Guía de seguridad online para personas mayores

Consejos útiles para ayudarte
a navegar por Internet de forma más segura

Google

Introducción

Con Internet es mucho más fácil obtener información sobre cualquier tema que te interesa, realizar tareas cotidianas y estar en contacto con las personas a las que quieres. Internet te permite comunicarte al instante con tu familia y amigos mediante correo electrónico, mensajes y videollamadas, así como compartir fotos y vídeos con ellos.

Tener acceso a Internet es tener el mundo al alcance de la mano. Con Internet puedes comparar precios en diferentes cadenas de supermercados, hacer la compra online y pedir que te la lleven a casa. Y por si eso fuera poco, también puedes aprender otro idioma, desarrollar tus conocimientos o conectar con personas que comparten tu mismo interés.

Internet es un lugar fascinante que ofrece un sinfín de posibilidades. Sin embargo, al igual que en el mundo real, es importante aprender a protegerse de posibles engaños. Esta guía te proporcionará información sobre algunas de las estafas más comunes en la Web y te ofrecerá consejos útiles para navegar por Internet de manera más segura.

Índice

Términos importantes

Hay varios términos que es bueno conocer antes de empezar a leer esta guía. Si tienes preguntas o dudas sobre alguno de los siguientes términos, puedes buscar más información online o preguntar a un amigo o familiar.

Tema Conocimientos generales

Término	Definición
Navegador	Se utiliza para acceder a la Web. Los más populares son Chrome, Firefox, Safari, Internet Explorer y Edge.
Correo electrónico	Servicio de correo que funciona de manera electrónica.
Wifi	La tecnología que te permite conectarte a Internet de forma inalámbrica.
SMS	Servicio de mensajes de texto disponible en la mayoría de teléfonos móviles.
Documento adjunto	Archivo que se envía junto a un mensaje de correo electrónico.
Descargar	Obtener un archivo, como una aplicación o un programa, a través de Internet para almacenarlo en tu teléfono u ordenador.
Subir	Transferir un archivo a un servidor o a la nube: es lo contrario a descargar.
Iniciar sesión	Introducir tu nombre de usuario y contraseña para identificarte y obtener acceso a tus cuentas online.
Cerrar sesión	Práctica de seguridad importante después de utilizar un ordenador público o el dispositivo de terceros para acceder a tu cuenta: es lo contrario a iniciar sesión.
URL	Es la dirección online de un sitio web (p. ej., google.com y gmail.com).

Tema Seguridad online

Término	Definición
Software malicioso	Es un término que abarca virus informáticos, troyanos, gusanos informáticos, software de publicidad y otros programas maliciosos.
Ingeniería social (phishing)	Cuando alguien intenta engañarte para que hagas algo peligroso online, como descargar software malicioso o compartir información personal.
Contraseñas	En esta vida es importante reutilizar y reciclar, excepto las contraseñas. Crea una contraseña diferente para cada una de tus cuentas online.
Autenticación de dos factores	La autenticación de dos factores añade una capa de protección adicional para proteger tu cuenta al iniciar sesión.
Antivirus	Te ayuda a proteger tu ordenador frente al software malicioso.
https	Cuando hagas compras online, comprueba que la dirección web empieza por https antes de introducir los datos de pago. La “s” de https significa seguro.
Cifrado	Es una forma de codificación que utilizan algunos proveedores de correo electrónico y sitios web para evitar que otros fisguen tu información.
Personal	Este tipo de información no debe compartirse online (p. ej., número de DNI, tus contraseñas, dirección de tu casa, etc.)
Spam	Correos electrónicos o mensajes no deseados o no solicitados que normalmente los estafadores envían a un gran número de usuarios.
Símbolo	Las contraseñas seguras contienen al menos uno, como por ejemplo ~, !, @, #, $, %, ^, & o *.
Llaves de seguridad	Dispositivos electrónicos que se pueden utilizar, además de la contraseña, para acceder a tu cuenta online.

