Programa y materiales para educadores de personas adultas

ANEXO 6: USO SEGURO DE LAS REDES SOCIALES

Co-funded by the Erasmus+ Programme of the European Union

El apoyo de la Comisión Europea para la producción de esta publicación no constituye una aprobación del contenido, el cual refleja únicamente las opiniones de los autores, y la Comisión no se hace responsable del uso que pueda hacerse de la información contenida en la misma.

Este producto intelectual ha sido concebido y desarrollado por la Asociación Estratégica en el marco del proyecto APRICOT bajo la coordinación y responsabilidad de *Šiuolaikinių didaktikų centras*/ *Modern Didactics Centre* (LT).

Gracias a todos los socios por sus valiosas contribuciones:

Apricot Training Management Ltd. (Reino Unido)
ItF Institut Kassel e.V. – Frauencomputerschule (Alemania)
Planeta Ciencias (España)

Coordinador editorial: Daiva Penkauskienė

Autores: Hilary Hale, Beate Hedrich, Betül Sahin, Alejandra Goded, Anca Dudau, Daiva Penkauskienė

Consejo editorial: Sophy Hale, Seda Gürcan, Konrad Schmidt, Cihan Sahin, Josafat Gonzalez Rodriguez, Roc Marti Valls, Virgita Valiūnaitė

Mes/ Año: Noviembre 2021

Co-funded by the Erasmus+ Programme of the European Union

Capítulo 9: Anexos

Anexo 6: Uso seguro de las redes sociales

1. Diferentes direcciones de correo electrónico y contraseñas seguras

Si es posible, es mejor utilizar diferentes direcciones de correo electrónico para las cuentas de las diferentes redes sociales. Esto hace que sea más difícil que la información que proporcionas en las diferentes páginas sea recopilada en un perfil completo. Las cuentas de correo gratuito se pueden utilizar para las diferentes direcciones de correo electrónico. Estas cuentas deben usarse ocasionalmente para que permanezcan activadas. Al elegir un proveedor, se debe tener cuidado para asegurarse de que la dirección de correo electrónico no caduque y sea reasignada a un nuevo usuario. De lo contrario, existe el riesgo de que otro usuario se haga cargo de esta dirección de correo electrónico y así acceda a la red social asociada.

También se recomienda el uso de contraseñas diferentes y seguras para los servicios individuales como Facebook o Twitter. Cuanto más larga sea la contraseña, mejor. Debe tener al menos ocho caracteres, no debe aparecer en el diccionario y constar de letras mayúsculas y minúsculas, así como de caracteres especiales y números. Un administrador de contraseñas, como keepass.info, puede facilitar el manejo de diferentes contraseñas. Nunca pase su contraseña a terceros..

2. Dos factores de autenticación

Con los dos factores de autenticación, la seguridad se mejora aún más. Esto significa que el primer factor es una contraseña segura (conocimiento de la categoría). Como segundo factor, se utiliza un token de seguridad, es decir, un componente de hardware como una llave, una tarjeta inteligente o una memoria USB especial, para autenticación adicional (posesión de la categoría). También se puede utilizar un SMS enviado por el proveedor. Esto proporciona una protección mucho mejor para la cuenta de usuario. Para el acceso no autorizado, los terceros necesitarían ambos factores, tanto el conocimiento de la contraseña como la propiedad del dispositivo.

Co-funded by the Erasmus+ Programme of the European Union

3. Precaución al instalar aplicaciones, add-ons o plug-ins

Muchas redes sociales permiten instalar aplicaciones de terceros, como juegos. Sin embargo, los criminales online también crean dichas aplicaciones y las explotan para obtener acceso al perfil. Antes de la instalación, se debe verificar la fiabilidad del proveedor y las fuentes.

4. Precaución especial para el uso del móvil

Las redes sociales se utilizan a menudo a través de dispositivos móviles como smartphones o tablets. Los operadores o proveedores externos proporcionan aplicaciones para este propósito. Estas aplicaciones suelen utilizar datos confidenciales disponibles en el dispositivo móvil, como la agenda de contactos, fotos, vídeos o información de ubicación. Además, el dispositivo móvil suele registrarse automáticamente en la red social posteriormente. Si el dispositivo se pierde, puede ser utilizado por quien lo encontró o robó haciéndose pasar por el propietario. Por esta razón, intente no almacenar contraseñas en dispositivos móviles y, en lugar de usar la aplicación, inicie sesión y cierre sesión directamente desde el sitio web de la red social.

