Guía sobre uso responsable y seguro de la tecnología

Diputación de Segovia

asuntos sociales
SUMAMOS JUNTOS

Guía elaborada por el Área de Asuntos Sociales y el Delegado de Protección de Datos (DPD) de la Diputación de Segovia.

Edita: Centro de Investigación e Innovación Social (CIIS) de la Diputación de Segovia.

D.L.: SG 231-2023

Usar la tecnología de manera responsable y segura

Probablemente ya seas consciente de que la protección de los datos personales es algo importante.

También de que las tecnologías en general, e Internet en particular, entrañan una serie de riesgos que van más allá del mero control sobre nuestros datos: fraudes, estafas o engaños son otros de los peligros que esconde la Red.

Aun así, ¿alguien te ha explicado de manera clara y sencilla cómo usar de forma responsable y segura la tecnología en el día a día?

Ese es el objetivo de la presente Guía, que contiene una serie de consejos y recomendaciones prácticas que te ayudarán a desenvolverte con mayor seguridad y responsabilidad en el mundo digital.

¿Comenzamos?

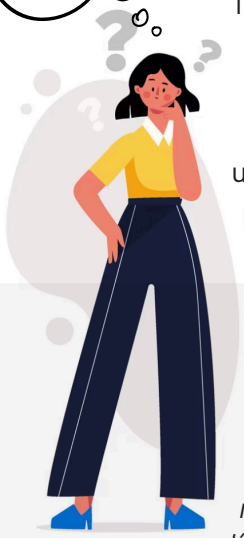
Diputación de Segovia

asuntos sociales
SUMAMOS JUNTOS

1 Una buena contraseña, la mejor protección para tu teléfono

Tu teléfono móvil contiene mucha información sobre la familia, amigas y amigos, y también sobre otras personas a las que aprecias.

La mejor forma de protegerlas a todas ellas es una contraseña en el teléfono que sea difícil de adivinar por parte de personas malintencionadas. Con una buena contraseña, también estarás protegiendo tu propia privacidad.



¿Cómo crear una contraseña segura para nuestro teléfono móvil?

*Para que una contraseña sea **segura**, no puede ser demasiado sencilla. Por ejemplo: "1234", "0000", "1111", o el año de nacimiento, no son buenas contraseñas. Sin embargo, cada día tenemos que recordar muchas cosas y es normal que una contraseña que sea complicada se nos pueda olvidar.*

Entonces, ¿Qué hacemos? ¿Apuntamos la contraseña en un papel que pegamos detrás del teléfono móvil? ¿Se la decimos a otras personas para que nos la recuerden cuando se nos olvide? Estas no son buenas ideas, porque para que una contraseña sea segura también tiene que ser secreta.

*Lo mejor es tratar de encontrar un número que solo tenga **sentido para ti**, pero **que no se te olvide nunca** (por ejemplo, el número de la matrícula del primer coche, la fecha de nacimiento de un ser querido o cualquier otra fecha significativa).*

*Recuerda también que, si el teléfono móvil lo permite, una **contraseña de seis números** es mejor que una de cuatro (cuantos más números tenga, más difícil será de adivinar para la ciberdelincuencia).*

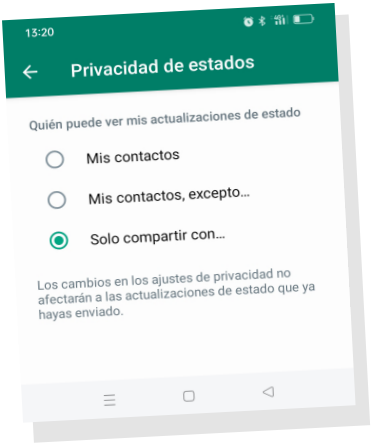
Otra buena posibilidad es proteger el teléfono móvil con la huella dactilar, el reconocimiento facial o un patrón sobre 9 puntos.

2 Antes de publicar una fotografía en las redes sociales o en el estado de wasap, debes saber que...

Nos hemos acostumbrado a publicar imágenes tanto nuestras como de los demás de manera impulsiva, a golpe de clic. No obstante, debemos ser conscientes de que cuando publicamos una fotografía en las redes sociales o en nuestro estado de wasap estamos compartiéndola con muchas personas, y un uso responsable de la tecnología se basa en el respeto de la dignidad y los derechos de los demás.

Piensa, además, antes de publicar una fotografía de un/a menor, si puede ocasionarle algún perjuicio al estar expuestos a más riesgos y más posibilidades de manipulación.

Las fotografías de tus vacaciones es mucho más seguro publicarlas cuando hayas vuelto del viaje, dejando claro que ha finalizado y estás en casa.



Tampoco es bueno dar muchas pistas sobre nuestro nivel económico y nuestra forma de vida: un exceso de publicaciones en este sentido puede ser un polo de atracción para la ciberdelincuencia.

Tienes que saber también que es posible limitar las personas que pueden ver tus publicaciones (en el apartado de "Privacidad de estados" de wasap, activando "Solo compartir con...").

3 Cuanta menos información a personas desconocidas, mucho mejor

Facilitar información a desconocidos/as sobre ti o sobre la familia o amistades, ya sea por teléfono, wasap, o correo electrónico, puede ser muy peligroso, especialmente si se refiere al DNI, datos de cuentas bancarias, número o fecha de caducidad de la tarjeta bancaria, domicilio, edad, si vives solo/a o acompañado/a, etc.

