Fuente : OSI

Tu información personal

A menudo no somos conscientes de la información que existe sobre nosotros en Internet, proporcionada por nosotros mismos o por otras personas u organizaciones. Tampoco pensamos que esa información permanece en Internet durante muchos años, accesible para quien quiera buscarla.

Identidad digital

En un mundo permanentemente conectado, cada paso que damos en Internet deja una huella muy difícil de borrar. Cuando algo se publica, en un instante está disponible en la otra punta del mundo y permanece accesible durante mucho tiempo.

Este rastro es la identidad digital y está compuesto por los datos que publicamos de forma consciente y por la información que se recopila sin que nos demos cuenta.

Se puede obtener una gran cantidad de información de una persona con unas simples consultas en un buscador. Nos sorprenderíamos de lo que se puede llegar a encontrar.

Debemos darle a nuestra información el valor que tiene. Igual que no dejaríamos un álbum fotográfico en un autobús, seamos cuidadosos con lo que publicamos en Internet: comentarios en redes sociales, fotografías personales, datos de geolocalización, etc.

No hay que olvidar la importancia de la privacidad. Del mismo modo que ponemos medios para que nadie curiosee por la ventana de nuestra casa, también nos debemos preocupar de evitar que un desconocido tenga acceso a nuestras publicaciones, fotos y mensajes en las redes sociales.

Es importante utilizar las herramientas que están a nuestro alcance para proteger nuestra información personal.

Debemos aprender a valorar y a proteger nuestra información. La información que publicamos en Internet puede volverse en nuestra contra o ser utilizada para perjudicarnos. Una vez publicada en Internet perdemos su control.

Información general

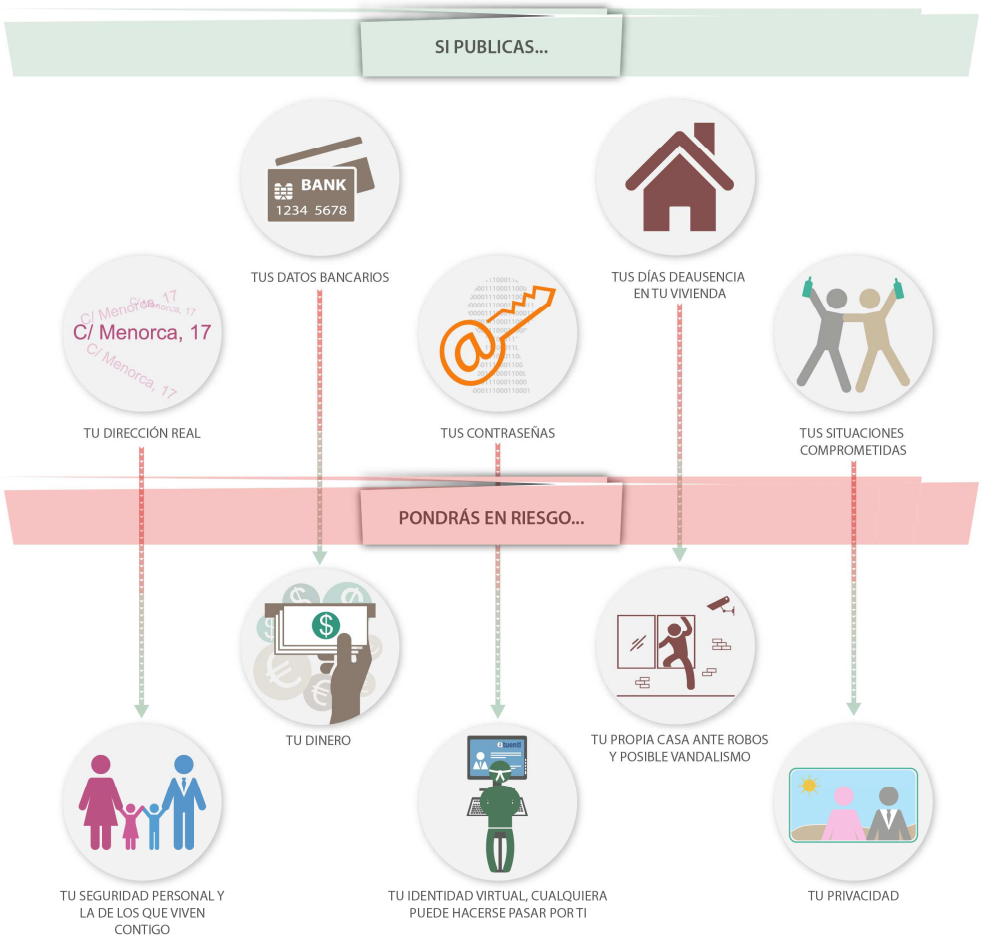
Gran parte de la información que se puede encontrar sobre nosotros en Internet la hemos compartido nosotros mismos: redes sociales, publicaciones en blogs, foros, etc. Cuanta más información se sepa de nosotros, más fácil se lo ponemos a los ciberdelincuentes.

