Excmo. Ayuntamiento de
Toledo

OMIC
Oficina Municipal de
Información al Consumidor

EN LA **OMIC** DEFENDEMOS TUS DERECHOS

Si necesitas más información puedes contactar con la
Oficina Municipal de Información al Consumidor (OMIC) del Ayuntamiento de Toledo
a través del teléfono **925 330 770**
o del correo electrónico **omic@toledo.es.**
Estamos en Pza. Consistorio, nº1.
45071.- Toledo.

1.- Protege la información privada de tu móvil u ordenador.

- Utiliza un **código de desbloqueo de la pantalla (patrón)**. Si te roban el móvil, no podrán acceder a la información.
- Haz **copias de seguridad de la información más importante en varios dispositivos** (en el disco duro y en un USB por ejemplo). Si tu dispositivo falla, la información la tendrás guardada en otro sitio.
- Descárgate **sólo aplicaciones seguras** y hazlo a través de la web del fabricante. Así te aseguras de que esas aplicaciones están revisadas.
- Comprueba los **comentarios que hacen otras personas** sobre una app, así sabrás si es sospechosa.
- Instala un **antivirus**, así protegerás tu móvil de intrusos.
- Si te conectas a **redes wifi públicas** (en bares, cafeterías, estaciones de tren, aeropuerto etc) **no hagas compras ni intercambies información personal** porque no sabes quién está conectado a esa misma red y los datos pueden no estar cifrados.

2.- Uso de contraseñas.

- **No uses la misma contraseña para todos los servicios** (Facebook, Instagram, PayPal, Gmail). Si la contraseña falla, podrían acceder a todos tus servicios.
- **No facilites tu contraseña a nadie**, porque podrían contestar a tus correos haciéndose pasar por ti, podrían publicar tu nombre y tus datos en redes sociales o hacer compras en tu nombre.
- **Usa contraseñas seguras** (mezclando mayúsculas, minúsculas, números y caracteres especiales como #,*, $ con 8 cifras o letras en total).

3.- Navega por sitios seguros.

- Para saber si el sitio web es seguro puedes comprobar lo siguiente:
  - Que aparezcan las **letras https:// (la "s" al final significa que el sitio es seguro).**
  - Que aparezca un **candado cerrado**, que se encuentra al pie de la página (si el candado está abierto, puede no ser seguro).
  - Que aparezca una **llave entera al pie de la página.**
- Conéctate mejor desde tu **wifi de casa** o con el 3G/4G del móvil y evita las wifis de sitios públicos.
- **Cierra la sesión** cuando te desconectes. Si tu sesión queda abierta, tus datos personales estarían visibles para las personas que se conecten después en el mismo dispositivo.

4.- No tienes obligación de dar todos los datos que te piden.

- Cuando te pidan **datos personales** en una página web, antes **deben decirte para qué los van a utilizar.**
- **No des información sobre ti, tu familia o amigos.** A veces te piden información sobre tus gustos, tu familia o amigos, que luego utilizan para mandar correos electrónicos o publicidad que no quieres recibir.
- Algunas redes sociales te piden **datos** como tu domicilio, el colegio en el que estudias, tus gustos, tus aficiones, quienes son tus familiares, etc., **que no son obligatorios**

5.- Las redes sociales.

- Aunque configures tu perfil en una red social para que lo que publiques sólo lo vean tus amigos, esa **información pueden verla otras personas sin que tú lo sepas.**
- Las personas a las que tú das amistad a través de las redes también tienen amigos en la red que podrán ver lo que publicas.
- Aunque creas que tienes controlado lo que publicas, **si subes una foto y uno de tus amigos da "me gusta", los amigos de tus amigos podrán ver esa foto.** Aunque después se borre, **no desaparece de la Red.**
- Las personas que conoces por internet son **desconocidos en la vida real,** en realidad no son tus amigos.
- **Nunca publiques** en tus perfiles datos que puedan utilizar contra ti o te puedan perjudicar como tu **número de móvil, insultos, dónde vas a ir en vacaciones etc.**
- Existe una colección de **vídeos de seguridad en redes sociales** que encontrarán en internet y que explican paso a paso cómo **configurar las opciones de privacidad y seguridad** para redes como Instagram, snapchat, twitter, Facebook, whatsapp, youtube.
- En las redes sociales comportarse con **respeto y educación**. No hagas a otros lo que no quieras que te hagan a ti.
- Si conoces a alguien que sabes que está siendo acosado, **denúncialo**.
- **Desconecta del móvil la opción de "geolocalización",** para que nadie sepa dónde estás cuando publiques algo en tu muro desde el móvil.

6.- La mensajería instantánea (whatsapp, snapchat ...)

- **No reenvíes los mensajes en cadena** que te dicen que si no los reenvías te pasará algo.
- Ten cuidado con los mensajes que te dicen que **descargues una aplicación o que recibirás un premio por rellenar una encuesta,** no suelen ser ciertos.
- Decide con quien quieres comunicarte y **bloquea a los usuarios** que no te interesen.
- En tu perfil **no pongas fotos muy comprometidas.**
- En tu **estado de whatsap no des información privada sobre ti.**
- Haz **copias de seguridad** de los mensajes del chat y utiliza la **opción de chat privado o secreto** para que las personas que no te interesen no puedan ver tu conversación.
- Pon una **contraseña de bloqueo en el móvil**, para que en caso de robo la persona que lo haya robado no pueda enviar mensajes en tu nombre.