CONSEJOS PARA NO SUFRIR FRAUDES INFORMÁTICOS

Cada vez son más numerosas y complejas las prácticas fraudulentas que ponen en serio peligro la identidad digital de las personas y los bienes a los cuales se puede acceder por esta vía. El phishing, la pérdida de datos, el robo de la señal Wi-Fi, el MalWare y el robo de la propia identidad son riesgos que este trabajo explica como minimizar.

La Caja Metropolitana de Lima, siempre en constante preocupación por la seguridad de la información en sus clientes, tiene a bien presentarles las diferentes técnicas que utilizan los atacantes informáticos que emplean tecnologías de información como correos electrónicos, mensajes de texto y llamadas telefónicas entre otros.

Tipos de técnicas:

1. **Phishing:**

   Se trata de una estafa que se realiza a través del correo electrónico. El estafador o phisher envía lo que parece una comunicación oficial de la Caja Metropolitana o de un banco o cualquier otro organismo con el **objetivo de obtener su información privada**, como la contraseña para operar a través de Internet con la Caja Metropolitana o con cualquier otra institución, etc.

Medidas contra el Phishing:

✓ La Caja Metropolitana o cualquier otra organización nunca va a solicitar datos a través de e-mail, ni siquiera por teléfono, por ello nunca rellene ningún formulario de su banco que le llegue a través de e-mail.

- ✓ Debe de utilizar navegadores de última generación como Firefox 7.0.x (http://www.mozilla.org) e Internet Explorer 8 o superior que vienen equipados con herramientas **antiphishing**. En el caso de Firefox, incluso puede informar acerca de la URL (Universal Resource Locutor) falsa, y el caso quedará registrado en la base de datos de sitios phishing de tal forma que si otro usuario ingresa (usando el mismo navegador Firefox), automáticamente se le avisará que ha ingresado a un sitio Web previamente notificado como falso.

2. **Pérdida de datos:**

   Perder lo que almacenamos en nuestra computadora puede ser una catástrofe: las fotos de nuestras vacaciones, nuestras películas, nuestra música, etc. Un simple apagón, un virus o un fallo en el disco duro pueden mandar al limbo informático todos estos datos.

   Medidas contra la Pérdida de Datos:

- ✓ Copia de seguridad o backup: es importante que se realice de forma periódica una copia de seguridad. Puede hacerlo de forma manual, guardando la información en medios extraíbles (disco duro, cd-rom grabable, cintas magnéticas, discos ZIP, JAZ o dispositivo de almacenamiento USB) o con programas especialmente creados para realizar copias de seguridad.
- ✓ Existen programas informáticos especializados en rescatar datos perdidos, pero de todas formas no siempre será rescatable el 100% de la información. Así que es mejor prevenir que tener que lamentar, es decir, realice regularmente copias de seguridad de su información.

3. **Robo de señal Wi-Fi:**

   Muchas veces hemos oído eso de “mi vecino me roba la señal inalámbrica de conexión a Internet".

   Medidas para proteger nuestra red inalámbrica:

- ✓ Habilitar contraseña de red y de administrador del router inalámbrico, cambiando las que vienen por defecto del fabricante u operador de telefonía (habitualmente “1234”, etc.).
- ✓ Filtros MAC: Cuando un equipo informático se conecta a Internet se le asigna una dirección IP. Sin embargo, hay otro tipo de identificador o número distintivo único que no pertenece a la PC, ni se configura mediante el Sistema Operativo, sino que está asociado a la tarjeta de red del equipo informático directamente, este identificador se denomina número MAC y es único a nivel mundial para cada una de

las tarjetas de red de los distintos fabricantes. Por ello es posible habilitar un filtro en los routers Wi-Fi para que sólo se conecten a nuestra red los dispositivos con un determinado número MAC.

- ✓ Límites DHCP: una forma sencilla de evitar robos de señal es limitar el número de computadoras que pueden conectarse a la misma. Esto es posible a través del servicio DHCP del router de Internet que usted maneja, que se encarga de asignar direcciones IP automáticamente a cada equipo informático que se conecta a él. Así, si tenemos dos PC, con direcciones IP correlativas, acotaremos el rango entre los números de estas direcciones y así ningún otro ordenador podrá entrar a nuestra red porque no habrá direcciones IP disponibles. Esto se configura habitualmente en los routers Wi-Fi en la sección DHCP : “Ip Inicial – Ip Final”.

4. **Robo de Identidad:**

En ocasiones usamos claves para acceso a servicios on-line fácilmente descifrables (la fecha de nuestro cumpleaños, nuestro nombre con algún número sencillo a continuación, o el básico 1234).

