

## FRAUDE ELECTRÓNICO

### 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 del banco del usuario o cualquier otro organismo de cara a obtener su información privada, como la contraseña para operar a través de Internet con el banco, etc.

Medidas contra el Phishing:

\* Nuestro banco o cualquier otra organización nunca nos 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.

\* Navegadores de última generación como Firefox 2.x (<http://www.mozilla.org>) e Internet Explorer 7 vienen equipados con herramientas antiphishing. En el caso de Firefox, incluso puede informar acerca de la URL (Universal Resource Locator) 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 puede 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 al 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, 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 <http://www.inixa.com> • info @ inixa.com 3/13 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.)

\* 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 departamento es el que mejores servicios ofrece”
- \* Número a recordar: 76
- \* Una posible contraseña de calidad 7 sobre 10 : “Mdeeqmso76”
- \* Otra posible contraseña de calidad 9 sobre 10 : “Mdeeqmso(76)”



## **5. Malware:**

Las formas más comunes de MalWare son los virus, que intentan provocar funcionamientos anómalos en nuestro ordenador, los troyanos que permiten el acceso remoto, y el spyware, adware y bots, que son MalWare (Malicious Software) que recopilan información sobre el dispositivo y la persona que lo utiliza para enviar ésta a al exterior (empresas de marketing para la elaboración de perfiles comerciales según nuestros hábitos de navegación, etc.).

## **6. Entrada no autorizada a nuestro ordenador desde redes de comunicación:**

Se estima que hoy en día un ordenador conectado 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 de comunicaciones. Por este motivo, junto a que MS Windows es un sistema que por defecto se instala con múltiples servicios de entrada activos (carpetas compartidas, etc.), es necesario tener en funcionamiento algún tipo de cortafuegos personal siempre en nuestro PC, el cual nos avisará ante cualquier intento de entrada o salida de datos de nuestro ordenador para que autoricemos ésta expresamente.

Algunas medidas para protegernos

- \* 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 a posteriori el chequeo. En el caso de CDs regrabables, deberán chequearse cada vez que se acceda a ellos y no tan solo una vez.
- \* Formatear todo disquete virgen, dispositivo USB, etc., adquirido nuevo, ya que pueden contener virus aún desde el proceso de fabricación.
- \* Revisar todo disquete o dispositivo externo que provenga del exterior, es decir que no haya estado bajo nuestro control, o que haya sido introducido en el PC.
- \* Si nos entregan un dispositivo de almacenamiento externo (disquete, 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 \* 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-mail 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 el PC completamente -análisis completo-. En caso de detectar un virus, proceder a verificar todos nuestros soportes que hayan tenido contacto con el PC (disquetes, CDs, USB, ZIP's, etc.)

## 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 fichero adjunto que le hayan enviado por correo electrónico, según el emisor del mismo, tenga en cuenta, que muchos virus y otro tipo 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 FICHERO ADJUNTO EN SU CORREO ELECTRÓNICO SIN ANTES VERIFICAR SU AUTENTICIDAD DE ORIGEN Y CHEQUEAR SU CONTENIDO CON UN ANTIVIRUS ACTUALIZADO.**

<http://orion.ciencias.uniovi.es/cripto/talks/JRilo-Seguridad-Oviedo-2007.pdf>

### La Condusef sugiere lo siguiente:

- \* No realizar transacciones financieras en computadoras de uso público o que no sean de tu confianza, por ejemplo las que hay en los cafés Internet y centros de negocios de hoteles, aerolíneas y universidades.
- \* Actualizar tu computadora con herramientas antispyware, antivirus y antiadware para que controlen las conexiones de entrada y salida.
- \* Procurar que el personal que instale programas en tu equipo o le dé mantenimiento sea de confianza, ya que algunos programas espías pueden ser instalados físicamente en las computadoras.
- \* Utilizar claves fáciles de recordar pero difíciles de adivinar.
- \* Cambiar tus contraseñas regularmente.
- \* Utilizar al menos ocho caracteres alfanuméricos (letras y números).
- \* Procurar utilizar contraseñas diferentes si cuentas con el servicio de banca por Internet en más de una institución financiera.
- \* Desactivar las opciones de “recordar contraseñas” y “auto completar” de tu navegador.
- \* No te apartes de la computadora cuando tengas abierta una sesión de banca por Internet.
- \* Sólo abrir correos electrónicos o archivos de fuentes conocidas.
- \* No proporcionar información confidencial, ni utilizar los números telefónicos que aparezcan en los correos fraudulentos.
- \* Evitar acceder al servicio de banca por Internet mediante hipervínculos. Teclea directamente la página de Internet de la institución bancaria.
- \* No revelar tu información personal como tu dirección, número de cuenta, número de tarjeta de crédito o de débito y NIP; si requieres hacerlo verifica que el sitio sea seguro y confiable.
- \* Recuerda que las instituciones financieras por lo general, no te pedirán mediante correo electrónico, actualizar información personal, identificadores de usuario y contraseñas.
- \* Mantén disponible la información para contactar los servicios de soporte técnico y de aclaraciones relacionados con la banca por Internet de la institución financiera.

<http://www.eluniversal.com.mx/tudinero/2322.html>

## Consejos generales para evitar fraudes en Internet

- 1- Analiza los siguientes puntos** antes de insertar el número de una tarjeta de crédito: primero y principal fijate si la **URL se corresponde con el sitio en cuestión** y que la misma comience con **HTTPS** (protocolo de seguridad)
- 2- Observa muy bien la interfaz del sitio.** Si la misma es una imágen, y sólo te da espacio para que realices la carga de datos, deberás salir rápidamente. Presta mucha atención a este dato.
- 3- No ingresar datos en correos sospechosos.** Ante esta situación te recomendamos comunicarte con la compañía u organismo supuesto antes de cargar algún formulario.
- 4- Si vas a realizar una compra online procura hacerlo en empresas reconocidas** que tengan una clara política de seguridad y de resguardo de los datos de sus clientes. Caso contrario no hagas ninguna transacción y comunícate con la compañía para obtener más datos.
- 5- Luego de realizar alguna transacción online te sugerimos hacer una copia del formulario o la página de transacción.**
- 6- Tus contraseñas deben ser mezclas de números y letras.** Si son difíciles de recordar ten a mano un cuaderno con las mismas pero nunca utilices contraseñas fáciles como fechas especiales y relacionadas con tu vida.
- 7- Evita todo tipo de correo electrónico que te ofrezca “Dinero fácil”** o te solicite montos de dinero por adelantado. En la mayoría de los casos son fraudulentos.

<http://gruvix.com/7-consejos-para-evitar-el-fraude-online/>

### Seguridad en Internet

Nunca bajar programas de un sitio dudoso o atender avisos emergentes que aseguran que tu computadora ha sido contagiada, ya que seguramente se tratará de un instalador de un software espía, para acceder a la información de tu computadora.

<http://mx.finanzaspracticas.com/1704-Como-protegerte-del-fraude.note.aspx>