Training Fiche IWS

|  |  |
| --- | --- |
| **Título** | **Seguridad online y creatividad: ¿qué pasa?** |
| **Área de formación** | *Por favor, selecciona una o más de las siguientes opciones:*   |  |  | | --- | --- | | Seguridad Online | *X* | | Alfabetización cultural y mediática | *X* | | Transacciones económicas |  | | Protección de los datos personales |  | | Identidad digital y reputación online |  | |
| **Palabras clave (meta tag)** | **Estafas, fraudes, consejos de seguridad online, internet** |
| **Proporcionado por** | **Internet Web Solutions** |
| **Idioma** | **Español** |
| **Objetivos / metas / resultados de aprendizaje** | |
| **Al final de este módulo, serás consciente de la seguridad online en el mundo digital multicultural. Esta unidad se centrará en:**  **Unidad 2.1 Las estafas online más comunes: ejemplos de las estafas online más comunes, proteger** **tu información online.**   * **Sección 2.1.1. Introducción** * **Sección 2.1.2. Ofertas de trabajo** * **Sección 2.1.3. Estafa bancaria** * **Sección 2.1.4. Compra online** * **Sección 2.1.5. Productos de terceros** * **Sección 2.1.6. Herencia por WhatsApp** * **Sección 2.1.7. SMS estafadores de tu banco** * **Sección 2.1.8. Estafa de lotería** * **Sección 2.1.9. Falsas organizaciones benéficas**   **Unidad 2.2. Seguridad online en el mundo cultural, cómo evitar estafas concretas del mundo cultural (entradas falsas, hackeo o phishing)**   * **Sección 2.2.1 Cómo actúan los estafadores** * **Sección 2.2.2. Pasos para protegerte** * **Unidad 2.3. Consejos de seguridad online** * **Sección 2.3.1. Cómo establecer una contraseña segura** | |
| **Descripción** | |
| **Este curso se dirige a las personas adultas, que están aprendiendo los fundamentos de internet. El módulo desarrollará los conceptos básicos necesarios para evaluar y proteger los sistemas de seguridad de la información, para dar a conocer los últimos datos digitales de las estafas o fraudes potenciales, que podrían encontrarse en la web mientras utilizan o buscan recursos culturales. Esta unidad de aprendizaje enseñará a los ancianos como detectar las estafas online financieras más comunes y cómo proteger su información financiera y sus cuentas.** | |
| **Contenidos organizados en 3 niveles:** | |
| **Modulo 2: Seguridad online y creatividad: ¿qué pasa?**  **Unidad 2.1 Las estafas online más comunes: ejemplos de las estafas online más comunes, proteger** **tu información online**  **Sección 2.1.1. Introducción**  Las estafas online más comunes: ejemplos de las estafas online más comunes, proteger tu información online.  Los fraudes en internet son cada vez más comunes, debido al número creciente de personas que utilizan internet a diario.  Estas estafas no solo quieren tu dinero, sino también tu información, y esta última es más difícil de detectar.  La operación básica de las estafas no ha cambiado, ofrecen productos o servicios en cambio de una cantidad de dinero “demasiado buena para ser verdad”, en cambio de algunas preguntas para obtener información.  Ellos pueden ofrecer incluso préstamos u ofertas de trabajo para que muerdas el anzuelo.  **Sección 2.1.2. Ofertas de trabajo**  Por ejemplo, una oferta de trabajo que propone un sueldo completo, con horas diarias a tiempo parcial y no pide ninguna experiencia previa. Que el sueldo sea muy alto, puede ser el primer indicio de que este anuncio sea una estafa.  Antes de rellenar el formulario o de proporcionar la información, es siempre bueno comprobar:   * la autenticidad de la página web donde han publicado el anuncio * la calidad de las imágenes o de los comentarios en caso de venta de productos * la empresa que publicó el anuncio * las prestaciones de trabajo ofrecidas   **Sección 2.1.3. Estafa bancaria**  Otros intentos de fraude pueden ser hacerse pasar por una entidad, como tu banco o una página web que frecuentes, con la excusa de que hay una gran oferta o algo está mal con una conexión sospechosa.  Si piensas que puede ser importante, como en el caso de tu banco, llámalo en lugar de clicar en el enlace.  **Sección 2.1.4. Compra online**  La compra online se ha hecho cada vez más común, por eso a continuación encontrarás algunos consejos para comprar online de manera segura.  - La página web debe tener una conexión cifrada segura, los protocolos de internet deben ser https. La encriptación permite que la información sea escondida, de manera que no puede ser leída sin un conocimiento especial (como una contraseña). Eso se hace con un código secreto o encriptado.  - Asegúrate que estés en una página web fiable. Una página web que inusualmente tiene precios bajos, todos los precios iguales, ningún comentario, o imágenes de productos sospechosos son un indicio que la página web es una estafa.  **Sección 2.1.5. Productos de terceros**  Algunaspáginas web venden productos de terceros. En estos casos, tienes que investigar también la empresa de donde llega el producto.   * Es una buena señal si la página web muestra claramente el coste y la información de envío, acepta diferentes formas de pago y envía una factura de compra. * Si crees que la página web sea genuina y realizas una compra, jamás guardes la información de tu tarjeta de crédito. Eso evitará que alguien acceda a tu dispositivo y realice compras no deseadas. * Periódicamente consulta tu sueldo y, si ves algún movimiento sospechoso, denúncialo a tu banco rápidamente. * Si el producto no llega, trata de contactar con el vendedor o con la plataforma donde lo venden.   **Sección 2.1.6. Herencia por WhatsApp**  En WhatsApp una persona habla contigo, te dice que es muy mayor, que tiene una herencia, pero no tiene sucesores, entonces te ofrece heredarla.  Otra persona te habla directamente de un truco para invertir sin riesgos, prometiéndote que puedes ganar €100,000 en sólo un mes.  Un hombre atractivo o una mujer atractiva está enamorado/a de ti.  Una persona con una fotografía atractiva, que no conoces del todo, trata de hablarte y te habla de asuntos provocativos.  Ten cuidado con cualquier persona del extranjero que encuentres online.  Aprende las señales de una estafa de relaciones. Qué sepas que hay que estar atento. Nunca mandes dinero.  Si ya le has dado este dinero, no vayas al extranjero para tratar de recuperarlo.  Confirma siempre su identidad y su legitimidad antes de ir al extranjero para verle.  **Sección 2.1.7. SMS estafadores de tu banco**  Un mensaje llega a tu móvil supuestamente por parte de tu banco, diciendo que hay un error en tu cuenta bancaria y tienes que rellenar un formulario.  Una persona finge ser un asesor de las redes sociales y te pide tu contraseña para resolver un problema.  En una página web de oferta de trabajo de terceros, ofrecen la doble cantidad de dinero de un sueldo normal.  Cuando tratas de comprar por un particular y te pide que le pagues el dinero antes, de manera que pueda enviarte el producto, o no te puede dar ninguna información sobre el envío.  **Sección 2.1.8. Estafa de lotería**  Una estafa de lotería es un tipo de fraude de pago por adelantado que empieza con la notificación de un correo inesperado, una llamada telefónica o un correo (algo que incluya un gran cheque) explicando que “¡Has ganado!" una gran suma de dinero en una lotería. Al receptor del mensaje — el objetivo de la estafa — se le suele decir que mantenga la noticia secreta, "debido a un error en algunos de los nombres y número” y que contacte con un “agente de reclamaciones”. Después de contactar el agente, al objetivo de las estafas se le pedirá pagar los "gastos de tramitación" o los "gastos de trasferencia" de manera que la ganancia puede ser distribuida, pero nunca recibirá ningún pago de lotería.  **Sección 2.1.9. Falsas organizaciones benéficas**  Los estafadores se hacen pasar por organizaciones benéficas, y piden donaciones o contactan contigo fingiendo recaudar dinero después de desastres naturales o eventos mayores.  Las falsas organizaciones benéficas tratan de aprovecharse de tu generosidad o compasión para los que tienen necesidad. Los estafadores robarán tu dinero haciéndose pasar por caridad genuina.Estas estafas no solo te cuestan dinero, sino también desvían donaciones muy necesarias de organizaciones benéficas y causas legitimas.  Falsos métodos de caridad ocurren todo el año y, a menudo, consisten en respuestas a desastres o emergencias reales, como inundaciones, ciclones, terremotos e incendios forestales.  **Unidad 2.2. Seguridad online en el mundo cultural, cómo evitar estafas concretas del mundo cultural (entradas falsas, hackeo, o phishing)**  **Sección 2.2.1 Cómo actúan los estafadores**  Los estafadores pueden:   * Crear sitios web falsos * Utilizar páginas web verdaderas para subir anuncios falsos sobre entradas de conciertos y pases de museos * Ofrecer falsas entradas V.I.P. y paquetes de entradas   Para evitar una estafa de entradas:   * Toma una decisión meditada cuando miras la página web del revendedor de entradas * Utiliza una página web acreditada   Hay revendedores de entradas legales, pero si una oferta parece demasiado buena para ser real, es probable que lo sea.  **Sección 2.2.2. Pasos para protegerte**   * Utiliza el sentido común antes de entregar información confidencial. * Nunca confíes en los mensajes alarmantes. * No abras archivos adjuntos en los correos sospechosos o raros — en particular archivos adjuntos en Word, Excel, PowerPoint, o PDF. * Utiliza una página web acreditada   **Unidad 2.3. Consejos de seguridad online**  Una vez que tengas una cuenta de redes sociales, puedes utilizarla para hablar con personas que conoces en la vida real y publicar opiniones o imágenes (mejor sin datos sensibles).  **Sección 2.3.1. Cómo establecer una contraseña segura**  Ten siempre cuidado para cumplir con los términos de uso de la página web y para no cumplir delitos.   1. Deja de creer en imágenes desconocidas. Deberías dejar de creer en imágenes como chat o capturas de pantalla. 2. No cliques en archivos adjuntos desconocidos. 3. Comprueba la fuente de tus mensajes. 4. Nunca compartas los datos personales. 5. Ten cuidado con posibles estafas. 6. Protege tus datos financieros. 7. Evita compartir datos personales. 8. Utiliza contraseñas o códigos pin con caracteres como &, \*. \_\_, minúsculas y MAYUSCULAS. | |
| **Contenidos en puntos clave** | |
| * Utiliza contraseñas o códigos pin con caracteres como &, \*. \_\_, minúsculas y MAYUSCULAS. * Una vez que tengas una cuenta de redes sociales, puedes utilizarla para hablar con personas que conoces en la vida real y publicar opiniones o imágenes (mejor sin datos sensibles). * Falsos métodos de caridad ocurren todo el año y, a menudo consisten en respuestas a desastres o emergencias reales, como inundaciones, ciclones, terremotos e incendios forestales. * Una estafa de lotería es un tipo de fraude de pago por adelantado que empieza con la notificación de un correo inesperado, una llamada telefónica o un correo (algo que incluya un gran cheque) explicando que “¡Has ganado!" una gran suma de dinero en una lotería. | |
| **5 entradas del glosario** | |
| **Estafa de lotería:**  *Una estafa de lotería es un tipo de fraude de pago por adelantado que empieza con la notificación de un correo inesperado, una llamada telefónica o un correo (algo que incluya un gran cheque) explicando que “¡Has ganado!" una gran suma de dinero en una lotería.*  **Organizaciones benéficas falsas:**  *Tipo de fraude que ocurre cuando las organizaciones caritativas solicitan fondos al público, para objetivos filantrópicos, como buscar curas para los desastres o ayudas para las familias de los policías muertos.*  **Productos de terceros:**  *Se refiere a cualquier producto y/o servicio de terceros que se ofrece por o a través de la mediación del banco.*  **Estafa:**  *Una estafa o engaño es un tentativo de defraudar a una persona o a un grupo ganando su confianza.*  **Phishing:**  *Phishing es un tipo de ingeniería social donde un atacador envía un mensaje fraudulento (por ejemplo, falsificado, falso o engañoso) diseñado para engañar a una víctima humana, para que la víctima reveles información sensible a los atacadores o utilice un software malicioso en su infraestructura, como los ransomware.* | |
| **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) ¿Cuáles son las señales de alarma para detectar una estafa bancaria?  A. Un enlace sospecho recibido por correo  B. Un correo oficial de tu banco  C. Un correo de una asociación benéfica  **Correcta: A**  2) ¿Qué deberías hacer si fueras la víctima de una estafa bancaria?  A) Proporcionar tus datos personales  B) Clicar en archivos adjuntos desconocidos  C) Llamar al banco y verificar el problema  **Correcta: C**  3) ¿Cómo evitar una estafa de entradas?  A) Evita comprar entradas online  B) Compra solo en los revendedores online oficiales  C) Utiliza un revendedor de billetes sospechosos  **Correcta: B**  4) ¿Cómo parecen los métodos de falsa caridad?  A) a menudo consisten en respuestas a peticiones de ayuda reales de un familiar verificado.  B) A menudo consisten en respuestas a peticiones de ayuda reales de un amigo de familia verificado.  C) A menudo consisten en respuestas a desastres o emergencias, como inundaciones, ciclones, terremotos e incendios forestales.  **Correcta: C**  5) ¿Cómo establecer una contraseña segura?  A) Utilizando tu dirección  B) Utilizando tu nombre completo  C) Utilizando caracteres como &, \*. \_\_, minúsculas y MAYUSCULAS.  **Correcta: C** |
| **Material relacionado** |  |
| **PPT relacionado** | [**SOS creativity Module 2 Online security and creativity what’s up**](http://ppts/SOS%20creativity%20Module%202%20Online%20security%20and%20creativity%20what%E2%80%99s%20up.pptx) |
| **Enlace de referencia** |  |
| **Video en formato YouTube (si hay)** | Online safety for grown ups, Bristol City Council Skills & Learning - Adult & Community Learning Service [**https://www.youtube.com/watch?v=iCs3aJYXLwo**](https://www.youtube.com/watch?v=iCs3aJYXLwo) |