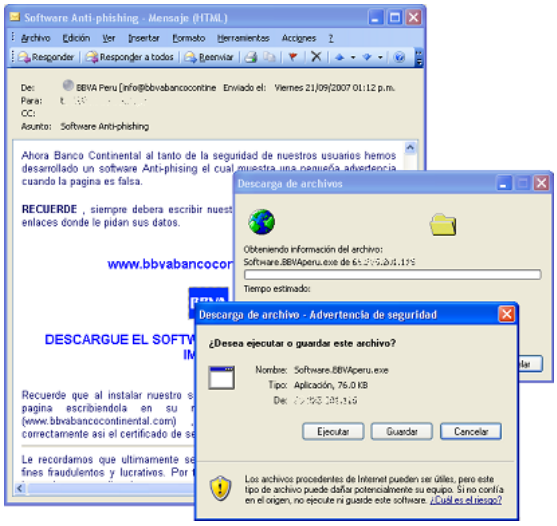
Medidas para protegernos contra el robo de identidad:

- ✓ Contar con una buena contraseña de construcción compleja. Para ello es importante evitar contraseñas que tengan algún significado, como nuestra fecha de nacimiento, nuestro teléfono, etc. Evitar palabras en cualquier idioma que puedan estar en un diccionario, ya que existen sofisticados programas de ataques por diccionario que comprueban las coincidencias con todas las palabras de un idioma. Es importante que la contraseña contenga letras mayúsculas, minúsculas y números, siendo deseable que también incluya algún carácter distintos de estos (*, -, +, etc.)
- ✓ Se debe de tomar las siguiente precauciones:
  - ➢ Nunca enviar contraseñas por e-mail, Messenger, chats, etc.
  - ➢ No emplear la misma contraseña para todos los servicios.
  - ➢ Intente cambiar periódicamente la contraseña.
- ✓ Una posible técnica para construir una contraseña puede ser recordar una frase que nos diga algo, coger la inicial de cada palabra, poner una letra en Mayúsculas y añadirle algún número significativo para nosotros, ej.
  - ➢ Frase a recordar: “Mi mama hace una comida exquisita”
  - ➢ Número a recordar : 07
  - ➢ Una posible contraseña de calidad 7 sobre 10 : “Mmahaucoex07”
  - ➢ Otra posible contraseña de calidad 9 sobre 10 : “Mmahaucoex(76)”

5. **Malware:**

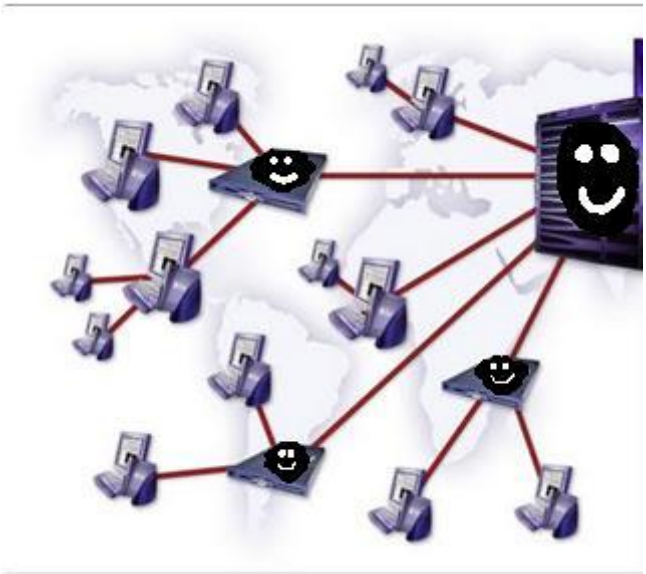
Las formas más comunes de MalWare son los virus, que intentan provocar funcionamientos anómalos en nuestra computadora, los troyanos que permiten el

acceso remoto, y el spyware, adware y bots, que son MalWare (Programas de Códigos Malicioso) que recopilan información sobre el dispositivo y la persona que lo utiliza para enviar ésta información al exterior (que por lo general son empresas de marketing para la elaboración de perfiles comerciales según nuestros hábitos de navegación, etc.).



