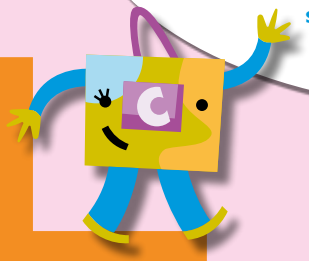
hablamos de ...

seguridad online

La tecnología ha entrado a formar parte de nuestro día a día, pero navegar por la red trae consigo algunos riesgos que afectan a la seguridad de los consumidores. Suplantar nuestra identidad haciendo uso de nuestras contraseñas, la solicitud telefónica o por medio de correo electrónico de datos personales o cuentas bancarias, el envío de SMS donde se nos solicita la descarga de un documento, o la necesidad de realizar una transferencia inmediata para recoger un envío, coloca al consumidor en una situación de vulnerabilidad en la red.



Información de interés para saber más sobre **la ciberseguridad en tus compras y operaciones en Internet**

CERCA

AYUNTAMIENTO DE ALICANTE

¿Qué es la ciberseguridad?

- La seguridad informática o ciberseguridad es el conjunto de acciones que realizamos con la finalidad de proteger la información que generamos o que se procesa a través de los ordenadores, las redes, los telefonos móviles o cualquier sistema electrónico. **En muchas ocasiones las páginas web que visitamos también facilitan información sobre los usuarios, ¿cómo?, por medio de lo que se conoce como cookies.**

¿Qué son las cookies?

- Las cookies son pequeños archivos que se almacenan en nuestro dispositivo y **contienen la información sobre nuestra navegación. Algunas tienen la única finalidad de enviarnos información acorde a nuestros intereses.**

- Las cookies, que permiten recopilar nuestro historial de navegación y enviarnos posteriormente información, son aceptadas por el consumidor al acceder a la página web. **Pero es la información confidencial la que más fraudes puede generar a los consumidores.**

¿Qué es información confidencial?

- **La información confidencial es cualquier información de una persona física** (nombre y apellidos, DNI, número de cuenta bancaria, tarjetas, domicilio, población, imagen, voz, ocupación, edad, enfermedades, etc.).

- Los **derechos del consumidor relativos al tratamiento de datos** son el de **información**, **acceso**, **rectificación**, **cancelación** y **oposición**.

- **Cuando el consumidor vea denegado el ejercicio de estos derechos puede ponerlo en conocimiento de la Agencia de Protección de Datos.**

- A través de la ingeniería social se puede obtener información confidencial y manipular la misma **suplantando a los legítimos usuarios, lo que puede originar grandes fraudes y perjuicios a los consumidores.** Los tipos de manipulación de datos más destacados: **Vishing, Phising** y **Smishing.**

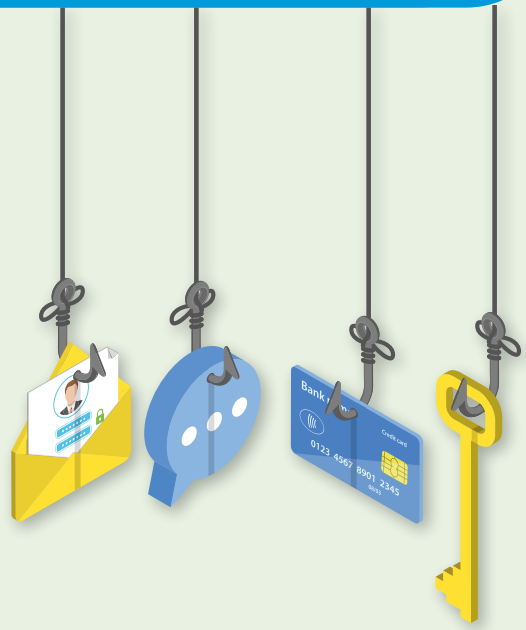
CERCA

Formas de manipulación de datos

- **Vishing**. **Es la suplantación de la identidad de un servicio telefónico y otros servicios mediante una llamada telefónica**, donde se nos solicita información confidencial o que accedamos a alguna página web.

- **Phishing**. Es la técnica más usada para acceder a datos bancarios o personales. En este caso **se suplanta la identidad de una entidad bancaria, empresa o similar que es de uso habitual para el consumidor** con lo cual es más fácil el engaño. El fin último es solicitar el acceso a una página web para acceder a nuestro dispositivo e infectarlo con un virus, solicitar el envío de alguna cantidad de dinero o bien reclamar nuestros datos confidenciales.

- **Smishing**. **Se realiza mediante el envío de SMS a nuestro terminal con la finalidad de que descarguemos un documento**, normalmente infectado, realicemos un pago o accedamos a algún enlace.



