

CECU alerta de nuevas fórmulas de *phishing* utilizando los nombres de VISA Y MasterCard

La Confederación de Consumidores y Usuarios (CECU) ha tenido conocimiento de nuevas fórmulas de *phishing* a través de correo electrónico que pueden confundir a los ciudadanos llevándoles a facilitar datos de su tarjeta de crédito, incluyendo tanto el número de la misma como el código PIN.

El correo, encabezado con los logotipos de las empresas de tarjetas VISA y MasterCard, señala al usuario que alguien ha intentado introducir tres veces consecutivas el código PIN de la tarjeta y, al considerarlo una conducta sospechosa, insta al consumidor a cambiar ese código llevándole a través de un enlace a un formulario en el cual se solicitan datos tan sensibles como el número de tarjeta, el código PIN y otros datos personales.

Ante esta nueva fórmula de fraude, CECU quiere recordar algunas cuestiones relacionadas con la banca on-line y cuestiones de seguridad a tener en cuenta para evitar ser víctima de una estafa de este tipo:

- Como regla general, hay que tener en cuenta que las entidades bancarias no funcionan solicitando datos a través de correo electrónico, por lo tanto, nunca hay que revelar nuestros datos bancarios o nuestras claves por este medio ni a través de un formulario al que se llegue a través de un correo electrónico.
- Para realizar cualquier transacción bancaria a través de internet se debe acceder a la web de la entidad, pero nunca haciéndolo a través de un enlace que recibamos en nuestro correo. Además, una vez en la web del banco hay que tener en cuenta que para dar cualquier dato debemos encontrarnos en una web cifrada: aquella cuya dirección comienza por *https://* y no por *http://*, como habitualmente. Una vez hecha la transacción bancaria se debe cerrar la sesión que hemos iniciado y, en caso de estar en un equipo que utilizan más personas, no dejar la pantalla abierta.
- Finalmente, hay que tener precaución con los correos que contengan archivos adjuntos, ya que es la forma habitual por la cual se puede infectar con virus un ordenador. Algunos virus troyanos son utilizados por los estafadores para captar y enviar la información que teclee el usuario en su ordenador con lo que se pueden facilitar números de cuenta y claves secretas. Utilice antivirus y cortafuegos convenientemente actualizados para evitar ser atacados por un virus de este tipo.



Si finalmente ha facilitado algún dato bancario en alguna de las situaciones señaladas anteriormente informe a su entidad financiera de la situación lo antes posible e infórmese de si es conveniente cerrar la cuenta y abrir una nueva. Observe los cargos realizados a su cuenta tras dar la información y haga saber a su entidad los que no reconoce como suyos. Es preferible que comunique estos cargos fraudulentos por escrito y tenga en cuenta que muchas tarjetas de crédito cuentan con seguros ante este tipo de casos.

Área de Comunicación CECU

N
O
T
A

D
E

P
R
E
N
S
A

