CAMPAÑA FUNCAS DE

CIBERSEGURIDAD EN TUS FINANZAS

funcas

CAMPAÑA FUNCAS DE *CIBERSEGURIDAD EN TUS FINANZAS*

CON motivo de la pandemia, se ha incrementado el número de operaciones financieras *online* lo que, a su vez, aumenta los riesgos relacionados con la ciberseguridad.

Desde el programa Funcas Educa, se ha articulado una campaña de *Ciberseguridad en tus finanzas*, con el objetivo de difundir una serie de recomendaciones para que las operaciones financieras virtuales se realicen de una forma segura, además de dar a conocer qué medidas están llevando a cabo las entidades financieras en este ámbito.

La campaña, se ha dividido en tres oleadas realizadas en junio, septiembre y octubre de 2021.

PRIMERA OLEADA (JUNIO 2021)

CONSEJOS PARA PROTEGER SUS FINANZAS EN INTERNET[1]

LA pandemia ha impulsado nuevos hábitos de los consumidores basados en la digitalización. Acciones cotidianas como la compra semanal o los trámites bancarios se realizan cada vez más por internet. Esa revolución se ha intensificado en los últimos dos años cambiando la manera de los ciudadanos de relacionarse con las entidades bancarias y de gestionar sus finanzas.

El porcentaje de clientes digitales de las entidades financieras sobre su base total de clientes se ha disparado por el efecto catalizador de la pandemia. En enero de 2020, apenas el 28 % de las entidades contaba con más del 60 % de su base de clientes digitalizada y, un año después, eran ya la mitad de las entidades las que tenían más de 6 de cada 10 clientes digitalizados, según una encuesta realizada por el Observatorio de la Digitalización Financiera de Funcas.

La operativa a través de internet es ya algo habitual, pero hay que ser conscientes de que no está exenta de riesgos: fraudes, suplantación de identidad, estafas… Para moverse en un entorno digital seguro, la mejor opción es tratar de prevenir los ataques. La información contenida en un ordenador o en el móvil puede ser mal utilizada por intrusiones no autorizadas y crear una crisis. Los ciberdelincuentes buscan atacar a otros equipos, sitios web o redes para generar caos, bloquear un sistema informático, propiciar la pérdida de datos o hacer que el servidor falle. A nivel individual debemos tomar medidas preventivas.

Este es un decálogo para saber cómo protegerse de estos delitos en el mundo digital.

- Acceder de forma segura. La forma más segura de acceder a la banca digital de cualquier entidad financiera es escribiendo la dirección de la entidad directamente en la barra del navegador y accediendo desde dicha página. También a través de la app del teléfono móvil. Si se accede vía web, debemos asegurarnos de que la dirección web dispone de un buen protocolo de seguridad, es decir, si al inicio de la URL aparece el código https. La 's' indica que es seguro.

- Proteger los datos personales. El banco nunca pedirá por correo electrónico o SMS información confidencial económica o personal, ni credenciales bancarias, números de cuenta o de tarjeta. Nunca debe compartirse información personal y confidencial en la red con desconocidos, especialmente al darse de alta en tiendas webs o plataformas de servicios.

- Crear una buena contraseña. El robo de contraseñas es uno de los ciberdelitos más comunes, por lo que saber crear y proteger nuestras contraseñas tiene que ser un hábito primordial. Lo ideal es que sean largas y complejas, con números y letras, para aplicaciones, redes WIFI y dispositivos. Debe cambiarse la contraseña de vez en cuando, utilizarse una distinta para cada cosa y evitar poner fechas o palabras que sean fácilmente identificables con el perfil.

- No descargar ficheros sospechosos. No se debe pinchar en enlaces ni descargase ficheros adjuntos que resulten sospechosos porque puede desembocar en la entrada de un virus que deje el dispositivo inoperativo. Además, es conveniente contar con un buen antivirus.

- Actualizar los dispositivos. No solo es necesario contar con un antivirus, sino también tenerlo actualizado. Esto se extiende al sistema operativo de cualquiera de nuestros dispositivos y a las aplicaciones de banca digital. Cada actualización añade nuevas funcionalidades y también incorpora mejoras en las condiciones de seguridad y corrige fallos de la versión anterior.

