Educar en seguridad digital y mostrar los riesgos a los que nos enfrentamos como usuarios son algunos de los objetivos de la entidad, que ofrece consejos y guías de buenas prácticas para aprender a utilizar los entornos digitales de forma responsable y segura.

Consejos para hacer frente a los ciberataques

Cualquiera de nosotros podemos ser víctimas de una estafa digital. ¿Quién no ha recibido alguna vez un correo fraudulento suplantando la identidad de una empresa o ha clicado por error en un anuncio falso en Internet? Hasta el 85% de todos los correos que se envían en el mundo son *spam*. En los últimos años, y especialmente durante la pandemia de la Covid-19, los *hackers* han intensificado y sofisticado sus ataques y son muchas las estafas a las que nos podemos enfrentar: fraudes telefónicos, webs y anuncios falsos, ataques por correo electrónico, fraudes a través de mensajería instantánea…

Conocer las amenazas *online* que circulan por Internet y seguir unas buenas prácticas digitales es clave para no convertirnos en víctima de estos ataques. Para ello, CaixaBank desarrolla acciones de concienciación dirigidas tanto a empleados como a clientes, a través de InfoProtect y CaixaBank Protect.

Coincidiendo en octubre con el **mes de la concienciación en ciberseguridad**, la entidad ha desarrollado una campaña para reforzar la cultura de seguridad entre empleados y clientes. A lo largo de todo el mes, CaixaBank difundirá diferentes contenidos relacionados con esta temática, organizará sesiones *online*, conferencias para explicar fundamentos y conceptos de ciberseguridad para prevenir ser víctima de un fraude… entre otras actividades.

Educar en seguridad digital y mostrar los riesgos a los que nos enfrentamos como usuarios son algunos de los objetivos de la entidad, que ofrece consejos y guías de buenas prácticas para aprender a utilizar los entornos digitales de forma responsable y segura.

1.Navegar por Internet con seguridad

A la hora de navegar por Internet debemos seguir algunas recomendaciones y tener en cuenta algunos consejos:

-Es fundamental ser precavido con las webs que visitamos y los archivos que descargamos.

-En caso de utilizar conexiones WiFi públicas, debemos evitar navegar por páginas web que pidan cualquier tipo de dato personal o financiero, usuario y contraseñas, etc. También debemos evitar hacer compras *online* con WiFi públicas.

-Contar con un antivirus actualizado y bien configurado nos evitará muchos problemas, aunque tenemos que ser conscientes de que el antivirus no garantiza nuestra seguridad al 100%.

-Tener correctamente actualizado el sistema operativo y las aplicaciones instaladas es un requisito técnico imprescindible para intentar que los ciberdelincuentes no puedan entrar en nuestros equipos, aunque nunca es suficiente.

-No acceder a sitios web de dudosa reputación. Para verificar la legitimidad de una web, debemos comprobar también la legitimidad de su certificado digital, revisando que está vigente y que ha sido emitido para la página web por la que queremos navegar. El “famoso” candado no significa que la web sea legítima, para ello es imprescindible comprobar el certificado asociado.

-Hay que vigilar especialmente con la ‘identidad digital’ que nos creamos y subir únicamente aquella información sobre nosotros mismos que consideramos 100% pública.

2.Claves de acceso

Las claves de acceso son personales e intransferibles. Protegen toda la información de nuestro entorno digital: datos personales, cuentas bancarias, redes sociales, información confidencial, imágenes y contenido de cualquier tipo.

-Es importante crear contraseñas robustas difíciles de adivinar. Para ello se recomienda que tengan como mínimo 8 caracteres, entre mayúsculas, minúsculas, símbolos y números. Y siempre será mejor si no contiene palabras incluidas en el diccionario. Hay que intentar ser creativo y original y no poner fechas personales señaladas, el clásico 1234 o el nombre de nuestra mascota.

-Compartir las contraseñas es una práctica muy peligrosa. La cesión de contraseñas tiene un papel clave en algunos de los fraudes más conocidos, como el fraude por proximidad. Este tipo de fraude se produce cuando cedemos nuestras claves a un familiar, amigo o conocido y éste las utiliza para cometer un delito o una operación fraudulenta de forma totalmente ilícita. Ante cualquier sospecha de compromiso de alguna de nuestras contraseñas, debemos cambiarla en la menor brevedad posible.

-Para almacenar y acordarnos de todas las claves de acceso que hemos generado, la opción más segura es utilizar gestores de contraseñas. Estas

aplicaciones las guardan de manera cifrada y protegidas con una contraseña única, que da acceso a todas ellas.

3.Detectar correos fraudulentos

El *phishing* es una de las técnicas más usadas por los ciberdelincuentes para robar datos personales y bancarios. Con la ayuda de técnicas de ingeniería social, el ciberdelincuente suplanta la identidad de entidades, personas, marcas o servicios conocidos para tratar de engañar a sus víctimas. Su objetivo final suele ser el dinero y/o la obtención de información sensible, generalmente solicitando los datos a través de páginas web falsas o infectando el equipo mediante la descarga de un *malware*. Cuando recibimos un nuevo correo, debemos formularnos algunas preguntas:

-¿Quién envía el correo? Es imprescindible analizar con detalle la dirección de correo del remitente y no fiarnos sólo del nombre que nos muestra. Es necesario confirmar que la dirección de correo tiene el dominio oficial de la empresa y no dejarse engañar por pequeños cambios a veces casi imperceptibles.

