Fraude en Internet para tontos: consejos prácticos para protegerte contra el fraude en Internet

26.11.2010 | **Comentar**

Darja Gudkova

El fraude en Internet prácticamente apareció junto con la red. Cada año los creadores maliciosos implementan nuevas técnicas y tácticas destinadas a engañar a sus potenciales víctimas. En este artículo analizaremos los diferentes tipos de fraudes y te aconsejaremos qué precauciones tomar.

Una particularidad que diferencia el fraude de otras amenazas que circulan en Internet, como virus, troyanos, programas espía, interceptores de SMSs, spam, etc., es que se trata de una persona real y no un ordenador el que manipula la estrategia. Esto significa que los creadores maliciosos tienen sus puntos débiles. Por otra parte es necesario tomar en cuenta que ningún programa ofrece una absoluta protección, y que los mismos usuarios deben adoptar una actitud proactiva para protegerse cuando navegan en la web.

No es la primera vez que tratamos los aspectos técnicos y los procedimientos característicos de los fraudes implementados por los ciberdelincuentes (puedes consultar nuestro anterior artículo). Es cierto que este tipo de información no es suficiente, por lo que en este artículo vamos a presentar algunas sencillas reglas que te ayudarán a evitar varias trampas en línea.

Los distintos tipos de fraudes

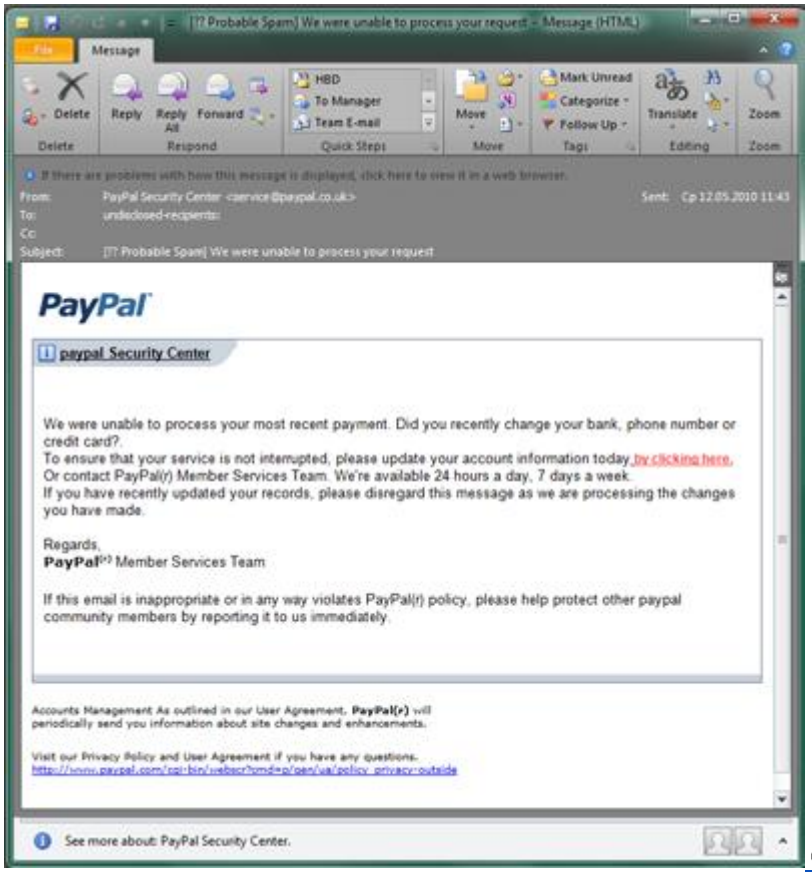
Robo de identidad o «phishing»

El correo phishing consta de mensajes fraudulentos supuestamente enviados por bancos, sistemas de pago en línea, proveedores de correo electrónico, redes sociales, juegos en línea, etc. El objetivo de estos mensajes es robar datos confidenciales del usuario, como nombres de usuario, contraseñas, etc. Los mensajes phishing bancarios se cuentan entre las tácticas más populares cuya intención es acceder a una cuenta bancaria en línea o a sistemas de pago electrónico. Cuando el ciberdelincuente logra capturar los datos confidenciales de un usuario, tiene la puerta abierta para acceder a todas sus cuentas.

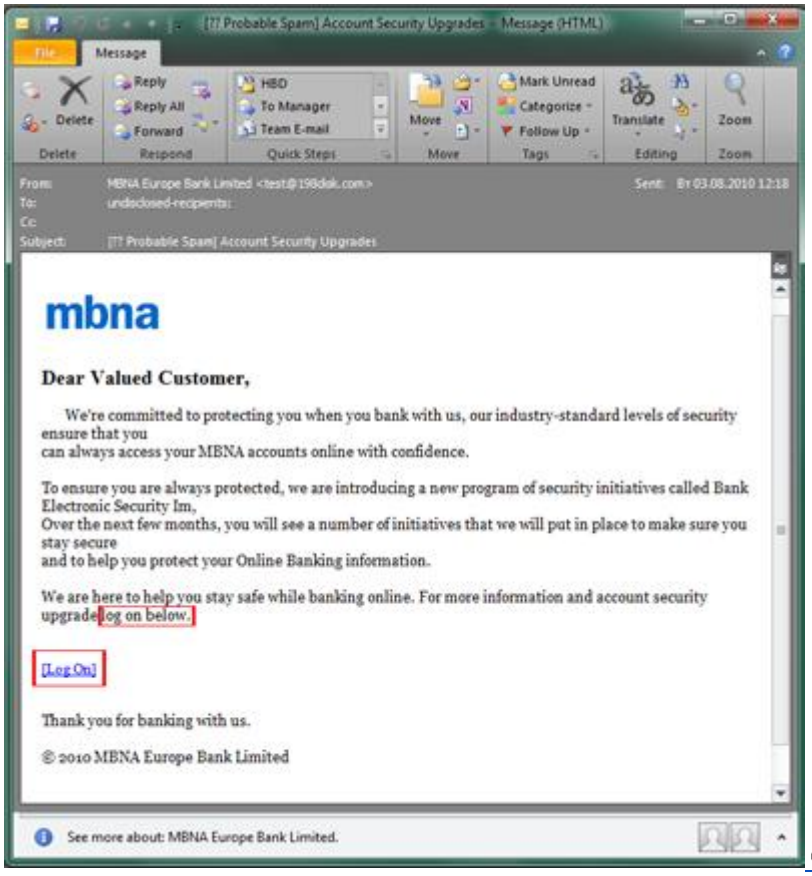
Los creadores de este tipo de fraude son expertos falsificadores y tienen la capacidad de crear mensajes corporativos o institucionales que parecen auténticos. Usan logotipos oficiales e imitan el estilo específico de la correspondencia oficial de una organización. Por lo general, el mensaje invita al destinatario a activar un enlace para robarle sus datos personales bajo la excusa de que la organización quiere mejorar la seguridad de su portal web y que es necesario que el usuario se comunique para completar la operación activando el enlace provisto: cuando lo hace, aparece en un sitio fraudulento que parece idéntico al sitio legítimo en el que se le solicita que introduzca sus datos de usuario. Sucede con mucha frecuencia que estos sitios fraudulentos contienen «exploits» que instalan programas espía en el ordenador de la víctima. Aunque el usuario ni siquiera se identifique, bastará, que active el enlace, por simple curiosidad, y sin que se dé cuenta se instalará en su ordenador un programa malicioso cuya función es la de capturar todo tipo de datos personales.

