Ficha de formación de E-Seniors

|  |  |
| --- | --- |
| **Title** | **Tema: Información y comunicación en las redes sociales**  **Unidad 3. Amenazas y desafíos en las redes sociales: qué hacer y qué no** |
| **Área de formación** | *Selecciona por favor una de las siguientes:*   |  |  | | --- | --- | | Seguridad *online* |  | | Alfabetización cultural y medática | *X* | | Transacciones económicas |  | | Protección de los datos personales |  | | Identidad digital y reputación *online* |  | |
| **Palabras clave (*tags)*** | **Redes sociales, comunicación, seguridad** |
| **Proporcionado por** | **E-Seniors** |
| **Idioma** | **Español** |
| **Metas/Objetivos de aprendizaje** | |
| Este módulo tiene como objetivo desarrollar los conocimientos y habilidades de los usuarios sobre cómo utilizar las redes sociales para la comunicación y la promoción de la cultura y la creatividad. Los usuarios mayores se familiarizarán con las herramientas de las redes sociales, recursos culturales en las redes sociales que les permitirán usarlas fácilmente y descubrir oportunidades culturales y de comunicación. | |
| **Descripción** | |
| El curso está organizado en 3 niveles: cada módulo se divide en unidades cuyos títulos dan una idea más detallada sobre el contenido del módulo. Este módulo en particular se organiza de la siguiente manera:  **Tema: Información y comunicación en las redes sociales.**  **Módulo 3. Amenazas y desafíos en las redes sociales: que hacer y qué no**  **Unidad 3.1:** Amenazas y desafíos  **Unidad 3.2:** 10 buenas prácticas que adoptar para la seguridad en las redes sociales  Buenas prácticas que adoptar para la seguridad en las redes sociales. | |
| **Contenidos divididos en 3 niveles** | |
| **Módulo 3: Amenazas y desafíos en las redes sociales: que hacer y qué no**  Hay muchas amenazas y desafíos involucrados en la navegación por Internet, tanto en el ordenador como en el teléfono. Las redes sociales no son una excepción. Hay diversos riesgos involucrados en el uso de las redes sociales. Sin embargo, si se toman precauciones, no es difícil usarlas con un riesgo mínimo.  **Unidad 3.1:** Amenazas y desafíos   * ***Phishing*:** El *phishing* es un tipo de ingeniería social en el que un atacante envía un mensaje fraudulento diseñado para engañar a una víctima humana. Estos mensajes están diseñados para engañarla y que revele información personal haciéndose pasar por una fuente de confianza. Los mensajes pueden provenir de personas que afirman ser amigos suyos o de una empresa conocida. Nunca compartas información confidencial y nunca hagas clic en un enlace que parezca sospechoso. * ***Hackeo* psicológico:** El *hackeo* psicológico es el proceso de obtener información confidencial de una persona a través del engaño. El estafador puede iniciar una conversación sobre cosas que lee en tu perfil, como dónde trabajas, etc. Luego intenta que reveles información personal, similar al *phishing*. * ***Malware*:** El *malware* es un *software* malicioso diseñado para infiltrarse en los dispositivos. Circula por las redes sociales en forma de enlaces con títulos pegadizos. Una vez que se infiltra el malware, puede enviar mensajes a los contactos, acceder a información personal o dañar el dispositivo. Se debe tener precaución cuando nos tiente clicar un enlace de una fuente desconocida. * **Discurso de odio:** El discurso de odio es común en las redes sociales porque sus autores pueden permanecer en el anonimato. Puede ocurrir que recibas discursos de odio, a veces sin ninguna red social, por lo que es importante apartarte de él y no dudar en denunciarlo como contenido no deseado y malicioso. * **Ciberacoso:** es el acoso que tiene lugar a través de dispositivos digitales como teléfonos, ordenadores y *tablets*. El ciberacoso puede ocurrir a través de mensajes de texto y aplicaciones, u *online* en las redes sociales, foros o juegos donde las personas pueden ver, participar o compartir contenido. El ciberacoso incluye enviar, publicar o compartir contenido negativo, dañino, falso o cruel sobre otra persona. Puede incluir compartir información personal o privada sobre otra persona que cause vergüenza o humillación. Parte