CONSEJOS PARA CONVERTIRTE EN UN/A IAI@ CONNECTAT

Protege tu información y la de tus equipos

Ten precaución y **no te fíes de nadie** que te pida información personal o te proponga la instalación de una aplicación en tu PC o móvil. Los bancos jamás pedirán información confidencial por teléfono, correo o SMS.

Mantén tus aplicaciones y dispositivos actualizados, activa las actualizaciones automáticas de tu ordenador, tu tablet y tu móvil.

Evita instalarte aplicaciones de dudosa procedencia o reputación y utiliza siempre los repositorios oficiales.

Utiliza algún tipo de antivirus en tu PC, así como las opciones de seguridad por defecto que te ofrezca tu equipo.

Precaución online y en público

Sé consciente de que **al publicar información en Internet** (Facebook, LinkedIn, Instagram, Twitter, etc.), **cualquiera puede acceder a ella** y utilizarla para intentar engañarte.

Revisa las configuraciones de privacidad de las redes sociales. Por ejemplo, que solo tus contactos directos puedan ver información personal.

Nunca publiques contraseñas, ubicaciones, tiempo de vacaciones donde estés ausente, números de teléfono, información sobre tarjetas bancarias, etc. En general, todo aquello que no contarías nunca a un desconocido por la calle.

Ten mucho **cuidado con los desconocidos que inicien una conversación** *online* o telefónica contigo, plantéate cuál es su motivación y hasta qué punto puedes verificar su identidad real. Mantén tus contraseñas seguras

Crea contraseñas robustas, que no sean fáciles de adivinar. Evita utilizar tu fecha de nacimiento, tu ciudad, nombre de un familiar, del perro, 1234, etc.

Nunca las anotes en papel ni las compartas. Y, sobre todo, no se las proporciones a nadie que contacte contigo *online* ni por teléfono.

Piensa siempre antes de hacer clic o responder

Ante la duda, lo mejor es no responder al correo, colgar el teléfono o borrar el mensaje de texto, así evitamos que nos engañen.

No existen chollos, ni tenemos el día de suerte

No existen las ofertas demasiado buenas, suelen ser engaños. Si sospechas, busca el contacto oficial de la supuesta tienda y cerciórate que lo que has recibido por correo es real, busca el teléfono de la marca y llama o visita el establecimiento para verificarlo.

No existen las inversiones hiper-rentables

No hay inversiones con altas rentabilidades. Duda de las inversiones que prometen grandes rentabilidades, especialmente con criptomonedas, y de “chiringuitos” poco fiables o no conocidos. Detrás suele haber un timo donde, una vez invertido el dinero, va a desaparecer.

Las ofertas de trabajo no caen del cielo

No existen ofertas de trabajo tan fabulosas. Duda de los anuncios que prometen fantásticas ofertas de trabajo que te hagan pensar que podrían ser para tus hijos o nietos. Detrás suele haber un timo donde se nos pide dinero y la oferta de trabajo no existe.

Si dudas, asesórate

Las estafas están muy bien diseñadas. Si dudas sobre si es o no una estafa, antes de hablar con un desconocido o entrar en un enlace, **habla con tus hijos, tus familiares o personas de confianza y cuéntales tus dudas.**

El mundo digital no es muy diferente del mundo real. Puede parecerte peligroso, pero con estas sencillas precauciones puede resultar más seguro y fiable que el presencial y con muchas más ventajas.

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic
TOTS A UNA veu
IVF INSTITUT VALENCIÀ DE FINANCES
iai@ connectat

iai@ connectat

Consejos para utilizar internet de forma segura

Vivimos en la era digital. El uso de las **nuevas tecnologías** para comprar *online*, interactuar con la banca o con la administración **nos pueden ser de mucha utilidad** al permitirnos hacer gestiones cómodamente, desde cualquier lugar, a cualquier hora, sin esperar colas y ahorrándonos tiempo.

A pesar de sus ventajas, muchas personas no dan el paso porque todavía tienen **miedo a usar internet.**

Sin embargo, con unas **precauciones básicas**, las compras *online* o la banca por internet pueden ser incluso **más fiables que la interacción presencial**, y tu dinero estará mucho más seguro que cuando lo llevas encima o lo tienes en casa.

