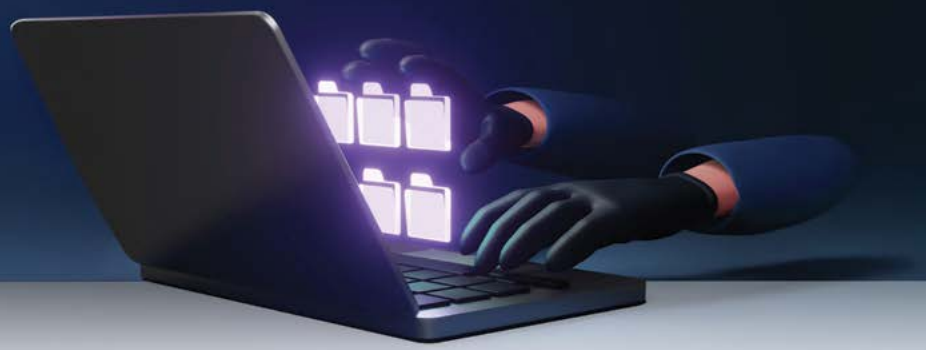
DELITOS INFORMÁTICOS

ES UN HECHO: cada vez hay más casos de ciberestafas, de engaños online con los que roban a los usuarios que pican el anzuelo cientos o miles de euros, además de su privacidad y su tranquilidad.

CONSEJOS BÁSICOS PARA PREVINIR FRAUDES ONLINE



1 **Priorizar las webs conocidas.** (que desarrollan su actividad en el ámbito de la Unión Europea). **Desconfíe siempre** de los comercios que no dan datos claros de contacto.

2 **No salir de la plataforma de compra.** Algunos fraudes se originan en webs muy conocidas, cuando el usuario se sale del guión. **No acepte invitaciones para tratar con la otra parte por correos electrónicos privados** ni mande dinero por transferencia.

3 **Desconfiar de los chollos,** los regalos y los productos no solicitados. **Evite las ofertas superflash de páginas desconocidas** que le urgen a hacer un desembolso para no perder una oportunidad de compra.

4 **Confirmar los enlaces que lleguen por SMS o al correo electrónico.** Si recibe un email o un SMS con enlaces, en relación a alguna compra o búsqueda que haya hecho, vaya a la web original a comprobar la actividad de su perfil; **no pinche los enlaces si tiene la menor sospecha.**

5 **Usar una tarjeta prepago.** Recargándola según el saldo que vaya a usar. Otra opción consiste en activar funciones de la tarjeta de crédito para limitar el saldo, prohibir las compras fuera de la UE, mantener la tarjeta apagada... **Si piden el PIN online, dé el fraude por asegurado.**

6 **Reclamar al banco cuanto antes.** Si detecta un pago no autorizado, **comuníqueselo a la entidad lo antes posible** y denuncie el hecho a la policía o a la guardia civil.

¿Y SI YA HA CAÍDO EN LA TRAMPA?

Si cree que ha podido ser víctima de alguna de estas estafas, póngase en contacto con su banco cuanto antes. La normativa establece la obligación de comunicar sin demora injustificada, en cuanto tenga conocimiento que se ha producido una operación de pago no autorizada. Así cumpliremos la principal obligación del consumidor en estos casos y evitaremos que la entidad pueda alegar que hemos actuado de manera negligente.

También, debe denunciarlo ante las Fuerzas y Cuerpos de Seguridad del Estado en cualquier comisaría o a través de sus portales web. Intente recopilar todas las evidencias que demuestren la trampa: el registro de llamadas de su teléfono, facturas del banco... todo esto ayudará con la denuncia.

Y si en algún momento detecta movimientos en tus cuentas o pagos con tus tarjetas que no ha realizado, lo primero que debes hacer es reclamarlo inmediatamente a su entidad. Y es que la ley dice que cualquier pago no autorizado por el titular no correrá por cuenta del usuario. No obstante, aún hay entidades que se hacen las remolonas, culpando al consumidor de haber sido negligente, considerando en muchas ocasiones que no son responsables de este tipo de estafas porque sus sistemas informáticos no están siendo atacados ni se están produciendo brechas de seguridad en los mismos.

MÁS INFORMACIÓN

Para más información o resolución de dudas puedes contactar:
WEB: https://www.ocu.org/ocu-castilla-lamancha-digitalizacion
Teléfono de atención gratuita de lunes a viernes de 9:00 a 14:00: 900801115 Email: ayudadigital@ocu.org

ocu

Castilla-La Mancha

CONSUMO

TIPOS DE FRAUDES ON LINE

PHISHING

es una técnica de engaño que utilizan los piratas informáticos para “pescar” nuestros datos personales y bancarios a través de un engaño.

