GUÍA BÁSICA DE SEGURIDAD EN INTERNET.

Lo que TODO el mundo debe saber, especialmente a la hora de hacer transacciones comerciales.

***Un mensaje previo*:**

ante todo, **tranquilidad**. Los datos de una tarjeta de crédito pueden ser robados/copiados online o en cualquier tienda o restaurante al ir a hacer el pago (esto pasa muchísimo más de lo que la gente cree). Normalmente, cuando esto ocurre, si se detectan rápido las compras irregulares y se avisa al banco, los emisores de las tarjetas suelen hacerse cargo del dinero defraudado.

Aunque el robo de los datos de tarjetas en internet es real y existe, es muchísimo más fácil perder la cartera con las tarjetas dentro. Así que la primera medida es revisar el estado de los bolsillos en todos nuestros pantalones o los cierres de los bolsos, y no comprar pantalones con bolsillos tan escasos que una cartera pueda caer fácilmente o llevar un bolso en el que sea fácil meter y sacar manos sin permiso...

Peligros

Al operar en internet hay 3 cosas que evitar:

1. Que lean nuestros datos **dentro de nuestro ordenador**.
2. Que lean nuestros datos **mientras viajan por internet**.
3. Que **el sitio al que damos nuestros datos para hacer el pago los pierda** (o se los deje quitar).

Vamos a ver qué hacer para evitar estos tres casos y poder comprar tranquilos por internet (u operar con el banco, porque lo visto aquí debería también aplicarse al uso de la banca online).

Antes, el RESUMEN FINAL

Aunque esta guía es muy breve, si no quieres leer más detalles, aquí tienes los consejos fundamentales:

- **No hacer click en cualquier link. Aprender a distinguir los enlaces de spam.**
- **Actualizar automáticamente los programas, sobre todo el navegador y el flash.**
- **Al enviar información importante a un sitio, comprobar siempre que la dirección empieza por https y que la información del certificado del sitio es correcta y está actualizada.**
- **Realizar los pagos en internet solo a través de entitades de mucho prestigio.**

1.- Que no lean nuestros datos desde dentro.

El peligro aquí es tener instalado en nuestro ordenador algún programa maligno (un troyano o keylogger) que pueda enviar lo que tecleamos a algún lugar externo. Sería como alguien que nos viera teclear por encima del hombro.

¿Cómo se evita?

- Teniendo un buen software antivirus, actualizado y funcionando siempre.
- **Activando las actualizaciones automáticas.** Sobre todo del navegador web, flash o java, pero también de Windows y los principales programas que utilizamos. Puede ser molesto, pero es MUY importante.
- **No haciendo click en los enlaces de emails o mensajes que nos llegan de forma extraña** y sin haberlo pedido, aunque procedan de algún amigo. Esos enlaces lo que buscan es llevarnos a páginas que se aprovecharían si no tenemos perfectamente actualizado alguno de los elementos anteriores. Y no solo se reciben por mail, sino que pueden existir en Facebook o cualquier página web.
- No instalando programas dudosos o que provengan de "cualquier sitio". El software pirata muchas veces se distribuye con este tipo de virus.

¿Y si estoy infectado?

Ante cualquier sospecha de tener un troyano en el ordenador, **no se deben realizar operaciones con información crítica utilizando ese ordenador**, al menos hasta que se haya reinstalado o se esté seguro de que ha sido correctamente revisado.

Un síntoma típico de infección es que tus amigos hayan recibido emails de spam procedentes de tu dirección de correo.

Comentario:

Este caso (el más importante hoy día) tiene dos aspectos importantes: por un lado cómo comportarse, y por el otro cómo mantener un ordenador.

