Ficha de formación

Título	**Ciberseguridad para mayores: herramientas para una navegación segura**
Palabras clave	Ciberseguridad, seguridad en línea, dependencia digital, navegación segura, salud tecnológica
Proporcionado por	Croatian Telecom Inc.
Idioma	Español

Área de formación	
	Alfabetización sobre información
	Comunicación y colaboración
x	Seguridad
	Resolución de problemas

Objetivos / Resultados de aprendizaje

Objetivo: El objetivo de esta formación es educar a los mayores en materia de ciberseguridad y proporcionarles las herramientas y conocimientos necesarios para navegar con seguridad por el mundo digital.
Resultados de aprendizaje – al final de esta formación, los participantes serán capaces de:

- Comprender la importancia de la ciberseguridad
- Reconocer las ciberamenazas más comunes
- Practicar una navegación segura por Internet
- Proteger la información personal
- Responder a incidentes cibernéticos
- Utilizar las tecnologías digitales para la salud y el bienestar

Descripción

Esta formación dota a las personas mayores de los conocimientos y herramientas esenciales para navegar con seguridad por el mundo digital. Los participantes conocerán los riesgos de la ciberseguridad y reconocerán las amenazas más comunes. Comprenderán la navegación segura por Internet y la seguridad del correo electrónico, protegerán los dispositivos personales, salvaguardarán la información personal y se mantendrán a salvo. La formación también cubre la respuesta a incidentes y la importancia de mantenerse al día sobre las ciberamenazas emergentes. También serán capaces de navegar con seguridad por las tecnologías digitales en relación con su salud y bienestar, tomando decisiones con conocimiento de causa y aprovechando las oportunidades que ofrecen. Al final, estarán capacitados para protegerse a sí mismos y a su información personal en Internet.

Co-funded by the European Union

Índice de contenidos (3 niveles)

Módulo: Herramientas de ciberseguridad para una navegación segura
Unidad 1: Introducción a la ciberseguridad
1.1. Comprender los riesgos de ciberseguridad
1.2. Tipos comunes de ciberamenazas
1.3. Importancia de la ciberseguridad para las personas mayores

Unidad 2: Navegación segura por Internet
2.1. Buenas prácticas para mantenerse seguro en el entorno digital
2.2. Aumentar la seguridad en línea con herramientas de navegación segura

Unidad 3: Salud y bienestar en la era digital
3.1. Riesgos de un tiempo de pantalla excesivo y dependencia digital
3.2. Salud y herramientas digitales

Contenido desarrollado

Module: Herramientas de ciberseguridad para una navegación segura

Unidad 1: Introducción a la ciberseguridad
Sección 1.1.: Comprender los riesgos de ciberseguridad
Piensa en los riesgos de ciberseguridad como peligros potenciales cuando te conectas a Internet. Al igual que tomas precauciones para mantenerte seguro en el mundo físico, como cerrar las puertas con llave, ser consciente de los riesgos cibernéticos te ayuda a mantenerte seguro en el mundo digital. Estos riesgos pueden incluir cosas como piratas informáticos que intentan robar tu información personal, estafas que te engañan para que des tu dinero o virus que pueden dañar tu ordenador. Además, la ciberseguridad hace hincapié en el fomento de una cultura consciente de la seguridad, promoviendo la concienciación y la educación sobre prácticas seguras en Internet.
Si conoces estos riesgos, podrás protegerte mejor. Es como conocer las señales de un suelo resbaladizo para caminar con cuidado y evitar caerte. Hablaremos de los riesgos cibernéticos más comunes y de cómo reconocerlos, para que puedas navegar por el mundo *online* con confianza y tomar decisiones informadas para mantener tu seguridad y la de tu información. Recuerda, el conocimiento es poder, y conociendo los riesgos de la ciberseguridad, estarás dando un paso importante para protegerte en Internet.

1.2. Tipos comunes de ciberamenazas
En esta unidad, exploraremos los tipos comunes de ciberamenazas, que son diferentes formas en que los malhechores intentan dañarte a ti o a tu ordenador cuando utilizas Internet. Comprender estas amenazas te ayudará a mantenerte seguro y evitar posibles daños. Desglosémoslo en términos sencillos.

Piensa en las ciberamenazas como trucos o trampas que los malos utilizan en Internet. Quieren robar tu información personal, infectar tu ordenador con software dañino o

Co-funded by the European Union

engañarte para que les des tu dinero. Algunos tipos comunes de ciberamenazas son el phishing, el malware y el robo de identidad.