Cómo identificar un mensaje phishing

Ejemplo 1. Recibes un mensaje de un banco, de un sistema de pago electrónico o de un proveedor de mensajería. Si no estás abonado a ningún servicio en particular, entonces el mensaje es a todas luces fraudulento: sólo elimínalo.



Ejemplo 2. Recibes un mensaje de un banco, de un sistema de pago electrónico o de un proveedor de mensajería al cual estás abonado. En este caso, lee el mensaje con mucho cuidado: si el mensaje te pide identificarte en línea, entonces se trata de un mensaje fraudulento. Ninguna organización legítima les pide a sus abonados o clientes que se identifiquen de esta manera.

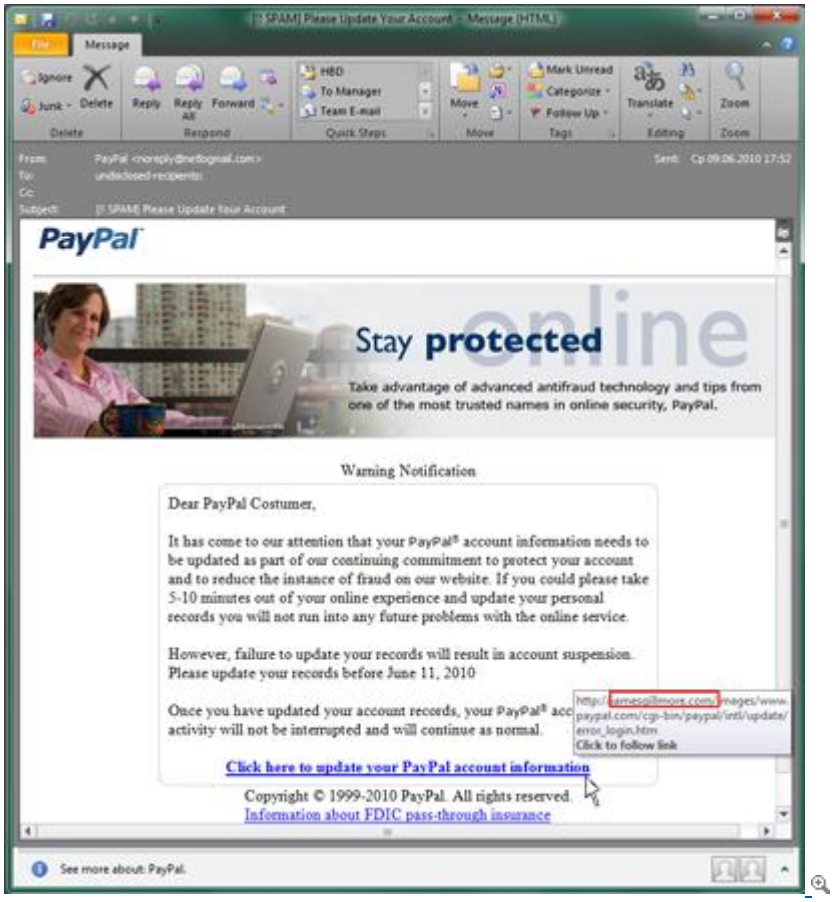


Otra sencilla forma de diferenciar un mensaje fraudulento de uno legítimo es la siguiente: pasa el ratón por encima del enlace. En la parte inferior izquierda del navegador podrás leer la verdadera dirección URL del sitio al que el enlace te conducirá. Observa con mucha atención: los dos últimos niveles del nombre del dominio (es decir, la porción de la dirección que está antes de la barra oblicua) deben pertenecer a la organización que supuestamente te envió el mensaje.

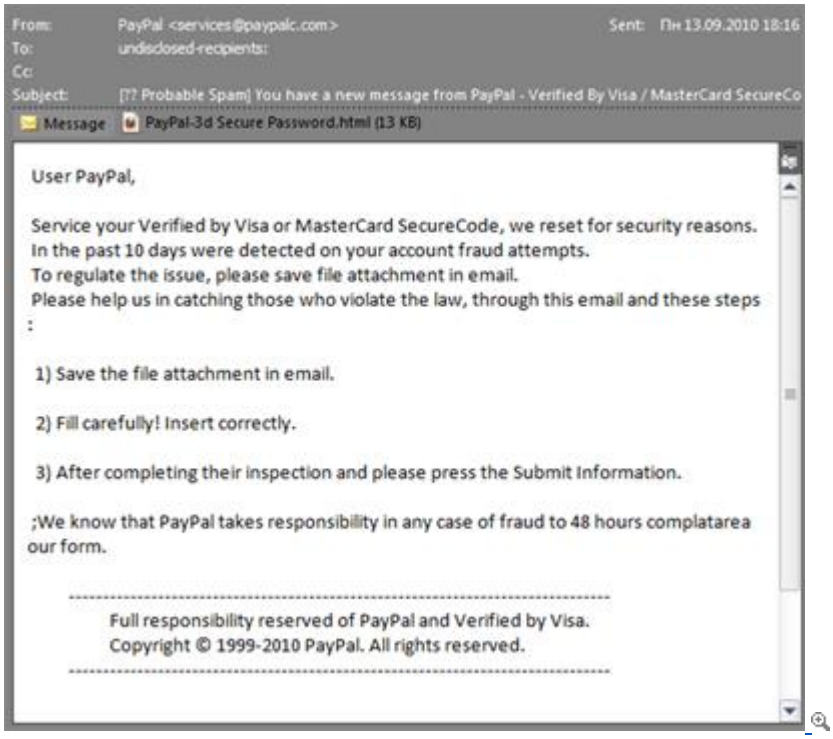
Por ejemplo, los mensajes de PayPal contienen un enlace como éste:
http://anything.**paypal.com/**anything