¿CÓMO EVITARLO?

- Suele llegar a través de un correo electrónico.
- Sospeche de cualquier email que le llegue de una empresa cuyos servicios no tiene contratados
- Mensaje con faltas de ortografía
- Que le urja a pinchar en un link.
- Si el contenido del mensaje te parece sospechoso probablemente lo sea (premios de sorteos, ofertas de trabajo, multas, contactos de empresas con las que no tienes vinculación...)
- Precaución con correos amenazantes (bloqueos de cuentas, deudas...)

QRISHING

al escanear el código QR, se dirige al usuario a una web falsa, que finge ser auténtica. El objetivo: que el consumidor, engañado, facilite sus datos a través de esos enlaces o páginas falsas.

¿CÓMO EVITARLO?

- La mejor opción es identificar la dirección web a la que nos remite el código QR.
- Use aplicaciones de lectura de QR que permitan ver el enlace antes de abrirlo.
- No escanee a la ligera QRs que se encuentren en panfletos o pegados en cualquier sitio...

WANGIRI

Timo de la llamada perdida: le llaman por teléfono y, antes de que pueda cogerlo, se corta. Si devuelve la llamada, nadie contesta. El problema es que ha llamado a un número de tarificación especial, (probablemente en el extranjero).

¿CÓMO EVITARLO?

- La única manera de prevenir esta estafa es no devolviendo la llamada perdida
- La única manera de prevenir esta estafa es no devolviendo la llamada perdida
- Si cree que podría tratarse de una llamada real, asegúrese de que el número le parece “sensato” antes de devolver la llamada que podría tratarse de una llamada real, asegúrese de que el número le parece “sensato” antes de devolver la llamada Si cree que podría tratarse de una llamada real, asegúrese de que el número le parece “sensato” antes de devolver la llamada.

SMISHING

los ciberdelincuentes recurren a los mensajes de texto al móvil, los famosos SMS: Nos mandan un mensaje alarmante simulando ser una entidad legítima (Hacienda, el banco, correos...) con el objetivo de robarnos información privada o realizarnos un cargo económico. El objetivo es siempre dirigir a la víctima a una página web falsa (a través de un enlace)para robar las credenciales de acceso al servicio bancario.

¿CÓMO EVITARLO?

- Desconfíe de este tipo de mensajes
- Si cree que hay un problema de verdad, llame directamente a su banco o a la empresa de mensajería para comprobarlo. Precaución con correos amenazantes (bloqueos de cuentas, deudas...)

CARDING

el robo “virtual” de tu tarjeta. Los delincuentes se hacen con los datos de sus tarjetas, por distintos medios (phishing, duplicados NFC...). Los datos obtenidos se replican en otra tarjeta virtual, y con ella van pagando compras y servicios hasta vaciar su cuenta.

¿CÓMO EVITARLO?

- Desconfía de mensajes o correos que no esperes o cuyo origen desconozca.
- Deje los datos de su tarjeta solo en páginas web que sean seguras: Asegúrese de que es una web que usa pasarelas de pago seguras.
- Active el doble factor de autenticación para los pagos con tarjeta.
- No haga compras ni pagos online en ordenadores públicos.
- Cuando pague en un establecimiento, no pierda de vista su tarjeta.
- Si detecta un uso fraudulento de su tarjeta anúlela cuanto antes y denuncie el posible robo de los datos de la tarjeta ante la policía.

VISHING

Se realiza a través de una llamada telefónica. Se utilizan técnicas de ingeniería social y de suplantación de identidad para que la víctima revele información personal o bancaria.

¿CÓMO EVITARLO?

- Cuelgue la llamada y no ofrezca ningún dato por teléfono (ni personales ni credenciales de medios de pago). Su banco nunca Se los pediría, así que si Se los piden por cualquier medio (correos electrónicos, SMS, llamadas de teléfono, páginas web...) seguramente se trata de un intento de fraude.
- Si duda, póngase en contacto con la entidad o empresa para aclarar lo que crea oportuno, siempre buscando el número de teléfono en su agenda o en la web.

SPOOFING

suplantación de identidad Consiste en que los interlocutores se hacen pasar por una entidad bancaria, institución pública, compañía de soporte informático... para engañarnos. Se caracteriza porque los suplantadores están bien preparados y utilizan la jerga perfectamente.

¿CÓMO EVITARLO?

- Desconfíe de llamadas de alerta: su banco nunca le pedirá claves, ni códigos que se envían por SMS, ni nada.
- Compruebe por sus propios medios lo que le dicen antes de hacer nada.

Mejor estar preparado: www.ocu.org/ocu-castilla-lamancha-digitalizacion