- Respecto a cómo comportarse: es fundamental **aprender a identificar los mensajes de correo maliciosos**, y jamás hacer click en los enlaces que incluyan, por muy sugerentes que sean los textos que invitan a hacerlo. Algunas pistas para identificar un correo malicioso:
  - Tiene palabras y formatos poco habituales, o en otros idiomas.
  - Tiene un texto, formato y temática un poco raros para ser de la persona que supuestamente nos envió el mensaje.
  - Su mensaje principal es hacer click en un enlace para ver algo.
- Respecto a cómo mantener un ordenador: los ordenadores deben estar bien instalados y mantenidos, y configurados para actualizarse. Cumplir correctamente con este apartado, especialmente al principio, es la mejor forma de controlar los riesgos

Curiosidad: los virus y troyanos son muy utilizados por el crimen organizado, pero normalmente se utilizan como base para atacar objetivos más grandes. Si no tienes mucho dinero, no eres uno de esos "objetivos grandes" y es poco probable que seas el objetivo final del robo.

2.- Que no lean nuestros datos mientras viajan por la red.

Simplificando, en internet el tráfico viaja dando “saltos” entre distintos ordenadores (servidores, routers y switches). Alguien que tuviera acceso a estos equipos intermedios podría copiar la información que enviamos. La forma de evitar que esto ocurra es encriptando la conexión entre los extremos. El protocolo seguro HTTPS sirve para que sólo tu ordenador y el servidor de la web con la que te comunicas sepan descifrar el mensaje.

HTTPS es un protocolo muy seguro, así que lo que hay que hacer es asegurarse de que está funcionando correctamente. El peor ataque en este caso tratará de hacernos creer que la conexión está encriptada entre los extremos, aunque no lo esté.

¿Cómo se evita?

JAMÁS envíe información importante, como la de una tarjeta, hasta asegurarse de que en la cajita del navegador **la dirección empieza con https://** (lo normal es que empiece con http:// sin la “s”).

Ilustración 1: En Firefox: lugar de ubicación de la zona verde y el protocolo HTTPS

Ilustración 2: En Chrome, lugar de ubicación de la zona verde y el protocolo HTTPS

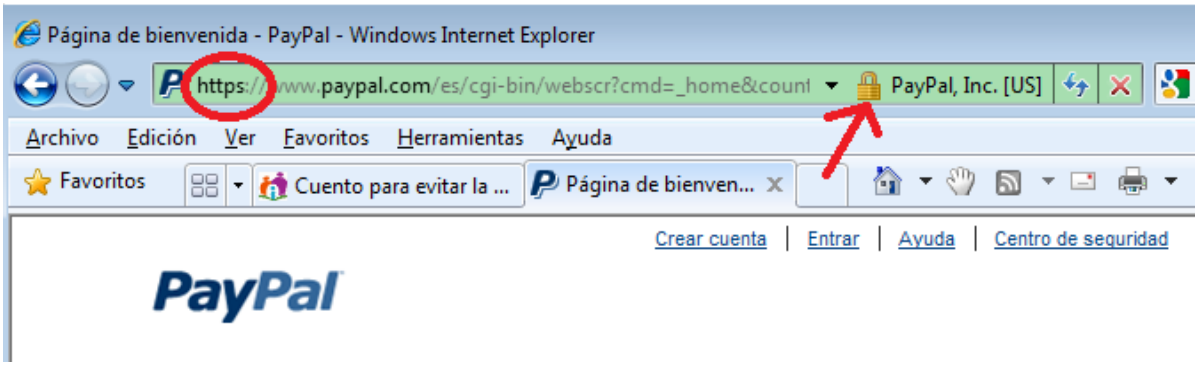

Ilustración 3: En Internet Explorer 8: lugar de ubicación de la zona verde, el icono y el protocolo HTTPS

Utilizar una versión moderna del navegador y comprobar el certificado. En las versiones modernas de los principales navegadores, el inicio de la barra se colorea de verde o aparece un icono (normalmente un candado) junto a la dirección que al pincharlo da información del sitio al que estamos conectados. Hay que asegurarse que la información que vemos ahí coincide con el sitio al que nos queremos conectar. **No basta con ver el candado**, porque alguien podría dibujar un candado que resultara engañoso. **Hay que revisar, SIEMPRE, la información que aparece al pinchar sobre el candado o la parte verde de la barra**. Y si hay dudas, no seguir.