En cambio, un mensaje fraudulento contiene un enlace falso, como los siguientes, que contiene otras cosas menos « paypal.com » antes de la barra oblicua:

http://paypal.confirmation.com/anything,
http://anything.pay-pal.com/anything,
http://anything.paypal.com.anything.com/anything

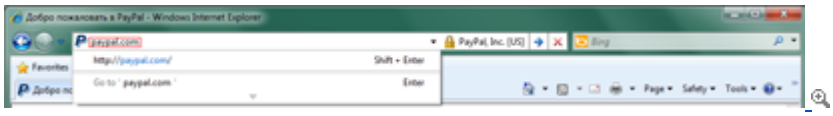


Desconfía también de los mensajes con adjuntos. ¡No sólo podría tratarse de mensajes phishing que intentan robarse tus datos, sino que podrían contener programas maliciosos!



Ante la menor duda, abre manualmente el sitio oficial de la organización en cuestión. No uses el enlace incorporado en el mensaje, sino más bien escribe la dirección oficial en el espacio de direcciones del

navegador. De esta manera te mantienes protegido, evitas abrir un sitio fraudulento, y podrás verificar la información respectiva en el sitio legítimo.

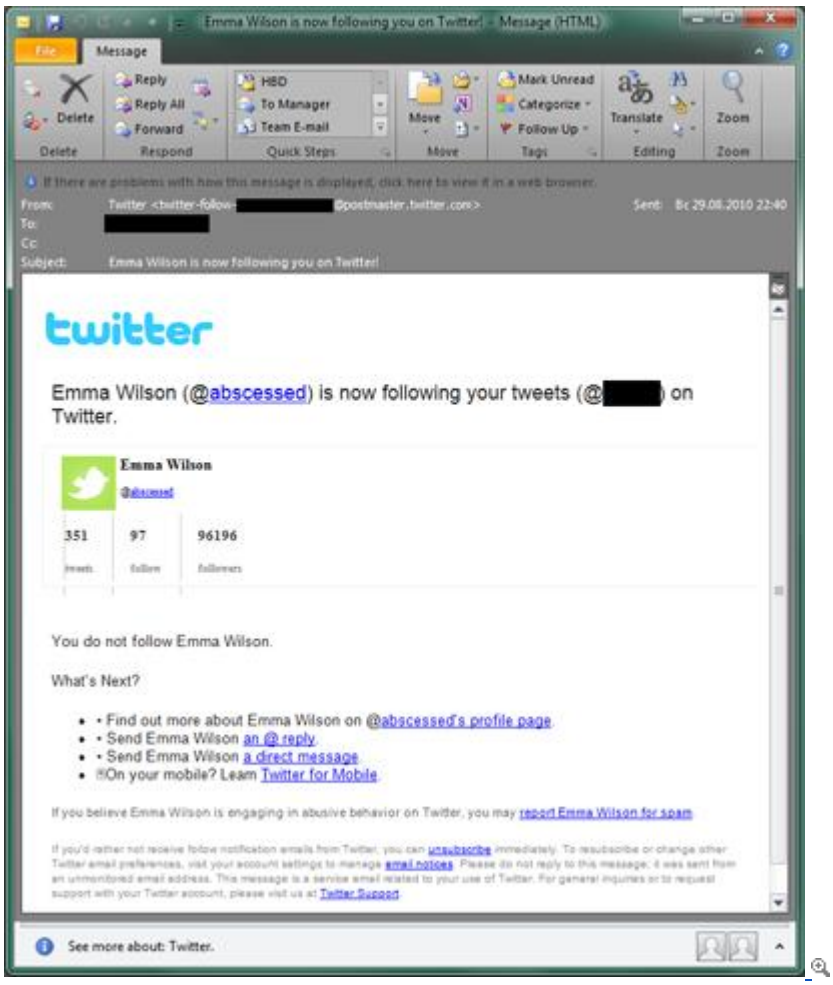


Ten en cuenta que los ciberdelincuentes no sólo desean tus datos bancarios o de pago electrónico, sino que van tras tu información personal, lo que explica por qué los creadores de mensajes phishing apuntan de la misma manera a sistemas de mensajería y a sitios de redes sociales o de juegos en línea, es decir, a cualquier sistema en el que tengas que introducir tus datos personales.

Phishing: el caso de las redes sociales

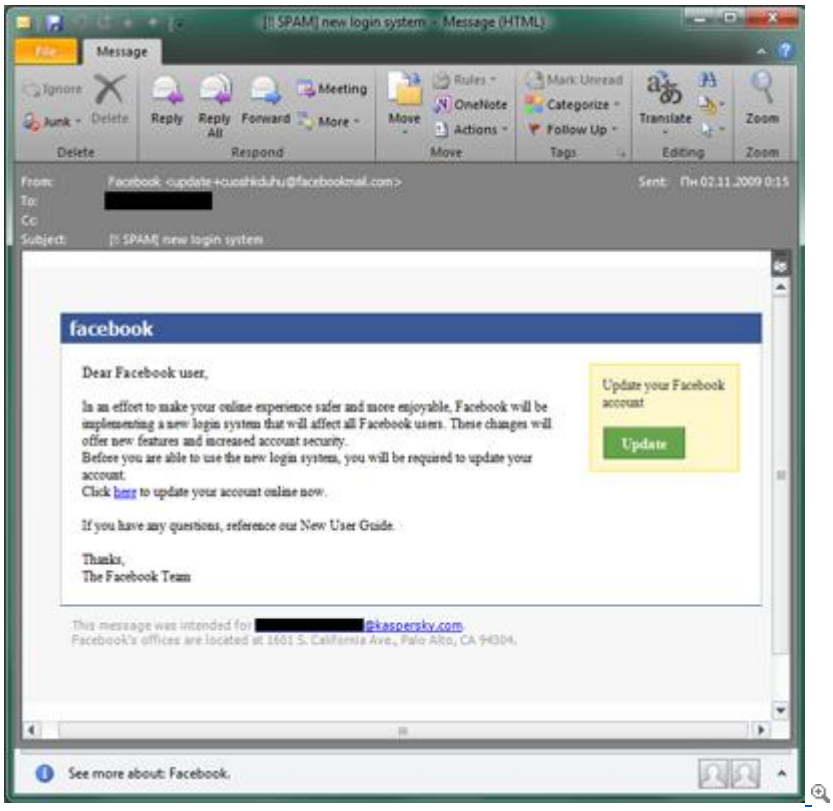
¿Tienes una cuenta en Facebook, Twitter, Orkut, LinkedIn o en otra red social? Si tu respuesta es afirmativa entonces ya sabes cómo son sus mensajes legítimos.