El phishing es un correo electrónico o mensaje falso que simula provenir de alguien en quien confías, pero que está intentando engañarte para que des tu información personal. Es como si alguien se hiciera pasar por un amigo para acceder a tus secretos. Los mensajes de phishing más habituales son: correos electrónicos falsos del banco, informes falsos de ganancias en apuestas o juegos de azar o premios gratuitos, cuentas falsas de proveedores de servicios informáticos o de pago o de tiendas en Internet, confirmaciones falsas de supuestos pedidos o falsos recordatorios de pago, mensajes falsos sobre políticas de privacidad de datos personales o condiciones que deben aceptarse.
El mensaje de correo electrónico de phishing puede decir: Su tarjeta de crédito ha caducado, su cuenta ha caducado, ha sido bloqueada temporalmente, o confirme sus datos de acceso. El formato (diseño corporativo), la dirección del remitente o el saludo directo al usuario pueden crear la impresión de que se trata de un correo electrónico enviado por un banco u otro servicio proveedor. Los mensajes de correo electrónico en formato HTML muestran un enlace "legal" al destinatario, que contiene un enlace oculto en segundo plano, que conduce directamente a contenidos fraudulentos o maliciosos.
El malware es como un virus que puede infectar tu ordenador y causar daños. Puede ralentizar tu ordenador o incluso robar tu información personal.
El robo de identidad se produce cuando alguien roba tu información personal, como tu nombre, dirección o datos de tu tarjeta de crédito, y los utiliza sin tu permiso. Es como si alguien se hiciera pasar por ti y utilizara tu dinero o comprara cosas en tu nombre.
Los ladrones de identidad también pueden integrar en sus mensajes de correo electrónico programas maliciosos como virus
o software troyano como enlace, archivo adjunto o código fuente en un mensaje de correo electrónico en formato HTML. El mero hecho de hacer clic en la imagen del mensaje de phishing puede tener graves consecuencias. Los estafadores que roban identidades suelen utilizar direcciones que sólo difieren ligeramente de las originales. Un ladrón de identidad puede sustituir caracteres para crear URL falsas. Por ejemplo, en lugar de las direcciones originales como http://www.onlinebank.com.hr puede ser una representación falsa utilizar una dirección como http://www.on1inebank.com.hr.
¿Cómo saber si algo es malicioso?

- DIRECCIÓN DEL REMITENTE FALSA

Pasa el ratón por encima de la dirección del remitente. ¿Contiene la dirección de correo electrónico elementos sospechosos? ¿Hay faltas de ortografía en la dirección, aunque sean insignificantes?

- PETICIÓN DE DATOS CONFIDENCIALES

¿El enlace contenido en el correo electrónico te pide que introduzcas información personal? ¿Se te exige que facilites información confidencial, como PIN o contraseñas?

Co-funded by the European Union

- URGENCIA

¿El mensaje te pide que actúes de forma inmediata o urgente? ¿Contiene el mensaje una amenaza o una advertencia?

- ENLACES A SITIOS WEB FALSOS

¿Qué aparece al pasar el ratón por encima de un enlace? ¿Es una página segura (la URL debería empezar por "https://") y cifrada (símbolo del candado delante de la URL)?

- FORMULARIOS EXTRAÑOS Y ERRORES ORTOGRÁFICOS

¿Es genérico el saludo del correo electrónico? ¿Contiene faltas de ortografía, puntuación incorrecta o signos especiales?

Si conoces estos tipos comunes de ciberamenazas, podrás reconocerlas y tomar medidas para protegerte. Discutiremos estrategias para permanecer seguro y evitar ser víctima de estas amenazas, permitiéndote disfrutar del mundo online con confianza y tranquilidad.

1.3. Importancia de la ciberseguridad para las personas mayores

Piensa en la ciberseguridad como tu guardaespaldas personal en el mundo digital, que vela por tu bienestar. Es como tener a alguien que te vigila, asegurándose de que tu información personal está a salvo y tus dispositivos permanecen seguros. Para garantizar la ciberseguridad, debemos poner en práctica hábitos seguros en Internet, como crear contraseñas seguras y únicas, ser precavidos a la hora de hacer clic en enlaces sospechosos o descargar archivos de fuentes desconocidas, y mantener nuestros dispositivos y programas actualizados.

