La privacidad se puede definir como el ámbito de la vida personal que se tiene derecho a proteger de cualquier intromisión. De la misma forma que no contamos lo mismo a un extraño que a nuestros padres y amigos, nuestra información no puede ser compartida con quien sea, existen diferentes niveles de privacidad. En este nivel vas a aprender a cuidar tu privacidad en Internet, a proteger tu identidad y a ser consciente de los riesgos que corres al compartir información personal en la red. ¡Vamos a ello!

Empecemos por lo básico. Cuando quieres entrar en una página web o usar los servicios de una aplicación, suelen pedirte que te registres con un **nombre de usuario** y una **contraseña**. De esta forma, creas una cuenta, una **identidad digital** que te diferencia de otros usuarios. Pero en realidad, **cualquiera podría usar esa cuenta si tiene tu nombre de usuario y contraseña**, ¿no? Cualquier persona que tenga acceso a esa información podría hacerse pasar por ti y hacer cosas que tú no quieres en tu nombre, ¡mientras el resto de los usuarios piensan que eres tú! Por eso **es muy importante usar contraseñas complicadas y con varios tipos de caracteres**. Aquí tienes algunos consejos para crear y proteger tu contraseña:

1. **Tu contraseña tiene que ser larga**. Algunos páginas o aplicaciones que usan contraseñas también te indican su longitud mínima. Por lo general, una contraseña de **más de 14 caracteres** se considera segura.

2. Es bueno que las contraseñas sigan una **temática para ayudarte a recordarlas**, como el colegio en el que estudias, el nombre de tu mascota o un deporte que te gusta. Pero es posible que gente con malas intenciones consiga esa clase de información y la use para adivinar tu contraseña. Para hacerles el trabajo más difícil, **intenta mezclar esas cosas para crear una contraseña segura**.

   Ejemplo:
   - Nombre de mi mascota: *Peter*
   - Mi deporte favorito: *Tenis*
   - Un juego: *Brawl Stars*

   

   Resultado: *starpetertenis* (14 caracteres)

3. **Dales variedad a tus contraseñas**. Usa letras mayúsculas y minúsculas (las mayúsculas al principio de la contraseña son muy comunes, prueba a ponerlas entre medias de la contraseña), números (puedes sustituir letras por números, como la "a" por el 4, la "e" por el 3 o la "i" por el 1) e incluso caracteres especiales (#, $, %, &, €, ...).

Ejemplo:

- Contraseña de antes: *starpetertenis*
- Nueva contraseña: *$t4rP3t3rT3n1$*

4. **Es muy importante NO compartir las contraseñas con nadie**, incluso si es de confianza. Las contraseñas son las llaves para entrar en nuestras cuentas. Piensa, ¿le darías las llaves de tu casa a cualquiera? Hacerlo supondría entrar en tu casa un día y ver que te faltan cosas o que hay gente que no conoces. Así que ya sabes, no des por ahí tus contraseñas, ¡mantenlas a salvo!

5. **No uses la misma contraseña en dos páginas o aplicaciones diferentes**. Hay mucha gente que usa la misma contraseña, pero cambiando el nombre de usuario, o usa varias contraseñas y usuarios y los va intercambiando. Esto no hace más segura una cuenta, de hecho, todo lo contrario. Si consiguen averiguar al menos una de las contraseñas, pondría en peligro todas las demás cuentas que usasen la misma. ¿Conclusión? **Una cuenta, una contraseña**.

6. Llega un punto en la vida en el que has acumulado muchas cuentas y empieza a ser difícil acordarse de todos los usuarios, sus contraseñas y las respectivas páginas o aplicaciones en las que se usan. Un hombre muy sabio dejo una vez: "Solo los necios se fían de su memoria". Así que **escribe todos estos datos en un cuaderno o libreta y ponla en un lugar seguro** para que no caiga en malas manos. No lo escribas en tu ordenador ni en el móvil, no vaya a ser que lo pierdas o te lo hackeen y consigan todas tus contraseñas de golpe.