Es importante estar siempre alerta, las personas delincuentes se hacen pasar por el banco, por un organismo oficial, por una empresa de mensajería,... para intentar engañarte y que facilites el número de la tarjeta, el código de seguridad CVV, el PIN que utilizas en el cajero, etc. y lo hacen por correo electrónico, un mensaje de texto, por wasap o incluso a través de una llamada telefónica. Ten cuidado porque es el intento de estafa más común.

A veces envían mensajes fraudulentos diciendo que tienes un paquete pendiente de entrega junto a un enlace. No pinches estos enlaces si no esperas nada, o si observas algo extraño en el mensaje.

En otras ocasiones envían mensajes de una persona que dice ser tu hija o tu hijo, pero desde un número de teléfono desconocido, diciendo que necesita que ingreses inmediatamente una cantidad de dinero a

una cuenta bancaria porque está en problemas. Se trata de una estafa muy habitual.

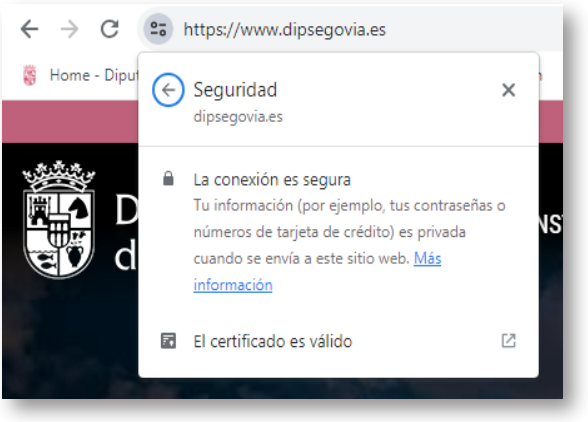
En definitiva, si algo parece raro o sospechoso ten mucha precaución y asegúrate de quién está realmente al otro lado del mensaje o de la llamada de teléfono, y ante la más mínima duda, lo más aconsejable es no facilitar ninguna información ni abrir ningún enlace hasta que lo hayas comprobado.

4 Navegando por Internet

Internet es una herramienta fabulosa, puedes consultar tus cuentas bancarias, pedir cita médica, ...pero atención, es importante asegurarse que la aplicación o la página web utilizada es segura y de confianza.

En las compras por internet, revisa que la página web por la que navegas tiene la correspondiente información legal y de contacto. Para poder confiar en una página es muy importante saber previamente cuáles son las condiciones de compra, formas de pago, envío y devoluciones, protección de tus datos (privacidad), etc.

Y, por supuesto, que disponga de información de contacto (un teléfono o una dirección de correo electrónico) y de dónde está ubicada la empresa, por si surgen problemas. Puedes probar a contactar incluso antes de comprar para asegurarte un poco más.



Fíjate en que la dirección que se muestra en la barra de direcciones del navegador de internet empieza por "HTTPS://" y no por "HTTP://". La letra "S" significa "Seguro" y hace referencia a que la información facilitada a través de dicha página web va a estar protegida frente a terceros (por ejemplo, un/a ciberdelincuente).

Asimismo, si vas a realizar gestiones bancarias o de pago, no lo hagas conectado a internet a través de una red wifi pública o abierta, y usa los datos móviles del propio teléfono, es mucho más seguro.

Sé muy prudente con los anuncios de gangas, chollos y superofertas que hay en internet, porque puede tratarse de un "anzuelo" para hacerse con tus datos personales y/o bancarios.

Por último, en la descarga de aplicaciones bancarias, contacta con tu entidad para asegurarte de que realmente es la correcta.

5 ¿Qué hacer si consideras que has sufrido un perjuicio en tus derechos?

Un primer paso puede ser hablar con la persona o la entidad que ha podido utilizar tus datos o tu imagen sin tu permiso. Algunas entidades tienen designado un Delegado de Protección de Datos (DPD) para atender este tipo de cuestiones.

Si no recibes respuesta o entiendes que ésta no es satisfactoria, puedes dirigirte a la Agencia Española de Protección de Datos (www.aepd.es), autoridad pública independiente encargada de velar por la privacidad y la protección de datos de la ciudadanía.

En el caso de un posible fraude, estafa o engaño (por ejemplo, una compra fraudulenta con tu tarjeta bancaria), ponlo en conocimiento de la Guardia Civil o Policía Nacional, y bloquea lo antes posible tu tarjeta.

La indiferencia es el peor enemigo de nuestros derechos: presta atención a las campañas informativas, recomendaciones y noticias que desde la administración o medios de comunicación nos proporcionan, y nos acercan a la cultura de la protección de datos y de la ciberseguridad.

La prevención es el mejor instrumento frente a los peligros del mundo digital.

AVISO IMPORTANTE:

La presente Guía no ha sido elaborada en nombre, por cuenta o en colaboración con ninguna autoridad competente. La información de carácter general presentada en la misma tiene como exclusiva finalidad contribuir al fomento de una cultura de la protección de datos y de la ciberseguridad, sin que constituya en caso alguno asesoramiento de ningún tipo, debiendo hacerse siempre un uso responsable de la misma.

Diputación
de Segovia

asuntos
sociales

SUMAMOS JUNTOS