- Nunca confirmes tu número de cuenta, contraseña u otra información secreta si te lo piden en un mensaje de correo electrónico. Los bancos y empresas de verdad nunca lo harían por motivos de seguridad.
- Comprueba el estado de seguridad de los sitios web antes de introducir tus datos personales. HTTPS no garantiza que un sitio web sea real. Haz clic en el símbolo del candado que aparece junto a la URL en tu navegador para comprobar el certificado de seguridad del sitio web.
- Creer en la infalibilidad de la tecnología puede dejar espacio para ataques de Phishing. Un nivel saludable de desconfianza evita que los atacantes roben tu identidad y el acceso a tus cuentas y sistemas de información.

Unidad 2: Navegación segura por Internet

2.1. Buenas prácticas para mantenerse seguro en el entorno digital

- Practica hábitos de navegación seguros: Cuando compres, realices operaciones bancarias o compartas información personal en Internet, limítate a sitios web de confianza. Busca el símbolo del candado y "https://" en la dirección del sitio web, lo que indica una conexión segura.
- Ten cuidado con la ingeniería social: Desconfía de llamadas, mensajes o correos electrónicos no solicitados en los que se pida información personal o datos

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

financieros. Las organizaciones legítimas no pedirán esa información por medios no solicitados.

- Haz copias de seguridad de tus datos con regularidad: Crea copias de seguridad de tus archivos y datos importantes en un dispositivo de almacenamiento independiente o en un servicio en la nube. Esto ayuda a protegerse contra la pérdida de datos debido a fallos de hardware, robo o ataques de ransomware.
- Activa la autenticación de dos factores (2FA): Activa 2FA siempre que esté disponible. Esto añade una capa adicional de seguridad al requerir un paso de verificación secundario, como un código único enviado a tu dispositivo móvil, además de tu contraseña.
- Ten precaución al compartir información en las redes sociales: Ten cuidado al compartir información personal, detalles de ubicación o planes de vacaciones en las redes sociales. Compartir información en exceso puede proporcionar información valiosa a ciberdelincuentes o posibles ladrones.
- Protege tus dispositivos móviles: Aplica funciones de seguridad, como contraseñas, huellas dactilares o reconocimiento facial, para bloquear tus smartphones y tablets. Instala apps de seguridad de confianza que ofrezcan funciones como el rastreo y borrado remotos en caso de pérdida o robo.
- Confía en tus instintos: Si algo parece demasiado bueno para ser verdad o te resulta sospechoso, confía en tus instintos. Sé escéptico ante ofertas inesperadas, peticiones de dinero o solicitudes urgentes de información personal.
- Borra los datos de navegación regularmente: Borra regularmente el historial de navegación, las cookies y los datos almacenados en caché. Esto ayuda a proteger tu privacidad eliminando la información almacenada a la que podrían acceder personas no autorizadas.

2.2. Aumentar la seguridad en línea con herramientas de navegación segura

Mejorar la seguridad en línea con herramientas de navegación segura es un aspecto importante de la ciberseguridad. Utilizando estas herramientas, puedes proteger tu privacidad, tu información personal y reducir el riesgo de amenazas en línea. Estos son algunos consejos esenciales para mejorar tu seguridad en línea con herramientas de navegación segura:

- Instala y utiliza un navegador web de confianza: Elige un navegador web de confianza, como Google Chrome, Mozilla Firefox o Microsoft Edge. Estos navegadores dan prioridad a la seguridad y publican actualizaciones periódicas para solucionar vulnerabilidades.
- Activa las funciones de seguridad del navegador: Familiarízate con las funciones de seguridad que ofrece tu navegador. Activa funciones como los bloqueadores de ventanas emergentes, el modo de navegación segura y la configuración de privacidad para mejorar tu seguridad en línea.
- Activa la protección contra phishing y malware: Activa las funciones integradas de protección contra phishing y malware que ofrece tu navegador web. Estas funciones pueden avisarte de sitios web sospechosos y evitar que visites sitios maliciosos conocidos.

Co-funded by the European Union

- Mantente informado y actualizado: Permanece informado sobre las últimas amenazas online y las mejores prácticas para una navegación segura. Lee regularmente fuentes fiables, como sitios web o blogs de ciberseguridad de confianza, para estar al día de la evolución del panorama de la seguridad en Internet.