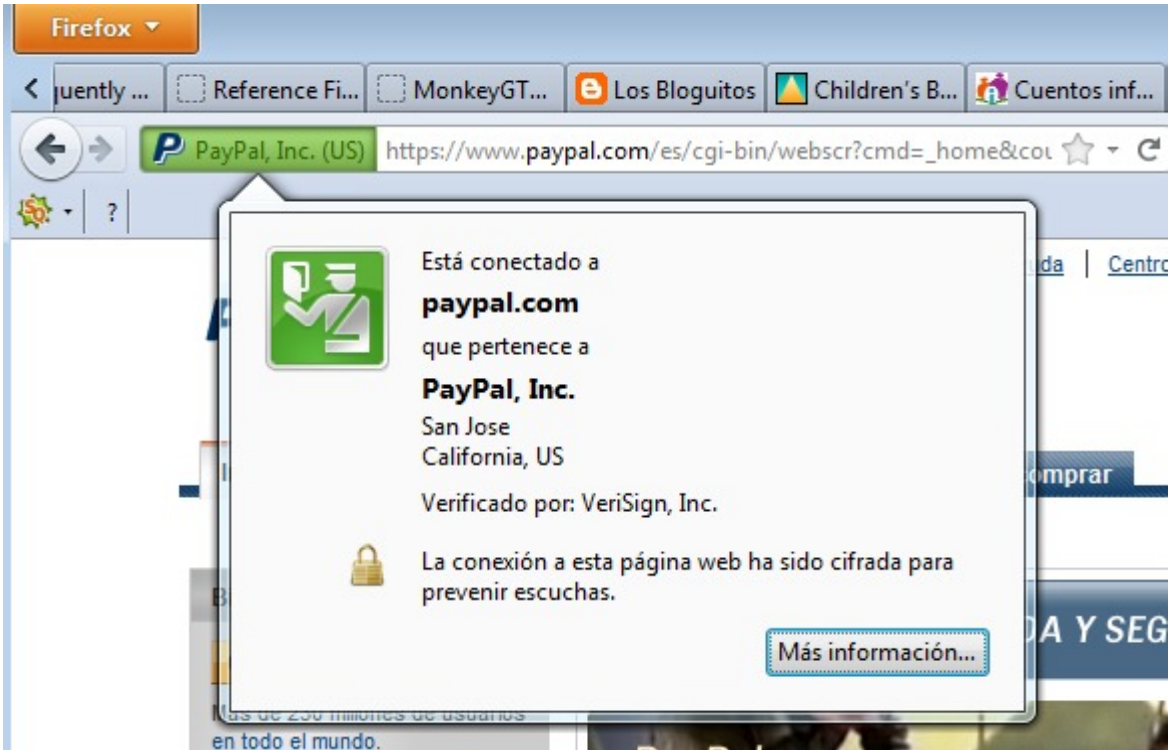

Ilustración 4: En Firefox, información que aparece al pulsar sobre la parte verde de la barra

Ilustración 5: En Chrome, información que aparece al pinchar sobre el candado o la parte verde de la barra