del ciberacoso cruza la línea y se convierte en comportamiento ilegal o delictivo. * **Edadismo**: La discriminación por edad se refiere a los estereotipos (cómo pensamos), los prejuicios (cómo nos sentimos) y la discriminación (cómo actuamos) hacia los demás o hacia uno mismo en función de la edad. La discriminación por edad afecta a todos. Los niños de tan solo 4 años se vuelven conscientes de los estereotipos de edad de su cultura. A partir de esa edad interiorizan y utilizan estos estereotipos para orientar sus sentimientos y conductas hacia personas de diferentes edades. También recurren a los estereotipos de edad de la cultura para percibirse y comprenderse a sí mismos, lo que puede resultar en edadismo autodirigido a cualquier edad. La discriminación por edad intersecta y exacerba otras formas de desventaja, incluidas las relacionadas con el sexo, la raza y la discapacidad. * **Qué tener en cuenta para evitar estafas en Facebook**   + Gente que no conozcas en persona pidiéndote dinero o tus datos del banco.   + Páginas sin verificar que digan representar a una gran organización o figura pública.   + Gente que te pida continuar vuestra conversación fuera de Facebook, en un lugar menos público o seguro, como una dirección de correo electrónico aparte.   + Gente que te pida enviarles tus datos del banco para recibir una recompensa o regalo.   + Cualquiera que diga ser un amigo o familiar en apuros.   + Gente que mienta sobre dónde vive   + Publicaciones que contengan errores de puntuación u ortográficos.   + Gente o cuentas que te redirijan a una página para reclamar un premio   **Unidad 3.2: 10 buenas prácticas que adoptar para la seguridad en las redes sociales:**  1- **Proteger el acceso a tus cuentas:** Usa contraseñas fuertes que sean diferentes de una cuenta a la otra. Las aplicaciones para la gestión de contraseñas pueden ayudarte a guardarlas de manera sencilla. Por ejemplo, tenemos **https://keepassxc.org/**  2- **Comproueba tus ajustes de privacidad**: Por defecto, los ajustes de privacidad están a menudo abiertos default, (en campos de información personal como el nombre, número de teléfono y correo electrónico). Todos los subscriptores de la red social pueden acceder a estos datos. Es posible limitar su visibilidad ajustando la configuración de cuenta para tener cierto control sobre lo que los otros usuarios ven.  3- **Controla tus publicaciones:** Tus publicaciones se pueden ir de las manos y ser republicadas o interpretadas más de lo que pretendes. No publiques información personal o delicada.  4- **Cuidado con quién hablas:** Tus amigos pueden estar compartiendo contenido malicioso sin saberlo o estar hackeados. Nunca envíes dinero sin verificar la identidad de la persona, no envíes vídeos privados, sé desconfiado con los concursos, ganancias inesperadas o “grandes ofertas” que puedan esconder estafas.  5-  **Controla las aplicaciones de terceros:** Algunas aplicaciones ofrecen interactuar con algunas de tus redes sociales. Requieren permisos que necesitan un examen cuidadoso, ya que algunos de ellos pueden acceder así a tus datos. Ten cuidado de no instalar aplicaciones que sospeches que son maliciosas.  6- **Evita los ordenadores y redes públicas:** Usar un ordenador o red wifi públicos es arriesgado ya que pueden estar comprometidos o bajo control de cibercriminales. Evita introducir información delicada o usarlos si es posible.  7- **Comprueba tus entradas a la cuenta regularmente:** La mayoría de redes sociales te permiten ver las conexiones o sesiones abiertas de tu cuenta. Comprueba esta información regularmente para asegurarte de que otro dispositivo no esté conectada a alguna de tus cuentas. Si lo estuviera, desconéctalo y cambia tu contraseña.  8- **Cuidado con las noticias falsas:** Parte de la información publicada puede ser falsa, deliberadamente o no. Antes de tomar en cuenta o compartir alguna información, comprueba su autenticidad.  9- **Comprueba tus credenciales con tus cuentas:** Algunas páginas te ofrecen registrarte con tu cuenta de redes sociales. Esto evita la necesidad de crearse una contraseña, pero puede proveer de datos personales a la página o permitir a un cibercriminal que hackee tu cuenta en esa red social acceder a tu cuenta en la página también.  10- **Borra tu cuenta si ya no la usas:** Para evitar los riesgos descritos arriba, para asegurarte de que tu cuenta no se usa sin tú saberlo, borra tu cuenta cuando ya no la necesites. | |
