LO SIGUIENTE SUCEDIÓ HOY EN MI CORREO ELECTRÓNICO..

Caso verídico de Phishing.. Acá no hay nada preparado...

Hoy, como todas las tardes, después de haber realizado las compras para mi hogar (eso no es todas las tardes) procedí a revisar el correo electrónico en busca de buenas noticias, pero para sorpresa mía, encontré un hermoso correo que en principio causó cierta preocupación (1 segundo).

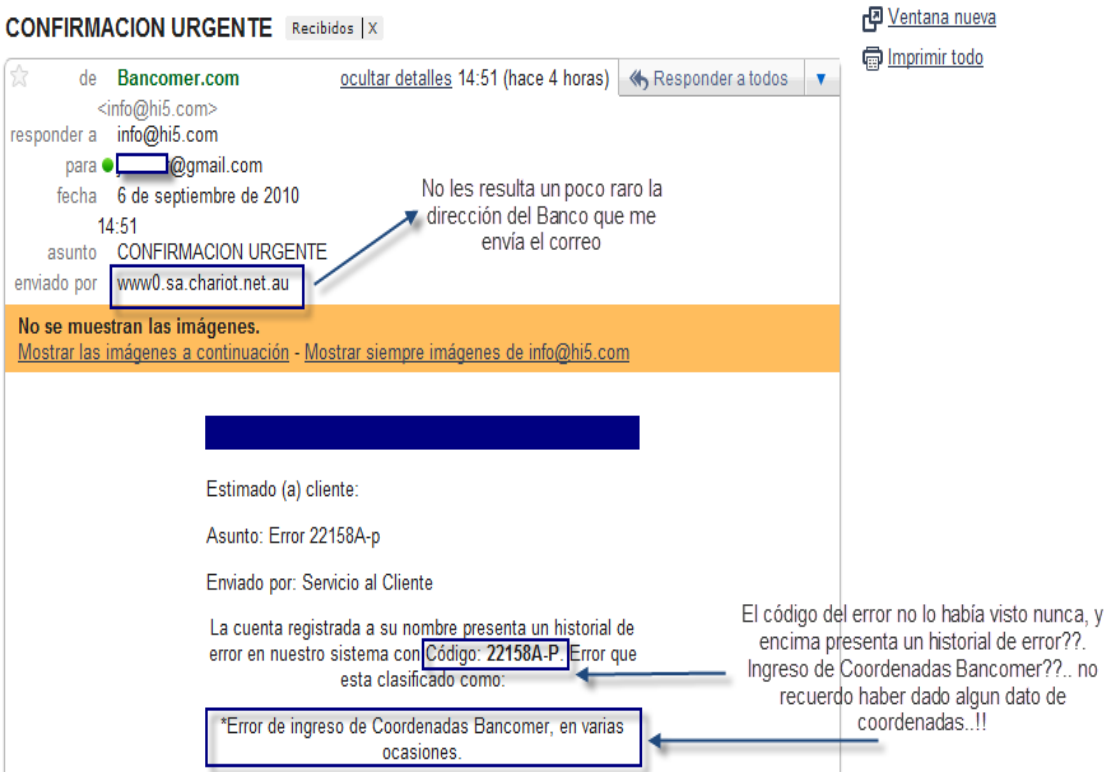
Al comenzar con la lectura del mismo, no entendí a lo que se estaba refiriendo, al llegar al final del mismo creo que entendía menos que al principio. De igual manera, traté de no sorprenderme demasiado, pero ya no podía más de la risa, digo de la risa ya que conocía por diferentes artículos sobre el tema del Phishing, quizás nunca lo había vivido en carne propia.. pero siempre hay tiempo.

Al ingresar en la Bandeja de Entrada, me encuentro con el siguiente correo:

Fíjense el Asunto del mensaje, proviene de un Banco que no es conocido en nuestro país, luego letra imprenta mayúscula de confirmación urgente (necesitan ponernos nerviosos).. y de paso el código del error 22158A-p, más que código de error, parece el código del salame que compré hoy por la tarde en el supermercado..