- Vigilar la conexión. Uno de los errores más comunes es realizar compras *online* e incluso acceder al servicio de la banca por internet cuando se está conectado a una wifi pública. Nunca debe conectarse a redes wifi públicas, enviar información confidencial a través de ellas o acceder a la banca digital *online*, tampoco desde dispositivos públicos, no confiables.

- Desconfiar de mensajes extraños. Desde hace décadas se han extendido los mensajes *spam*, es decir, correos electrónicos o SMS basura con publicidad o que buscan timar al destinatario. Normalmente, los buzones virtuales los detectan automáticamente y los desechan, pero en los últimos años los piratas informáticos han buscado maneras de saltarse ese filtro y engañar a los usuarios. Las estafas son cada vez más sofisticadas y reales por lo que hay que desconfiar de cualquier mensaje que ofrezca algún premio, ingreso o beneficio o intente forzar con urgencia a realizar una acción relacionada con revelar algún dato personal.

- Mantener la alerta con el *phishing*. Los mensajes engañosos suelen remitir a una web idéntica a la del banco. Debemos fijarnos en la barra de direcciones: si hay faltas de ortografía, en qué idioma está, además de comprobar que en la url sale un candado y pone 'https'. También pueden llegar mensajes falsos de instituciones oficiales o de empresas de *ecommerce*.

- Comprar con medios de pago seguros. Las tarjetas de crédito o de débito virtuales, los *wallets* o tarjetas prepago son alternativas de confianza. Del mismo modo que las contraseñas, las tarjetas de crédito también se pueden guardar en gestores para proteger los datos y las claves.

- Cerrar siempre la sesión. Para acabar, hay que cerrar siempre la sesión en las aplicaciones o web: banca virtual, redes sociales, tiendas *online*, etcétera. También es importante apagar el portátil o bloquear el móvil para no dejar la puerta abierta a ciberdelincuentes. Una opción es activar la desconexión automática para garantizar que el móvil o portátil se bloquee tras varios minutos sin uso.

SEGUNDA OLEADA (SEPTIEMBRE 2021)

ASÍ LE PROTEGE SU BANCO CONTRA LOS CIBERATAQUES[2]

AL margen de las medidas que los usuarios pueden adoptar de manera individual para proteger la información personal y el dinero, las entidades financieras tienen la obligación de proteger a sus clientes de posibles ciberataques. Para ello desarrollan las medidas necesarias a nivel tecnológico, ofrecen las herramientas para poder defenderse y establecen pautas de actuación frente a potenciales fraudes.

En general, España es uno de los países de la Unión Europea con menos incidencia en este tipo de problemática, entre otros motivos, por la seguridad de la encriptación y otros sistemas de protección que ha desarrollado así como en el uso de sistemas de alerta y de doble autenticación para evitar los fraudes.

Como explica Santiago Carbó, director de Estudios Financieros de Funcas, los bancos españoles han hecho una correcta labor a la hora de ayudar a sus usuarios: "Sus pasarelas de pago son de las más seguras, muchas de ellas en colaboración con emisores de medios de pago reconocidos. También es destacable el caso de bizum, que cada vez más se usa como medio de pago para 'ecommerce' y no solo como herramienta de transferencia de dinero".

A nivel jurídico, en 2019 entró en vigor la normativa PSD (Payment Service Providers), una regulación europea sobre servicios de pago electrónicos y sus procesos de seguridad en los pagos realizados en Europa, promoviendo la innovación y originando un mercado único de pagos en la Unión Europea (UE). En enero de 2021 llega actualizada la Segunda Directiva de Servicios de Pago (PSD2), que refuerza la intención de evitar el fraude en las gestiones *online* así como de mejorar la protección del consumidor aumentando la seguridad de las transacciones *online* (transferencias, compras por Internet, pagos con tarjetas…) para usuarios, comercios y bancos.