10 TIMOS USADOS POR LOS CIBERDELINCUENTES Y CÓMO PROTEGERTE

LLAMADAS DE TELÉFONO DE DESCONOCIDOS (Vishing)

Si recibes una **llamada de teléfono de un número desconocido** en la que te ofrecen un servicio o producto o te avisan de un problema con tu cuenta bancaria **DEBES COLGAR SIN DAR CONVERSACIÓN.**

Aunque te intenten alertar o dar miedo debes desconfiar y colgar, sin tener reparos en ser poco educado/a con el interlocutor. Jamás debes entablar conversación ni dar información. Tu banco JAMÁS te pedirá información por internet.

LLAMADAS DE TELÉFONO DE FALSOS TÉCNICOS (Vishing)

Si recibes una **llamada de teléfono de un número desconocido** en la que te avisan de un problema en tu ordenador **DEBES COLGAR SIN DAR CONVERSACIÓN.**

Los servicios técnicos no llaman si no les has llamado previamente o no tienes contratado un soporte técnico para tu ordenador. JAMAS debes entablar conversación, ni seguir ninguna instrucción que te den, ni dar información.

MENSAJES DE TEXTO (Smishing)

Si recibes un SMS con la recepción de un paquete que no has pedido, o un problema en la cuenta bancaria o un pago que no esperas **DEBES BORRARLO.**

Aunque el SMS sea “aparentemente” de Correos o de nuestro banco. Ni Correos, ni nuestro banco nos pedirán JAMÁS información por internet.

CORREOS ELECTRÓNICOS (Pishing)

Si recibes un correo electrónico en el que se te piden datos personales o te lleva a visitar una página web o a descargar una aplicación **DEBES BORRARLO.**

Aunque el correo sea “aparentemente” de Correos o de nuestro banco habitual. Ni Correos, ni nuestro banco nos pedirán JAMAS información por internet.

OFERTAS FANTÁSTICAS O REGALOS POR INTERNET

Si navegando por internet ves una oferta muy buena de un producto, oferta de trabajo o se te notifica que has sido agraciado/a con un premio **NO DEBES HACER CASO.**

Evita entrar en el enlace. Si dudas, cerciórate a través del contacto oficial con el comercio para ver si es real o es un engaño. Si aun así dudas, antes de hacer nada coméntalo con familiares o personas de tu confianza.

FALSOS BIZUM

Si recibes un mensaje de Bizum en el que parece que vas a recibir dinero NO DEBES HACER CASO.

Debes leer bien el mensaje que nos llega porque, en lugar de recibir, podría ser una petición de dinero. En todo caso, los organismos oficiales no utilizan Bizum.

NOTIFICACIONES DE PROBLEMAS CON LA CUENTA DEL BANCO

Si se ponen en contacto por SMS/correo para decirnos que hay un problema en nuestra cuenta NO DEBES HACER CASO.

Sospecha siempre de los SMS o de correos electrónicos que lleven a un enlace o te pidan datos de cualquier tipo. Tu banco JAMÁS te pedirá información por internet.

ESCANEO DE CÓDIGOS QR (QRjacking)

Si te piden que escanees un código QR desde tu teléfono móvil NO DEBES HACER CASO.

Evita el escaneo de códigos QR y/o desactiva en el móvil la opción de abrir automáticamente los enlaces al escanear un código QR.

DISCOS USB (Baiting)

Si una persona desconocida te pide introducir una memoria USB en tu ordenador o conectar tu móvil a un ordenador **NO DEBES PERMITIRSELO.**

Sospecha de dispositivos de desconocidos, evita conectarnos y mantén actualizado el antivirus del ordenador.

COMPRAS POR INTERNET

Si ves páginas web de tiendas *online* con ofertas increíblemente buenas NO DEBES HACER CASO.

También puedes buscar información sobre la empresa o consultar con tus personas de confianza.

No hay “duros a cuatro pesetas” y tampoco pienses que es tu día de suerte. Evita entrar en el enlace. Si dudas, cerciórate a través del contacto oficial con el comercio para ver si es real o es un engaño. Si aun así dudas, antes de hacer nada coméntalo con familiares o personas de tu confianza.