6. Entrada no autorizada a su computadora desde otras redes.

Se estima que hoy en día una computadora conectada a una red pública de comunicaciones, como Internet, no aguantará más de 15 minutos sin sufrir algún intento de intrusión directa desde la red pública del Internet. Por este motivo, junto a que el Sistema Operativo Windows es un sistema que por defecto se instala con múltiples servicios de entradas que siempre se encuentran activos (carpetas compartidas, etc.), es necesario tener en funcionamiento algún tipo de cortafuegos (firewall) personal siempre en nuestra PC, el cual nos avisará ante cualquier intento de entrada o salida de datos de nuestra computadora para que autoricemos ésta expresamente.



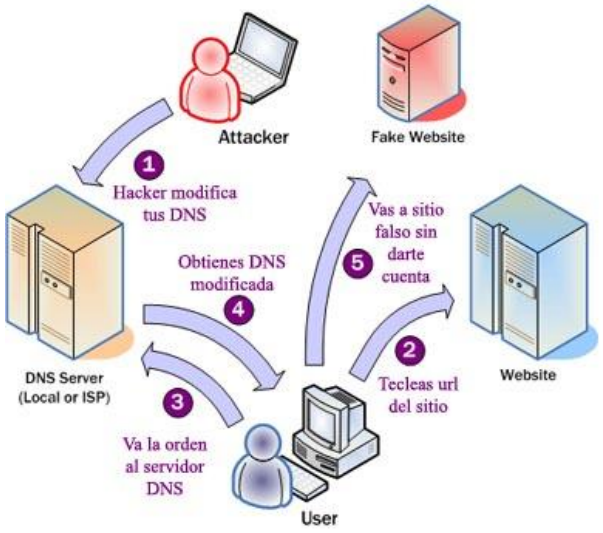
7. Explotación de vulnerabilidades de su Sistema Operativo y programas de Internet (navegador Web, etc.):

Los sistemas operativos actuales, y en especial los de la familia de Microsoft, contienen múltiples vulnerabilidades que los atacantes informáticos aprovechan para, mediante su explotación, entrar en nuestra computadora o enviarnos algún tipo de Malware. Es muy importante, para evitar esto, mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles del fabricante. Ej. Actualizaciones Windows:

http://windowsupdate.microsoft.com

8. Pharming:

Es una de las formas de estafa que desvía al usuario desde el sitio original hacia uno de apariencia similar que busca obtener las claves de éste. Hay que poner atención porque el sitio puede ser idéntico al original, e incluso imitar la dirección web.



Medidas contra el Pharming:

- ✓ Actualice sus claves bancarias, utilice una que sea simple de recordar, pero no considere su nombre, el de su mascota, su cumpleaños o el clásico 1234. Tampoco las anote en ningún documento.
- ✓ Nunca envíe contraseñas ni datos de tarjetas de crédito, cuentas bancarias o similares por email. Ninguna entidad seria se los solicitará por ese medio. Y si recibe un mail que parece legítimo y requiera ese tipo de información, no envíe esos datos.
- ✓ Cuando quiera ingresar al sitio Web de la Caja Metropolitana, digite la url en el navegador, no la copie y pegue de algún mail.
- ✓ No use la opción "guardar contraseña" en las pantallas iniciales de sitios de Internet.
- ✓ Fíjese en los íconos de seguridad: suele ser un candado en la barra del navegador o en que la url comience con https.
- ✓ Actualice periódicamente su antivirus y antispyware, así como los parches de seguridad de su(s) navegador(es).
- ✓ Mientras más software tenga a su disposición (firewall, antivirus, antispam, detección de intrusos, etc.) menor será el riesgo al que se verá expuesto, pero nunca utilice software ilegal para protegerse
- ✓ Desconfíe de las aplicaciones que le prometen mostrarle quiénes lo han eliminado de alguna red social.
- ✓ Desconfíe de regalos, concursos o promociones fáciles de obtener, ni responda a mensajes que solicitan datos en forma urgente.
- ✓ Desconfíe de los enlaces: verifique el dominio al cual apunta un link antes de hacer clic o enviar datos a un mail.

9. Skimming:

También conocido como clonación de tarjetas de crédito o debito, consiste en la duplicación de tarjetas de crédito o debito sin el consentimiento del dueño de la tarjeta. Los delincuentes que se dedican a esto utilizan diferentes tipos de dispositivos electrónicos que los ayudan a clonar de las tarjetas.

El problema es que los dueños de las tarjetas de crédito o debito no se dan cuenta de esto hasta que les llega el estado de cuenta o cuando van a comprar algo en una tienda o por internet con su tarjeta y le dicen que su tarjeta está al límite o se la rechazan (declined). Y cuando esto sucede quiere decir que ya le robaron su identidad.

