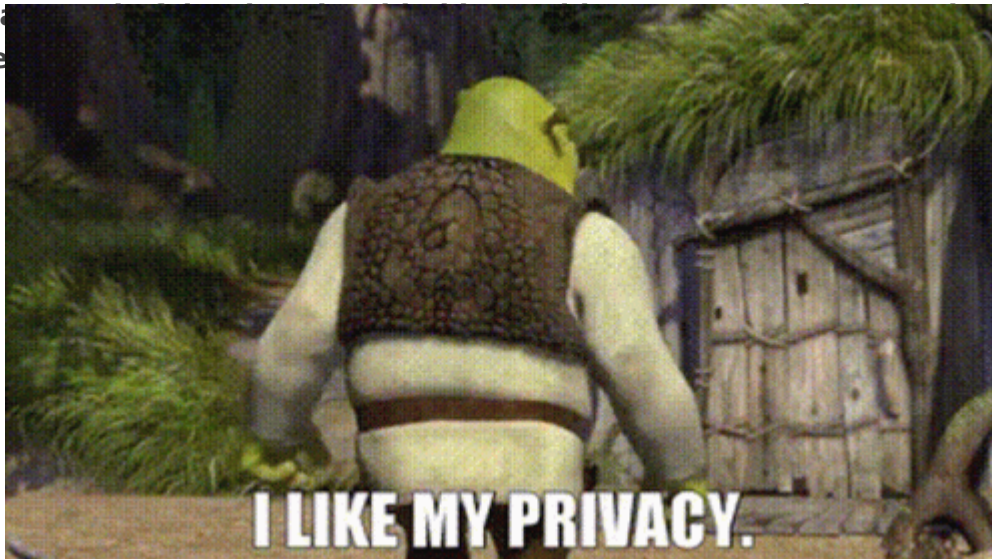


2. Transmitir la importancia de la protección de datos al alumnado

Como docentes, **debemos fomentar la conciencia entre nuestros estudiantes sobre la importancia de los datos personales y la privacidad**, especialmente en el contexto del uso de las redes sociales. Desde una edad temprana, es esencial educar a los estudiantes sobre la privacidad en línea, haciendo hincapié en que sus datos personales son valiosos y deben protegerlos. Para lograr esto, **podemos utilizar ejemplos y casos reales de situaciones en**



[Shrek I Like My Privacy GIF](#)

de mansoncarr2244 vía Tenor

Además, debemos crear un ambiente de clase en el que los estudiantes se sientan cómodos compartiendo sus inquietudes y preguntas relacionadas con la privacidad en línea. Les animaremos a hacer preguntas y expresar sus pensamientos libremente. Enseñarles **cómo configurar perfiles privados en redes sociales** para limitar quién puede ver su información personal es fundamental. También debemos abordar el tema de las **contraseñas seguras y únicas**, explicándoles cómo crearlas y gestionarlas de manera efectiva.

Otro aspecto importante es la **concienciación sobre el control de etiquetas y la información de ubicación en las publicaciones**, ya que esto puede revelar su ubicación y actividades. Los riesgos de compartir en exceso en línea deben ser discutidos para que los estudiantes comprendan los peligros que esto implica. Además, es esencial que los estudiantes conozcan sus derechos y responsabilidades en línea, incluido el respeto por la privacidad de los demás y el cumplimiento de las leyes de privacidad.

Enseñarles el **uso de herramientas de seguridad en línea**, como **bloquear usuarios, informar sobre comportamientos inapropiados y configurar notificaciones de privacidad**, es otra parte fundamental de esta educación. A través de proyectos y debates en clase, los estudiantes pueden explorar en profundidad los desafíos y las soluciones relacionados con la privacidad en línea.

Además, debemos **mantenerlos informados sobre las actualizaciones y cambios en las políticas de privacidad de las plataformas en línea que utilizan**, ayudándoles a tomar **decisiones informadas**. Finalmente, recordemos que la educación sobre la privacidad en línea es una conversación continua y debemos revisar y reforzar regularmente estos conceptos a medida que los estudiantes crecen y enfrentan nuevas situaciones en línea.

