apricot for parents

Programa y materiales para educadores de personas adultas

ANEXO 5: COMPORTAMIENTO SEGURO DE NAVEGACIÓN

Co-funded by the Erasmus+ Programme of the European Union

El apoyo de la Comisión Europea para la producción de esta publicación no constituye una aprobación del contenido, el cual refleja únicamente las opiniones de los autores, y la Comisión no se hace responsable del uso que pueda hacerse de la información contenida en la misma.

Este producto intelectual ha sido concebido y desarrollado por la Asociación Estratégica en el marco del proyecto APRICOT bajo la coordinación y responsabilidad de *Šiuolaikinių didaktikų centras*/ *Modern Didactics Centre* (LT).

Gracias a todos los socios por sus valiosas contribuciones:

Apricot Training Management Ltd. (Reino Unido)
ItF Institut Kassel e.V. – Frauencomputerschule (Alemania)
Planeta Ciencias (España)

Coordinador editorial: Daiva Penkauskienė

Autores: Hilary Hale, Beate Hedrich, Betül Sahin, Alejandra Goded, Anca Dudau, Daiva Penkauskienė

Consejo editorial: Sophy Hale, Seda Gürcan, Konrad Schmidt, Cihan Sahin, Josafat Gonzalez Rodriguez, Roc Marti Valls, Virgita Valiūnaitė

Mes/ Año: Noviembre 2021

Co-funded by the Erasmus+ Programme of the European Union

Capítulo 9: Anexos

Anexo 5: Comportamiento seguro de navegación

1. Características de una fuente de Internet fiable[1]

1. Introduzca el nombre del sitio web que está buscando en un buscador, por ejemplo, en el buscador de Google. Se puede tomar una decisión preliminar basada en los resultados. Las calificaciones de los usuarios de sitios populares se muestran en los resultados de búsqueda anteriores. Vea reseñas y comentarios de fuentes no relacionadas con el sitio web.

2. Si un sitio web comienza con "https", generalmente es más seguro y, por lo tanto, más seguro que una página con "http". Sin embargo, una conexión "https" puede no ser fiable. Es mejor comprobar si el sitio web utiliza otros medios. Asegúrate de que la página de pago del sitio web en particular sea una página "https".

3. Los sitios web "seguros" muestran un candado verde a la izquierda de la URL del sitio web. Verifique el estado de seguridad del sitio web en la barra de direcciones. Al hacer clic en el candado, puede consultar más detalles sobre el sitio web, por ejemplo, la certificación y el tipo de cifrado utilizado.

4. Incluso después de determinar que la conexión es segura, debe estar atento a las siguientes señales de advertencia:

   A. Múltiples guiones o símbolos en el nombre del dominio.

   B. Nombres de dominio que imitan a empresas reales (por ejemplo, “Amaz0n” o “Nike Outlet”).

   C. Páginas únicas que utilizan las plantillas de páginas creíbles (por ejemplo, "visihow").

   D. Terminaciones de dominio como ".biz" y ".info". Estos sitios tienden a no ser confiables.

   E. También hay que tener en cuenta que los sitios ".com" y ".net" son los nombres de dominio más fáciles de obtener, que no implica que sean necesariamente

[1] https://de.wikihow.com/Herausfinden-ob-eine-Webseite-seriös-ist from 26.05.2020

Co-funded by the Erasmus+ Programme of the European Union

dudosos. Sin embargo, no tienen la misma credibilidad que un sitio web con la terminación de dominio ".edu" (para institutos educativos) o ".gov" (gobierno).

5. Hay que prestar atención al idioma del sitio web. Muchas palabras mal escritas (o que faltan), generalmente mala gramática u oraciones con frases extrañas indican páginas dudosas. También estas páginas son cuestionables, incluso si el aspecto técnico del sitio web parece ser serio.

6. Los anuncios también pueden indicar sitios dudosos. Tenga cuidado si observa los siguientes tipos de anuncios:

A. Anuncios que cubren toda la página.

B. Anuncios en los que debe completar una encuesta (o hacer otra cosa) antes de continuar.

C. Anuncios en los que se le redirige a otra página.

D. Anuncios para adultos o anuncios ofensivos

7. Asegúrate de que haya una página de "Contacto" disponible. La mayoría de los sitios web tienen una página de contacto donde puedes comunicarte con el propietario del sitio web. Si es posible, llama al número proporcionado o escribe a la dirección de correo electrónico para verificar la seriedad del sitio web. Si el sitio web no tiene una página de contacto, es una señal de advertencia inmediata.

