Alfabetización Digital

Transcripción

# Participar de forma segura y responsable en línea

En este camino de aprendizaje, se le presentarán los riesgos de seguridad que puede enfrentar mientras utiliza Internet. Usted aprenderá acerca de las estafas en línea y cómo evitarlos. También aprenderá acerca de las prácticas recomendadas para compartir información en línea. Además, se le introducirá en el ciberacoso.

---

*Este archivo contiene la transcripción de audio de todos los videos que forman parte de este curso para que puedas, cuando lo necesites, acceder a contenidos específicos y revisar los conceptos presentados.*

*Puede utilizar el **Resumen** haciendo clic en el número de página para acceder directamente al Módulo y al tema que está buscando.*

*¡Buenos estudios!*

---

## Resumen

# Módulo 1 – Seguridad y privacidad en línea

## Protéjase del phishing

### Vídeo: Protéjase del phishing

Internet nos trae muchas posibilidades. Podemos hablar con los demás, hacer compras en línea y hacer negocios personales desde un solo lugar. Pero estas interacciones en línea no siempre son seguras. Hablemos de una estafa en línea popular que debes conocer.

Una forma común de capturar un pez es poner comida en un anzuelo para que el pez quiera comerla. Una vez que muerde la comida, estará enganchado. Las estafas de phishing en Internet funcionan de la misma manera. Las personas que quieren robar tu información son como pescadores. Te envían un correo electrónico o mensaje instantáneo a través de sitios de redes sociales o un juego en línea. A menudo pretenden ser alguien que no son y te piden información privada o hacer clic en un hipervínculo para que puedas realizar una tarea importante. Si les proporcionas la información o haces clic en el hipervínculo, estarás enganchado. Pero no te preocupes. Estas cuatro prácticas pueden ayudar a protegerte de las estafas de phishing.

**Práctica número uno**: ten cuidado de los mensajes sospechosos. Los estafadores tratan de hacer que sus mensajes se vean oficiales y familiares para que confíes en ellos. Piensa dos veces cuando recibas un mensaje sospechoso y evita compartir información personal a través de mensajes o correos electrónicos. Esto incluye la dirección de tu casa, información bancaria, contraseñas y más. No hagas clic en un enlace o no descargues un archivo si no sabes o confías en el remitente.

**Práctica número dos:** busca señales de que una página web es segura y está protegida. Antes de proporcionar información de tu tarjeta de crédito, ingresar una contraseña o dar otra información personal, verifica que estés en un sitio web seguro y de confianza. Los sitios web más seguros tienen el prefijo https al principio de la dirección URL en la barra de direcciones del explorador. Además, asegúrate de que estás en la página web correcta. Los estafadores a menudo tratan de llevarte a páginas web que parecen ser oficiales y usan variaciones de nombres de empresas para engañarte. www.microsoft.net no es lo mismo que el sitio web oficial de Microsoft en www.microsoft.com.

Comprueba siempre la URL para asegurarte de que estás en la página web correcta.

**Práctica número tres**: mantén tu navegador web y tu sistema operativo actualizados. Puedes activar las actualizaciones automáticas para asegurarte de que las últimas versiones de software sean instaladas automáticamente en tu computadora. Mantener el software del dispositivo actualizado significa que recibirás las últimas actualizaciones de seguridad que ayudan a proteger tu computadora.

**Práctica número cuatro:** instala software antimalware verificado en tus dispositivos. Este es un software especial diseñado para proteger tu computadora de software dañino y hackers. No seas el próximo pez enganchado. Cuando uses Internet, recuerda pensar antes de hacer clic, descargar o compartir para protegerte de estafas de phishing en línea.

## Comunicarse de forma segura en línea

### Vídeo: Comunícate de forma segura en línea

Usando Internet, podemos comunicarnos con otras personas en todo mundo de nuevas maneras. Esto tiene muchos beneficios, pero también hay algunos peligros. Hay depredadores en línea usando Internet todos los días. Estos depredadores a menudo fingen ser personas que no son. Por lo tanto, puede ser difícil saber con quién estás hablando en línea. Aquí hay tres consejos que puedes usar para protegerte de depredadores en línea cuando te comunicas.

