MIG-DHL

Migrants Digital Health Literacy

Manual

Módulo 6

Ser activo en el entorno de la salud digital

Autores:

Josemar Alejandro Jiménez, Oxfam; Jenny Wielga, IAT

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

El apoyo de la Comisión Europea a la producción de esta publicación no constituye una aprobación de su contenido, que refleja únicamente las opiniones de los autores, y la Comisión no se hace responsable del uso que pueda hacerse de la información contenida en ella. Número de proyecto: 2020-1-DE02-KA204-007679.

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

MIG-DHL
Migrants Digital Health Literacy

Este manual forma parte del Programa **MIG-DHL que** contiene 6 módulos de aprendizaje en total, que ha sido desarrollado dentro de la Asociación Estratégica Erasmus+ **MIG-DHL- Migrants Digital Health Literacy.**

Los contenidos de la formación de un vistazo:

Programa MIG-DHL

- Módulo 1: Qué es la alfabetización digital sanitaria y su relevancia
- Módulo 2: Principales cuestiones sanitarias al aterrizar en un nuevo país
- Módulo 3: Servicios de salud
- Módulo 4: Alfabetización digital
- Módulo 5: Exploración de las herramientas de salud digital
- **Módulo 6: Ser activo en el entorno de la salud digital**

Puede encontrar más información en la página web: https://mig-dhl.eu/

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

MIG-DHL Migrants Digital Health Literacy

Declaración sobre los derechos de autor:

Contenido

6. Ser activo en el entorno digital

Para ser activo en el entorno digital, es muy importante saber cómo proteger la privacidad para mejorar la protección de los datos personales en el entorno digital y también para proteger la salud física y psicológica.

Por lo tanto, este módulo se centra en la protección de la privacidad. La información de este módulo es una continuación de los temas ya tratados en el módulo 4. Especialmente relacionado con el desarrollo de competencias en relación con la seguridad y la privacidad. Estas competencias se refieren a la capacidad de proteger los dispositivos, los contenidos, los datos personales y la privacidad en el entorno digital. La implicación de esta acción permite también la protección de la salud física y mental, el bienestar y la inclusión social. Esta parte está relacionada con el área de competencia 4 "Seguridad" de DigiComp, que ya se introdujo en el módulo 4.

6.1 Proteger la privacidad y los datos personales en el entorno digital

Para la privacidad y los datos personales existen muchos factores de riesgo diferentes en el entorno digital. Algunos de los principales factores de riesgo, que también se señalan en los materiales de formación, se describen en la siguiente parte de forma más detallada.

6.1.1 Hackear

El hacking se refiere a las actividades que buscan comprometer los dispositivos digitales, como ordenadores, teléfonos inteligentes, tabletas e incluso redes enteras. Y aunque el pirateo no siempre tiene fines maliciosos, hoy en día la mayoría de las referencias al pirateo y a los piratas informáticos lo caracterizan como una actividad ilegal de los ciberdelincuentes, motivada por el beneficio económico, la protesta, la recopilación de información (espionaje) e incluso por la simple "diversión" del desafío.

El hackeo suele ser de naturaleza técnica. Pero los hackers también pueden utilizar la psicología para engañar al usuario para que haga clic en un archivo adjunto malicioso o proporcione datos personales.

De hecho, es correcto caracterizar el hacking como un término general que engloba la actividad que está detrás de la mayoría, si no de todos, los malware y los ciberataques maliciosos contra el público informático, las empresas y los gobiernos. Las técnicas de hacking más comunes son:

- Botnets
- Secuestros del navegador
- Ataques de denegación de servicio (DDoS)

- Ransomware
- Rootkits
- Troyanos
- Virus
- Gusanos

Tipos de hacking/hackers

En términos generales, se puede decir que los hackers intentan entrar en los ordenadores y las redes por cualquiera de las cuatro razones:

- Hay un beneficio financiero criminal, es decir, el robo de números de tarjetas de crédito o la estafa a los sistemas bancarios.
- Además, ganar credibilidad en la calle y pulir la reputación dentro de la subcultura hacker motiva a algunos hackers, ya que dejan su marca en los sitios web que vandalizan como prueba de que han realizado el hackeo.
- También está el espionaje corporativo, cuando los hackers de una empresa tratan de robar información sobre los productos y servicios de la competencia para obtener una ventaja en el mercado.

Prevención de la piratería informática

- Protección antimalware: Lo primero y más importante es descargar un producto antimalware fiable (o una aplicación para el teléfono), que pueda detectar y neutralizar el malware y bloquear las conexiones a sitios web de phishing maliciosos.
- Tenga cuidado con las aplicaciones: En segundo lugar, sólo descargue aplicaciones para el teléfono de los mercados legítimos que se vigilan a sí mismos en busca de aplicaciones portadoras de malware, como Google Play y Amazon Appstore. (Ten en cuenta que la política de Apple restringe a los usuarios de iPhone la descarga sólo de la App Store). Aun así, cada vez que descargue una aplicación, compruebe primero las calificaciones y los comentarios. Si tiene una calificación baja y un número reducido de descargas, es mejor evitar esa aplicación.
- Proteja su información: Sepa que ningún banco o sistema de pago en línea le pedirá sus credenciales de acceso, número de seguridad social o números de tarjeta de crédito por medio de un correo electrónico.