Consejos de Ciberseguridad sobre el dispositivo utilizado

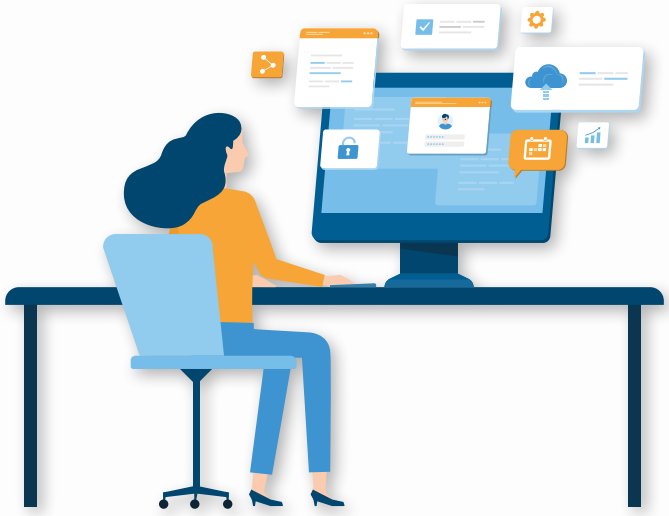
- **Accede con contraseñas seguras** y cámbialas si observas el envío de correos maliciosos.
- Protege tu ordenador, si haces uso de datos confidenciales, con la **instalación de un antivirus que esté actualizado y sea confiable.**
- Bloquea o **apaga el ordenador cuando no lo estés utilizando.**
- **No uses programas que no estén autorizados.** Actualiza el software. Es necesario mantener tanto el sistema operativo como los programas actualizados.
- **Instala solo aplicaciones desde páginas web que sean oficiales** y si observas la instalación de alguna aplicación desconocida debes desinstalarla.
- **Si accedes mediante una wifi pública no introduzcas tus datos.**
- No ignores los avisos del ordenador sobre **certificados digitales.**

Consejos de ciberseguridad sobre los mensajes recibidos

- Debes ignorar los correos no esperados que tengan apariencia de organismos oficiales ya que **los organismos oficiales nunca solicitan datos confidenciales por correo electrónico.**
- Observa con detenimiento la dirección de correo del remitente, no solo el nombre sino el dominio que usa, **si es un dominio no corporativo o genérico debes sospechar. En el caso de ser de alguna entidad bancaria con la que estamos trabajando debemos contactar con nuestro gestor. Si es de alguna administración pública, no facilitar información y contactar para informar sobre el fraude.**
- En ocasiones los mensajes que se envían de modo masivo se realizan a nivel internacional y **la traducción no es correcta o tienen faltas de ortografía o frases mal construidas.**
- **El envío de información confidencial, la solicitud de realización de un pago, el acceso a un documento de descarga o el envío de datos bancarios** son acciones que nos llevan a desconfiar y en las que hemos de tomar precauciones.
- **Atención a los enlaces trampa que nos remiten a direcciones que nos descargan algún archivo.**
- Desconfía de los mensajes que requieran **alguna acción con carácter urgente.**
- **Las páginas que comienzan por HTTPS son la versión segura** y nos garantizan que la información que se transmite está cifrada y protegida.
- **Descarga únicamente los archivos necesarios** y antes de hacerlo comprueba quién lo envía y la importancia del mismo.

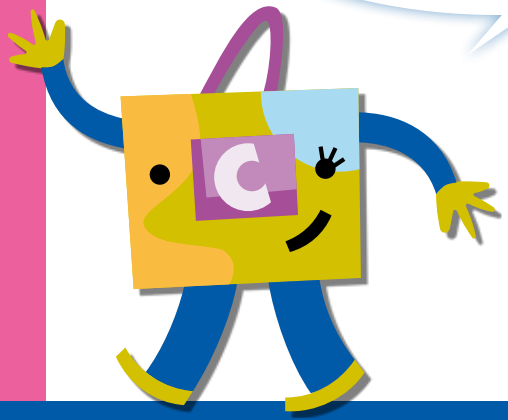
Ten esto siempre en cuenta

1. **Usa contraseñas largas y cámbialas cada tres meses.** Utiliza un mínimo de 10 caracteres con números, mayúsculas, minúsculas y signos.
2. **Evita guardar contraseñas en el ordenador.** Cuando te lo preguntan para facilitarte la navegación, recházalo.
3. **Utiliza un gestor de contraseñas.** Es un programa en el que puedes guardar diferentes passwords, teniendo una contraseña maestra.
4. **Cuida tu privacidad.** No facilites tus datos personales ni los publiques en las redes sociales.
5. **Respalda tu información personal en la nube.** Ante el riego de robo de información por los ciberdelincuentes para suplantar tu identidad, haz respaldos en espacios de almacenamiento seguro en la nube. (Google, One Drive...).



estamos aquí para informarte, estamos para ayudarte

Si te interesa el tema y quieres saber más, contacta con nosotros. Somos CERCA y te acompañamos en la formación en materia de consumo para ayudarte en tu día a día.



CERCA

CENTRO EDUCATIVO DE RECURSOS DE CONSUMO ALICANTE

C/ Calderón de la Barca • Mercado Central

cerca.alicante.es cerca@alicante.es 965 145 294

cercalicante

AYUNTAMIENTO DE ALICANTE