**Consejo número uno**: usa tus instintos. Si alguien te hace sentir nervioso o incómodo, deja de comunicarte con esta persona y cuéntale a alguien de confianza inmediatamente. La mayoría de los sitios web y sitios de redes sociales tienen herramientas que puedes utilizar para reportar actividad sospechosa.

**Consejo número dos**: limita lo que compartes. Los depredadores en línea a menudo tratan de conseguir que compartas tu información personal a través de correos electrónicos y mensajes. Evita compartir información personal con un extraño en línea.

**Consejo número tres**: mantén la distancia. Piensa dos veces antes de conocer a alguien en persona con quien sólo has hablado en línea. Los depredadores en línea a menudo usan redes sociales para pretender ser alguien más mediante la creación de perfiles falsos usando fotos de otras personas. Incluso si alguien parece amigable, puede ser difícil saber con seguridad con quién estás hablando en línea. Cuéntale siempre a uno de tus padres o a alguien en quien confíes cuando un extraño en línea te pida conocerte en persona, para que no termines en una situación peligrosa. Muchos depredadores en línea usan tácticas inteligentes para atraerte a situaciones peligrosas, pero puedes ser más inteligente que ellos.

Ten en cuenta estos riesgos y consejos para que puedas mantenerte seguro cuando hablas con personas en línea.

## Crear contraseñas seguras

### Vídeo: Crear contraseñas seguras

Las contraseñas ayudan a proteger tu información personal y cuentas de otras personas. Una contraseña es tan importante como la cerradura de una puerta. La idea es tener una cerradura fuerte que sea difícil de romper y evite que personas peligrosas entren. Además, tampoco querrás que nadie encuentre las llaves de la cerradura. Una contraseña segura es como una buena cerradura para tu cuenta, debe ser difícil de adivinar y también debe ser segura para que otros no puedan encontrarla. Sigue estos consejos para crear contraseñas seguras y mantenerlas en secreto.

**Consejo número uno:** usa una combinación de letras, números y símbolos en tu contraseña. Usar una combinación de letras mayúsculas y minúsculas, caracteres y números, puede aumentar la seguridad de tu contraseña.

**Consejo número dos:** evita usar palabras comunes en tu contraseña. Esto incluye palabras y frases comunes como contraseña o sitio web, así como palabras clave personales como tu cumpleaños, tu nombre o tu ciudad natal. Los hackers pueden adivinar fácilmente estas frases en tu contraseña. Una combinación única de caracteres y números crea una contraseña más fuerte.

**Consejo número tres**: usa diferentes contraseñas para cuentas diferentes. Si alguien adivina tu contraseña de correo electrónico, tu seguridad y privacidad pueden estar comprometidas si utilizas la misma contraseña para tu cuenta bancaria. En su lugar, usa contraseñas diferentes para cada cuenta en línea que tengas.

**Consejo número cuatro:** tu contraseña es solo para ti. Cuando la compartes con otras personas, incluso con amigos y familiares, es más probable que alguien la use o no la mantenga segura. Guarda tus contraseñas para ti mismo. Al iniciar sesión en cuentas, asegúrate de cerrar sesión cuando termines y no guardes tu información de inicio de sesión en una computadora pública.

Además, evita hacer transacciones personales en computadoras públicas y redes públicas; esto facilita a los hackers acceder a tu información. Recuerda que usar contraseñas seguras y mantenerlas en privado es importante para tu seguridad y privacidad en línea. Ten en cuenta estos consejos al crear una nueva contraseña.

# Conocer las prácticas recomendadas para compartir información en línea

## Video: Compartir en exceso en línea

Internet nos permite mantenernos conectados con amigos y familiares en todo el mundo. Podemos usar las redes sociales y otras plataformas para ver lo que está pasando en la vida de nuestros amigos, compartir noticias personales y permanecer en contacto con los demás, pero compartir cosas en línea, no siempre es seguro.

Considera este escenario, Harold compra un carro nuevo y quiere que sus amigos lo vean. Entonces, publica una foto del carro en las redes sociales. Esto puede parecer bien, pero la imagen incluye una gran cantidad de información personal sobre Harold. Cualquiera puede ver su número de matrícula, qué tipo de carro está conduciendo y dónde vive en una sola imagen.

