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

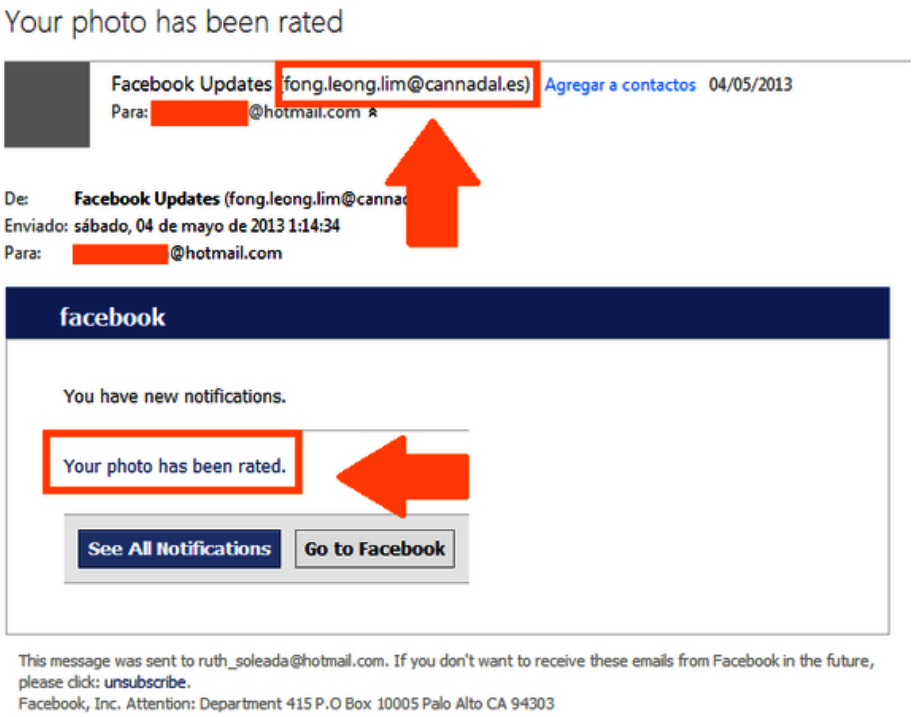
Nada más abrir un mensaje, lo primero que debemos observar en la dirección desde la que se ha enviado el mensaje. En la mayoría de las ocasiones, los ciberdelincuentes utilizan la imagen de un servicio conocido para engañar a los usuarios. Hay que cerciorarse de que esta dirección corresponde con la 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.

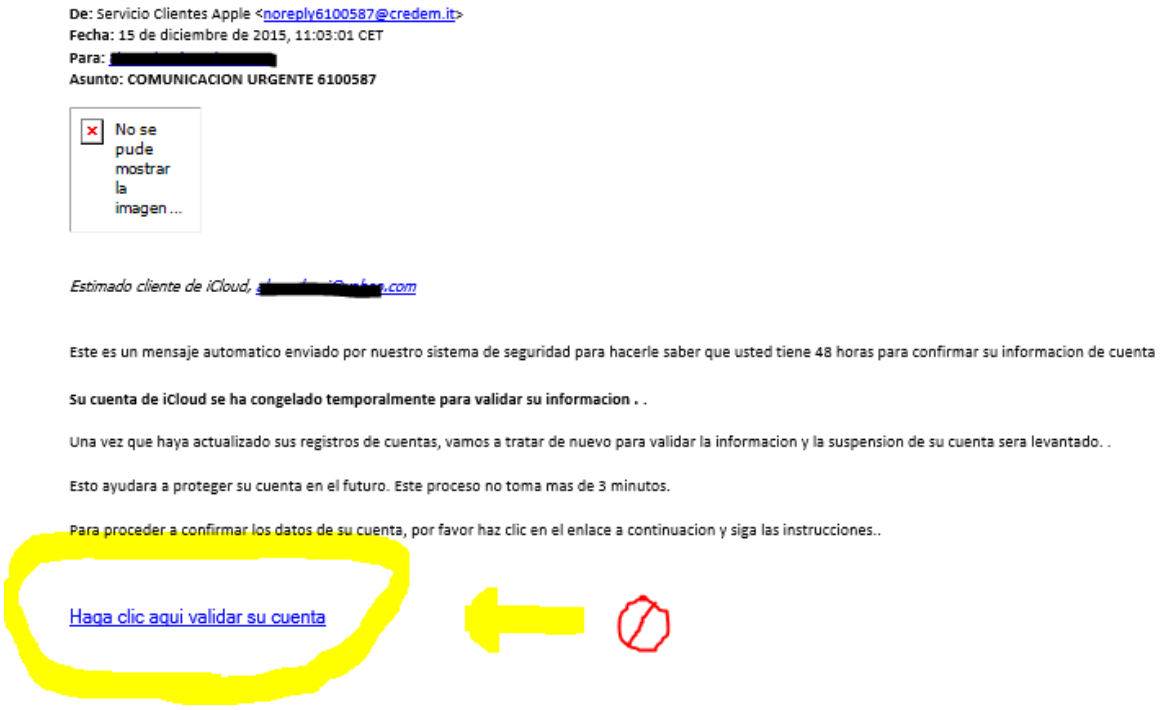
Hay que tomar en cuenta 3 reglas básicas del hacking ético, para identificar estos correos:

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:



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



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 absalutamente 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, collegas del estudio y collegas 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 quemo 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, collegas de la escuela y collegas 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.

