Training Fiche IWS

|  |  |
| --- | --- |
| **Título** | **Identidad digital y reputación online** |
| **Área de formación** | *Por favor, selecciona una o más de las siguientes opciones:*   |  |  | | --- | --- | | Seguridad Online |  | | Alfabetización cultural y mediática |  | | Transacciones económicas |  | | Protección de los datos personales |  | | Identidad digital y reputación online | *X* | |
| **Palabras clave (meta tag)** | **Identidad digital, reputación online, internet, fraudes, online, estafas, redes sociales** |
| **Proporcionado por** | **Internet Web Solutions** |
| **Idioma** | **Español** |
| **Objetivos / metas / resultados de aprendizaje** | |
| **Al final de este módulo, serás capaz de:**  **Conocer lo que deberías de saber sobre tu identidad digital y la reputación online.**  **La unidad se centrará en:**  **Unidad 3.1. El doctor Jekyll y el Señor Hyde (Quién eres y quiénes son los otros en internet y cómo protegerlo)**  **Sección 3.1.1 Introducción**  **Sección 3.1.2. Robo de identidad: ¿qué pasa si roban tu identidad?**  **Sección 3.2.3. Robo de cuenta: ¿qué pasa si utilizan tu cuenta? Algunos consejos para evitarlo.**  **Sección 3.2.4. Más consejos** | |
| **Descripción** | |
| Esta unidad proporcionará “lo que hacer y lo que no”, como por ejemplo “No utilices los ordenadores públicos”, “Establece una contraseña fuerte y compleja”, asegúrate que estás utilizando una conexión segura”, doble factor de identificación, etc. para proteger tu identidad digital. Esta unidad hablará también de maneras seguras de utilizar las redes sociales y de no revelar en línea. | |
| **Contenidos organizados en 3 niveles:** | |
| **Unidad 3.1 El doctor Jekyll y el Señor Hyde (Quién eres y quiénes son los otros en internet y cómo protegerlo)**  **Sección 3.1.1 Introducción**  En internet eres todo lo que subes y todo lo que comentes a otros usuarios.  Todo lo que subes online puede ser visto por los otros usuarios.  Incluso si puedes configurar los ajustes de privacidad eligiendo que sean visibles “solo a los amigos” y similares, una persona que quiere ver tus posts tiene maneras de hacerlo.  Que la gente no pueda verte, no significa que puedes actuar de manera diferente, sólo porque estás detrás de una pantalla.  A diferencia de la vida real, todo lo que subes en internet tiene exposición mundial.  Eso significa que la gente de todo el mundo puede saber de ti, y así mismo, tú puedes saber de la gente de todo el mundo.  Un estafador puede buscar mucha más gente y elegir su víctima más cuidadosamente. Este y otros factores, hacen que las estafas online sean mucho más comunes.  **Sección 3.1.2. Robo de identidad: ¿qué pasa si roban tu identidad?**  Una persona que accede ilegalmente a tu cuenta, puede poner en marcha muchas acciones maliciosas.  En el mejor de los casos, ellos pueden hacerse pasar por ti para crear posts comprometedores o ilegales.  En el peor de los casos, ellos pueden hacerse pasar por ti y hablar con tus conocidos o con tu familia, diciéndoles que tienes un problema y necesitas dinero, así les estafan. El robo de identidad no te afecta solo a ti.  Otro caso grave es si alguien tiene acceso a tus datos bancarios, ellos pueden comprar online o hacer unas transacciones y robarte el dinero.  Si eso pasa, trata de hablar con el soporte de la plataforma, donde tu cuenta ha sido robada, cambia la contraseña, notifícalo a las personas afectadas, y si el ladrón ha sido capaz de hacer una compra, notifícalo también a tu banco.  ¡El robo de identidad no solo te afecta a ti!  **Sección 3.2.3 Robo de cuenta: ¿qué pasa si utilizan tu cuenta? Algunos consejos para evitarlo.**  Otro caso grave es si alguien tiene acceso a tus datos bancarios, ellos pueden comprar online o hacer transacciones y robarte el dinero.  Si eso pasa, trata de hablar con el soporte de la plataforma, donde tu cuenta ha sido robada, cambia la contraseña, notifícalo a las personas afectadas, y si el ladrón ha sido capaz de hacer una compra, notifícalo también a tu banco.  Hay unas cuantas cosas que puedes hacer para evitar el robo de la cuenta:  - No guardes las contraseñas en ningún dispositivo, trata de recordarlas.  - Trata de utilizar contraseñas diferentes para diferentes páginas web. Si alguien descubre tu contraseña de una plataforma, ellos no serán capaces de acceder a otras páginas.  - No utilices tu nombre, nombre de usuario u otras informaciones personales en la plataforma porque hacen más fácil que las descubran.  - Utiliza contraseñas más largas de 8 caracteres, y usa un número o un carácter especial para evitar ataques de fuerza bruta para descubrir tu contraseña.  Nunca compartas tu contraseña online, incluso si una persona te dice que es un asesor, administrador o personal de soporte de la página web.  **Sección 3.2.4. Más consejos**  De hecho, también debes tener más cuidado sobre lo que publiques en las redes sociales.  Trata de publicar menos informaciones posibles sobre de ti, sobre todo datos sensibles, datos identificativos o datos bancarios.  