-¿El mensaje es sospechoso? El ciberdelincuente puede crear correos que inspiren confianza o curiosidad, suplantando la identidad de una empresa, de una plataforma de vídeo en *streaming* o simplemente escribiendo un mensaje atractivo que impulse a clicar en un enlace o archivo. No se debe confiar en correos inesperados o en respuestas que no hemos solicitado.

-¿Es una petición urgente? Crear sensación de urgencia es un recurso habitual entre los *hackers*. Además, el concepto de la confidencialidad también es muy usado en este tipo de estafas.

Ante la más mínima duda, es recomendable contactar con el remitente por otra vía (teléfono…) para confirmar la legitimidad (aunque nunca por el teléfono que pueda aparecer en el correo).

4.Proteger el móvil

Los teléfonos móviles son pequeños ordenadores con una gran cantidad de información muy valiosa. Son dispositivos que debemos tratar con mucho cuidado, ya que están expuestos a riesgos de seguridad.

-Activar y fijar el bloqueo automático del teléfono. Con esta sencilla medida, ayudamos a mantener nuestros datos personales seguros cuanto no lo estemos usando.

-No dejar los dispositivos con el Bluetooth ni la conexión WiFi activadas permanentemente y evitar el uso de conexiones WiFi desconocidas.

-De forma periódica, es conveniente realizar copias de seguridad de la información que contiene el dispositivo móvil, para poder recuperarla en caso de incidencias o pérdida.

-Actualizar puntualmente el sistema operativo del móvil, así como las aplicaciones.

-Es indispensable instalar alguna aplicación antimalware, ya que los móviles también pueden ser infectados.

5.Instalación de aplicaciones

Cuando descargamos aplicaciones en nuestros dispositivos móviles, nos solicitan permisos para acceder a determinadas funcionalidades del dispositivo. Algunas requieren lo estrictamente necesario para cumplir su cometido, pero otras intentan acceder a nuestra información personal pidiendo permisos que no necesitan. Antes de aceptar la descarga de una *app*, debemos poner atención a los privilegios que solicita y valorar si están justificados o son excesivos.

-Revisar los permisos que nos solicitan. Los accesos más comunes son las llamadas y mensajes, el calendario, los contactos, la ubicación, la cámara y galería de imágenes y el micrófono. ¿Son realmente necesarios para el funcionamiento de la *app*?

-Descargar *apps* solo de fuentes oficiales.

-Cuando eliminamos las limitaciones de seguridad impuestas por el fabricante del móvil para, por ejemplo, evitar pagar por ciertas *apps,* estamos haciendo un *jailbreak*, una acción nada recomendada. Con esto, eliminamos las barreras de seguridad que vienen de fábrica y puede suponernos más problemas que beneficios.

-Todos corremos el riesgo de ser infectados, pero para protegernos debemos instalar una *app* de seguridad en el móvil, ya sea Android o iOS.

-Cuando queramos descargarnos una aplicación, es preferible hacerlo desde una red WiFi segura. Las WiFi públicas no ofrecen ninguna garantía de seguridad.

6.Compras *online* seguras

Cada día más usuarios deciden realizar sus compras *online*. El comercio electrónico, que ha experimentado un gran auge en los últimos años, es cómodo y práctico, y aplicando las medidas de protección adecuadas, también es seguro.

-Cuidado con las superofertas y los enlaces. Los precios anormalmente bajos pueden ser una trampa para atraer a compradores incautos; por ello es mejor indagar otras webs y otros distribuidores para confirmar el valor real de mercado del artículo.

-No hay que utilizar nunca una conexión pública para realizar las compras *online*, ya que no ofrecen ninguna garantía de seguridad.

-Priorizar la compra en tiendas que tengan dado el alta el servicio de Comercio Electrónico Seguro (CES), por ejemplo “Verified by Visa” o “Mastercard Secure Code”.

-Revisar periódicamente el estado de nuestras tarjetas y cuentas es una buena medida de seguridad para compradores *online.*

Además de todo lo mencionado, siempre hay nuevas vías para los ciberdelincuentes, como por ejemplo el **fraude del romance** (tipo de fraude que se produce principalmente en las aplicaciones de citas o webs de contactos cuyo objetivo es atacar a los sentimientos y la confianza de la víctima como principal baza para convencerla y así lograr engañarla para conseguir estafarle grandes cantidades de dinero), los **falsos anuncios de alquiler vacacional en Internet** (los ciberdelincuentes utilizan plataformas web legítimas y fiables en las que publican falsos anuncios de viviendas, a precios muy atractivos y con fotografías que atraen la atención de las víctimas) o el **vishing** (estafas a través de llamadas o mensajes de voz).

Con el objetivo de convertirse en una fuente de referencia por clientes y usuarios, CaixaBank ha renovado el espacio de seguridad de la web pública de la entidad. Por otro lado, cada tres meses, el equipo de Seguridad coordina con diferentes áreas la creación de tres artículos sobre temas de actualidad relacionados con la seguridad digital. Otra iniciativa que lleva a cabo es la *newsletter* de InfoProtect Security News, que se envía cada 15 días a los empleados de CaixaBank con artículos y reportajes relacionados con el mundo de la ciberseguridad. La entidad también realiza cursos, sesiones *online,* simulaciones y otras acciones para sensibilizar a los empleados sobre la importancia de saber identificar correos *phishing*, entre otros temas sobre ciberseguridad.

Además de tener en cuenta todos estos consejos y recomendaciones**, la cautela y la máxima atención por nuestra parte**, así como **saber cuándo sospechar** es clave para no ser víctima de ciberataques.