8. Utiliza una página de "quién es quién" para averiguar quién registró el dominio del sitio web. Antes, todos los dominios debían tener información de contacto de la persona o empresa. Esta información se puede encontrar en la mayoría de los sitios de registro de dominios o en https://whois.check-domain.net// (Inglés: https://who.is/). Sin embargo, debido al Reglamento General Europeo de Protección de Datos (EU-GDPR), solo se muestra el estado del dominio cuando se realizan consultas.

9. Una huella ausente o incompleta también es un indicio de alerta. De acuerdo con el artículo 5 de la Ley de Telemedia, los proveedores comerciales están obligados a indicar su nombre y dirección y, en el caso de personas jurídicas, la forma jurídica debe aparecer en el pie del texto. Toda persona que muestre un solo anuncio de pago en un sitio web se considerará proveedor comercial.

Co-funded by the Erasmus+ Programme of the European Union

10. El diseño [2] y la navegación pueden dar pistas sobre un proveedor dudoso. Los sitios seguros tienden a tener un diseño claro y conciso y la navegación permite orientarse de forma rápida y en gran medida intuitiva. Un sitio web confuso también podría llevarnos a hacer clic en un enlace por el que se cobra una tarifa. Por lo tanto, preste atención a su instinto.

¡No haga click en los enlaces de fuentes desconocidas o dudosas! ¡Descargue solo de fuentes seguras!

2. Reconocer y evitar peligros

Internet se ha convertido en una parte indispensable de la vida cotidiana. Sin embargo, los peligros que encierra Internet a menudo se reprimen. Estos peligros pueden tener efectos negativos graves, especialmente para los niños más pequeños. En particular, el anonimato representa un gran peligro. En Internet, se puede asumir una identidad diferente. Los adultos pueden hacerse pasar por niños o adolescentes en los chats y comunicarse con los niños. Los menores pueden entonces convertirse en víctimas de acoso (sexual). Si un agresor persuade a los menores de edad para que envíen fotos inapropiadas de ellos mismos o para que vayan a conocer a la persona que no conocen, puede ser muy peligroso.

Una consecuencia de este anonimato puede ser el ciberacoso, el sexting y los discursos de odio. Desafortunadamente, no hay filtros ni aplicaciones para esto. Especialmente en este caso se requiere el pensamiento crítico y la competencia mediática de padres e hijos .

3. Derechos en Internet

Es muy fácil copiar textos de Internet, descargar música y películas o utilizar imágenes. Sin embargo, esto no está permitido legalmente.

Para publicar fotos o videos en Internet, se necesita obtener el permiso de todas las personas que aparecen en las fotos o videos. Esto también se aplica a las personas a las que solo se les ha fotografiado por detrás o que han sido distorsionadas con filtros.

Si descubres imágenes tuyas o de tu hijo que se han publicado ilegalmente en la web, debes conservarlas como prueba y pedir a los operadores del sitio web que las eliminen.

Todas las imágenes, música o películas están protegidas por derechos de autor. Si se publican copias de películas cinematográficas en Internet, la descarga y distribución de estas películas también es ilegal y será procesada. Desafortunadamente, muchas

Co-funded by the Erasmus+ Programme of the European Union

personas no ven esto como un robo, ya que no se roba nada físico. Sin embargo, es un robo de propiedad intelectual. Debemos descargar música / películas de los servicios de transmisión legales, incluso si no son gratuitos. En Alemania, la infracción de los derechos de autor se castiga con fuertes multas o incluso con prisión.

Verifique los derechos de autor en su país.

4. Trampa de costes: publicidad

Otro peligro son los anuncios. Estos anuncios no son visibles inmediatamente en aplicaciones o en ciertos sitios web. Con un click incorrecto o involuntario, puedes llegar a ofertas de compra o se te pueden pedir tus propios datos. Las suscripciones o compras también se pueden ocultar detrás del clic, por ejemplo, tras tonos de llamada o fondos de pantalla. Se pueden activar funciones adicionales o nuevos niveles en juegos gratuitos. Estas compras se facturan a través de tu proveedor de telefonía móvil, lo que se denomina facturación WAP. Los delincuentes también utilizan este tipo de pago con mucha frecuencia. Porque para muchos usuarios la facturación WAP no es lo suficientemente clara.

5. Adicción a Internet

Internet ofrece una gran cantidad de servicios que se pueden utilizar durante todo el día. No hay distinción entre el día y la noche. Pero si pasas demasiado tiempo en el mundo digital, puedes perder la relación con el mundo real. Presta atención a los tiempos de uso y da un buen ejemplo a tus hijos.