- Actualiza tu software: Ya sea en el teléfono o en el ordenador, asegúrate de que tu sistema operativo se mantiene actualizado.
- Navegue con cuidado: Evite visitar sitios web inseguros y no descargue nunca archivos adjuntos no verificados ni haga clic en enlaces de correos electrónicos desconocidos.
- Seguridad de las contraseñas: Todo lo anterior es higiene básica, y siempre es una buena idea. Pero los malos siempre están buscando una nueva forma de entrar en tu sistema. Si un hacker descubre una de tus contraseñas que utilizas para varios servicios, tiene aplicaciones que pueden vulnerar tus otras cuentas. Así que haz que tus contraseñas sean largas y complicadas, evita usar la misma para diferentes cuentas y, en su lugar, utiliza un gestor de contraseñas. Porque el valor de una sola cuenta de correo electrónico hackeada puede hacer que el desastre caiga sobre ti (Malwarebytes, 2020).

6.1.2 Virus informáticos

Un virus informático es una de las formas más comunes de piratería informática. Al igual que un virus de la gripe, está diseñado para propagarse de un huésped a otro y tiene la capacidad de replicarse. Del mismo modo, al igual que los virus de la gripe no pueden reproducirse sin una célula huésped, los virus informáticos no pueden reproducirse y propagarse sin una programación como un archivo o documento. En términos más técnicos, un virus informático es un tipo de código o programa malicioso escrito para alterar el funcionamiento de un ordenador y está diseñado para propagarse de un ordenador a otro. Un virus funciona insertando o adhiriéndose a un programa o documento legítimo que admita macros para ejecutar su código. En el proceso, un virus tiene el potencial de causar efectos inesperados o perjudiciales, como dañar el software del sistema corrompiendo o destruyendo datos.

¿Cómo ataca un virus informático? Una vez que un virus se ha unido con éxito a un programa, archivo o documento, el virus permanecerá latente hasta que las circunstancias hagan que el ordenador o el dispositivo ejecuten su código. Para que un virus infecte su ordenador, tiene que ejecutar el programa infectado, lo que a su vez hace que se ejecute el código del virus. Esto significa que un virus puede permanecer latente en su ordenador, sin mostrar signos o síntomas importantes. Sin embargo, una vez que el virus infecta su ordenador, el virus puede infectar otros ordenadores de la misma red. Robar contraseñas o datos, registrar las pulsaciones del teclado, corromper archivos, enviar spam a tus contactos de correo electrónico e incluso tomar el control de tu máquina son algunas de las cosas devastadoras e irritantes que puede hacer un virus. Mientras que algunos virus pueden ser juguetones

en su intención y efecto, otros pueden tener efectos profundos y dañinos. Por ejemplo, pueden borrar datos o causar daños permanentes en el disco duro. Y lo que es peor, algunos virus están diseñados para obtener beneficios económicos.

¿Cómo se propagan los virus informáticos? En un mundo constantemente conectado, se puede contraer un virus informático de muchas maneras, algunas más obvias que otras. Los virus pueden propagarse a través de los archivos adjuntos de los correos electrónicos y los mensajes de texto, las descargas de archivos de Internet y los enlaces fraudulentos de las redes sociales. Sus dispositivos móviles y teléfonos inteligentes pueden infectarse con virus móviles a través de descargas de aplicaciones sospechosas. Los virus pueden esconderse disfrazados como archivos adjuntos de contenido socialmente compartible, como imágenes divertidas, tarjetas de felicitación o archivos de audio y vídeo. Para evitar el contacto con un virus, es importante tener precaución al navegar por Internet, descargar archivos y abrir enlaces o archivos adjuntos. Para estar seguro, no descargue nunca archivos adjuntos de texto o de correo electrónico que no espere, ni archivos de sitios web en los que no confíe.

¿Cuáles son los signos de un virus informático? El ataque de un virus informático puede producir una serie de síntomas. Estos son algunos de ellos:

- Ventanas emergentes frecuentes. Las ventanas emergentes pueden incitarle a visitar sitios inusuales. O pueden incitarte a descargar antivirus u otros programas de software.
- Cambios en tu página de inicio. Tu página de inicio habitual puede cambiar a otro sitio web, por ejemplo. Además, es posible que no puedas restablecerla.
- Envío masivo de correos electrónicos desde su cuenta de correo. Un delincuente puede tomar el control de su cuenta o enviar correos electrónicos en su nombre desde otro ordenador infectado.
- Fallos frecuentes. Un virus puede causar daños importantes en tu disco duro. Esto puede hacer que su dispositivo se congele o se bloquee. También puede impedir que tu dispositivo vuelva a encenderse.
- Rendimiento inusualmente lento del ordenador. Un cambio repentino en la velocidad de procesamiento podría indicar que su ordenador tiene un virus.
- Programas desconocidos que se inician al encender el ordenador. Es posible que se dé cuenta del programa desconocido cuando inicie su ordenador. O puede darse cuenta al comprobar la lista de aplicaciones activas de su ordenador.