Unidad 3: Salud y bienestar en la era digital

3.1. Riesgos de un tiempo de pantalla excesivo y dependencia digital

Para mitigar los riesgos del tiempo excesivo frente a la pantalla y la dependencia digital, he aquí algunas estrategias y prácticas a tener en cuenta:

- Establecer límites de tiempo de pantalla: Establece límites de tiempo específicos para el uso de pantallas, tanto para actividades de ocio como para tareas relacionadas con el trabajo. Esto ayuda a crear un equilibrio saludable entre el tiempo frente a la pantalla y otras actividades.
- Tomar descansos regulares: Incorpora descansos regulares de las pantallas a tu rutina diaria. Ponte de pie, estírate y realiza actividades físicas o pasatiempos que no impliquen el uso de dispositivos digitales.
- Practicar la desintoxicación digital: Dedica periodos concretos, como fines de semana o tardes, a desconectar por completo de los dispositivos digitales. Utiliza este tiempo para realizar actividades fuera de Internet, pasar tiempo con tus seres queridos o dedicarte a tus aficiones.
- Practicar un uso consciente de la tecnología: Sé consciente de cómo utilizas la tecnología y del impacto que tiene en tu bienestar. Reflexiona sobre tus hábitos digitales, evalúa sus efectos en tu vida y toma decisiones conscientes para minimizar las consecuencias negativas.
- Buscar apoyo y responsabilidad: Comparte tus preocupaciones con familiares, amigos o grupos de apoyo de confianza. Establece una responsabilidad mutua para fomentar el uso responsable de la tecnología y proporcionar apoyo para mantener hábitos saludables.
- Establecer límites digitales: Define límites claros para el uso de la tecnología, como desactivar las notificaciones durante horas específicas, evitar el tiempo de pantalla antes de acostarse o establecer directrices para el uso de dispositivos durante las comidas familiares.

Recuerda, el objetivo es desarrollar una relación sana con la tecnología y asegurarte de que enriquece tu vida en lugar de convertirse en una fuente de dependencia excesiva. Poniendo en práctica estas estrategias, puedes mitigar los riesgos asociados al tiempo excesivo frente a la pantalla y promover un estilo de vida más equilibrado y satisfactorio**.**

3.2. Salud y herramientas digitales

La tecnología puede ofrecer numerosas formas de apoyar y mejorar tu salud. Éstas son algunas de las formas en que la tecnología puede ayudarte con tu salud:

- Acceso a la información: Internet proporciona una gran cantidad de información relacionada con la salud, lo que te permite investigar síntomas, afecciones, tratamientos y medidas preventivas. Los sitios web fiables, las aplicaciones

Co-funded by the European Union

sanitarias y las comunidades en línea pueden ayudarte a tomar decisiones informadas sobre tu salud.

- Control de la salud: Los dispositivos *wearables*, como los dispositivos de seguimiento de la actividad física y los relojes inteligentes, pueden controlar diversos aspectos de tu salud, como la frecuencia cardiaca, los patrones de sueño, la actividad física y las calorías quemadas. Estos dispositivos pueden proporcionar información valiosa sobre tu bienestar general y ayudarte a seguir el progreso hacia tus objetivos de salud.
- Telesalud y consultas a distancia: Los servicios de telesalud te permiten consultar a profesionales sanitarios a distancia mediante videollamadas o chats en línea. Este cómodo método ahorra tiempo y puede ser especialmente beneficioso para citas de seguimiento, revisiones rutinarias o consultas médicas no urgentes.
- Gestión de la medicación: Las aplicaciones móviles y los organizadores inteligentes de la medicación pueden ayudar a gestionar los medicamentos mediante recordatorios para tomar las pastillas, el seguimiento de los horarios de medicación y las alertas para rellenar la receta. Esta tecnología puede evitar la omisión de dosis y fomentar el cumplimiento de los regímenes de medicación.
- Apoyo a la salud mental: Diversas aplicaciones de salud mental y plataformas en línea ofrecen recursos para gestionar el estrés, la ansiedad y la depresión. Estas herramientas pueden incluir meditación guiada, ejercicios de respiración, seguimiento del estado de ánimo y sesiones de terapia a través de plataformas digitales.
- Gestión de historiales médicos: Las historias clínicas digitales y los portales de pacientes permiten acceder y gestionar el historial médico, los resultados de las pruebas y la agenda de citas. Esto agiliza la comunicación con los proveedores sanitarios y garantiza la continuidad de la atención.
- Apoyo y motivación: Las comunidades en línea y las plataformas de redes sociales dedicadas a la salud y el bienestar pueden proporcionar apoyo, motivación y aliento. Conectar con personas de ideas afines puede fomentar un sentimiento de comunidad y ayudarte a rendir cuentas de tus objetivos de salud.
- Seguimiento de la salud y análisis de datos: La tecnología permite realizar un seguimiento y analizar los datos de salud a lo largo del tiempo, como la tensión arterial, los niveles de glucosa en sangre o el peso. Mediante el seguimiento de tendencias y patrones, puedes identificar áreas de mejora y realizar los ajustes necesarios para optimizar tu salud.