Tema Compartir online

Término	Definición
Sobreexposición	Compartir demasiada información personal.
Ajustes	Es importante configurarlos para decidir qué quieres compartir y con quién quieres compartirlo.
Pública	Es la información sobre uno mismo que todo el mundo puede ver.
Privada	Es la información sobre uno mismo que solo puede ver su propietario.
Privacidad	Es la capacidad de elegir de forma selectiva la cantidad de información sobre ti que revelas a los demás.
Normas de la comunidad	Reglas comunitarias que sirven para que las redes sociales y otros sitios web en los que se comparte contenido sean del agrado de todos.
Denunciar	Acción que puedes realizar cuando ves algo inapropiado en las redes sociales y quieres que lo revisen.
Bloquear	Acción que puedes realizar para evitar la interacción con usuarios ofensivos en las redes sociales y algunos servicios de mensajería.
Reputación	Es la percepción que las personas tienen de ti, tanto online como offline.
Viral	Una imagen, un vídeo o una publicación se hacen virales cuando circulan de forma rápida por la Web.
Huella digital	Todo lo que hay en la Web sobre ti, incluidos vídeos, fotos, menciones y mucho más.
Geolocalización	Es la estimación de la ubicación geográfica de un teléfono móvil o un ordenador conectado a Internet.
Perfil	Información sobre alguien en un sitio web. Incluye su foto, nombre y otros detalles personales.
Avatar	Representación gráfica que algunas personas usan en lugar de una foto real para crear un perfil en redes sociales.
Defensor	Persona que interviene y toma medidas cuando ve que alguien recibe un tratamiento injusto: es lo contrario de espectador.
Ciberacoso	Se da cuando alguien es acosado o intimidado a través de las redes sociales y de otros medios electrónicos.

Protege tus cuentas en Internet

Tus cuentas personales en redes sociales te permiten compartir información con tu familia y amigos, como por ejemplo las fotos de la fiesta de cumpleaños de la semana pasada. Otras cuentas online, como la bancaria, te permiten hacer transacciones comunes desde tu casa, tal y como transferir dinero, pagar facturas o hacer compras en Internet.

Puesto que tus cuentas de Internet están vinculadas a tu identidad personal, es importante tomar medidas para protegerlas frente a intrusiones. Para ello, necesitas contraseñas seguras.

Crea contraseñas seguras

Una contraseña segura es el primer paso para defenderte de usuarios malintencionados que quieran entrar en tu cuenta y acceder a tu información personal.

Las principales características de una contraseña segura son:

- Longitud: utiliza un mínimo de 8 ó 9 caracteres.
- Complejidad: utiliza una combinación de letras mayúsculas y minúsculas, números y símbolos.
- Evia utilizar información personal (p.ej., no utilices tu fecha de nacimiento ni el nombre de tus hijos).

Veamos cómo puedes crear fácilmente tu propia contraseña segura.

1. Piensa en una frase fácil de recordar, como por ejemplo, "**T**engo **d**os **g**atos **e**n **c**asa **l**lamados **T**om **y** **J**erry".
2. A continuación, toma la primera letra de cada palabra usando letras mayúsculas y minúsculas donde corresponda. En este ejemplo, debería quedar así: **TdgeclTyJ.**
3. Donde sea posible, reemplaza letras con números o símbolos: **T2geclT&J.**

Utiliza contraseñas únicas

Ahora que tienes una contraseña fuerte y fácil de recordar, es normal que quieras usarla para todas tus cuentas en Internet. Sin embargo, reutilizar contraseñas es arriesgado. Si alguien descubre la contraseña de una de tus cuentas, como por ejemplo la de tu correo electrónico, podría acceder también a otras de tus cuentas usando la misma contraseña. Para reducir las posibilidades de que eso ocurra, puedes crear contraseñas únicas para cada una de tus cuentas online, sobretodo para hacer compras o acceder a la banca online.

Pero, ¿cómo puedes recordar múltiples contraseñas de forma sencilla? Además de crear tus contraseñas a partir de una frase fácil de recordar, también puedes usar un administrador de contraseñas, como passwords.google.com.

Recupera tu cuenta

A todos se nos ha olvidado la contraseña alguna vez. Afortunadamente, la mayoría de servicios online ofrecen la opción de añadir un número de teléfono de recuperación o una dirección de correo electrónico secundaria para recuperar el acceso a tu cuenta en caso de olvidar la contraseña. Para asegurarte de que puedes volver a acceder a tus cuentas de forma rápida y fácil, debes configurar las opciones de recuperación de contraseña antes de que eso pase.

Otras herramientas

¿Quieres revisar y ajustar los controles de seguridad de tu cuenta de Google? Accede a myaccount.google.com y haz la revisión de seguridad para consultar qué dispositivos has utilizado para acceder a tu cuenta de Google, y toma medidas adicionales para proteger tu cuenta, como activar la verificación en dos pasos (g.co/2step).