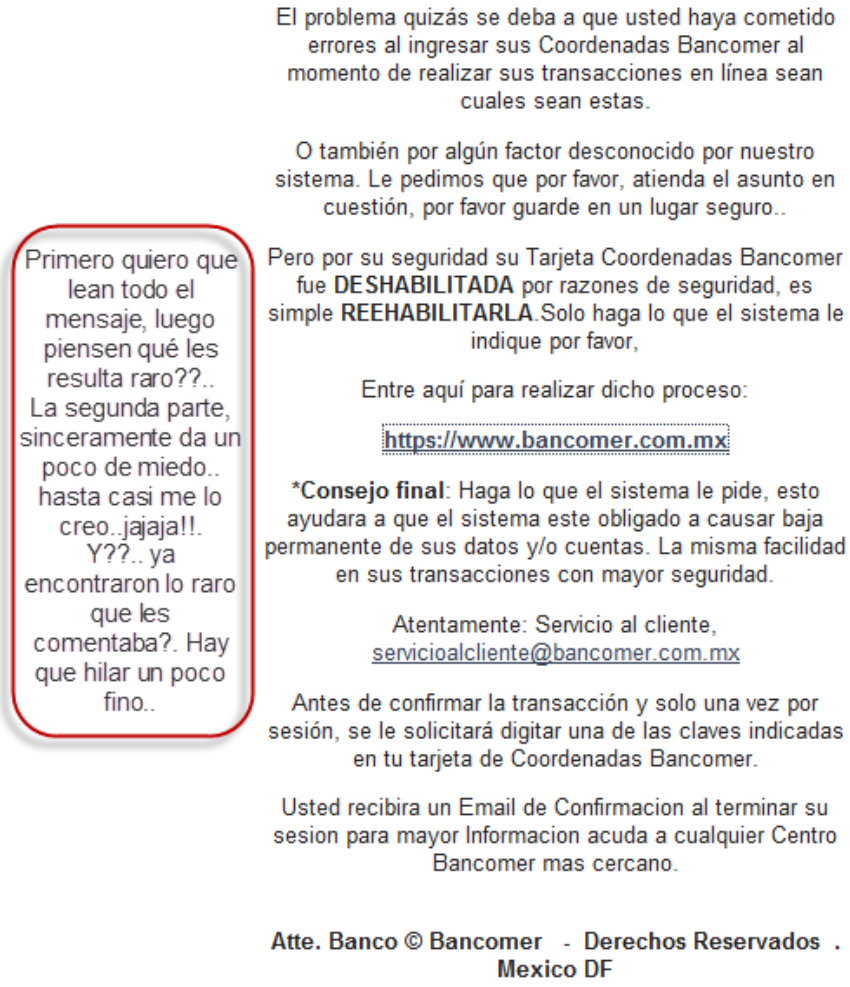
(RECUERDEN QUE PARA VER MEJOR LA IMAGEN, LE REALIZAN UN CLIC SOBRE LA MISMA, SE ABRIRÁ UNA NUEVA VENTANA CONTENIENDO SÓLO LA IMAGEN CLICKEADA. LUEGO CIERRAN DICHA VENTANA O HACEN CLIC SOBRE EL BOTÓN PARA REALIZAR UN PASO ATRÁS)

Después de ver el asunto del mensaje, como es de esperar, arremetí contra la lectura del mismo, con lo cual me encontré con la siguiente pantalla:



Para gran sorpresa, mi primer duda surge al ver la dirección de la página Web a la que hacen mención, no me resultaba una dirección común y corriente a la cual estoy acostumbrado a ver de los grandes Bancos Nacionales o Extranjero.
Luego, el código del error (como ya había nombrado anteriormente) me sonó a zaraza.. y la explicación del mismo, evidenciaba un hermoso caso de Ingeniería Inversa, es decir, la explicación muy escueta, y en demasía confusita. Quién se podría creer semejante mentira??.. bueno!!, hay mucha gente que en su desconocimiento pueden llegar a confundirlo.
Pero, la segunda parte del mensaje, cuando ya se explayan sobre el tema, ese fue el plato fuerte del día. Les solicito que por favor lean bien el mensaje.. primero una lectura rápida como para conocer bien

a qué están haciendo referencia, y luego una lectura con más profundidad.



El problema quizás se deba a que usted haya cometido errores al ingresar sus Coordenadas Bancomer al momento de realizar sus transacciones en línea sean cuales sean estas.

O también por algún factor desconocido por nuestro sistema. Le pedimos que por favor, atienda el asunto en cuestión, por favor guarde en un lugar seguro..

Pero por su seguridad su Tarjeta Coordenadas Bancomer fue **DESHABILITADA** por razones de seguridad, es simple **REEHABILITARLA**.Solo haga lo que el sistema le indique por favor,

Entre aquí para realizar dicho proceso:

https://www.bancomer.com.mx

***Consejo final**: Haga lo que el sistema le pide, esto ayudara a que el sistema este obligado a causar baja permanente de sus datos y/o cuentas. La misma facilidad en sus transacciones con mayor seguridad.