Los mensajes falsos pueden replicarlos con gran exactitud. Estos mensajes fraudulentos están diseñados para capturar tus datos personales y para acceder a tus cuentas en redes sociales. El procedimiento utilizado se parece al ya descrito en el caso de los bancos: una notificación del sitio web de la red te informa que alguien te ha dejado un mensaje o que desea añadirte a su lista de amigos, o incluso que debes actualizar tus datos de cuenta. Si activas el enlace provisto, en lugar de abrir el sitio oficial, aparecerás en un sitio falsificado, idéntico al original. Tan pronto como introduzcas tus datos, se transmitirán a los ciberdelincuentes; posteriormente te enviarán al sitio legítimo.



Los mensajes fraudulentos de las redes sociales no siempre te piden que introduzcas tus datos (se parecen a los mensajes legítimos, a excepción de los enlaces provistos). Analiza cuidadosamente la

dirección real del sitio que el mensaje te pide abrir. A menudo, los estafadores usan nombres de sitios fraudulentos que se parecen mucho a los legítimos, por ejemplo: http://fasebook.com/, en lugar de http://facebook.com/



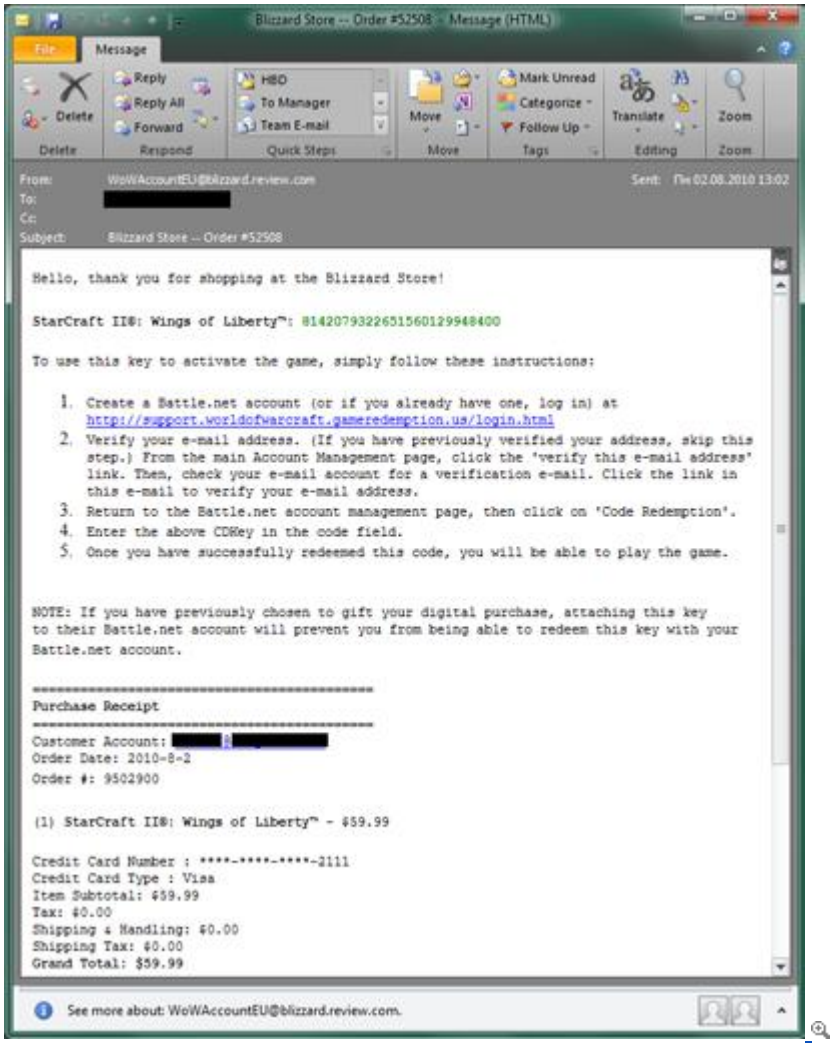
Phishing: el caso de los juegos en línea

Aunque sean gratuitos, los juegos en línea suelen ofrecer opciones de pago: motores o artículos especializados, avatares originales o bonos suplementarios. Si se trata de dinero, puedes estar seguro de que el fraude está al acecho. El procedimiento es bastante estándar: se trata de engañar a los usuarios para que visiten un sitio web falsificado. Como sucede en los otros casos de phishing, la dirección del sitio fraudulento puede parecerse mucho a la del sitio legítimo.

Sólo un usuario meticuloso podrá notar la letra « i » insertada en el nombre de dominio *worlidofwarcraft.com*, en el enlace URL provisto. Pero si uno está familiarizado con los métodos phishing,

la trampa se detecta inmediatamente, pues un mensaje legítimo ¡nunca pedirá a sus usuarios que activen un enlace para identificarse!