Esto puede no ser un problema si lo ven sus amigos, pero puede ser peligroso si la persona equivocada encuentra esta información y quiere usarla para algo malo. Es importante tener en mente la seguridad y privacidad al compartir cosas en línea.

Cuando configuras perfiles en sitios web de redes sociales, asegúrate de revisar la configuración de privacidad de tu cuenta. Si tu cuenta está establecida en pública, cualquier persona puede ver tu información y lo que compartes. En lugar de esto, utiliza la configuración privada en las cuentas, para que sólo tus contactos personales puedan ver lo que compartes.

También debes ser selectivo cuando aceptes invitaciones para conectarte con alguien a través de las redes sociales. La mayoría de las plataformas de redes sociales te permiten aceptar y rechazar solicitudes, y permitir que alguien sea tu amigo o seguidor en el sitio. Una vez que aceptes a alguien, esta persona tiene acceso directo a tu perfil y las cosas que compartes. Ten esto en cuenta cuando recibes una solicitud y asegúrate de sólo interactuar con personas que conoces y en las que confías.

Incluso cuando controlas quién tiene acceso a tus perfiles y cuentas, no puedes controlar lo que otras personas hacen con tu información. Cuando compartes algo en línea, no puedes borrarlo. Nunca compartas algo en línea que no quieras que extraños y el público vean. Recuerda siempre pensar antes de compartir. Ten en cuenta tu seguridad y toma decisiones inteligentes cuando compartes cosas en línea.

# Conocer la importancia de administrar su huella digital

## Vídeo: Gestione su huella digital

Si utilizas Internet, debes ser consciente de la información digital que dejas. Al igual que las huellas físicas que muestran los pasos de alguien en un camino de tierra, tu huella digital es una historia de toda la actividad que haces en línea. Cualquier publicación en las redes sociales que hagas, cualquier sitio web que visites y cualquier información que compartas en línea contribuye a tu huella digital.

Una vez que publiques algo en línea, no se puede borrar. Por lo tanto, tu huella digital puede durar por siempre. Esto puede ser algo bueno si tu huella digital incluye cosas que te dan una reputación positiva en línea. Esto puede ayudarte a construir tu marca personal. Tu historial en línea también puede ayudar a las aplicaciones que usas a saber más sobre ti. Pueden usar esta información para servirte mejor al adaptarse a las cosas que te gustan y a tus hábitos diarios. Pero también pueden utilizar esta información de manera equivocada y compartirla con otras personas. Ten en cuenta los siguientes consejos cuando estés en línea para gestionar tu huella digital.

**Consejo número uno:** conoce lo que dice tu huella sobre ti. Otras personas usan tu huella digital para emitir juicios sobre ti en línea. Esto puede incluir a empleadores cuando aplicas a un trabajo o cuando aplicas a programas académicos. Es importante saber qué dice tu huella digital acerca de ti y cómo se utiliza tu información. Para ver cuál es tu marca personal en línea, puedes buscarte a ti mismo. Busca tu nombre en el motor de búsqueda de Bing y observa qué resultados se muestran. Si estos resultados no muestran lo que quieres, piensa en lo que compartes en línea y qué información permites ver a otras personas.

**Consejo número dos**: administra la configuración de privacidad. Puedes modificar la configuración de privacidad de la mayoría de los sitios de redes sociales y aplicaciones en línea que utilices. Esto puede ayudarte a controlar quién ve lo que compartes y qué información se muestra cuando alguien te busca en línea.

**Consejo número tres:** administra tus cookies. Las cookies son notas dadas a tu navegador web mientras navegas. Estas cookies ayudan a las aplicaciones a rastrear la información que necesitan mientras usas la aplicación. Esto puede ayudar a que la aplicación funcione mejor para ti. Pero estos datos también contribuyen a tu huella digital. Puedes utilizar la configuración de tu navegador para limitar o bloquear el uso de cookies en ciertos sitios web.

**Consejo número cuatro:** piensa antes de compartir. Una vez que compartas algo en línea, no puedes retirarlo. Asegúrate de estar de acuerdo con que algo forme parte de tu huella

digital pública antes de compartirlo. Tu huella digital puede vivir por siempre. Ten en cuenta estos consejos para asegurarte de estar satisfecho con tu huella digital y la forma en que se utiliza.