Configurar perfiles privados en diferentes redes sociales y apps

En cada título de la RRSS o de la app vas a encontrar **un hipervínculo a su configuración de seguridad**, tratando de tener un *link* actualizado. Los pasos pueden variar con las actualizaciones. Cuando quieras conocer la configuración de seguridad de una app concreta, puedes consultarla en su web o en cualquier navegador.

1. Facebook:

Inicia sesión en tu cuenta de Facebook.

Haz clic en el ícono de flecha hacia abajo en la esquina superior derecha y selecciona "Configuración y privacidad".

En el menú desplegable, selecciona "Configuración".

En la barra lateral izquierda, elige "Privacidad".

En la sección "Cómo las personas te encuentran y se ponen en contacto contigo", configura quién puede enviarte solicitudes de amistad y seguirte.

En la sección "Tu actividad", ajusta quién puede ver tus futuras publicaciones y la configuración de privacidad de tu biografía.



Haz cambios según tus preferencias y asegúrate de hacer clic en "Guardar cambios" cuando termines.

2. Instagram:

Abre la aplicación de Instagram en tu dispositivo móvil.

Toca el ícono de tu perfil en la esquina inferior derecha.

Toca las tres líneas horizontales en la esquina superior derecha para abrir el menú.

Ve a "Configuración" en la parte inferior del menú.

Toca "Privacidad" y luego selecciona "Cuenta privada" para activarla. Esto hará que tus seguidores actuales sigan viendo tu contenido, pero las personas que quieran seguirte en el futuro necesitarán tu aprobación.

3. Twitter:

Inicia sesión en tu cuenta de Twitter.

Haz clic en tu foto de perfil en la esquina superior derecha y selecciona "Configuración y privacidad".

En la barra lateral izquierda, selecciona "Privacidad y seguridad".

En la sección "Tweets" en "Protección de tus Tweets", marca la casilla "Proteger tus Tweets".

Esto hará que tus tweets sean privados, y solo tus seguidores aprobados podrán verlos.

Asegúrate de guardar los cambios.

4. LinkedIn:

Inicia sesión en tu cuenta de LinkedIn.

Haz clic en tu foto de perfil en la esquina superior derecha y selecciona "Configuración y privacidad".

En la barra lateral izquierda, selecciona "Privacidad".

En "Controles de privacidad", configura quién puede ver tus conexiones, tu actividad de red y otras preferencias según tus necesidades.

Guarda los cambios realizados.

5. TikTok



Inicia sesión en tu cuenta de TikTok si aún no lo has hecho.

Toca el ícono "Yo" en la esquina inferior derecha de la pantalla para acceder a tu perfil.

En la esquina superior derecha de tu perfil, verás un ícono con tres puntos (o tres líneas, dependiendo de la versión de la aplicación). Tócalo para abrir el menú de configuración.

Desplázate hacia abajo en el menú de configuración y selecciona "Privacidad y seguridad".

En la sección "Seguridad", verás la opción "Cuenta privada". Activa esta opción deslizando el interruptor hacia la derecha. Una vez activada, tu cuenta de TikTok será privada.

TikTok te pedirá que confirmes tu elección para configurar tu cuenta como privada. Confirma la acción.

6. Google Classroom

Inicia sesión en tu cuenta de Google Classroom.

Ve al aula que deseas configurar como privada.

En la esquina superior derecha, haz clic en el icono de configuración (engranaje).

Selecciona "Configuración del curso".

En la sección "Visibilidad del curso", elige "Solo miembros del curso".

Asegúrate de hacer clic en "Guardar" para aplicar la configuración.

7. Gmail

Inicia sesión en tu cuenta de Gmail.

En la esquina superior derecha, haz clic en tu foto de perfil.

Selecciona "Administrar tu cuenta de Google".

En la barra lateral izquierda, haz clic en "Privacidad y personalización".

En la sección "Tus datos en Gmail", verifica la configuración de privacidad, como la visibilidad del perfil y quién puede enviarte correos electrónicos.