Atentamente: Servicio al cliente,
servicioalcliente@bancomer.com.mx

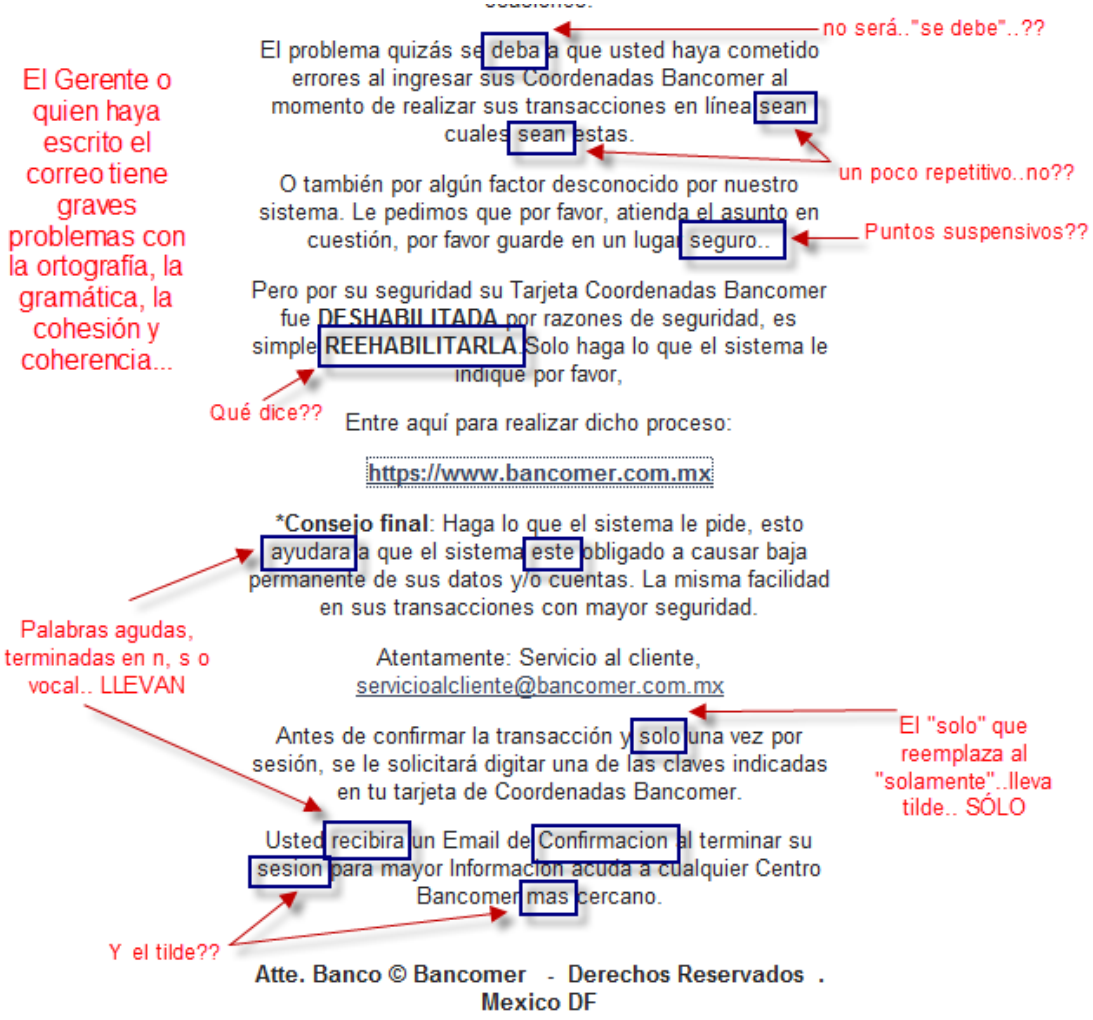
Antes de confirmar la transacción y solo una vez por sesión, se le solicitará digitar una de las claves indicadas en tu tarjeta de Coordenadas Bancomer.

Usted recibira un Email de Confirmacion al terminar su sesion para mayor Informacion acuda a cualquier Centro Bancomer mas cercano.