Informaciones importantes que NO deberías compartir públicamente son:  - el sitio donde vives  - el correo electrónico  - el número de teléfono  - contenidos multimediales comprometedores  - documentos personales  - informaciones sobre tus transacciones bancarias  - información sobre el sueldo  - contraseñas de cualquier tipo  Robo de cuenta y de identidad  Evita acceder a tus cuentas por los ordenadores de otras personas, sobre todo por ordenadores públicos.  Muchas plataformas utilizan la autenticación en dos pasos, por ejemplo, utilizando el número de teléfono, utilizándolo cuando tengas la oportunidad.  Lo que pasa online, siempre se queda online. Lo que subes, lo que dices, cómo actúas, será disponible para todo el mundo, incluso para: posibles empleados futuros, tu familia, tus hijos y tus amigos. Y no solo ahora, sino también en futuro. | |
| **Contenidos en puntos clave** | |
| * **Trata de publicar menos informaciones posibles sobre de ti, sobre todo datos sensibles, datos identificativos o datos bancarios.** * **Lo que pasa online, siempre se queda online. Lo que subes, lo que dices, cómo actúas, será disponible para todo el mundo, incluso para: posibles empleados futuros, tu familia, tus hijos y tus amigos. Y no solo ahora, sino también en futuro.** * **Utiliza contraseñas más largas de 8 caracteres, y usa un número o un carácter especial para evitar ataques de fuerza bruta para descubrir tu contraseña** | |
| **5 entradas del glosario** | |
| **Identidad digital:**  *Hoy en día, la identidad digital se utiliza a menudo para adquirir los datos personales almacenados en los sistemas informáticos, para estar vinculado a las identidades civiles o nacionales.*  **Reputación online:**  *Es la reputación de una empresa, persona, producto, servicio o cualquier otro elemento en internet o en las plataformas digitales.*  **Autenticación en dos pasos:**  *Es un método de autenticación electrónica, en el cual un usuario tiene acceso a una página web o a una aplicación, solo después de presentar con éxito dos o más evidencias (o factores) a un mecanismo de autenticación.*  **Robo de identidad:**  *La práctica fraudulente de utilizar otro nombre de persona e información personal para obtener crédito, prestito, etc.*  **Estafador:**  *Un estafador puede documentarse sobre muchas más personas y elegir su víctima más cuidadosamente. Este y otros factores hacen que las estafas online sean cada vez más comunes.* | |
| **Bibliografía y otras referencias** | |
| [**https://www.careercast.com/career-news/10-ways-build-your-online-identity**](https://www.careercast.com/career-news/10-ways-build-your-online-identity)  [**https://www.emtwodigital.com/5-tips-for-building-a-commanding-online-identity/**](https://www.emtwodigital.com/5-tips-for-building-a-commanding-online-identity/)  [**https://www.interviewsuccessformula.com/job-search-advice/easy-tips-on-how-to-build-your-online-identity.php**](https://www.interviewsuccessformula.com/job-search-advice/easy-tips-on-how-to-build-your-online-identity.php)  [**https://www.lifelock.com/learn-identity-theft-resources-whats-your-digital-identity.html**](https://www.lifelock.com/learn-identity-theft-resources-whats-your-digital-identity.html)  [**https://whatis.techtarget.com/definition/digital-identity**](https://whatis.techtarget.com/definition/digital-identity)  [**https://businesscollective.com/8-ways-to-use-social-media-for-good/index.html**](https://businesscollective.com/8-ways-to-use-social-media-for-good/index.html)  [**https://www.techopedia.com/definition/23915/digital-identity**](https://www.techopedia.com/definition/23915/digital-identity)  [**https://www.techopedia.com/definition/1327/domain-name**](https://www.techopedia.com/definition/1327/domain-name) | |
| **5 preguntas de autoevaluación de opción múltiple** | 1. En internet   A. Sólo las personas que te conocen pueden encontrarte  B. Sólo los estafadores pueden encontrarte  C. Las personas de todo el mundo pueden encontrarte  **Correcta: C**  2) ¿Qué puede hacer un robo de identidad?  A. Un robo de identidad accede solo a tus datos bancarios  B. Un robo de identidad llega a tu casa y roba tu portátil  C. Un robo de identidad accede a tu cuenta y pone en marcha acciones maliciosas  **Correcta: C**  3) ¿Cuáles son las informaciones personales que recomendamos no publicar en internet?  A. Tu talla de zapatos  B. Tu número de teléfono  C. Tu perfil de Facebook  **Correcta: B**  **4**) Contraseña y seguridad. ¿Cuál de las siguientes afirmaciones es cierta?  A. Es mejor no guardar la contraseña en ningún dispositivo  B. Utiliza una contraseña más corta de 8 caracteres  C. Utiliza tu número de teléfono como contraseña  **Correcta: A**  5) ¿Por qué es tan importante evitar acceder a tu cuenta por el ordenador de otras personas?  A. Porque es descortés.  B. Para proteger tu contraseña.  C. Para proteger tu identidad digital.  **Correcta: C** |
|  |  |
| **Material relacionado** | [**SOS creativity Module 3 Digital Identity and Online Reputation**](PPTs/SOS%20creativity%20Module%203%20Digital%20Identity%20and%20Online%20Reputation.pptx) |
| **PPT relacionado** |  |
| **Enlace de referencia** |  |