Ajusta estas configuraciones según tus preferencias.

8. Google Drive

Inicia sesión en tu cuenta de Google Drive.

Haz clic en "Mi unidad" en la barra lateral izquierda.

Selecciona el archivo o carpeta que deseas configurar como privado.

Haz clic derecho y selecciona "Compartir".

Cambia la configuración de compartición a "Privado" o selecciona usuarios específicos con los que deseas compartir.

Asegúrate de hacer clic en "Guardar" para aplicar los cambios.

9. Genially

Inicia sesión en tu cuenta de Genially.

Abre la presentación que deseas configurar como privada.

Haz clic en el icono "Compartir" en la esquina superior derecha.

Cambia la configuración de compartición a "Privado" o selecciona usuarios específicos con los que deseas compartir.

Asegúrate de hacer clic en "Guardar" para aplicar los cambios.

10 . Canva

Inicia sesión en tu cuenta de Canva.

Abre el diseño que deseas configurar como privado.

Haz clic en "Compartir" en la esquina superior derecha.

Cambia la configuración de compartición a "Privado" o selecciona usuarios específicos con los que deseas compartir.

Asegúrate de hacer clic en "Guardar" para aplicar los cambios.

Debemos recordar que las instrucciones **pueden cambiar con el tiempo debido a las actualizaciones de las redes sociales**, por lo que es importante **consultar la configuración de privacidad actualizada** en cada plataforma para asegurarte de que tus perfiles estén protegidos de acuerdo con tus preferencias de privacidad.



Filip Filip Gonciarczyk GIF de Filip GIFs vía Tenor.com

La contraseña no puede ser "contraseña"

...aunque la Ñ no está nada mal, no todos los teclados la tienen. A continuación dejamos una serie de consejos o *tips* para crear contraseñas seguras que podemos explicar al alumnado.

1. **Longitud:** Utiliza contraseñas largas, de al menos 12 caracteres. Cuanto más larga sea la contraseña, más segura será.
2. **Combinación de caracteres:** Usa una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como !, @, #, \$, %, etc.).
3. **Evita información personal:** No uses información personal, como tu nombre, fecha de nacimiento o palabras obvias como "contraseña".
4. **No uses palabras del diccionario:** Evita palabras reales que puedan encontrarse en un diccionario. En su lugar, crea contraseñas basadas en secuencias aleatorias de letras, números y símbolos.
5. **No uses secuencias obvias:** Evita secuencias numéricas o de teclado obvias, como "123456", "asdf" o "qwerty".
6. **Contraseñas únicas:** Utiliza contraseñas diferentes para cada cuenta. No reutilices contraseñas en múltiples sitios web.
7. **Frase de contraseña:** Crea una frase de contraseña larga y fácil de recordar, luego cámbiala usando sustituciones de letras, números y símbolos.
8. **Usa un administrador de contraseñas:** Considera utilizar un administrador de contraseñas confiable para generar y almacenar contraseñas de forma segura.
9. **Cambia tus contraseñas regularmente:** Aunque no es necesario cambiarlas con demasiada frecuencia, es recomendable hacerlo periódicamente.
10. **Verificación en dos pasos:** Habilita la autenticación de dos factores (2FA) siempre que sea posible. Esto proporciona una capa adicional de seguridad.
11. **Sé consciente del phishing:** Ten cuidado con los correos electrónicos y sitios web falsos que intentan obtener tus contraseñas. Siempre verifica la fuente antes de proporcionar tus credenciales.
12. **Mantén tu software actualizado:** Asegúrate de tener actualizado tu software y sistema operativo para proteger contra vulnerabilidades conocidas.
13. **Usa una pregunta de seguridad segura:** Si se requiere una pregunta de seguridad, elige una respuesta que no sea fácilmente adivinada o que esté relacionada con información pública.

Revision #6

Created 11 September 2023 16:59:39 by Elena I. Moncayo

Updated 11 September 2023 18:37:49 by Elena I. Moncayo