Atte. Banco © Bancomer - Derechos Reservados .
Mexico DF

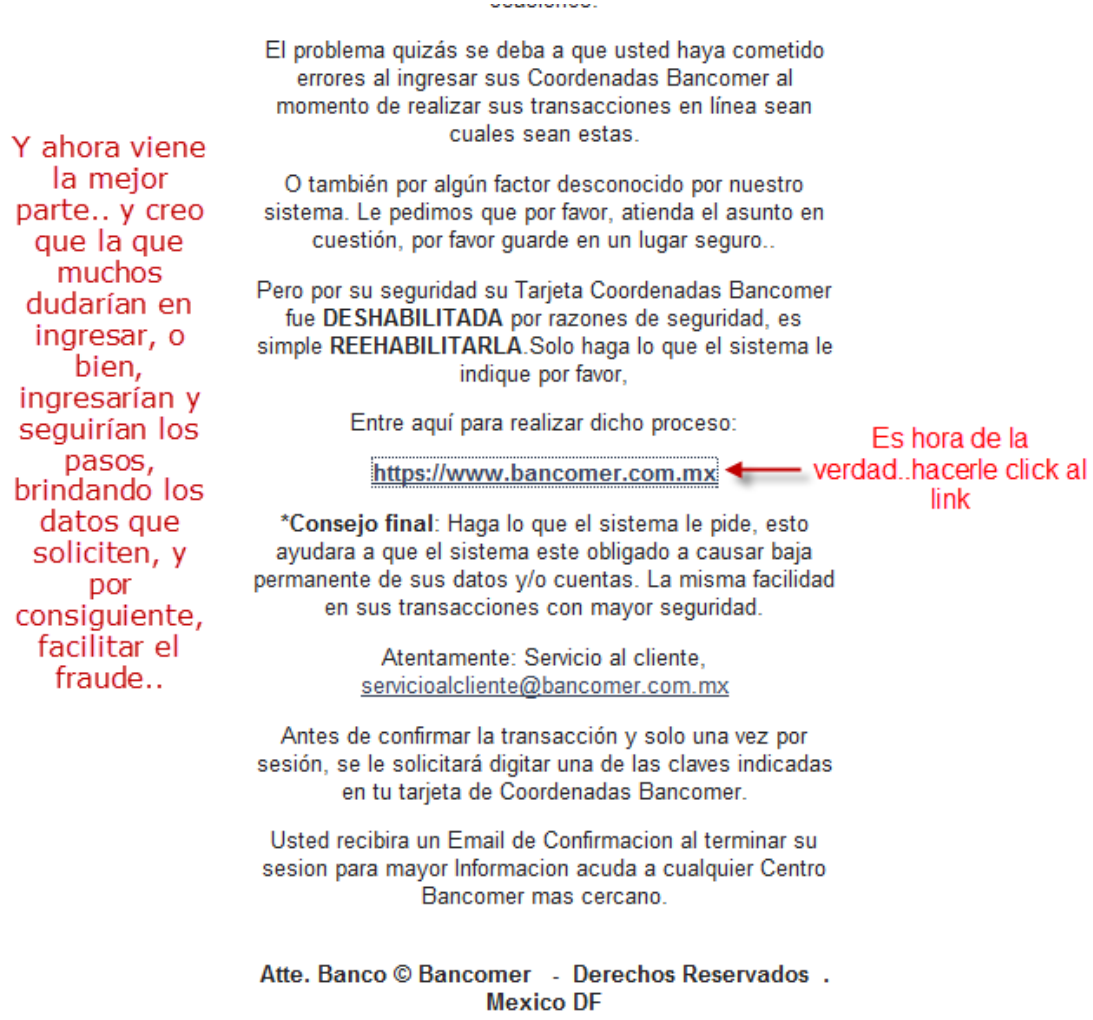
Primero quiero que lean todo el mensaje, luego piensen qué les resulta raro??.. La segunda parte, sinceramente da un poco de miedo.. hasta casi me lo creo..jajaja!!. Y??.. ya encontraron lo raro que les comentaba?. Hay que hilar un poco fino..

Ahora bien, después de un breve análisis queda en evidencia la falta de profesionalismo, que a la hora de redactar un documento denotan errores tanto de ortografía, como así también de expresión.
Veamos:



Bueno.. ehhhh!!.. creo que queda evidenciado lo anteriormente dicho sobre todos tipos de errores en la redacción del documento. Parece ser que estas criaturas pasaron por alto, el darle la oportunidad de corrección a un profesional que al menos posea una correcta forma de escribir.
No estaría escribiendo esto, si primero no lo hubiese chequeado utilizando a otras personas para que leyeran el mail y preguntando si encontraban algo raro, aparte de los seudo-tecnicismos mal utilizados.
Una vez que la persona terminó de leer el documento, preguntó: ¿Cómo te das cuenta que esto es falso?.. y de la respuesta dada es que surge este artículo, tratando de ser los más explicativo posible y con un lenguaje adaptado para la fácil comprensión..