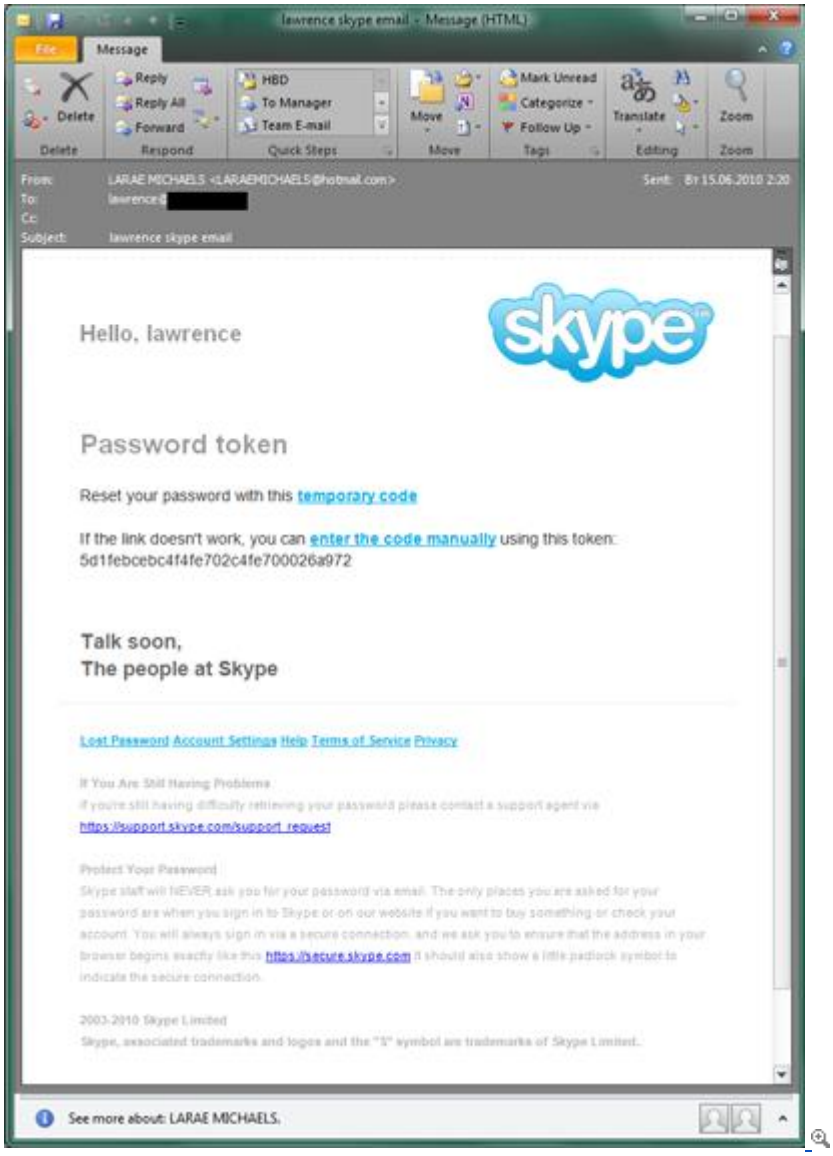
Para llamar aún más la atención de los usuarios, los estafadores a veces recurren a tácticas más sutiles. Por ejemplo, uno puede recibir una invitación para probar un programa de juegos, o una oferta gratuita ¡con sólo activar el enlace! Pero si aceptas la invitación, caíste en la trampa, ya que, con toda seguridad, aparecerás en un sitio web falsificado en el que los ciberdelincuentes intentarán capturar tus datos confidenciales; también corres el riesgo de abrir un sitio infectado que descargará todo tipo de programas maliciosos en tu ordenador.



La mejor protección contra cualquier tipo de phishing consiste en no activar nunca un enlace ni introducir tus datos personales. En cambio, si visitas el sitio oficial, evitarás el riesgo de caer en la trampa de los enlaces fraudulentos.

Otras formas de phishing

Existen otras formas de fraudes phishing porque los estafadores son capaces de crear innumerables mensajes fraudulentos para todos los recursos de Internet que solicitan a sus usuarios identificarse. Cualquiera que sea el tipo de servicio: hosting, revistas en línea u otros, todos los sitios son blancos; los ciberdelincuentes se inclinan en general por los servicios más utilizados o que tengan fama de ser seguros.

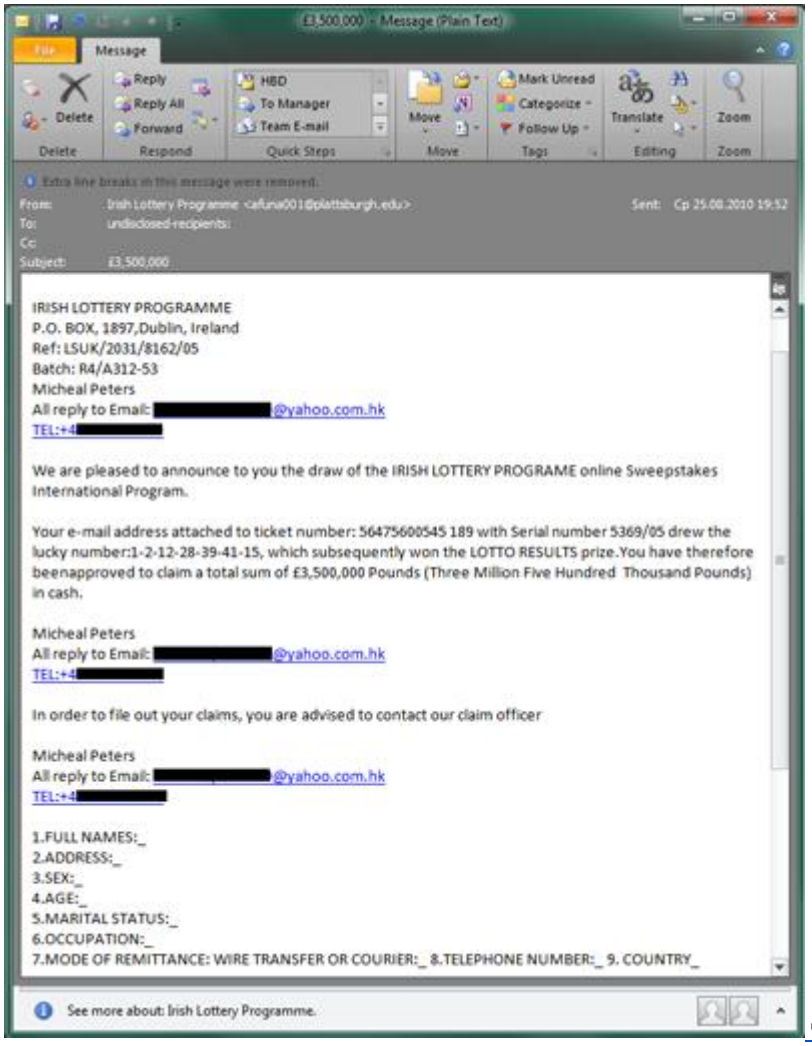


El ejemplo de arriba es bastante interesante. Los estafadores utilizan un típico mensaje fraudulento supuestamente enviado por Skype, y asumen que los destinatarios no leerán la letra chica que dice: «El personal de Skype NUNCA le pedirá su contraseña por correo».