Medidas contra el Skimming:

- ✓ Cuando pague en una tienda con su tarjeta de crédito o debito, preste mucha atención de por donde el empleado pasa la tarjeta, no pierda de vista su tarjeta.

También este atento sobre las manos del empleado ya que algunos Skimmers son tan pequeños que caben en la palma de la mano.

- ✓ Cuando termine de comer en un restaurante NO le entregue la tarjeta al mesero, vaya usted mismo y pague la cuenta antes de irse. El mesero no lo puede obligar a usted a que le entregue la tarjeta para cobrarle.
- ✓ Cuando vaya a retirar dinero de los cajeros asegúrese de que no tenga ningún dispositivo extraño instalado por donde se introduce la tarjeta. Si sospecha de algo extraño notifíqueselo inmediatamente al Administrador o Jefe Operativo de la Agencia del establecimiento donde se encuentra el cajero.
- ✓ Cuando vaya a entrar su número secreto (PIN) en un cajero cubra con su otra mano el cuadro de botones, ya que los delincuentes que se dedican al Skimming instalan pequeñas cámaras que apuntan hacia el cuadro de botones del cajero para ver el número secreto que usted entra.
- ✓ La Caja Metropolitana le ofrece servicios online (por Internet) aproveche esta ventaja ya que le permite a usted monitorear sus estados de cuentas y transacciones diariamente, así no tendría que esperar hasta que le llegue su estado de cuenta todos los meses para verificar si hay alguna compra, retiro de dinero o transacción sospechosa.

MEDIDAS DE PREVENCION

Además de las medidas indicadas en el apartado anterior, expondremos a continuación algunas medidas adicionales necesarias de aplicar para minimizar el riesgo de sufrir un fraude informático.

Consejo 1: Un protocolo de seguridad antivirus/MalWare

- ✓ Instalar un antivirus de calidad y software anti espía (spyware) y asegurar al menos semanalmente, siendo deseable a diario, la actualización de las bases de datos de virus.
- ✓ Chequear CDs antes de acceder a sus contenidos, sólo una vez, al comprarlos o adquirirlos y marcarlos de tal modo que se pueda verificar posteriormente. En el caso de CDs regrabables, deberán chequearse cada vez que se acceda a ellos y no tan solo una vez.
- ✓ Formatear todo dispositivo USB, etc., adquirido nuevo, ya que pueden contener virus aún desde el proceso de fabricación.
- ✓ Revisar todo dispositivo externo que provenga del exterior, es decir que no haya estado bajo nuestro control, o que haya sido introducido en la computadora.
- ✓ Si nos entregan un dispositivo de almacenamiento externo (CD, USB, etc.) y nos dicen que está revisado, NO CONFIAR NUNCA en los procedimientos de otras personas que no seamos nosotros mismos. Nunca sabemos si esa persona sabe operar correctamente su antivirus. Puede haber revisado sólo un tipo de virus y dejar otros sin controlar durante su escaneo, o no tener actualizado su antivirus.
- ✓ Para bajar páginas de Internet, archivos ejecutables, etc., definir siempre en el PC una carpeta o directorio para recibir el material, y escanear con el antivirus. Nunca ejecutar o abrir antes del escaneo ningún tipo de software.
- ✓ Evite navegar por sitios Web de dudosa reputación, como sitios warez (sitios que ofrecen programas y cracks, serial, key maker u otros para activación de software).
- ✓ Nunca abrir un adjunto de un e-email sin antes chequearlo con nuestro antivirus. Si el adjunto es de un desconocido que no nos avisó previamente del envío del material, directamente borrarlo sin abrir.

- ✓ Al actualizar el antivirus, verificar la computadora completamente, realice un análisis completo. En caso de detectar un virus, proceder a verificar todo lo que haya tenido contacto con la computadora (CDs, USB, ZIP's, etc.)

Quien navega en Internet nunca estará totalmente exento de ser víctima de algún software maligno o de un ataque informático, pero con los anteriores consejos se puede minimizar la exposición. De su grado de cuidado y precaución dependerá el no ser víctima de este tipo de fraudes.

