Protegerse de las estafas en Internet

Utilizar la Red para comprar, efectuar gestiones bancarias o disfrutar de servicios de pago requiere tomar unas mínimas precauciones

"¡Saludos, respetado cliente! Estamos en el deber de comunicarle que el servicio de apoyo técnico de nuestro banco debe realizar una serie de trabajos profilácticos". Esta frase es real y ha llegado a cientos de miles de buzones de correo electrónico atribuida a una conocida caja de ahorros. Su contenido es más que sospechoso y, sin embargo, en muchas ocasiones consigue su objetivo: pasar por un correo legítimo. Es el típico caso de 'phishing' (la variante de estafa más conocida de Internet) donde se engaña al usuario para que recale en una determinada página web haciéndole creer que es la de su banco (suelen ser copias de las reales) y deje sus datos bancarios. Después, los delincuentes utilizan esos datos en la página real del banco, introducen las claves del usuario y sacan dinero de su cuenta sin que éste se dé cuenta.

Un reciente estudio del Instituto Nacional de Tecnologías de la Comunicación (INTECO) estima que con esta estafa los ladrones obtienen de media casi 600 euros por cada internauta 'que pica'. Además, se calcula que una tercera parte de la población 'conectada' ha sido objeto de fraude en alguna ocasión. No se conocen cifras precisas, pero se calcula que el fraude en Internet mueve miles de millones de euros en todo el mundo.

¿Por qué picamos?

Más que con la tecnología punta, los estafadores juegan con la buena fe del usuario. Los 'correos trampa' están diseñados para que el internauta crea que está en la página de su banco y ofrezca datos tan importantes como las contraseñas. Otros correos buscan generar un impulso de adquisición de objetos o de ganancia económica. Por ejemplo, un clásico es el truco del 'heredero nigeriano' en el que un exdictador africano pide ayuda para sacar fondos del país. Todo mentira, claro. En este caso, como en muchos otros, la falta de información juega un papel importante: según el estudio del INTECO, aproximadamente la mitad de los intenautas no relacionan la palabra 'phishing' con estafas: no saben lo que es y es posible

que hayan sido estafados en más de una ocasión sin saberlo. Simplemente contestan a estos mensajes creyendo que se tratan de correos enviados por su banco de toda la vida.

¿Cómo defenderse y navegar con seguridad?

La mejor manera de mantenerse protegido ante los correos tramposos es facilitar la dirección de correo electrónico personal únicamente a las personas allegadas sin que, en ningún momento, queden registrados en alguno de los servicios de la red en los que se solicita al usuario una inscripción inicial para entrar. Sin embargo, esta máxima no siempre es posible, ya que son muchas las ocasiones en que es imprescindible dejar una dirección de correo, como en el momento de contratar un billete aéreo on line o de realizar cualquier compra. En estos casos se puede optar por un email desechable como los de Spamgourmet.com que se autodestruyen en unos minutos, o de los servicios análogos de Yahoo! Mail que permiten crear decenas de emails de usar y tirar.

Otra precaución a tener en cuenta es no contestar a las cadenas de mensajes masivos (generalmente jocosos) que corren por la Red entre amigos. Ante la invasión de correos como estos es importante pedir que nos eliminen del envío porque cualquiera que esté incluido puede ver las direcciones de los demás. Esta es una de las principales vías de entrada de los estafadores, ya que muchos ordenadores están infectados por programas espía que captan estas direcciones para revenderlas. Afortunadamente, la eficacia contra los correos electrónicos no solicitados (lo que se conoce como 'spam') de los servicios de correo online (como Gmail o Yahoo! Mail) es muy alta, y filtra la mayoría de mensajes. Pero siempre se cuela alguno, por lo que conviene eliminarlo y enviarlo a la carpeta de 'spam' ante la mínima duda sobre el origen y asunto de un correo. Tampoco hay que fiarse de las direcciones web que se ofrecen en los 'correos trampa', aunque sean del tipo 'https' (lo que se conoce como conexiones seguras).

El correo que contenía el texto con el que se ha iniciado este reportaje ofrecía una conexión teóricamente segura (comenzaba por 'https') que, sin embargo, llevaba al usuario a una página trampa, por lo que el inicio 'https' es una condición necesaria para que una página de pago sea segura, pero no suficiente. Para rematar, se hizo la prueba del filtro anti-phishing del navegador Internet Explorer 7, y éste certificó la página como buena. ¿La solución? No entrar nunca a la página de nuestro banco haciendo clic en el enlace de un correo electrónico o de otra página web y escribir siempre 'a mano' en el navegador las direcciones más comprometidas. Ni siquiera guardarlas en favoritos. No hay que olvidar que los bancos no piden las claves del usuario porque ya las conocen.

MEDIDAS PARA COMPRAR CON SEGURIDAD

La mayoría de webs de comercio electrónico (las que venden entradas para espectáculos, libros, discos o cualquier otro servicio) tienen hoy sistemas de seguridad más que eficientes. Dejar los números de las tarjeta en estos servicios no tiene por qué ser peligroso. Sin embargo, hay una serie de reglas fundamentales para evitar disgustos:

 # No comprar en cualquier sitio de la Red. Buscar siempre los más renombrados o pertenecientes a empresas reconocidas.

 # Comprar siempre que se pueda contra reembolso. En su defecto, se pueden utilizar servicios de micropagos específicos para la Red como PayPal, que son cuentas que el usuario recarga periódicamente según su necesidad, pero que no muestran sus datos bancarios.

 # Asegurarse de que el servicio ofrece la posibilidad de emitir una factura, tal y como obliga la ley. Es una garantía de seriedad.

 # Comprobar que la página donde se dejan los datos de la cuenta es del tipo 'https'. Se muestra un candado o una llave en la barra de direcciones y ésta, además, tiene un color diferente. Sólo así nos aseguraremos de que nadie "capta" la transacción en el camino.