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.

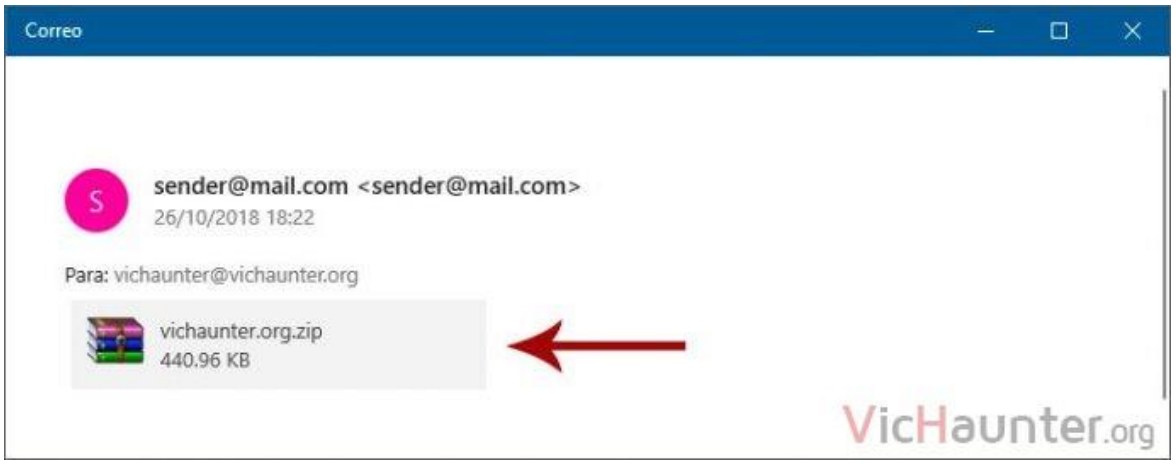
Una de las plataformas más usadas para el engaño es Apple, pero también podemos encontrarnos encabezados de DROPBOX, GMAIL, BANCOS, ETC.

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.

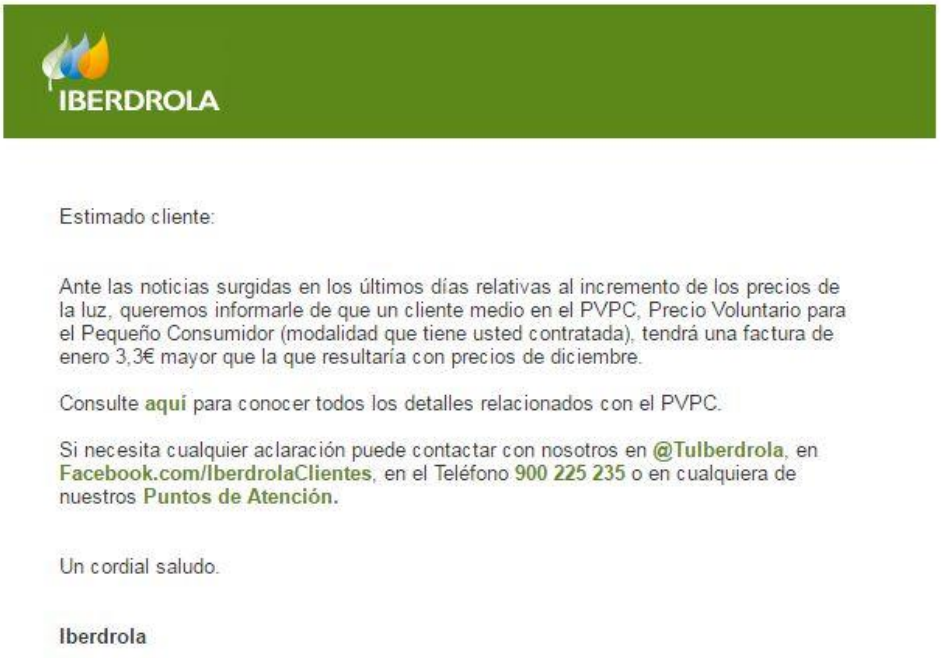
Un ejemplo de esto, pude ser el que se muestra a continuación:



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.



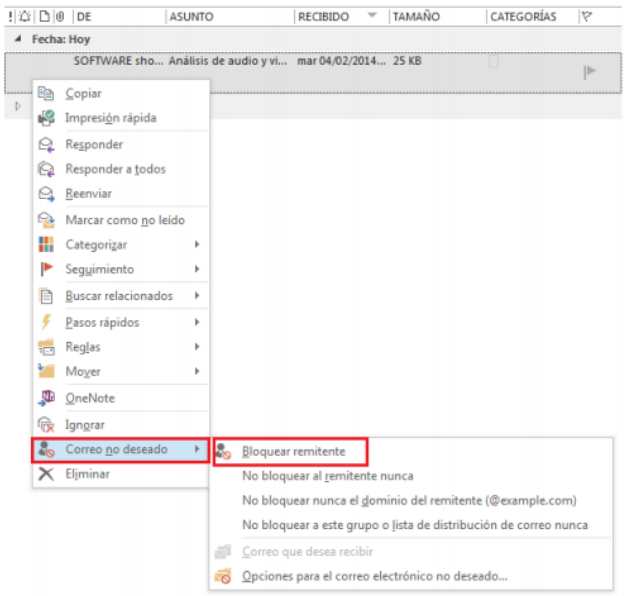
Recomendaciones de seguridad.

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 victimas 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.