Estas son algunas de las medidas que los bancos españoles ya implementan para proteger su dinero en internet:

- Accesos seguros y encriptados. Actualmente todos los bancos españoles disponen de conexiones seguras e incluso encriptadas. Además, suelen estar atentos a posibles campañas de 'phishing' para, en caso de que alguien esté usando su nombre para cometer fraudes, poder avisar a sus usuarios de cara a que mantengan la prudencia en todo momento.
- Doble autenticación. A la hora de pagar en un comercio electrónico o de operar en la web del banco, a menudo no basta con poner los datos de la tarjeta. Cuando las operaciones son especialmente comprometidas (pagos, transferencias, contratación de productos…), los bancos recurren a la autenticación reforzada o doble autenticación. Es decir, cuando se realice una operación de este nivel, el banco le pedirá identificarse una segunda vez mediante un código enviado por SMS, la introducción de nuevo de la contraseña o la inserción del código de seguridad de la tarjeta, entre otras posibilidades.

Estas protecciones son comunes a todos los bancos españoles, ya que vienen marcadas por la normativa legal europea, concretamente por la citada PSD2. Esta reglamentación es común a todos los países de la Unión Europea (UE), de modo que si su entidad financiera está adscrita a este territorio tendrá obligatoriamente todas estas herramientas para reforzar su seguridad.

¿Qué datos exigen al realizar una operación online *?*

- La forma en que se autoriza la compra ha variado con la nueva legislación.
- Se incide sobre todo en los factores de autenticación reforzada: solicitud del PIN correspondiente y otro código enviado al móvil del usuario que en ese momento está realizando la compra.
- Datos de la tarjeta bancaria: se sigue solicitando, pero como un factor complementario para reforzar la seguridad.

TERCERA OLEADA (OCTUBRE 2021)

QUÉ HACER SI SE HA SIDO VÍCTIMA DE UN CIBERFRAUDE[3]

NO existe ningún sistema capaz de repeler el 100 % de los ciberataques, por lo que es recomendable tomar todas las precauciones oportunas y, sobre todo, actuar con prudencia y sentido común. Debemos fortalecer la seguridad de nuestros dispositivos manteniendo los sistemas actualizados, aplicando parches de seguridad y mediante el uso de antivirus, así como asegurar nuestra identidad digital modificando las contraseñas y utilizando el doble factor de autenticación en aquellos casos en los que sea posible.

Tomar todas estas precauciones ayudará a evitar ser víctima de un ciberfraude. Además, las plataformas de las entidades financieras están dotadas de fuertes medidas de seguridad como cortafuegos, sistemas de detección de intrusiones, antivirus, etc. y las someten de forma periódica a auditorías de seguridad.

Pero el fraude está ahí. De todos los ciberdelitos, las ciberestafas suponen más del 65 %, según datos del Ministerio del Interior. Si cree que ha podido ser víctima de un ciberfraude, así debería actuar.

- Uso fraudulento de la tarjeta. Una de las estafas más comunes es el fraude con tarjeta de crédito o de débito. Los ciberdelincuentes pueden intentar replicar la banda magnética de su tarjeta, interceptarla en el correo o robar los datos de la tarjeta durante un pago *online* mediante un código informático.

  Si ha detectado un uso fraudulento, lo primero que debe hacer es llamar al banco para anular las tarjetas.

  Si es un robo, tiene que denunciarlo ante la Policía.

  En caso de copia o duplicado de la tarjeta, el banco le deberá devolver el importe total de la operación no autorizada. Si el fraude se debe a robo o pérdida de tarjeta, el consumidor es responsable por el uso fraudulento antes de la comunicación del robo o la pérdida, por una cuantía máxima de 50 euros excepto por culpa o negligencia grave.

- Ataque de *phishing*. Lo primero que debe hacer es llamar al banco para cancelar tarjetas y cambiar claves de seguridad. Las entidades también suelen tener una dirección de correo electrónico destinada a la ciberseguridad para consultar dudas, informar de algo sospechoso o exponer su caso.

  Recopile toda la información relevante, prueba o indicio que pueda (enlaces, archivos descargados, etc…) para ponerla en conocimiento de la entidad financiera y de los organismos pertinentes.

  Si tiene instalado un antivirus realice un análisis del dispositivo para intentar desinstalar la aplicación maliciosa.

  Puede denunciar el suceso a la Policía Nacional, la Guardia Civil o en el Instituto Nacional de Ciberseguridad (INCIBE).