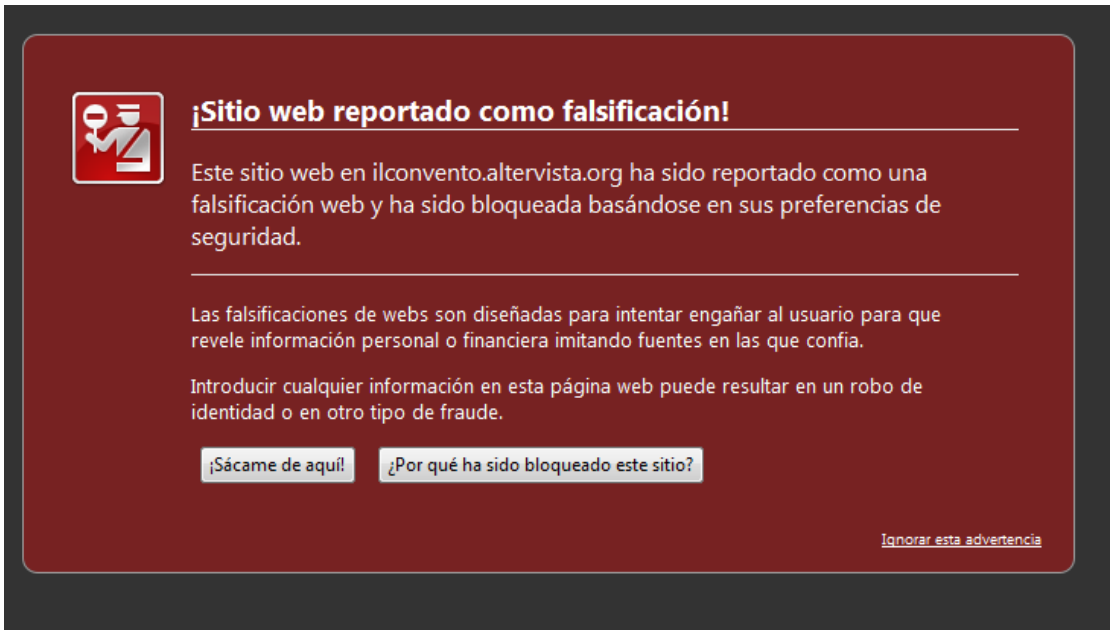
Visto todos los errores cometidos, y ya dándose cuenta que se trataba de un fraude que seguro tiene como objetivo el robo de contraseñas de algún tipo de cuenta, o bien, el número de tarjetas de Crédito, vamos a continuar desarrollando el final de este artículo.
Ahora viene la parte más emocionante, y lo digo de esta manera ya que hay que tomar una decisión importante:



Es la hora en que todos tenemos dos opciones:

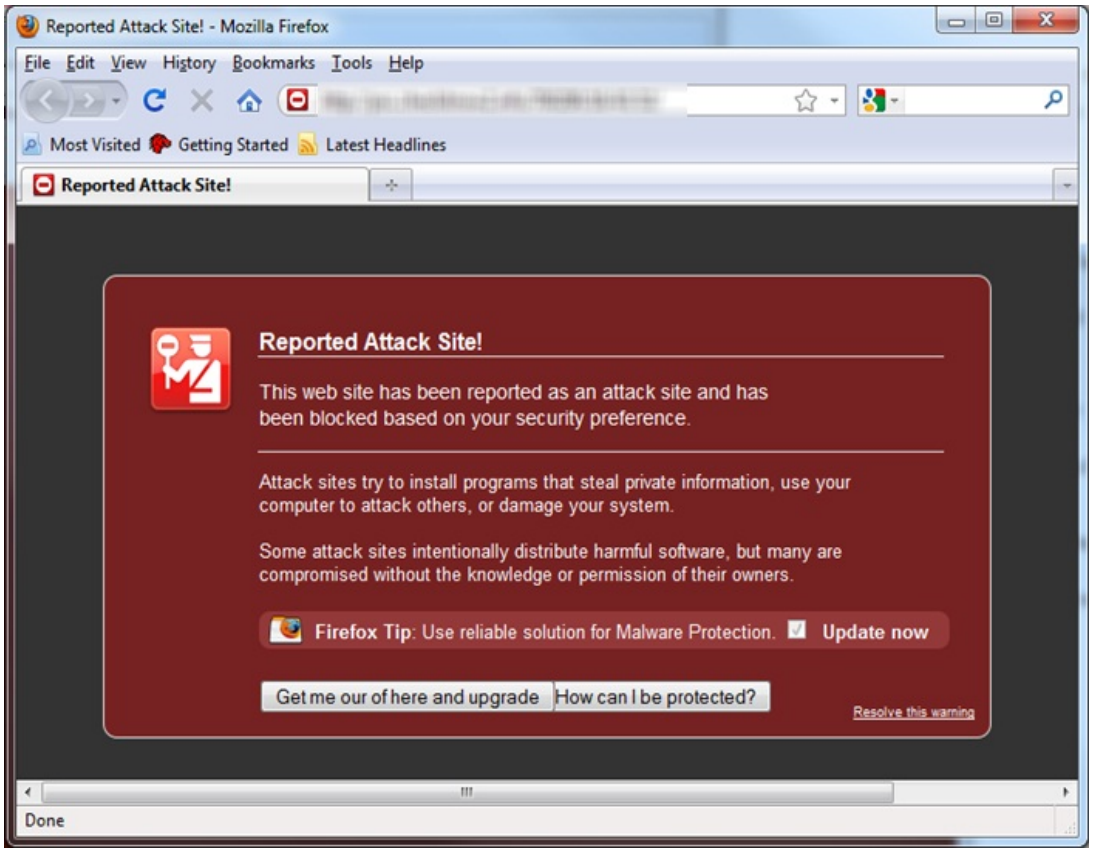
- a) borrar el correo recibido: utilizado en el caso de no conocer su procedencia. Creo que para los que todavía no manejan temas como: actualización de antivirus, Spyware, malware, gusanos, caballos de Troya, phishing y otros más; es la opción que más los puede ayudar.
- b) seguir adelante en la investigación para ver hasta dónde pueden llegar, y por lo consiguiente, poder re-transmitir esta experiencia a personas que puedan verse implicadas en este tipo de fraude.