Pero no sólo debemos ser cuidadosos con lo que publicamos sobre nosotros, también debemos proteger la privacidad de nuestros amigos y familiares.

Es importante conocer los riesgos de hacer públicos ciertos datos:

Fuente : OSI

- **Correo electrónico.** Que nuestro correo deje de ser privado hará que comencemos a recibir cada vez mayor número de spam, mensajes con intentos de engaño (phishing), fraude, etc.
- **Datos bancarios.** Facilitar nuestros datos bancarios nos puede exponer a una pérdida económica. Seamos muy precavidos con las páginas web donde utilizamos estos datos para realizar compras online y nunca facilitemos este tipo de datos por correo electrónico. En 2012 y 2013 fue muy común en España el virus de la Policía. Éste alertaba al usuario que era culpable de algún delito y pedía el pago de una multa de 100 euros. El mensaje incluía el logo de la Policía Nacional y en ocasiones la fotografía del propio usuario, capturada con la webcam.
- **Ubicación geográfica.** Publicar los lugares que solemos frecuentar proporciona información que permite que alguien malintencionado pueda localizarnos en persona o pueda conocer nuestra rutina y hábitos diarios. También permite averiguar en qué momento nos encontramos ausentes de nuestro domicilio.
- **Fotografías y vídeos.** Nuestras fotografías y vídeos personales contienen mucha más información de la que pensamos: ubicaciones físicas, quiénes son nuestros amigos y familiares, cuál es nuestro nivel económico, qué aspecto tiene nuestro domicilio, gustos, preferencias, etc.