Otras formas comunes de fraudes

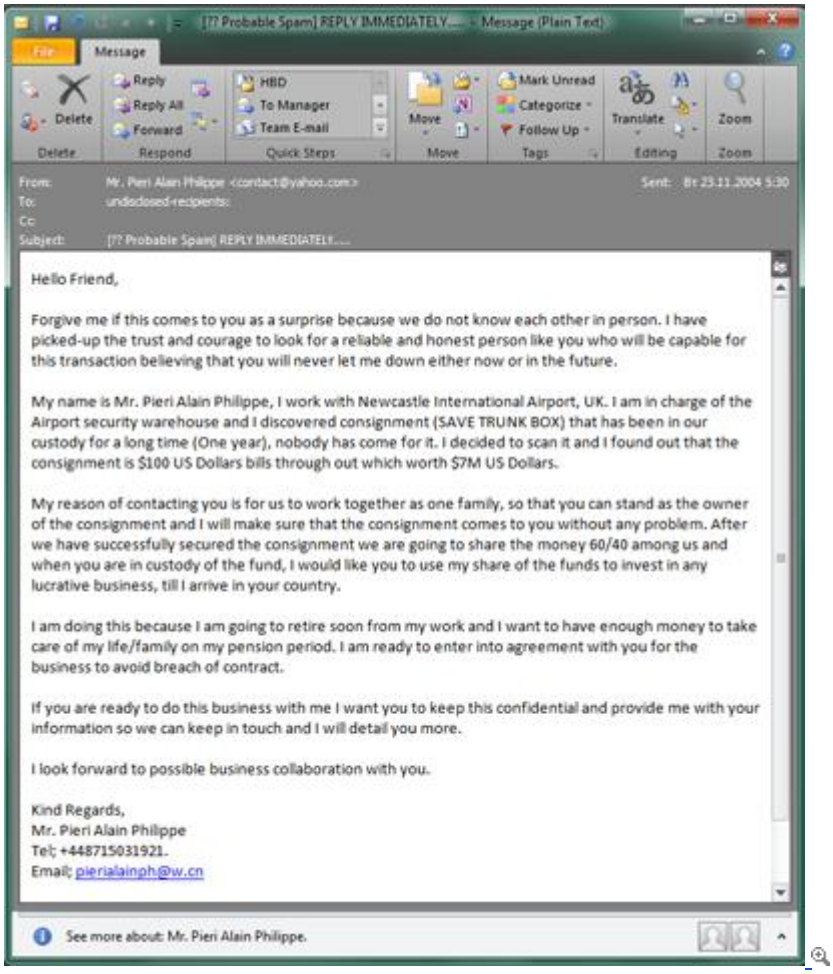
El refrán «saber es poder» se puede aplicar como regla de seguridad contra el fraude cibernético. A veces es indispensable conocer las distintas tácticas que los ciberdelincuentes usan para poder identificar los intentos de fraude. A continuación presentamos las categorías más comunes.

Anuncio falso de ganador de lotería: (Ver aquí)
Estos mensajes te avisan que eres el afortunado ganador de una lotería. Para recibir el «premio», el estafador pide que se le envíe una cantidad de dinero con el pretexto de pagar trámites.



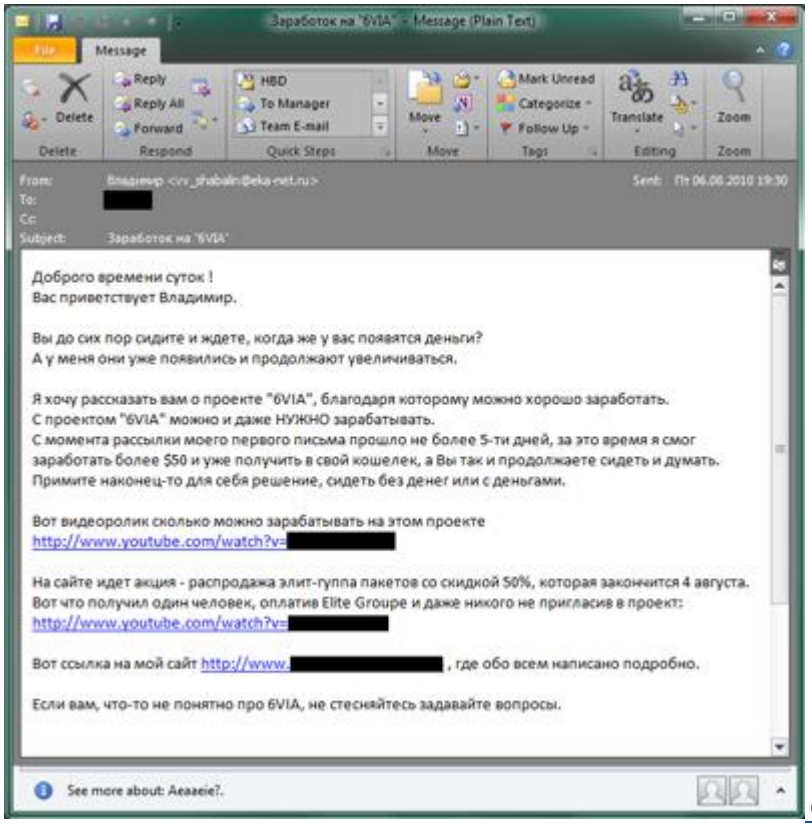
Las cartas nigerianas (Ver aquí)
Estos mensajes piden que transfieras cierta suma de dinero a un remoto país africano (o en otro continente) a costa tuya, a cambio de una gran comisión. Enseguida los estafadores piden un número de cuenta para depositar la comisión. Pero, evidentemente, en vez de realizar la transferencia, lo que en realidad hacen es vaciar los fondos en esta cuenta. Una variante de esta carta nigeriana consiste en convencer a la víctima de que transfiera cierta suma de dinero bajo el pretexto de que hay que pagar servicios jurídicos o gastos de envío. Tras recibir el dinero, los delincuentes suspenden toda comunicación con la víctima que se queda esperando la comisión prometida.