Como es de esperar, mi opción es la segunda, ya que de otra manera no podría estar explicando para ustedes lo que puede llegar a suceder.
Por supuesto que ahora, vamos a seguir el link para ver a dónde somos redirigidos.



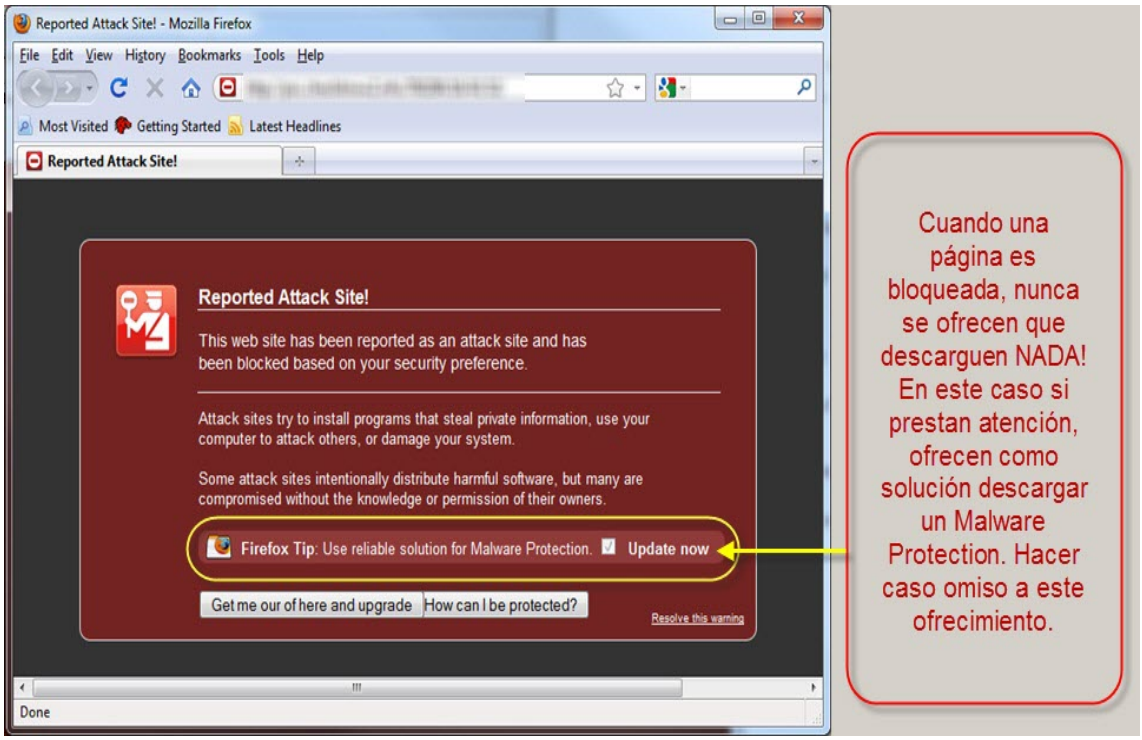
Caramba, el mismo navegador me avisa que se trata de una página que fue reportada como falsificación (Phishing). Eso sucede en este caso por mantener el explorador (Mozilla Firefox) en su última versión y sus debidos complementos bien actualizados.