Comparte con prudencia

Internet ha revolucionado la manera en que nos comunicamos, facilitando la comunicación a distancia desde cualquier ordenador o dispositivo móvil conectado a la red. Aunque es posible compartir archivos, experiencias y recuerdos en cuestión de segundos, es importante ejercer prudencia y compartir ciertos tipos de contenido solamente con personas de confianza.

Recuerda que todo lo que compartes online (ya sea en las redes sociales, en foros de Internet, o en aplicaciones de mensajería instantánea) puede ser visto en el futuro por personas que no deseas.

Por eso, antes de enviar algo, es importante saber **qué** vas a compartir, con **quién** vas a compartirlo y, más importante aún, **por qué** vas a compartirlo: ¿realmente es necesario compartirlo?

Sé consciente de lo que compartes

Aunque en algunos casos puedes compartir información sobre ti mismo sin problemas, es necesario tener más cuidado con la información sensible. Por ejemplo, si estás en una fiesta, seguramente no tengas problema en compartir tu nombre con alguien a quien acabas de conocer, pero es poco probable que compartas la dirección de tu casa con esa misma persona. De la misma forma, es importante tratar con prudencia tu información personal en Internet.

Algunos ejemplos de información sensible incluyen:

- **Tu nombre completo y dirección de correo electrónico:** es posible que necesites compartir esta información con personas que conoces, pero lo más sensato es no publicarla en foros o grupos públicos en Internet.

- **Fotos tuyas, o fotos de familiares y amigos:** las fotos pueden revelar más información de la que pretendías. Por ejemplo, una foto de tu familia con tu casa al fondo podría revelar dónde vives.

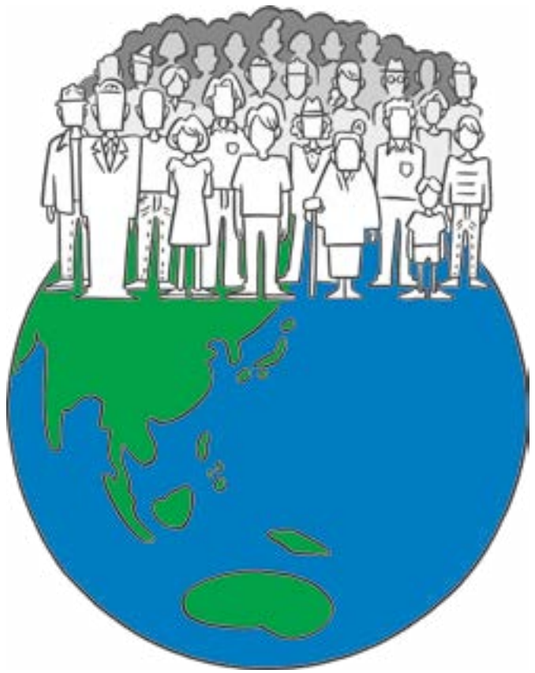
  Además, las fotos hechas con un teléfono o dispositivo móvil pueden contener las coordenadas del lugar en el que se tomaron, lo que se conoce como etiquetas geográficas. Esta información podría ser útil para recordarte dónde hiciste la foto, pero es importante eliminarla si no quieres compartirla con los demás. Comprueba los ajustes de la cámara de tu teléfono para activar o desactivar las etiquetas geográficas.

- **La información, el PIN o la contraseña de tu cuenta bancaria:** esta información es extremadamente confidencial y no la debes compartir online con los demás. Introduce esta información tan solo cuando accedas de forma directa al sitio web o la aplicación oficial de tu banca online. Para evitar posibles estafas o engaños, no hagas clic en enlaces en correos electrónicos o mensajes de texto que dicen ser de tu banco o de una empresa conocida, aun cuando parezcan legítimos. En su lugar, accede de forma directa al sitio web introduciendo la dirección web en la barra de direcciones del navegador.

Piensa con quién compartes y por qué motivo

La confidencialidad de la información que quieres compartir depende en parte de con quién piensas compartirla. Por ejemplo, tal vez quieras compartir las fotos de tu fiesta de cumpleaños solo con familiares y amigos cercanos, y escribir tu opinión sobre el restaurante donde tuvo lugar la fiesta en un sitio web de opiniones para que cualquier persona pueda leerla.
Para saber con qué público puedes compartir distintos tipos de información, es bueno conocer las opciones que te ofrecen la mayoría de redes sociales:

1. **Compartir de forma pública:**
   con esta opción, todo el mundo podrá ver lo que publicas. Por ejemplo, algunas personas comparten opiniones de películas, restaurantes y productos de forma pública para ayudar a los demás a decidir qué película ver, dónde comer o qué comprar.