7. **Es bueno ir cambiando la contraseña de tus cuentas cada cierto tiempo**, dependiendo de si usas la cuenta a menudo o si contiene información muy preciada para ti. De esta forma, haces infinitas veces más difícil que otros consigan tu contraseña y hagan cosas con tu cuenta que no quieres. Lo único que no se te olvide cambiar la contraseña en tu cuaderno, si es que las estás apuntando.

8. Si quieres hacerle la vida imposible a cualquiera que intente conseguir tus contraseñas, puedes prepararles la siguiente sorpresa, llamada **doble factor de autenticación**. Es un nombre largo, pero básicamente es tener dos llaves para un candado con dos cerraduras distintas y que una llave la tengas tú y la otra esté escondida. Cuando tienes una cuenta protegida con el doble factor de autenticación, lo que ocurre es que, además de usar tu contraseña para acceder a la aplicación, también necesitarás un código aleatorio que cambia cada poco tiempo. Si te interesa tenerlo, hay muchas herramientas para el doble factor de autenticación (como por ejemplo Authy) y miles de vídeos en Internet que explican cómo instalarlo y ponerlo en marcha.

Ahora que ya sabes cómo crear una contraseña segura y protegerla llega el siguiente paso. ¿Cómo cuido mi privacidad? **No basta solo con proteger mis contraseñas**. Si consiguen información sobre mí, como mi deporte favorito o el nombre de mi mascota, pueden adivinar cuál es mi contraseña. Aquí te dejo más consejos para **proteger tu información**:

1. En la mayoría de las redes sociales tienes la opción de configurar la privacidad de tu cuenta para que solo las personas que tú quieras puedan ver tu contenido. **Lo más seguro es poner tu cuenta en "privado" en vez de en "público"**, ya que esto te permite saber quién puede ver tu contenido. Si por algún casual no te interesa tener tu cuenta en "privado", no te preocupes que tenemos más consejos para ti.

2. **Cuida el contenido que subes a las redes sociales, ya sean vídeos, fotos o comentarios**. Si tienes la cuenta en privado, solo las personas que tú quieras podrán ver esos vídeos y fotos que pones en tu cuenta, pero no pasa lo mismo con los comentarios. Si escribes un comentario en la publicación de otra persona, cualquiera puede verlo, incluso gente que conoces. Por tanto, es bueno **revisar bien nuestros vídeos, fotos y comentarios antes de hacerlos públicos en Internet**, no vaya a ser que publiquemos algo vergonzoso o hiriente por ser descuidados. **Una vez que se publica algo en Internet, deja de ser tuyo y pasa a ser de todos**.

3. Si te vas de vacaciones y tu familia va a dejar la casa sola, no tengas prisa en publicar en tus redes sociales que estás en la playa o en otro país y hazlo una vez hayáis vuelto. No sería la primera vez que unos ladrones ven que alguien se ha ido de vacaciones porque lo ha publicado en su cuenta y aprovechan para entrar a robar. Si aun así quieres publicar algo mientras estás de vacaciones, **no escribas en ningún lado que estás fuera de casa**.

4. Desde muy pequeños, nuestros padres nos repetían hasta la saciedad que no hablásemos con extraños. Pues aquí lo tienes otra vez, por si acaso. Si alguien que no conoces te envía un mensaje, un correo o lo que sea, **es muy probable que no sea nada bueno**. La mayoría de las veces son personas que quieren aprovecharse de ti de alguna u otra forma, ya sea para conseguir tu cuenta y repetir el proceso con tus contactos o para que “accidentalmente” pagues algo que no quieres. Por tanto, **la mejor decisión es contárselo a tus padres o a algún mayor de confianza** y que ellos te guíen en qué hacer al respecto.

Con todo esto, ya tienes las bases para cuidar tu privacidad y proteger tu información mediante contraseñas seguras, y así evitar que personas con malas intenciones te causen problemas. Para terminar, **hay un botón abajo que te lleva a un test**. De esta forma puedes demostrar los conocimientos que has aprendido y superar completamente el nivel. ¿Te ves capaz?