Otra variante más peligrosa consiste en que los estafadores utilizan la cuenta sonsacada de tal manera que si la víctima sigue sus instrucciones será responsable del delito de lavado de dinero. En esta variante, las víctimas pueden ir a prisión en lugar de los verdaderos delincuentes.



Montajes piramidales y dinero fácil

Se trata de un montaje en el que se invita a potenciales víctimas a invertir una pequeña suma de dinero bajo la promesa de recuperarla multiplicada. En realidad, las víctimas terminan sin recibir absolutamente nada.



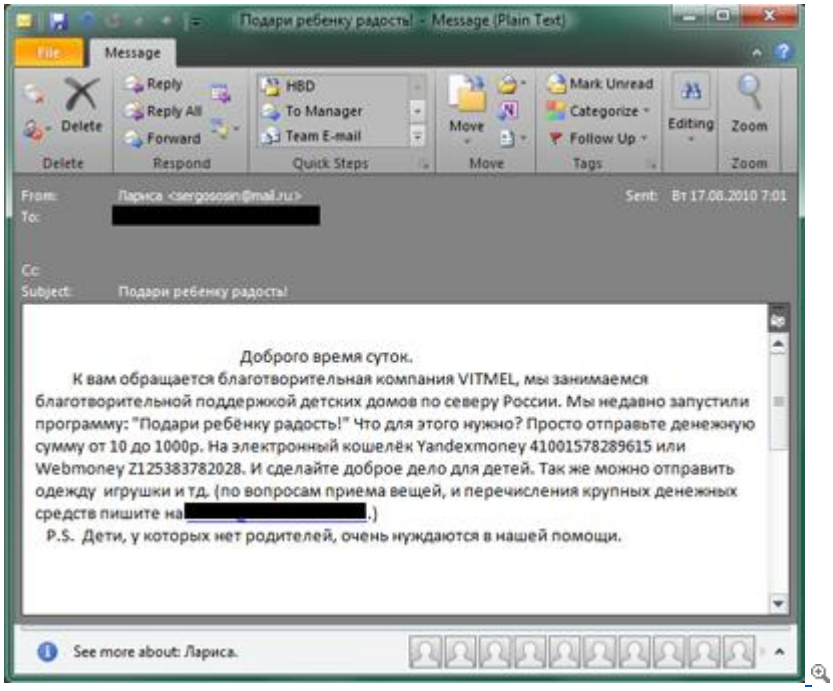
En este ejemplo de mensaje, se invita al destinatario a enviar cierta suma de dinero para participar en un proyecto supuestamente lucrativo.

La gallina de los huevos de oro

Este tipo de fraude consiste en ofrecer una supuesta ventaja basada en “lagunas” o “informaciones privilegiadas” explotable en distintos sitios, como por ejemplo casinos en línea, sistemas de pago electrónico y otros similares.

Peticiones de donaciones

En este tipo de fraude, los mensajes provienen supuestamente de organizaciones humanitarias para enviar fondos. A menudo, estos mensajes son completamente falsos, o pueden incluir enlaces auténticos a sitios de organizaciones legítimas, pero las instrucciones para enviar el dinero son fraudulentas.



En este mensaje se invita al destinatario a realizar una donación a favor de orfelinatos en el norte de Rusia vía pago electrónico (se indican dos cuentas distintas). Los estafadores apuestan a la sensibilidad de sus víctimas concluyendo el mensaje de esta manera: "P.D. Nuestros huérfanos necesitan tu ayuda".

Analicemos: las organizaciones humanitarias no recurren al correo electrónico pues disponen de otros medios para recaudar fondos. Si de todas maneras se quiere verificar la información en el mensaje, hay que buscar la dirección de la referida organización y ponerse en contactacto directamente con ellos ofreciéndoles una donación.

Mensajes de texto (SMS) spam
Pertenecen a esta categoría diferentes tácticas para convencer a los usuarios a que envíen un mensaje de texto SMS a un número de pago. Este tipo de fraude involucra también a los sitios de prepago vía SMS por un servicio inexistente. Cualquiera que sea la promesa anunciada, el usuario terminará pagando decenas de euros (o más) por nada a cambio.

¿Qué hacer al respecto? Lo primero es eliminar los mensajes que contengan ofertas especiales de dinero o los que provengan de desconocidos:

- propuestas de dinero fácil (enriquecimiento rápido, ayuda para giros, inversiones con alto retorno)
- peticiones de donaciones (tratamientos médicos, para una bella nigeriana pobre, etc.);
- todo tipo de « loterías »
- ofertas gratuitas de software o productos multimedia, etc.

Aspectos técnicos del fraude

Evidentemente resulta imposible incluir en un solo artículo todos los tipos de fraudes. Sin embargo, a parte del contenido, a veces se puede reconocer estos mensajes por su redacción y formato. Es por ello que trataremos algunos aspectos técnicos que una vez conocidos permitirán distinguir sin dificultad los mensajes legítimos de los fraudulentos.

Los siguientes indicios revelan indirectamente una procedencia fraudulenta:

El campo « A: » contiene otros nombres además del tuyo.

Se trata entonces de un correo spam en el que el destinatario no tiene nada que ver con el contenido del mensaje, ya que fue seleccionado al azar.

La dirección que aparece en el campo « De: » es desconocida.

Esto significa que el mensaje no proviene de la organización referida, pues su identidad ha sido robada. Ninguna organización seria recurre a la mensajería gratuita para enviar su correspondencia.

Algunas palabras están con letras MAYÚSCULAS.

Se trata de una táctica de los creadores de spam para llamar la atención de los usuarios.

Algunas palabras aparecen deformadas (« Lloan » o « Crrédito" en vez de « Loan » o "Crédito», o « Usted haganado » en vez de "Usted ha ganado »).