2. **Compartir solo con personas específicas:**
   con esta opción, solo algunas personas podrán ver lo que publicas. Las fotos y los vídeos que tomas con tu móvil son un ejemplo de contenido que tal vez quieras compartir con personas específicas. Es importante recordar que en algunos casos las personas con las que compartes contenido pueden a su vez compartirlo con otros usuarios.

3. **Publicar de forma privada:**
   algunos sitios web o redes sociales te permiten subir contenido, como fotos o archivos, que solo tú puedes ver.

Cómo identificar y evitar estafas online

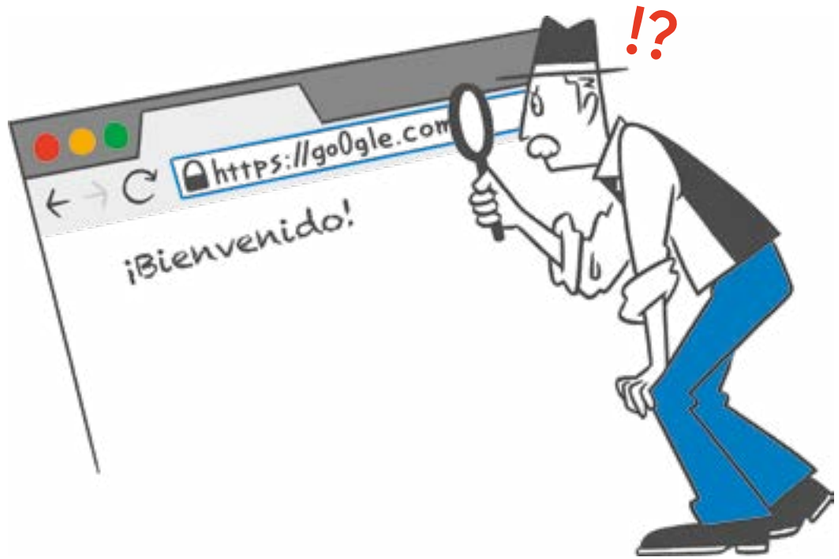
La mayoría del contenido que encuentras en la Web es bueno y puede ser útil. Sin embargo, al igual que en el mundo real, debes tener cuidado con los engaños ocasionales. Los estafadores online usan varias técnicas para engañar a los usuarios y conseguir que revelen su información personal y sus datos financieros.
A continuación te ofrecemos algunos consejos para ayudarte a evitar las estafas online.

Piénsalo dos veces antes de darle a enviar

Párate siempre a evaluar con cuidado cualquier petición que recibas online, independientemente de lo que te pida o exija el remitente. De este modo tendrás tiempo para pensar y actuar con prudencia en lugar de reaccionar.

- Piensa dos veces si realmente es necesario enviar información personal, como cuentas y contraseñas: recuerda que las empresas legítimas nunca te pedirán que compartas tus nombre de usuario y contraseña por teléfono, correo electrónico, mensaje de texto o redes sociales.

- Ten cuidado incluso cuando hagas transacciones rutinarias como consultar el saldo de tu cuenta bancaria a través de la banca online: asegúrate de que el sitio web en el que estás es el correcto. Los estafadores pueden crear sitios web similares a los auténticos para robar tu información de inicio de sesión. Para garantizar que un sitio web sea seguro y esté cifrado, comprueba que la dirección empiece con “https” y no con “http”.



Los estafadores utilizan a menudo técnicas de manipulación emocional para cogerte por sorpresa, así que sé consciente de cómo te sientes cuando recibes un correo electrónico o lees una publicación en las redes sociales solicitando información o recomendando que tomes una acción concreta, como llamar a un número de teléfono. Los estafadores intentarán que sientas:

- **Urgencia:** siempre sospecha de las ofertas especiales o precios que son demasiado bajos para ser verdad. Aunque la oportunidad sea tentadora, es importante pararse a pensar. Te recomendamos que hagas una búsqueda en Internet para ver si otras personas avisan de que la oferta es una estafa, o bien ir al sitio web real para ver si la oferta es verdadera.

