CONSEJOS PARA UN USO SEGURO DE INTERNET

PRECAUCIONES EN TRANSACCIONES ECONOMICAS.

- No abandonar las copias de los resguardos de compra en las proximidades de los Terminales de Punto de Venta (T.P.V.), pues contienen información sobre las tarjetas que puede ser utilizada tanto en Internet como fuera de red.
- No teclear número de tarjeta ni clave alguna en casillas de correo electrónico ¡aunque parezca que viene de tu banco!.
- No teclear número de tarjeta ni clave alguna si en la dirección de tu navegador no se ve el comienzo de la dirección de tu banco que tu tecleaste al entrar. Vamos que si tu banco es el BBVA, pues que ahí se vea BBVA por algún lado antes del ".com" o el ".es". Y no se te ocurra poner clave alguna en una página del tipo "www.vayaustedasaber.com" por mucho que la pagina tenga el mismo aspecto que la de tu banco.
- Evidentemente, no es lo mismo "www.tubanco.es" que "www.tubanco.com": el ".com" o él ".es" ¡son importantes! pues se refieren a ¡ sitios distintos !.
- No utilizar la tarjeta, si el establecimiento no merece su confianza. Se conocen casos en los que ese ha utilizado el número de la tarjeta y el nombre de su titular, por personal del propio establecimiento.
- No introducir el número de la tarjeta en páginas de contenido sexual o pornográfico, en los que se solicita como pretexto, para comprobar la mayoría de edad.
- No facilitar más datos personales de los necesarios.
- Al enviar información, compruebe que, en la parte inferior del navegador Explorer, aparece un candado amarillo o un candado cerrado, en el caso de Netscape. Esto indica que sus datos viajan encriptados.
- Compruebe que los cargos recibidos se corresponden con los realizados.

PRECAUCIONES SOBRE EL CORREO ELECTRONICO.

- No abrir mensajes de correo, de origen desconocido. Eliminarlo, directamente.
- No ejecutar ningún archivo adjunto que venga con mensajes sugerentes.
- Adopte las medidas necesarias, cuando le ofrecen "regalos" sustanciosos y, para recibirlos, tiene que llamar por teléfono a prefijos 906.
- No facilitar la dirección electrónica con "demasiada" ligereza.
- Tenga activado, constantemente, un antivirus.
- Viste páginas especializadas sobre seguridad informática.
- Para que sus datos viajen seguros, envíe sus mensajes cifrados.

MEDIDAS DE SEGURIDAD PARA USUARIOS PARTICULARES.

- No facilitar datos personales si no existe una completa seguridad sobre quién los va a recibir.
- No facilitar más datos personales que los necesarios.

- Exigir, siempre, "conexiones seguras". Asegúrese que, al transmitir datos sensibles, en la parte inferior del navegador Explorer, aparece un candado amarillo y, en el caso de Netscape, un candado cerrado.
- Comprobar los certificados de seguridad, en páginas que requieren datos personales.
- Comprobar los certificados de seguridad, en páginas que requieren datos personales.
- Utilizar un buen producto antivirus y actualizarlo, frecuentemente.
- Extremar la precaución en los archivos que reciben en sesiones de chat.
- Actualizar los sistemas operativos y navegadores, con los parches que publican las firmas especializadas de software.

MEDIDAS A DOPTAR POR PEQUEÑAS EMPRESAS.

- Cambia las contraseñas, periódicamente.
- Exigir contraseñas de calidad.
- No dejar las contraseñas guardadas en el disco duro.
- Confiar la gestión de la red a un responsable.
- Diseñar un protocolo del uso de la red.
- Controlar las operaciones y transacciones, en horario no habitual por ello.
- Establecer una política adecuada de copias de seguridad.

MEDIDAS PARA EVITAR FRAUDES TELEFÓNICOS

- Control de las facturas, para vigilar si el gasto facturado se corresponde con las comunicaciones realizadas.
- Comprobar los números de teléfonos a los que se ha llamado, para identificarlos como conocidos. Se dan casos de facturaciones de llamadas no realizadas por el interesado. En ese caso, antes de adoptar otras medidas, consulte a los usuarios.
- Ante posibles sustracciones, tenga precaución con la correspondencia procedente de bancos y operadoras telefónicas para que, en caso de no recibir información puntual sobre consumos, ponerlo en conocimiento de la compañía, solicitando un duplicado y advirtiendo de lo sucedido.
- No facilitar los números de teléfono, tanto fijo como móvil, a personas desconocidas que los soliciten, bajo cualquier pretexto, ya que se han detectado casos en los que, sólo, intentan conocer las características de las línea para posibles desviaciones.
- Ante una llamada telefónica equivocada, cortar la comunicación, rápidamente, para evitar el posible desvío de llamadas con cargo a la factura de la persona que recibe la llamada.
- En el caso de tener contratada la modalidad de "llamada a tres", extremar las precauciones, ya que, con un programa informático, se puede rastrear la línea y producirse una intrusión a ella, para realizar llamadas internacionales, con cargo al titular del teléfono.
- No aceptar llamadas a cobro revertido si no se está absolutamente seguro de conocer a quien lo pide. Puede tratarse de una llamada fraudulenta y pagar gastos de miles de pesetas por el engaño