| **Contenidos por puntos** | |
| * Las amenazas y desafíos más frecuentes al usar las redes sociales son defenderte del *phishing, malware*, discurso de odio, etc... * Puedes evitar las amenazas y riesgos en las redes sociales al seguir las recomendaciones y consejos estipulados en este módulo | |
| **Entradas del glosario** | |
| **Seguridad en las redes sociales:** se refiere a todas las medidas que el usuario debería tomar para evitar riesgos, estafas y ataques a su cuenta personal.  **Discurso de odio:** se compone de palabras habladas que son ofensivas y/o amenazantes para una persona o grupo y que se basan en un atributo de dicha persona o grupo a la que se dirigen.  **Hackeo psicológico:** es el proceso de obtener información confidencial sobre una persona con métodos poco éticos.  **Ciberacoso:** acoso efectuado en dispositivos digitales como los móviles, ordenadores y *tablets.*  **Edadismo**: se refiere a los estereotipos (cómo pensamos), prejuicios (como nos sentimos) y discriminación (cómo actuamos) hacia otros o nosotros mismos basándonos en la edad, afectando a todos. | |
| **Bibliografía y referencias adicionales** | |
| [**https://understandthesocialmedia.com/**](https://understandthesocialmedia.com/)  [**https://wtccentralpa.org/wp-content/uploads/2013/01/socialmedia-2.pdf**](https://wtccentralpa.org/wp-content/uploads/2013/01/socialmedia-2.pdf) | |
| **Test de autoevaluación** | **1) Usar los ordenadores públicos es seguro**   1. **Verdadero** 2. **Falso**   **Correcta: B**  **2) ¿Qué es el *malware*?**   1. ***Software* diseñado para infiltrarse en los dispositivos** 2. **Fraude de identidad** 3. **Discurso de odio**   **Correcta: A**  **3) ¿Qué es el discurso de odio?**   1. **El discurso de odio se compone de palabras habladas que son ofensivas y/o amenazantes para una persona o grupo y que se basan en un atributo de dicha persona o grupo a la que se dirigen.** 2. **El discurso de odio es el proceso de obtener información confidencial sobre una persona con métodos poco éticos.** 3. **El discurso de odio es información maliciosa diseñada para infiltrarse en los dispositivos y atacar a las personas**   **Correcta: A**  **4) La Seguridad en las redes sociales:**   1. **Se refiere a todas las medidas que las empresas usan para defenderse de los fraudes *online*** 2. **Se refiere a todas las medidas que el usuario debería tomar para evitar riesgos, estafas y ataques a su cuenta personal.** 3. **Se refiere a las herramientas diseñadas por la red social diseñadas para los usuarios.**   **Correcta: B**  **5) ¿Que hacer si te encuentras con el discurso de odio *online?***   1. **Intentar evitar a los atacantes** 2. **Intentar reportar a los atacantes** 3. **Todas son correctas**   **Correcta: C** |
| **Material Relacionado** | **Cómo identificar y evitar las estafas en las redes más comunes:** [**https://www.onpointcu.com/blog/how-to-identify-and-avoid-common-social-media-scams/**](https://www.onpointcu.com/blog/how-to-identify-and-avoid-common-social-media-scams/)  **Cómo evitar el fraude en las redes:** [**https://www.nbc.ca/personal/advice/security/social-medias-fraud-scams.html**](https://www.nbc.ca/personal/advice/security/social-medias-fraud-scams.html)  **Ciberacoso y discurso de odio:** [**https://www.ditchthelabel.org/wp-content/uploads/2020/05/Cyberbullying-and-hate-speech.pdf**](https://www.ditchthelabel.org/wp-content/uploads/2020/05/Cyberbullying-and-hate-speech.pdf) |
| **PPT relacionado** |  |
| **Enlace de referencia** | **https://www.stopbullying.gov/cyberbullying/what-is-it** |
| **Vídeo de YouTube** | **¿Qué son las redes? En inglés simple**  [**https://www.youtube.com/watch?v=jQ8J3IHhn8A**](https://www.youtube.com/watch?v=jQ8J3IHhn8A)  **Un lector de mentes increíble revela su “don”:** [**https://www.youtube.com/watch?v=F7pYHN9iC9I**](https://www.youtube.com/watch?v=F7pYHN9iC9I) |