5. Solicitud de contacto

El robo de identidad es uno de los riesgos de la era digital. Las solicitudes de contacto deben aceptarse con precaución. Si se reciben solicitudes dudosas de conocidos, siempre verifique la fiabilidad de estos mensajes. Como cuestión de principio, solo debemos incluir a personas conocidas del mundo real en nuestra lista de contactos. Las personas desconocidas pueden tener malas intenciones. Los "amigos falsos" pueden asumir una identidad extranjera con la ayuda de cuentas falsas o robadas y usarlas para delitos o negocios ilegales online.

6. Evalúe de antemano cada clic en enlaces

Los delincuentes online utilizan las redes sociales para atraer a los usuarios a través de publicaciones o enlaces en chats hacia sitios web preparados de antemano. Estos sitios web se utilizan para acceder a datos o infectar dispositivos con malware. Un clic inocente puede provocar la instalación de un virus en tu dispositivo. Este malware puede, por ejemplo, encender la cámara del dispositivo sin que nadie se dé cuenta, grabar conversaciones a través del micrófono o consultar la ubicación. La agenda de contactos, las fotos o los videos almacenados en el dispositivo pueden caer en manos no autorizadas.

Co-funded by the Erasmus+ Programme of the European Union

7. Proteja la privacidad

Todas las redes sociales ofrecen numerosas configuraciones de privacidad. Esta configuración se puede utilizar para mostrar tu perfil y tus publicaciones solo a amigos. Debe considerarse la estrecha integración de los operadores de redes sociales con otros servicios de Internet. Esto permite crear un perfil muy completo del usuario. De vez en cuando, debes realizar una búsqueda en internet para averiguar qué información se puede encontrar sobre tu persona o los miembros de tu familia. También debes verificar regularmente la configuración de seguridad de las cuentas de redes sociales que usas y prestar atención a los enlaces a otras cuentas. Los proveedores de redes sociales pueden cambiar esta configuración por propia iniciativa.

No proporcione ninguna información personal en la red. Una vez que algo se publica en Internet, es muy difícil o imposible eliminarlo.

8. Informar sobre acoso cibernético y comentarios de odio

- Denuncia a las personas que acosan o insultan a otras al operador de la red social. Los operadores pueden investigar y eliminar perfiles dudosos.
- En el caso de delitos obvios o sospechosos, busca el consejo de la policía.
- Informa a los afectados y, si es necesario, presenta una denuncia.

9. Eliminar cuenta

Si una cuenta ya no está en uso, haz una copia de seguridad de tus datos y luego elimina la cuenta.

Lee la normativa de protección de datos y los términos y condiciones generales (AGB)

10. Derechos y responsabilidades

Las redes sociales son gestionadas por empresas con ánimo de lucro, que en su mayoría se financian con publicidad. Los términos y condiciones proporcionan información sobre cómo el proveedor maneja tus datos personales y cómo estos datos se transmiten a la industria publicitaria. Antes de crear un perfil, lee detenidamente los términos y condiciones y la normativa de protección de datos.

Algunas redes sociales se otorgan derechos de uso sobre tus publicaciones. Esto significa, por ejemplo, que los derechos de uso de fotos y videos se transfieren al operador de la red social. Además, es bastante común que los derechos de uso otorgados permanezcan incluso si el usuario ha abandonado la red y eliminado el perfil.

Co-funded by the Erasmus+ Programme of the European Union

Por tanto, hay que pensárselo dos veces antes de publicar lo que sea. También se debe tener cuidado para garantizar que los derechos de terceros no se infrinjan al publicar imágenes, textos o videos.

Las redes sociales también tienen reglas de conducta (netiqueta) que deben observarse.

La netiqueta se refiere a las reglas que la mayoría de las personas dan por sentado. Casi todos los foros y sitios web, salas de chat, etc. tienen su propia netiqueta de red. Sin embargo, las pautas son en gran medida las mismas.

- Primero leer, luego pensar, luego publicar
- Escribir textos breves
- Respetar las normativas legales
- ¿Escribir con "tú" o "ella"?
- Ser amable y tolerante
- No usar excesivamente la tecla Mayús o signos de puntuación como signos de exclamación
- No hacer ataques verbales
- ¡Tener en cuenta la ortografía!
- ¡Usar signos de puntuación!
- Decir "gracias" no hará daño a nadie.
- No spam
- No usar excesivamente de emoticonos
- No discriminar, ni usar consignas sexistas o racistas
- No publicar datos personales, números de teléfono o publicidad

En los foros a menudo se regula en la netiqueta que se utilice primero la función de búsqueda antes de hacer una pregunta. En la mayoría de los casos, esto evita que una pregunta que ya se haya formulado se vuelva a escribir una y otra vez.