# Módulo 2 – Civilidad en línea

## Conocer las prácticas recomendadas para el uso de la información que se encuentra en la web

### Vídeo: Use la información de manera responsable

Internet nos da información y posibilidades ilimitadas. Podemos encontrar cualquier cosa desde videos divertidos, hasta nuestras canciones favoritas, o información sobre cómo resolver un problema para una tarea, pero debemos ser responsables con la información que encontramos en línea.

Considera este escenario. Harold quiere escribir un libro de cocina y venderlo en línea. No es bueno para tomar fotos, por lo cual busca imágenes en línea. Descarga imágenes de diferentes alimentos y las incluye en su libro. Esto puede parecer bien porque es fácil de hacer, pero no es una manera justa o responsable de utilizar la información que se encuentra en línea.

Cuando alguien pone su trabajo original en línea incluyendo sus palabras, imágenes, videos, música y más, se convierte en el propietario del contenido. Como propietario, tiene ciertos derechos, generalmente considerados derechos de autor, para decidir cómo se puede utilizar ese contenido. Si usas las palabras o el trabajo de otra persona como si fueran propios, se considera plagio. Esto no es justo para el autor original y puede meterte en problemas.

Si quieres usar el contenido de otra persona en tu trabajo, asegúrate de hacer referencia a ella para darle crédito por su trabajo. Cuando utilizas el trabajo de alguien en un producto que estás vendiendo, primero debes obtener permiso del autor. Es posible que también tengas que pagar por una licencia para usar el trabajo de alguien. Algunas veces, los autores de contenido hacen que su trabajo esté disponible para uso gratuito.

Puedes utilizar motores de búsqueda como Bing para encontrar imágenes, videos y otro tipo de contenido disponibles para el uso de otras personas. A medida que utilizas Internet y encuentras información en línea, asegúrate de usarla de manera justa y responsable.

# Conocer las implicaciones de tratar a los demás mal en la web

## Video: Tratar a los demás respetuosamente en línea

Internet y las plataformas de redes sociales nos conectan con nuestros amigos, familia y compañeros de nuevas formas. A veces las personas aprovechan estas plataformas y las utilizan para difundir mensajes negativos sobre los demás.

El ciberacoso, o el acoso que tiene lugar en Internet, puede ser tan malo como el acoso en persona. Las personas pueden usar Internet para enviar mensajes negativos a alguien, difundir rumores falsos o compartir información privada de alguien sin permiso. Cuando alguien es acosado a través de la red, sus sentimientos pueden ser heridos y se puede dañar su reputación. No siempre puedes prevenir el ciberacoso, pero puedes ayudar a hacer de Internet un lugar más amigable y seguro para todos.

**Estas son algunas pautas que puedes seguir para promover el civismo digital en línea:**

- Vive según la regla de oro. Trata a los demás de la forma en que quieres que te traten, ya sea en persona o en línea.
- Evita enviar mensajes negativos e incurrir en comportamientos que puedan herir a otra persona.
- Respeta las diferencias. Todos somos diferentes en muchos sentidos. Cuando interactúas con personas en línea, respeta sus diferencias de opinión, experiencia y cultura. Incluso si no estás de acuerdo con algo que otra persona comparte en línea, debes tratarla con respeto y hacer de Internet un espacio amigable para la comunicación.
- Haz una pausa antes de responder. Antes de compartir algo en línea, haz siempre una pausa y piensa en las consecuencias. ¿Tu mensaje lastimará a otra persona? ¿Dañará tu reputación, la seguridad o la reputación de otros?
- Piensa dos veces antes de compartir en línea. Defiéndete a ti mismo y a los demás. Si te sientes inseguro en línea, puedes alejarte de una situación y reportarla a alguien en quien confíes.
- Cuando veas actividad cruel o peligrosa en línea, ofrece apoyo a los involucrados, y reporta el incidente a alguien en quien confíes. Todos podemos ayudar a hacer de Internet un lugar seguro y amigable para todos.
- Haz tu parte y sé un ciudadano digital responsable en línea.