Consejo 2: Protección en el uso de correo electrónico

- ✓ No ejecute ficheros de programa, o cualquier otro tipo de ficheros adjuntos -típicas gracias navideñas, etc.-, que le envíen por correo electrónico, a menos que esté seguro de su origen y contenido. Así evitará virus, troyanos y otro tipo de MalWare en su equipo informático.
- ✓ A la hora de confiar en algún documento adjunto que le hayan enviado por correo electrónico, según el emisor del mismo, tenga en cuenta, que muchos virus y otros tipos de MalWare, una vez ha infectado un equipo informático, pueden reenviarse automáticamente a todas las direcciones de correo de la libreta de direcciones del equipo infectado, simulando ser el propietario del equipo. Por este motivo, incluso en el caso de confiar en el origen de un correo -correo proveniente de un emisor conocido-, desconfíe de éste y sus ficheros adjuntos en aquellos casos en que el Asunto de dicho correo incluya textos en inglés, no habituales de la persona que le envía el correo -emisor-, etc.
- ✓ En cualquier caso recuerde, **NO ABRA NUNCA UN DOCUMENTO ADJUNTO EN SU CORREO ELECTRÓNICO SIN ANTES VERIFICAR SU AUTENTICIDAD DE ORIGEN Y CHEQUEAR SU CONTENIDO CON UN ANTIVIRUS ACTUALIZADO.**

Nota. Para escanear un documento adjunto, guárdelo en una carpeta temporal sin abrir este, y a continuación chequee dicho archivo con su antivirus, tan solo en el caso de que su Antivirus dé el visto bueno al fichero adjunto tras su escaneo, puede proceder a abrir éste.

- ✓ Desactive la visualización automática de los documentos adjuntos y contenido de correos, en su software de correo electrónico. De este modo evitará otros tipos de ataques que se producen, ya no mediante ficheros adjuntos infectados, sino mediante códigos de ataque introducidos en el propio contenido del correo electrónico en el texto del mensaje.
- ✓ De este modo, al pinchar sobre la línea de un nuevo correo, este no mostrará su contenido automáticamente, pudiendo usted eliminarlo de forma segura en casos de no reconocer claramente al emisor. Para ver su contenido deberá hacer expresamente "doble clic" sobre el correo.

Consejo 3: Como protegerse del phising

- ✓ El phishing es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Resumiendo "todos los datos posibles" para luego ser usados de forma fraudulenta.
- ✓ Se puede resumir de forma fácil, engañando al posible estafado, "suplantando la imagen de una empresa o entidad pública", de esta manera hacen "creer" a la posible víctima que realmente los datos solicitados proceden del sitio "Oficial" cuando en realidad no lo es.

- ✓ El phishing puede producirse de varias formas, desde un simple mensaje a su teléfono móvil, una llamada telefónica, una Web que simula una entidad, una ventana emergente, y la más usada y conocida por los internautas, la recepción de un correo electrónico. Pueden existir más formatos pero en este documento solo mencionamos los más comunes;
- ✓ Una primera y eficaz medida de protección, es no hacer clic en enlaces a direcciones
- ✓ Web que le envíen entre el texto de un correo electrónico, dado que la dirección de destino puede estar falseada y usted sufrir un ataque de "PHISING".
- ✓ Recuerde, para visitar sitios Web que le envíen en un correo electrónico, teclee la dirección de cada sitio directamente en la barra de direcciones -URL- de su navegador Web. No acceda NUNCA POR ENLACES PROCEDENTES DE CUALQUIER SITIO, y en especial que le hayan llegado por correo electrónico.
- ✓ Finalmente, recuerde que nosotros como la Caja Metropolitana o alguna otra entidad bancaria o similar, NUNCA le enviará una solicitud de cambio de contraseña, modificación de sus datos bancarios, etc., por correo electrónico.
- ✓ No atienda a correos enviados por entidades de las que no es cliente en los que le pidan datos íntimos o que afecten a su seguridad.
- ✓ No atienda a sorteos u ofertas económicas de forma inmediata e impulsiva.
- ✓ No atienda a correos que le avisen del cese de actividades financieras recibidos por primera vez y de forma sorpresiva.
- ✓ No atienda a correos de los que sospeche sin confirmarlos telefónica o personalmente con la entidad firmante.

Software básico de seguridad para el puesto de usuario bajo Windows XP/2000/2003

✓ **Antivirus:**

Puede ser un Antivirus comercial de reconocido prestigio y muy ligero: debe de ocupar pocos recursos de la PC.

✓ **Navegador Web:**

Se debe de utilizar navegadores web con los ultimos niveles de seguridad y actualizaciones automáticas transparentes al usuario.

✓ **Firewall. Windows XP**

Microsoft Windows incorpora un cortafuegos básico por defecto, asegúrese que está activo en "Inicio>Panel de control>Firewall de Windows".

✓ **Anti Spyware:**

Las herramientas de este tipo eliminarán los distintos tipos de software espía que muchas páginas de Internet por la simple navegación en sus contenidos se instalarán la PC.