6. Privacidad

Todos deben cuidar su propia privacidad. Las fotos o los números de teléfono se comparten demasiado rápido en Internet. Recuerda siempre el dicho: "Internet nunca olvida". Todo el contenido subido probablemente se almacenará allí para siempre. Antes de subir fotos o información personal, siempre debes considerar si quien lo demanda realmente necesita este contenido o si más tarde podrías arrepentirte de haberlo compartido. No introduzcas tu dirección privada o número de cuenta en ningún lugar sin dudarlo y considerarlo. En el peor de los casos, el contenido puede generar costos o efectos negativos posteriormente.

Co-funded by the Erasmus+ Programme of the European Union

7. Cookies

Las cookies son información de texto que el navegador guarda automáticamente cuando se visitan sitios web. Las cookies incluyen información personal y configuraciones de los sitios web visitados. Las cookies en el navegador tienen aspectos tanto positivos como negativos. Si una página web se usa repetidamente, las cookies son ventajosas ya que no es necesario iniciar sesión nuevamente e ingresar contraseñas largas en la página visitada. La desventaja es que también se almacenan datos personales. Una visita a una tienda online donde se hayan visto artículos dará como resultado que se ofrezcan anuncios coincidentes en otros sitios web posteriormente.

Dado que las cookies tienen ventajas y desventajas, surge la pregunta "¿Aceptar o bloquear las cookies?

Aunque las cookies no siempre son ventajosas, todavía se utilizan en muchas áreas. Existen las llamadas "Cookies de seguimiento" y las "Cookies de sesión". Las “cookies de seguimiento" se utilizan para cambiar la publicidad personalizada y las "cookies de sesión" se utilizan, por ejemplo, en la banca online para la sesión actual. Tan pronto como el usuario cierra la sesión, se eliminan inmediatamente. Muchos contenidos online se basan en el uso de cookies. Algunas páginas solo se pueden usar de manera limitada o casi no se pueden usar sin cookies.

En la configuración del navegador, las cookies se pueden bloquear por completo o solo las de los sitios web visitados o se pueden permitir todas las cookies. Las cookies de terceros se pueden bloquear sin vacilar. Y se pueden aceptar las cookies de los sitios web visitados en un equilibrio saludable entre la privacidad y el aprovechamiento de los beneficios de aceptarlas.

8. Recomendaciones para los padres

Todos estos peligros disuaden a las personas de utilizar Internet. Uno preferiría prohibir a los niños que usen Internet. Pero esto no es posible, porque Internet se ha convertido en una parte integral de nuestra vida cotidiana. Tampoco tendría sentido. El trabajo en la red trae muchas ventajas y nos ahorra tiempo. Pero, ¿pueden los padres afrontar estos peligros?

Una recomendación sería la combinación de restricciones técnicas (ver Capítulo 7.2) y la educación digital de los padres. Pero la tecnología también tiene sus límites, por lo que es importante fortalecer las habilidades mediáticas de los niños.

Co-funded by the Erasmus+ Programme of the European Union

Para fortalecer las capacidades mediáticas y la conciencia de los niños, se debe comprender el mundo de los niños.

- ¿Qué aplicaciones usa el niño?
- ¿Cómo maneja estas aplicaciones?
- ¿A qué juegos le gusta jugar?
- ¿Qué series / películas le interesan?

Estas preguntas se pueden responder mejor si los padres muestran a sus hijos su interés en todas las áreas digitales. El niño debe poder mostrar y explicar libremente y sin miedo lo que está haciendo en Internet. Sería un error que los padres siguieran a sus hijos en las redes sociales o intentaran pasar junto a ellos al siguiente nivel de un juego de ordenador.

Tu propio comportamiento mediático sirve como modelo para los niños. Los padres no deben pasar todo el día frente al televisor o usando sus teléfonos móviles. Si el uso de los medios de comunicación juega un papel muy importante en la vida de los padres, el niño aprenderá lo mismo.

Los padres no deben regañar si el niño ha caído en una trampa de costos, sino que deben brindar apoyo preventivo. Deben hablar con el niño sobre los peligros mencionados anteriormente en Internet y darle ejemplos prácticos que sean comprensibles para el niño. Debe alentar al niño a examinar críticamente el contenido y a no creer todo lo que se puede leer en plataformas o sitios web. Los niños aprenden en la vida real cómo tratar con sus semejantes. Estos principios sociales se aplican exactamente igual en el mundo digital.

Los padres deben ser la primera persona a quien el niño acuda si no se siente seguro o es atacado por otros. Son las personas de confianza más importantes para el niño.

Co-funded by the Erasmus+ Programme of the European Union