Se trata de una táctica que usan los spammers para burlar los filtros antispam.

El enlace no corresponde a la dirección oficial de la organización ;

Como mencionamos anteriormente se trata de un claro indicio de conducir al usuario hacia un sitio fraudulento.

Un saludo impersonal como « Estimado amigo, Estimado cliente, Estimado abonado, ¡Buen día! ».

Este tipo de saludos revela que el remitente no te conoce y que, por lo tanto, se trata de un mensaje spam.

Algunas palabras sobre la ingeniería social

Como se sabe, el factor humano es siempre el eslabón más débil de los sistemas de seguridad, y el fraude cibernético no omite esta regla. Ninguna tecnología de seguridad será lo suficientemente efectiva si nos rendimos ante los cantos de sirena. Demos un vistazo a las debilidades humanas favoritas de los estafadores.

La avaricia

La avaricia está entre los principales defectos de la naturaleza humana y los delincuentes saben utilizarla. Dinero fácil, loterías, desvío de pagos electrónicos y otros — **todas las estafas se basan en el mismo principio: «danos un adelanto y te lo devolveremos multiplicado»**.

Evidentemente nunca hay respuesta. Ten siempre presente esta idea y nunca te dejes timar.

El miedo

El miedo es otra dimensión de la naturaleza humana que los estafadores manipulan con destreza. Mensajes como este: « Activa este enlace o tu cuenta se bloqueará», «Si no envías un SMS a este número en 10 minutos tras leer este mensaje, tu cuenta de mensajería se cancelará», y otros mensajes similares juegan con el miedo y llevan a los usuarios a actuar de inmediato y sin reflexionar.

Recuerda siempre esta regla: **ningún proveedor bloqueará jamás tu cuenta** de esta manera. Como mencionamos anteriormente, ningún proveedor te pedirá nunca en un mensaje que actives un enlace para identificarte. En general, ningún servicio legítimo te obligará a hacer nada. Entonces elimina directamente todos los mensajes que intentan asustarte o que te obligan a hacer algo porque son fraudulentos.

La ingenuidad, el altruismo, la credulidad

Es lamentable, pero los delincuentes intentan aprovecharse de nuestras virtudes y buenos sentimientos.

Nunca olvides que **todas las peticiones de ayuda que te llegan en mensajes spam son falsas.** Si realmente deseas contribuir, puedes hacerlo a través de los mecanismos específicos de recaudación, que nunca incluyen el envío masivo de mensajes.

La curiosidad

Es notable cómo la simple curiosidad puede llevar a ciertas personas a enviar dinero a los estafadores. Incluso cuando el contenido del mensaje nos parece extraño, o no esperamos obtener realmente cientos de miles de dólares, nos carcome la curiosidad de saber lo que podría ocurrir al activar el enlace: ¿De qué se trata? ¿Cómo funciona? ¿Qué pasará?

¿Realmente quieres saber lo que ocurrirá? **Perderás tu dinero** — ¡Eso es!

La falta de atención

En general, la vida en Internet tiene un ritmo más acelerado que el de la vida real. A menudo hacemos varias cosas a la vez; trabajamos, chequeamos nuestro correo, leemos periódicos, escuchamos música, chateamos, etc. De manera inevitable, nuestra atención se dispersa y disminuye, lo que nos lleva a tomar un mensaje fraudulento por legítimo, y no es sino después que nos damos cuenta del fraude, cuando lo volvemos a leer con más atención.

No te precipites en responder un mensaje. Tómate tu tiempo para pensar y releer el mensaje.

Piensa que además de los fraudes, hay otras amenazas, comenzando por innumerables programas maliciosos capaces de robar tu información confidencial, los códigos de tus tarjetas de crédito, u otros datos confidenciales; los ciberdelincuentes ni siquiera tienen que prometerte algo para conseguirlos.

Al navegar en Internet, sigue estas sencillas reglas de seguridad:

Utiliza un programa antivirus :

los modernos programas antivirus se actualizan regularmente y ofrecen una eficaz protección contra las amenazas que circulan en Internet.

Descarga regularmente las actualizaciones de tus programas:

las actualizaciones de tus programas contienen reparaciones para vulnerabilidades que los ciberdelincuentes podrían aprovechar.

Nunca des tu información personal en espacios accesibles:

los datos que des en Internet son interceptados por robots y transmitidos a los ciberdelincuentes que enseguida los usan, por ejemplo, para enviar mensajes spam desde tu propia dirección.

Nunca descargues nada desde sitios desconocidos:

Existen muchas probabilidades que el programa, el libro o la película que descargues traigan consigo programas maliciosos.

Nunca actives los enlaces incorporados en un mensaje:

estos enlaces suelen conducir a sitios falsos o infectados con programas maliciosos.

Nunca abras los adjuntos en los mensajes si no conoces al remitente

Es muy probable que un adjunto contenga un programa malicioso (incluso en un simple documento de Word).

Nunca optes por « dar de baja la suscripción » de un mensaje spam, menos aun si el mensaje incluye la opción de un enlace para ello:

conseguirás el efecto contrario porque en vez de deshacerte de mensajes no deseados, estarás aumentando su volumen. Te expones a dos riesgos. Primero, que tu dirección de correo electrónico alimente una base de datos de personas que, como tú, ya cayeron en la trampa, y que en un futuro serán blanco de numerosos mensajes spam. Segundo, si activas el enlace de la supuesta « baja de suscripción », te conducirán a un sitio infectado que instalará programas maliciosos en tu ordenador.

Desconfía de las ofertas tentadoras, sobre todo si ofrecen dinero fácil:

Se trata de tácticas creadas para robarte tu dinero o llevarte a realizar acciones ilegales por las que corres el riesgo de terminar en prisión.

A manera de conclusión

Siempre existirá el fraude. Está en todos los rincones de Internet: mensajería, redes sociales, todo tipo de sitios web. Con el tiempo, los ciberestafadores rediseñan sus fraudes, pero todos se resumen en ciertos procedimientos repetidos. En última instancia, los usuarios son los únicos que realmente pueden protegerse en el espacio virtual.

Esperamos que los consejos y la información de este artículo te sean útiles.

Fuente:

- Kaspersky Lab