Dependiendo del portal, blog, etc., la lista de reglas puede variar. Generalmente, la netiqueta también se usa en Facebook, en correos electrónicos y en otros lugares donde puede escribir sus propios textos y comentarios en la red.

11.Ataques personales y ciberacoso

Las redes sociales, los servicios de mensajería y otras aplicaciones permiten o facilitan el ciberacoso. A menudo ofrecen no solo las plataformas en las que tiene lugar el acoso o el hostigamiento, sino que también hacen que la información privada de los usuarios sea accesible al público.

Co-funded by the Erasmus+ Programme of the European Union

12. Ciberacoso

El ciberacoso consiste en insultar, amenazar, exponer o acosar deliberadamente a otras personas a través de Internet y los servicios de telefonía móvil durante un período de tiempo. El agresor busca una víctima que no puede o tiene dificultades para defenderse contra los ataques. El perpetrador utiliza este desequilibrio de poder y, por lo tanto, lleva a su víctima al aislamiento social.

El ciberacoso se produce en las redes sociales, en los portales de video y a través de los smartphones en las aplicaciones de mensajería instantánea como WhatsApp o por medio de molestas llamadas telefónicas, etc. El acosador suele actuar de forma anónima, por lo que la víctima no sabe de quién proceden los ataques. Por el contrario, en el caso de niños y jóvenes, generalmente sí conocen al acosador, que forma parte de su entorno personal "real". Por lo tanto, las víctimas casi siempre sospechan quién podría estar detrás de los ataques.

13. Diferencia entre el acoso cibernético y el acoso

El acoso cibernético difiere en algunos aspectos del acoso en el mundo real.

- El acoso cibernético no termina después de la escuela o el trabajo. Porque los ciber agresores pueden atacar a través de Internet las 24 horas del día. Puedes ser acosado incluso en tu casa.
- El nivel de acoso cibernético es mayor que el acoso en el mundo real porque
    - la audiencia es inmensamente grande
    - El contenido se propaga extremadamente rápido
    - Los contenidos que se han olvidado durante mucho tiempo siempre pueden volver a publicarse
- Los acosadores pueden actuar de forma anónima:

El agresor no se muestra directamente a su víctima. No saber quiénes son los perpetradores puede asustar y perturbar a la víctima.

- La víctima no se ve afectada directamente:
  El agresor no ve las reacciones de la víctima a una declaración hiriente o una imagen irrespetuosa y, por tanto,no es consciente del alcance de sus ataques.

Co-funded by the Erasmus+ Programme of the European Union

14. Facetas del acoso

El acoso tiene diferentes facetas:

- **Chicane**: enviar mensajes ofensivos e hirientes repetidamente por correo electrónico, SMS, mensajería instantánea o en chats.
- **Calumniar:** Difundir rumores a través de Internet y los servicios de telefonía móvil a un gran grupo de personas.
- **Exponer:** La información que originalmente se puso a disposición de una persona de forma confidencial se envía a otros para comprometer a la víctima.
- **Excluir / Ignorar**: Exclusión deliberada de actividades sociales, grupos, charlas, etc.

15. Influencia del ciberacoso en la cultura web

Internet está provocando cambios masivos en la forma en que las personas se comunican entre sí. Por un lado, es positivo que siempre nos podamos contactar sin problemas o comprobar rápidamente lo que ha escrito un amigo. O qué foto se acaba de publicar. Por otro lado, sin embargo, también se pueden observar tendencias negativas en esta nueva "cultura de la comunicación online".

16. Ritmo de vida acelerado

La velocidad de transmisión de Internet se ha vuelto más rápida y el Internet móvil también mejora constantemente su rendimiento. La información llega al usuario en intervalos cada vez más cortos. Sin embargo, los usuarios también se han adaptado a esto. La comunicación es cada vez más rápida e inquieta. Un día sin conexión implica que al día siguiente habrá varios mensajes de amigos, conocidos o colegas en el ordenador o en el smartphone.

Sin embargo, esta velocidad también lleva a que las publicaciones, imágenes o videos se compartan y envíen de manera espontánea. No solo los contenidos positivos, sino también instantáneas o comentarios despectivos que son desfavorables para una persona. Esta información se difunde muy rápidamente a través de varios servicios a un grupo incontrolable de personas.