Ahora bien, todo parece muy fácil, el navegador (Internet Explorer, Mozilla Firefox, Google Chrome, etc.) pueden detectar páginas fraudulentas (se hacen pasar por otros), pero hecha la ley.. hecha la trampa. También se las ingeniaron para, si el explorador detecta la página maliciosa, y aparezcan estos carteles de aviso (imagen anterior), pueda suceder lo siguiente:
(Prestar mucha atención y que la vista se agudice más de lo normal)

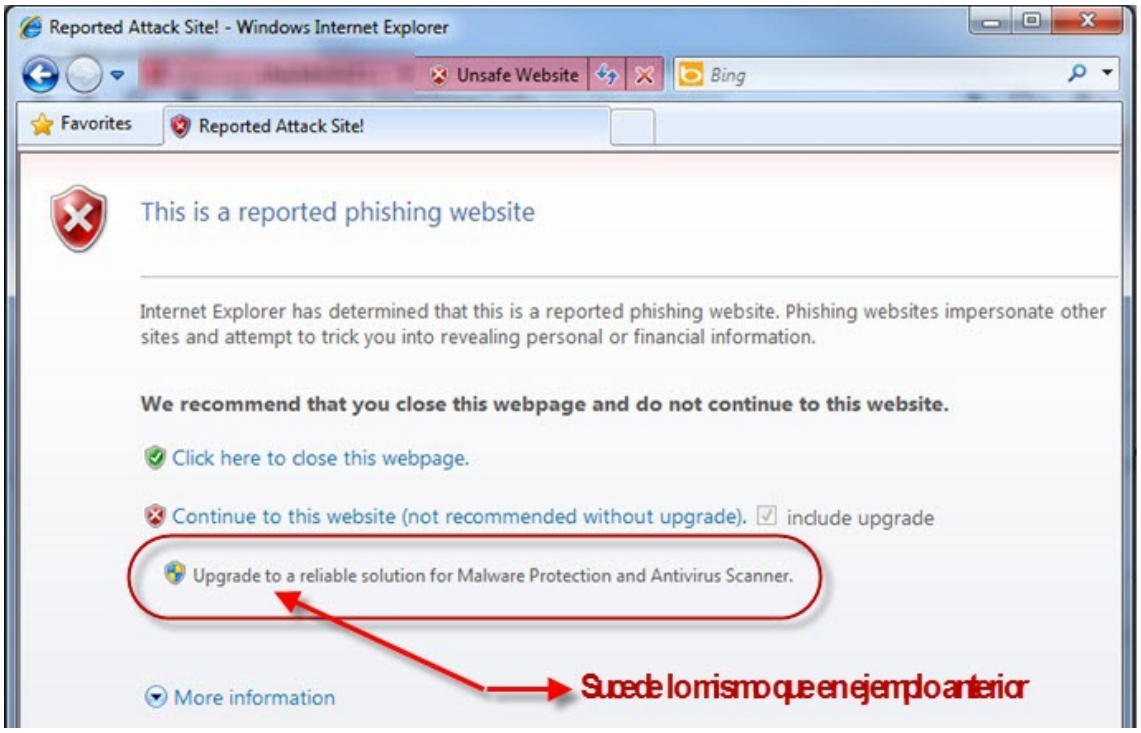


¿Han visto algo fuera de lo normal comparado con la imagen anterior?.