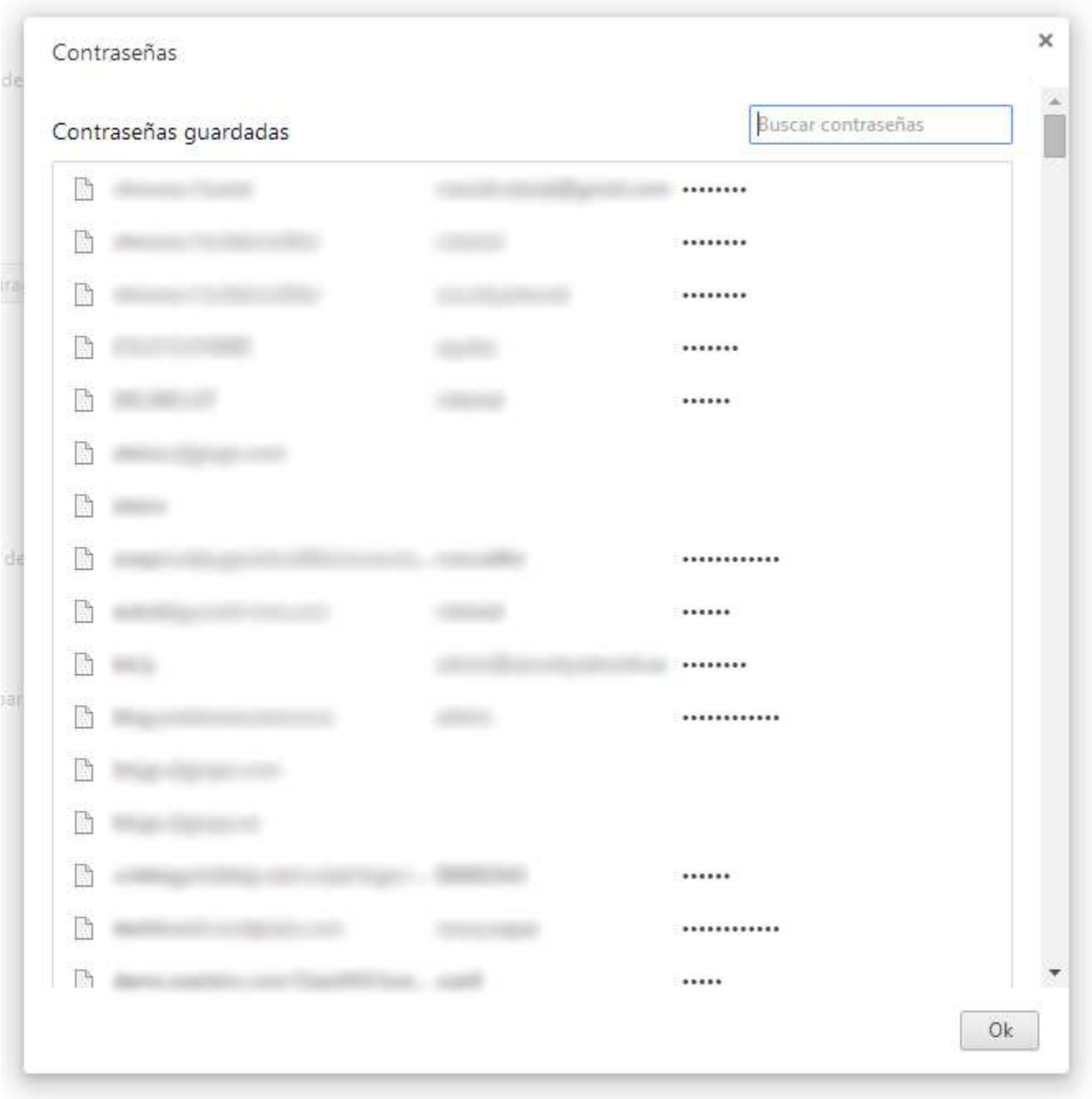


Datos de navegación

Mientras navegamos también estamos proporcionando involuntariamente mucha información. El navegador puede almacenar ciertos datos como son el historial (páginas que visitamos), las

Fuente : OSI

contraseñas que utilizamos para acceder a algunos servicios, los datos que introducimos en formularios, las cookies de navegación, etc. Aunque en el caso de las cookies, la legislación española impide que las páginas webs las instalen en nuestros ordenadores a menos que hayamos dado un consentimiento expreso para ello.



Todos estos datos guardados por el navegador aportan mucha información sobre nosotros. Por este motivo, existen determinados programas diseñados para robarla y cederla a ciberdelincuentes.

Para incrementar nuestra seguridad, es conveniente que borremos periódicamente estos datos de nuestro navegador o lo configuremos para que directamente no los almacene.

Fuente : OSI

Registro en servicios online

Para registrarnos en algunos servicios de Internet, en ocasiones se nos pide diversos datos personales: nombre y apellidos, teléfono, fecha de nacimiento, correo electrónico, etc.

Al proporcionar estos datos corremos un riesgo, ya que no podemos controlar con exactitud quién va a acceder a ellos ni para qué. La ley española obliga a las empresas a mantener en secreto estos datos y a otras obligaciones, pero a algunas no les aplica por residir en otros países.

Por este motivo, debemos valorar antes de darnos de alta en algún servicio, qué datos nos piden y qué uso van a hacer de ellos. Para ello es importante que leamos las condiciones de uso y la política de privacidad del servicio antes de facilitar cualquiera de nuestros datos.

Dispositivos móviles

Los dispositivos móviles como tabletas, smartphones o portátiles almacenan gran cantidad de información privada: fotos y vídeos, correos electrónicos, contactos, acceso a redes sociales, datos de pago online, etc. Si alguien accede a toda esta información conocerá nuestros datos privados e incluso podrá hacerse pasar por nosotros en Internet. Debemos proteger la información que almacenamos en ellos frente a posibles pérdidas o robos del dispositivo. Podemos establecer modos de acceso seguros mediante contraseñas o patrones de pantalla, lo que ayudará a proteger nuestra información. También son recomendables las aplicaciones que permiten el bloqueo y el borrado de datos remoto, que protegen nuestra información en caso de extravío del dispositivo.

Lugares y equipos públicos

A veces utilizamos equipos ajenos para conectarnos a Internet: locutorios, aulas de formación, hoteles, etc. Además, lugares como aeropuertos, bibliotecas, universidades, hoteles, etc. ofrecen WiFi abiertas o públicas a las que nos podemos conectar nosotros y otras muchas personas a las que no conocemos.

En todos estos casos, lo más recomendable es evitar el envío de información personal ya que desconocemos el nivel de protección del equipo o de la red. Alguien con suficientes conocimientos técnicos puede conectarse a la misma red y capturar lo que enviamos, incluso las contraseñas.

Consejos finales

Todo lo que hacemos en Internet deja un rastro y nuestra información personal no solo es valiosa para nosotros, también para los ciberdelincuentes. Siguiendo algunos consejos básicos podremos incrementar la seguridad de nuestra información en la red:

- **Sé cuidadoso con la información que publicas.** Una vez en Internet, ésta es permanente, escapa de tu control y es accesible desde cualquier lugar del mundo.

Fuente : OSI

- **Configura adecuadamente la privacidad de tus redes sociales.** Todas ellas ofrecen opciones de privacidad para que controlemos quién tiene acceso a tus publicaciones.
- **Conoce tus derechos** La ley de protección de datos obliga a todas las empresas españolas a proteger y a mantener en secreto tus datos, sin embargo no a todas las empresas les aplica esta ley por residir en otros países. Infórmate, lee las condiciones de privacidad y haz valer tus derechos.
- **Sé precavido con tus dispositivos y los lugares públicos.** No olvides la seguridad de tus dispositivos, y utilizar siempre redes seguras para compartir información.
- **Solicita a Google o a otros buscadores la retirada de información publicada sobre ti que te pueda estar perjudicando.**Tienes derecho al olvido en Internet.