Co-funded by the Erasmus+ Programme of the European Union

17. Anonimato y distancia

El anonimato favorece una comunicación online desinhibida. Cualquiera que navegue de forma anónima en Internet difícilmente debe esperar consecuencias negativas por sus acciones. Además, la reacción directa de la otra parte no se puede ver a través de la comunicación online, excepto en un chat de video. Por lo tanto, el usuario a menudo no puede evaluar cómo reciben otros usuarios sus declaraciones porque no puede ver cómo reacciona la otra persona en sus expresiones faciales y gestos. Dado que uno no se encuentra cara a cara con la otra persona, es fácil herir los sentimientos de otros en internet.

18. Intercambio excesivo de información personal

Las redes sociales y muchos servicios, como WhatsApp, Twitter, Instagram, etc., viven del hecho de que los usuarios comparten muchas cosas con los demás. Los niños y adolescentes se ven tentados fácilmente a revelar mucho sobre sí mismos, porque quieren probar cómo llegar a sus compañeros. Sin embargo, los comentarios de otros sobre las fotos, videos y otras contribuciones publicadas no siempre son positivos y el usuario se ve desacreditado y acosado por su autodescripción ante los demás.

19.Amigos versus conocidos

Usando las redes sociales y la mensajería instantánea, es muy fácil encontrar nuevos conocidos de forma rápida y sencilla. Estos se agregan inmediatamente en Facebook, WhatsApp y demás redes. Con el tiempo, se acumulan más y más contactos, provenientes de una amplia variedad de contextos. Cada vez es más difícil ver de un vistazo toda la lista. Pero es importante saber quién puede leer las publicaciones y ver las fotos, porque no todo es apto para todos los contactos.

Muchas redes sociales ofrecen a los usuarios la opción de ordenar sus contactos en diferentes grupos. Las publicaciones que sube el usuario se pueden compartir específicamente para los grupos individuales (amigos, conocidos, etc.). De esta forma, se pueden evitar reacciones desagradables de extraños a las publicaciones personales.

Co-funded by the Erasmus+ Programme of the European Union

20. Consejos para los padres

¿Cómo pueden saber los padres que su hijo está siendo acosado?

El ciberacoso se puede detectar y combatir en sus primeras etapas. Si nota que el niño cambia repentinamente de comportamiento, la ayuda es necesaria. Los signos que puede observar en el niño:

- se comporta con contención,
- pierde el deseo de comunicarse,
- ha cambiado drásticamente el uso de internet,
- se aísla del mundo exterior,
- reacciona con agresividad,
- tiene muchas excusas o molestias físicas inexplicables,
- su apariencia se orienta hacia modelos e ideales de belleza
- minimiza su propia situación.

Si se presentan estos síntomas, los padres deben hablar con su hijo de inmediato, porque los inicios del ciberacoso deben abordarse con urgencia para evitar daños. Si el niño ya está siendo acosado masivamente, siempre es recomendable consultar a un experto. Puede encontrar ayuda online en Bündnis gegen Cybermobbing eV - Mobbing Internet / Netz ((https://www.buendnis-gegen-cybermobbing.de) y en Klicksafe

(https://www.klicksafe.de/themen/kommunizieren/cyber- mobbing).

Co-funded by the Erasmus+ Programme of the European Union

21. ¿Cómo pueden los padres ayudar a sus hijos?

Es importante acercarse activamente a las víctimas de acoso, hablar sobre sus problemas y brindar apoyo emocional. Sin embargo, los padres también deben buscar el consejo y la opinión de un experto. Por ejemplo, la línea directa de asesoramiento telefónica gratuita. Se puede acceder a esta línea directa de forma anónima las 24 horas del día y cuenta con personas de contacto debidamente capacitadas. También es importante afrontar los problemas del niño y actuar abiertamente. Uno debe estar abierto a hablar con familiares y amigos y a discutir y tomar medidas adicionales conjuntamente.

22. ¿Cómo puedes protegerte del ciberacoso?

No hay garantía de que no una se convierta en víctima de ciberacoso. Se pueden utilizar métodos simples pero efectivos para reducir el peligro. Como siempre, lo mismo que hemos visto anteriormente se aplica aquí:

- nunca reveles demasiado de tu vida privada en Internet,
- controla de cerca la configuración de privacidad y las listas de amigos,
- piensa en con quién o qué haces en Internet,
- nunca hables públicamente sobre preocupaciones y problemas en Internet,

Una vez más, "¡el conocimiento es poder!"

Los padres deben sensibilizar a sus hijos sobre cómo manejar el acoso cibernético hablando abiertamente con ellos sobre el acoso e informándoles sobre las diferentes variantes. Un punto muy importante es que los padres den a sus hijos la seguridad de saber que siempre pueden hablar con ellos.

Co-funded by the Erasmus+ Programme of the European Union