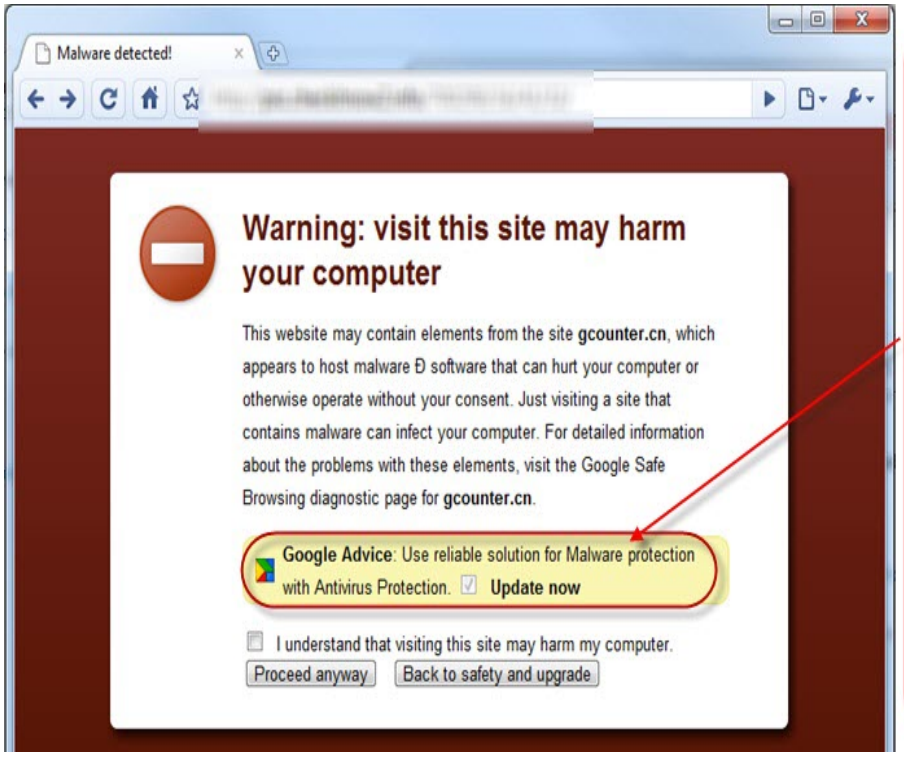
Esa diferencia, marca otra posibilidad de ataque que a simple vista y desconociendo estos temas puntuales, permitirían la entrada nuevamente de todo tipo de programas malicioso, por lo cual la recomendación más grande que se puede dar, es no descargar lo que no se conoce. En este caso, diseñaron un bloqueador muy similar al anterior, con la diferencia de que en este caso ofrecen la descarga mencionada anteriormente, y que se muestra a continuación:



Es ejemplo se da en el Mozilla Firefox, pero también puede suceder lo mismo en el Internet Explorer:

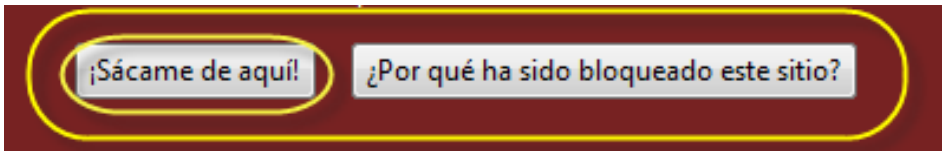


También se puede dar el caso del navegador Google Chrome:



En el Google Chrome, sucede lo mismo que en los navegadores anteriores. Ofrecen la descarga de un Malware protection.. FALSO TOTALMENTE

Para finalizar, lo que podemos dejar bien en claro es que, ante un correo electrónico del cual no se conoce su fuente, proceder a eliminarlo directamente, no dando importancia para nada al contenido del mismo, diga lo que diga.
Segundo, en el caso de que el bloqueador nos avise que se trata de una página de phishing, lean bien lo que se les solicita en el mismo. No descarguen nada, de lo cual no tengan seguridad alguna.
Un buen bloqueador, no nos solicita descargar nada, por el contrario nos ofrece sacarnos inmediatamente del sitio en cuestión, como lo muestra la primera imagen del Firefox.



Esta es la manera correcta en que debe proceder un navegador, ante la presencia de una página sospechosa.

Espero sinceramente haber podido ser lo mas claro posible, y que este artículo sirva para poder orientar a las distintas personas que empiezan a incursionar en el campo de la informática, la navegación por Internet, el uso del correo electrónico y demás servicios que se prestan.
Cualquier duda o inquietud, escriban a mi correo electrónico que en la medida que el tiempo me lo permita, obtendrán una respuesta rápida y concisa.

Algo muy importante a tener en cuenta a la hora de realizar una transacción bancaria de cualquier tipo, antes de loguearse (Usuario y Contraseña) es verificar bien que se encuentran ante una página segura. Seguro que se estarán preguntando: ¿Cómo me doy cuenta que es una página segura?. A continuación, les voy a mostrar una característica muy importante de los sitios en los cuales se puede operar de manera segura.

Una de esas características, es la dirección de la página web que en lugar de empezar con http://, lo hacen con https:// el agregado de la "s" es de "security", es decir, un sitio seguro. Es decir, que en las páginas en las cuales se suelen realizar transacciones, es obligatorio que comiencen con el "https".

Vean:

Otra característica cuando ya se encuentran dentro de un sitio seguro, es la aparición en al ángulo inferior derecho de la página de un candado chiquito, lo que significa también que ya se hayan dentro de un site seguro.

Atte.
Prof. José Luis Conforti
Fuente de imágenes utilizadas:

http://spamloco.net/2010/09/fakeav-con-paginas-de-advertencia.html