darle una pátina de oficialidad a su correo, pero han tenido que recurrir a imágenes de segunda mano
- **Falta de referencias a tu persona**: no se usan tus nombres y apellidos ni otros datos que solo una empresa puede conocer, lo que hace que los mensajes tengan un aspecto de plantilla sin rellenar
- **Sentido de urgencia:** los textos son casi siempre alarmistas y apelan a la emoción más visceral de todas, el miedo. Se hace mención a consecuencias temibles, asuntos de dinero o posibles multas

Copia y pega las frases más extrañas en un buscador y mira bien los resultados: podrás comprobar de primera mano si estás ante un correo legítimo o un posible intento de estafa.


PROCEDIMENTO INVESTIGATÓRIO N.º 498.613/2013 FECHA

GOBIERNO DE ESPAÑA · MINISTERIO DEL INTERIOR

DIRECCIÓN GENERAL DE LA POLICÍA

CUERPO NACIONAL DE POLICÍA

19/06/201

Assunto:NOTIFICACIÓN DE ASISTENCIA EN LA AUDIENCIA en el procedimiento de investigación de que se trata en esta conducta regional
Para que se adjunta. com el documiento anexo. Procediemento de esclareciemiento anti drogas.

1 ANEXO: NOTIFICACIÓN-MPF.SCR (1306k)
PROCEDIMENTO INVESTIGATÓRIO N.º 498.613/2013 FECHA 19/06/2013

El nuevo mail engañoso que contiene el virus de la policía como adjunto

3. ¿Hay un archivo adjunto? Ni se te ocurra hacer doble-clic

Per se, el texto de un correo nunca es peligroso (a menos que se trate de un chiste muy malo). El auténtico peligro se esconde tras los enlaces y los archivos adjuntos. Estos últimos son los **responsables de casi todas las infecciones** por correo. Fíjate en la extensión del archivo adjunto. Las que deben ponerte en alerta roja son:

- Las extensiones ejecutables clásicas: **EXE, COM, BAT, PIF**
- Los documentos que pueden contener código: **PDF, DOC, XLS, PPT**
- Archivos de sistema ejecutables: **DLL, CPL, MSC, CMD**
- Instaladores y archivos comprimidos: **MSI, ZIP, CAB, RAR**
- Salvapantallas: **SCR** (¡son programas también!)
- Archivos con doble extensión (por ejemplo, **ARCHIVO.DOC.EXE**)

Los navegadores más seguros y las aplicaciones de correo más avanzadas suelen efectuar controles por ti -un ejemplo es Gmail-, pero nunca está de más pasar el archivo por un antivirus actualizado.

4. ¿Hay enlaces? Analízalos antes de hacer clic sobre ellos

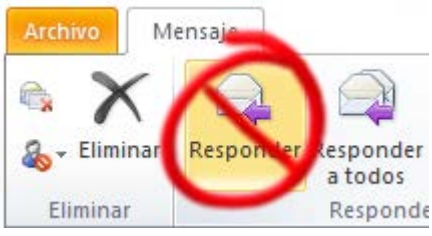
Otro método que los ciber-criminales usan para atraer a los incautos hacia las trampas son los enlaces falsos o enmascarados. Si estás ante un enlace en apariencia legítimo, pasa el puntero del ratón por encima para ver cuál es la dirección real:

La dirección real se ve al pasar el puntero del ratón

Los enlaces acortados son otra amenaza en potencia, puesto que impiden saber de antemano hacia dónde conducen. Normalmente, las empresas o instituciones no recurren a este tipo de enlaces en sus comunicaciones por correo electrónico.

Para desenmascarar un enlace acortado, puedes usar servicios como UnShorten, que además de desentrañar el enlace cifrado, te indica la reputación del enlace usando los datos de WOT, un conocido servicio de evaluación de sitios web. Si eres un usuario avanzado, puedes "diseccionar" el encabezado del mail para ver cuál es su auténtico origen, pero ten en cuenta que este método, amén de complejo, no siempre conduce a respuestas concluyentes.

5. No contestes nunca ni tampoco lo reenvíes



Contestar un correo sospechoso **proporciona datos valiosos al cibercriminal**. Para empezar, le dice que tu dirección de correo es real y que estás a la escucha, lo que aumenta en varios puntos su valoración en el mercado negro de direcciones. *No contestes nunca un mail sospechoso*

No le contestes, pues, pero tampoco lo reenvíes, puesto que vas a hacerle un favor a esos mismos piratas que te enviaron el correo al principio. Acabarías por generar una cadena de correo perniciosa.

6. En caso de duda, contacta a través de otro medio

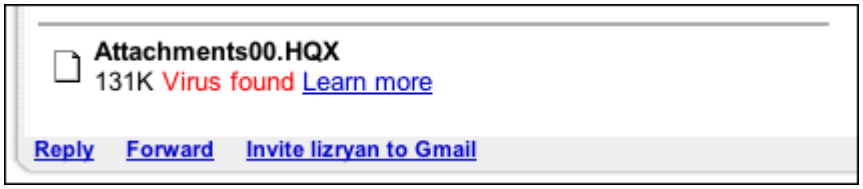
¿Sigues dudando acerca de la veracidad del correo que acabas de recibir? Ponle un freno a tus impulsos clicadores y piensa en otras formas de contactar a la persona o empresa que se hallan supuestamente detrás del mensaje.

- Si es una persona, llámala, ábrele un chat o envíale un SMS (pero no le envíes un correo)
- Si es una empresa, ve a su página web y contacta a través de su formulario oficial (o llámales)

Por supuesto, si se trata de un mail enviado por un conocido, no lo agredas: lo más probable es que no sepa de qué le estás hablando. Es posible que su buzón o dirección hayan sido suplantados o secuestrados para enviar correo fraudulento.

7. Usa un navegador seguro y lee tu correo a través del web

Los clientes de correo clásicos, como Outlook Express, son muy vulnerables ante todo tipo de ataques por correo. La única línea de defensa ante mensajes maliciosos que llegan a Outlook o Thunderbird es un buen antivirus con protección residente. ¿Nuestro consejo? Usar un cliente web (GMail, Hotmail, Yahoo! Mail, etc) en un navegador seguro (Chrome o Firefox).



Un virus detectado por Gmail, que impide bajarlo (imagen de AskDaveTaylor)

Lo primero asegura que el contenido del correo haya sido escaneado por los sistemas de seguridad usados por los proveedores de correo, mientras que lo segundo dificulta que el malware pueda llegar a tu ordenador.