- **Miedo:** algunos estafadores envían advertencias y alertas de virus falsas que afirman que han infectado tu ordenador o teléfono, o que tu información está comprometida y te piden que descargues software para arreglarlo.

  Recuerda: Un sitio web o un anuncio no pueden detectar si tu dispositivo está infectado. Descarga software y aplicaciones únicamente desde fuentes de confianza, como la tienda de aplicaciones oficial de tu teléfono móvil. También es posible que algunos estafadores te digan que tu cuenta online ha sido vulnerada y que tienes que cambiar la contraseña de inmediato para evitar daños mayores. En lugar de sentir miedo o pánico, recuerda parar y comprobar si el mensaje es legítimo. Si te preocupa, accede directamente a tu cuenta y cambia tu contraseña, pero no hagas clic en los enlaces que aparecen en correos electrónicos u otros mensajes sospechosos.

- **Enfado o entusiasmo:** algunos estafadores crean artículos con títulos sensacionalistas que generan enfado o entusiasmo con tal de conseguir más visitas a sus sitios web, donde generan ingresos a través de la publicidad. No compartas artículos u otros contenidos si crees que contienen información difícil de verificar.

- **Compasión o devoción:** es posible que algunos estafadores intenten añadirte como amigo en redes sociales. Por ello, ten siempre cuidado, sobretodo cuando la persona te declare sus sentimientos al poco tiempo de conocerte, te cuente que está pasando por un mal momento y te pida ayuda económica, o simplemente intente enviarte regalos caros.

  Recuerda: si sientes que alguien te presiona online para que actúes de manera rápida y sin pensarlo, haz siempre lo contrario, es decir, tómate tu tiempo, evalúa la situación con cuidado, y piénsalo dos veces antes de enviar información personal.

Distingue la información legítima de la sospechosa

La mayoría de personas reciben una gran cantidad de información todos los días, ya sea a través de los periódicos o la televisión, o a través de sitios web, redes sociales o mensajes instantáneos. A menudo, compartimos esa información con familiares y amigos. Pero el hecho de que algo esté en Internet no significa que sea cierto o de confianza. Para distinguir entre información legítima y sospechosa, puedes hacerte estas cuatro preguntas:

1. **¿Dónde** se ha publicado este contenido originalmente? ¿Es una fuente de confianza? Para asegurarte, puedes comprobar si el contenido aparece publicado como mínimo en 3 medios de información legítimos y de confianza.

2. **¿Quién** lo ha escrito? ¿Puedes identificar al autor? ¿Está cualificado para hablar del tema?

3. **¿Cuál** es el punto de vista del mensaje o el artículo? ¿La información se presenta de forma equilibrada? ¿El autor es totalmente imparcial?

4. **¿Cuándo** se escribió el artículo? ¿La información es relevante y actual?