- Estafa a través de bizum. Lo primero que debe saber si le han estafado por bizum es que no es posible anular el pago. Además, si ha pagado voluntariamente, aunque engañado, su entidad no está obligada a devolver el dinero, pero los bancos suelen tener seguros para estos casos. Infórmese en su entidad.

  En caso de estafa hay que denunciarlo ante las Fuerzas y Cuerpos de Seguridad del Estado y la Agencia Española de Protección de Datos. Si se han facilitado datos bancarios, también debe contactar con su entidad y cambiar las claves de acceso para evitar que secuestren la cuenta.

  También es recomendable denunciar el fraude ante la Oficina de Seguridad del Internauta. La información se envía al INCIBE y sirve para detectar mejor páginas web fraudulentas, mensajes maliciosos o portales con datos robados.

- Clic en un SMS fraudulento. Si es víctima de *smishing* o mensaje fraudulento, lo primero que debe hacer es ponerse en contacto con su entidad para que bloquee la operación.

  Después modifique la contraseña de acceso a la banca electrónica y cualquier otra información que haya facilitado. Y, sobre todo, debe denunciar el fraude a la Policía Nacional, la Guardia Civil o en los juzgados, aportando pruebas.

- Malware. El malware es un programa malicioso creado para atacar la seguridad del móvil, ordenador o tableta infiltrándose en ellos para tomar el control o robar datos. En muchos casos, el malware intenta acceder a la información bancaria confidencial y las claves de acceso y contraseñas. Usar un antivirus ayuda a protegerte de este fraude.

  Si detecta que has sufrido un ataque o robo de datos tiene que seguir los siguientes pasos:

  - Cambie la clave de seguridad y desactive la validación móvil.
  - Bloquee la tarjeta bancaria.
  - Verifique los movimientos y cargos de la tarjeta en la cuenta.
  - Denuncie ante la Policía Nacional, la Guardia Civil o los juzgados.

Estas son las estafas más comunes, pero en cualquier caso los consumidores están protegidos por la Ley de Servicios de Pago o la Ley General para la Defensa de los Consumidores y Usuarios. Por último, organismos como el Banco de España, la Comisión Nacional del Mercado de Valores (CNMV), la Policía Nacional o la Guardia Civil agradecen la colaboración de los ciudadanos para informar de este tipo de estafas y ser más eficaces en la lucha contra el ciberfraude.

Los ciberataques o tipos de fraude más comunes

La información y la formación son las mejores armas para protegerse de los ataques cibernéticos. Algunos de los fraudes más comunes son:

Phishing: Es una de las técnicas más utilizadas por los estafadores y sirve para averiguar datos bancarios y contraseñas. Envían un email haciéndose pasar por un banco u otra empresa y piden que se rellenen unos datos. Nunca deben compartirse claves, ni por teléfono ni por correo ni por otro medio. Si alguien solicita una clave, es señal inequívoca de que se trata de un fraude.

Vishing: Se trata de otra variante del *phishing* pero a través de una llamada de voz. En el caso de que se produzca la estafa con un SMS se le conoce somo *SMishing*.

Carding: En este tipo de estafa se realiza un uso no autorizado de su tarjeta de crédito, cuentas bancarias o cualquier tipo de información bancaria. Con estos datos pueden realizar cargos y operar libremente con su cuenta.

Fraude al CEO: Un ciberdelincuente suplanta a un alto cargo de una compañía con el propósito de engañar a los empleados para que efectúen órdenes de pagos.

Fraude de facturas: Intento de suplantar la identidad de un proveedor o de un empleado con el fin de desviar el cobro de facturas.

Falso virus: Cuando salta un banner y avisa de un falso virus o vulnerabilidad en su sistema para que haga clic, lleva a una página de descarga de un *software* que promete eliminar el virus.

Falsas multas: Envían un email diciendo que ha realizado alguna actividad ilegal como descargar películas, canciones, libros… y que debe pagar una multa por ello.

---

[1] Publicado en los siguientes medios:

ABC
EL PAÍS
elPeriódico
HERALDO

[2] Publicado en los siguientes medios:

ABC
EL MUNDO
El Confidencial

[3] Publicado en los siguientes medios:

ABC
El Confidencial