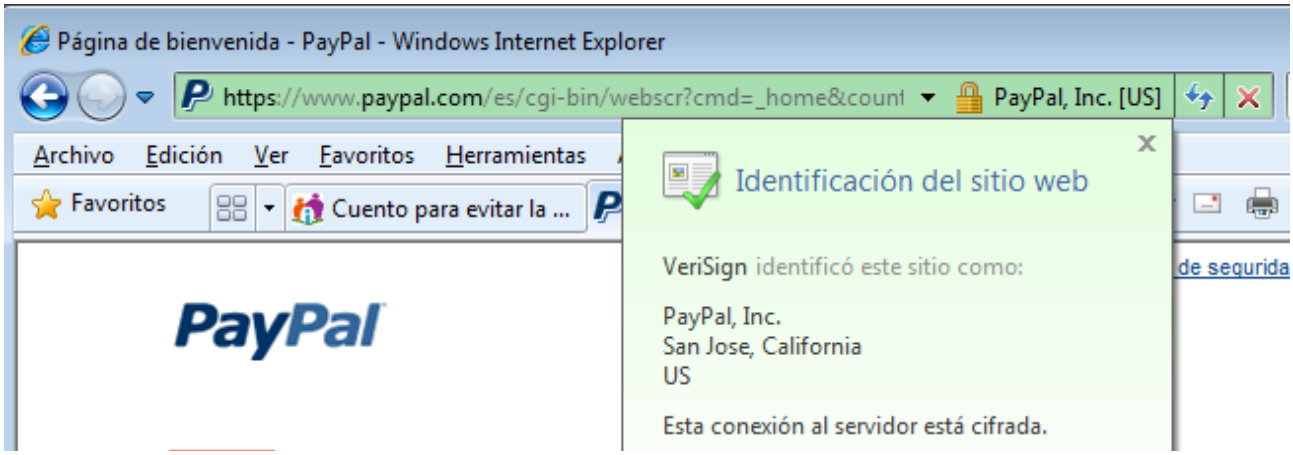

Ilustración 6: En Internet Explore 8: información que aparece al pinchar sobre el candado

Comentario:

Con hacer estas dos sencillas comprobaciones siempre que se envíen datos importantes, se aumenta muchísimo la seguridad de la operación.

3.- Que el lugar de destino no pierda nuestros datos.

Aunque no lo parezca, este es uno de los problemas que podría ocurrir con más facilidad, si los sistemas de esa página web fueran atacados incluso mucho tiempo después de nuestra transacción con ellos. Es decir, que si la web donde pagamos no es muy diligente gestionando sus servidores, podrían poner en peligro la información que guardan sobre nosotros.

¿Cómo se evita?

Aunque no dependa de nosotros, este caso es muy sencillo: basta con **no dar los datos de la tarjeta en cualquier web**, aunque esté bien encriptada y sea segura. Uno no dejaría su tarjeta en un sitio mugriento con pinta de ocultar cientos de ladrones, ¿verdad? Pues como no podemos verlos, así son todos los sitios en internet hasta que demuestran lo contrario.

Por eso lo mejor es **pagar sólo a través de las webs y procesadores de pago de las empresas con mejor reputación**. Para ellas los controles son más severos, sus medidas de seguridad más eficaces, y están en mejores condiciones de compensar al usuario en caso de problemas.

¿Cuáles son estas webs de empresas más fiables?

- Bancos conocidos y webs de organismos oficiales.
- gestores principales de pagos online, como PayPal, Authorize.net, WorldPay, Verisign o Google Checkout
- tiendas online de gran reputación como Amazon

... pero no son muchas más. Sólo con las mencionadas arriba puede pagarse en la gran mayoría de los sitios web.

Por supuesto hay muchas más webs totalmente fiables. Pero si se quiere ir sobre seguro, y no se tiene un conocimiento claro del asunto, lo mejor es asegurarse.

Comentario:

Esto no nos protege de los problemas de seguridad que pudieran tener estas grandes empresas, pero un problema en ellas sería tan grave y afectaría a tanta gente que se contaría con el apoyo de los emisores de tarjetas, la policía y todos los medios necesarios para limitar al mínimo los daños.

¿ALGO MAS?

Pues no, nada más. Simplemente **aplicando estos controles, tus transacciones en internet estarán entre el 1% más seguro** de todas las que se producen. Y el robo de información de tarjetas en internet, a pesar de todo lo que se dice, está muy, muy lejos de llegar al 99%.

RESUMIENDO:

- No hacer click en cualquier link. Aprender a distinguir los enlaces de spam.
- Actualizar automáticamente los programas, sobre todo el navegador y el flash.
- Al enviar información importante a un sitio, comprobar siempre que la dirección empieza por https y que la información del certificado del sitio es correcta y está actualizada.
- Realizar los pagos en internet solo a través de entitades de mucho prestigio.