Recuerda que, aunque la tecnología puede ser una valiosa herramienta de apoyo a tu salud, es importante utilizarla con prudencia y junto con asesoramiento médico profesional. Consulta siempre a profesionales sanitarios para obtener un diagnóstico preciso, recomendaciones de tratamiento y orientación personalizada.

5 entradas de glosario

Ciberseguridad se refiere a la práctica de proteger los sistemas informáticos, las redes y la información digital de accesos no autorizados, robos y daños. Implica la aplicación de medidas para prevenir las ciberamenazas, como la piratería informática, la violación de datos y los ataques de malware. El objetivo de la ciberseguridad es

Co-funded by the European Union

garantizar la confidencialidad, integridad y disponibilidad de los activos digitales, salvaguardando a las personas y organizaciones frente a los riesgos y vulnerabilidades potenciales en un mundo digital interconectado.

Robo de identidad se refiere a la adquisición y uso fraudulentos de la información personal de alguien, como su nombre, número de la seguridad social o datos financieros, sin su consentimiento. Consiste en hacerse pasar por la víctima para llevar a cabo diversas actividades ilegales, como fraudes financieros, realizar compras no autorizadas o cometer otras formas de delitos relacionados con la identidad.

Ingeniería social es una técnica de manipulación utilizada por los ciberdelincuentes para engañar a las personas y explotar su confianza y sus emociones. Utiliza la manipulación psicológica en lugar de métodos técnicos para engañar a las personas para que revelen información sensible o realicen acciones que puedan comprometer su seguridad. Ejemplos de técnicas de ingeniería social son los correos electrónicos de phishing, las estafas telefónicas, los pretextos y la suplantación de identidad. El objetivo de la ingeniería social es manipular el comportamiento humano para obtener acceso no autorizado a sistemas, redes o información personal.

5 preguntas y respuestas de elección múltiple

1. En ciberseguridad, los riesgos se refieren a:
a) Peligros potenciales al conectarse a Internet.
b) Medidas de seguridad físicas.
c) Precauciones contra los suelos resbaladizos.
d) Prácticas seguras en Internet.
Opción correcta: a

2. ¿Cuáles son los tipos más comunes de ciberamenazas?
a) Ataques físicos a ordenadores.
b) Trucos o trampas utilizados por malas personas de Internet.
c) Medidas de seguridad para las compras en línea.
d) Estrategias para proteger la información personal.
Opción correcta: b

3. ¿Qué es la ingeniería social?
a) Una técnica utilizada por los ciberdelincuentes.
b) El estudio del comportamiento humano.
c) Una herramienta de navegación segura.
d) Un tipo de virus informático.
Opción correcta: a

4. ¿Cómo puedes mejorar la seguridad en línea con herramientas de navegación segura?
a) Utilizando navegadores de confianza y activando las funciones de seguridad.
b) Aumentando el tiempo de pantalla y la dependencia digital.
c) Compartiendo información personal en las redes sociales.
d) Ignorando los correos electrónicos de phishing y las advertencias de malware.

Co-funded by the European Union

Opción correcta: a

5. ¿Cuáles son algunas estrategias para mitigar los riesgos del exceso de tiempo frente a la pantalla?

a) Establecer límites de tiempo de pantalla y hacer descansos regulares.
b) Aumentar el uso de la tecnología para mejorar la salud.
c) Desconectarse por completo de los dispositivos digitales.
d) Buscar apoyo y responsabilidad.

Opción correcta: a

Bibliografía y referencias

- https://staysafeonline.org/
- https://www.consumer.ftc.gov/topics/online-security
- https://www.cisa.gov/cybersecurity
- https://www.getsafeonline.org/
- https://us.norton.com/internetsecurity
- https://www.staysmartonline.gov.au/
- https://www.commonsense.org/education/digital-citizenship/privacy-and-security

Material relacionado	BOOMER_Cyber_security_HT
Enlace de referencia	
Vídeo en formato Powtoon	https://www.youtube.com/watch?v=lvLhhqDhZJY

Co-funded by the European Union