Crucigrama

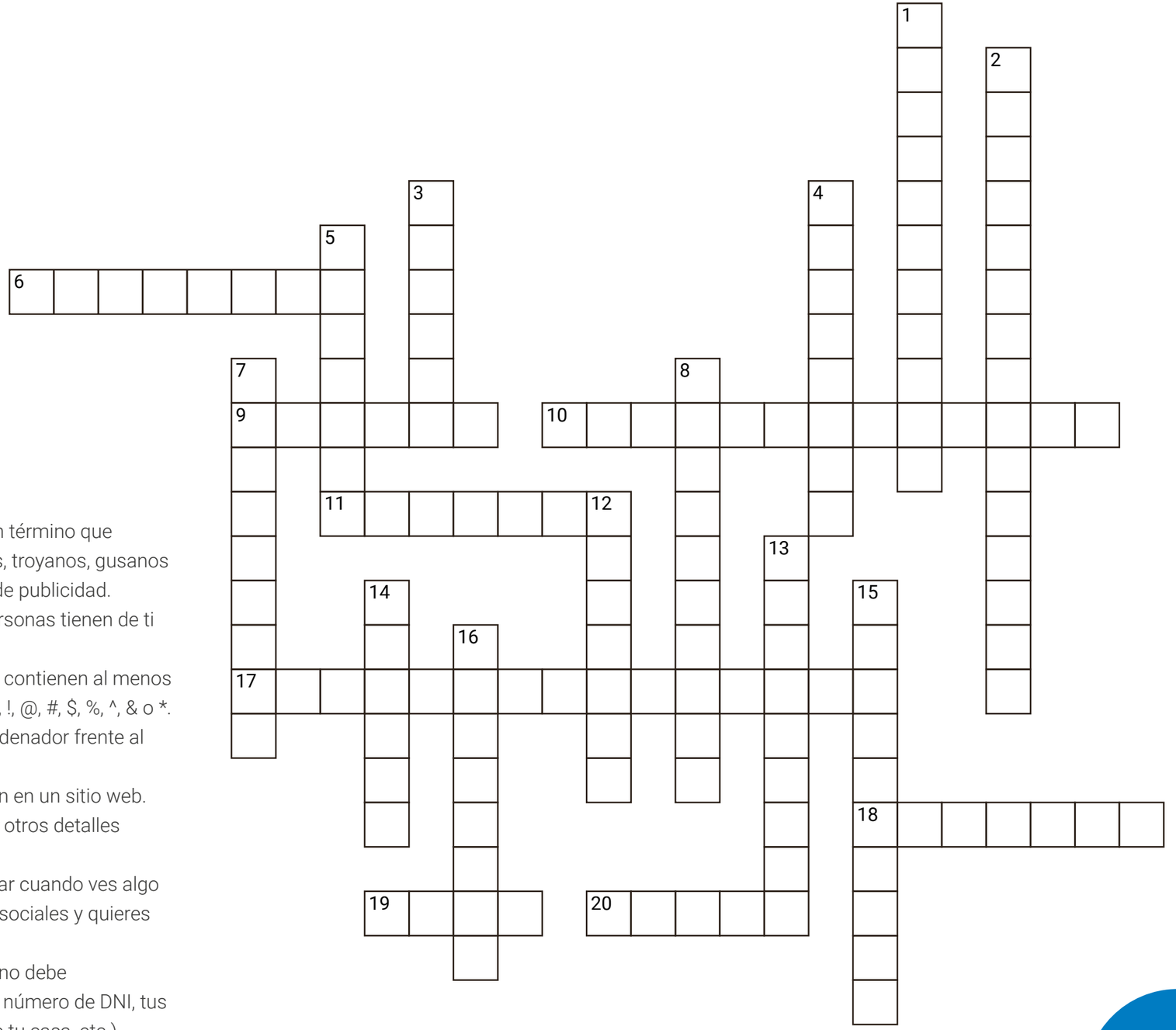
Para obtener las respuestas, consulta Términos que merece la pena conocer en la página 5.

Horizontal

6. Acción que puedes realizar para evitar la interacción con usuarios ofensivos en las redes sociales y algunos servicios de mensajería.
9. Representación gráfica que algunas personas usan en lugar de una foto real para crear un perfil en redes sociales.
10. La _____ de dos factores añade una capa de protección adicional para proteger tu cuenta al iniciar sesión.
11. Es importante configurarlos para decidir qué quieres compartir y con quién quieres compartirlo.
17. Compartir demasiada información personal.
18. Es una forma de codificación que utilizan algunos proveedores de correo electrónico y sitios web para evitar que otros fisguen tu información.
19. Correos electrónicos o mensajes no deseados o no solicitados que normalmente los estafadores envían a un gran número de usuarios
20. Cuando hagas compras online, comprueba que la dirección web empieza por ____ antes de introducir los datos de pago

Vertical

1. En esta vida es importante reutilizar y reciclar, excepto las _____. Crea una diferente para cada una de tus cuentas online.
2. Estimación de la ubicación geográfica de un teléfono móvil o un ordenador conectado a Internet.
3. Tu ____ digital es todo lo que hay en la Web sobre ti, incluidos vídeos, fotos, menciones y mucho más.
4. La ingeniería social o ____ ocurre cuando alguien intenta engañarte para que compartas información personal.
5. Información sobre uno mismo que solo puede ver su propietario.
7. El software _____ es un término que abarca virus informáticos, troyanos, gusanos informáticos y software de publicidad.
8. La percepción que las personas tienen de ti en Internet o fuera de él.
12. Las contraseñas seguras contienen al menos uno, como por ejemplo ~, !, @, #, $, %, ^, & o *.
13. Te ayuda a proteger tu ordenador frente al software malicioso.
14. Información sobre alguien en un sitio web. Incluye su foto, nombre y otros detalles personales.
15. Acción que puedes realizar cuando ves algo inapropiado en las redes sociales y quieres que lo revisen.
16. Este tipo de información no debe compartirse online (p. ej., número de DNI, tus contraseñas, dirección de tu casa, etc.)



Guía de seguridad online para personas mayores