- Actividades inusuales como cambios de contraseña. Esto podría impedirle iniciar sesión en su ordenador.

¿Cómo ayudar a protegerse contra los virus informáticos? ¿Cómo puede ayudar a proteger sus dispositivos contra los virus informáticos? Estas son algunas de las cosas que puede hacer para ayudar a mantener su ordenador seguro.

- Utilice un producto antivirus de confianza y manténgalo actualizado con las últimas definiciones de virus.
- Evite hacer clic en los anuncios emergentes.
- Analice siempre los archivos adjuntos al correo electrónico antes de abrirlos.
- Analice siempre los archivos que descargue mediante programas de intercambio de archivos (Norton, 2020).

6.1.3 Robo de datos

(incluye: Robo de identidad asociado, información de cuentas de tarjetas de crédito, credenciales de clientes)

El robo de datos es el acto de robar información digital almacenada en ordenadores, servidores o dispositivos electrónicos de una víctima desconocida con la intención de comprometer la privacidad u obtener información confidencial. La información puede incluir cualquier cosa, desde información financiera, como números de tarjetas de crédito o cuentas bancarias, hasta información personal, como números de la seguridad social, números de permisos de conducir y registros sanitarios.

¿Cómo se produce el robo de datos? El robo de datos se produce por diversos medios. La mayoría de las veces ocurre porque alguien ha pirateado un sistema informático para robar información sensible, como su tarjeta de crédito o información personal, o porque un empleado de una empresa ha manejado mal la información. En un mundo cada vez más digitalizado, cientos de empresas y organizaciones diferentes tienen su información personal, como su número de la seguridad social, su dirección postal, su fecha de nacimiento y la información de su cuenta bancaria.

¿Cómo protegerse? El robo de datos es un problema real y puede ocurrirle a cualquiera. Aunque no hay forma de evitar por completo el robo de datos, hay varias medidas que puede tomar hoy para limitar su riesgo.

- Pagar en efectivo en lugar de con tarjetas de crédito o débito.
- Utilice una tarjeta de crédito o débito con tecnología de pin y chip.
- Proteja su ordenador de virus y programas maliciosos instalando, utilizando y actualizando el software antivirus y antiespía en todos sus ordenadores y dispositivos electrónicos.
- Mantenga todos los sistemas operativos y programas de software al día instalando regularmente las actualizaciones de seguridad, navegadores web, sistemas operativos y programas de software tan pronto como estén disponibles.
- No abra correos electrónicos dudosos ni archivos adjuntos, ya que podrían ser correos de phishing.
- Compruebe regularmente los extractos de su tarjeta de crédito y el informe de crédito para ver si hay cargos no autorizados y nuevas líneas de crédito.
- Utilice una contraseña fuerte y única para todos los sitios web que requieran un inicio de sesión. Cámbielas con regularidad, especialmente si la contraseña de una cuenta se ha visto comprometida en una filtración de datos.
- Utiliza sólo conexiones Wi-Fi seguras.
- Elimine correctamente los documentos que contengan información sensible destruyendo el papel y eliminando todos los datos de los dispositivos electrónicos (Michaud, 2021).

6.1.4 Correos basura

A veces se reciben correos electrónicos no deseados. Por un lado, esto supone una gran pérdida de tiempo porque hay que clasificar los correos no deseados, pero por otro lado, los llamados correos spam también pueden contener peligros como virus o programas dañinos que se instalan en su ordenador cuando abre el correo y pueden, por ejemplo, espiar sus datos de acceso. El phishing es también un tipo común de estafa en línea en la que los delincuentes envían correos electrónicos con apariencia oficial para intentar que el usuario revele detalles que pueden ser utilizados para el robo de identidad.

- Por lo tanto:
    - Evite abrir los archivos adjuntos a menos que hayan pasado por un programa antivirus,
    - Acuérdate de cerrar la sesión, especialmente cuando utilices un ordenador público compartido,
    - eliminar todos los correos electrónicos de personas desconocidas,

- nunca respondas al spam.

- ¿Cómo identificar los correos basura?
  - Errores gramaticales y ortográficos
  - Correos en un idioma extranjero
  - Falta el nombre
  - Necesidad urgente de actuar, especialmente en combinación con una amenaza
  - Solicitud de introducción de datos personales (por ejemplo, PIN o TAN)
  - Solicitud de apertura de un expediente
  - Nunca ha recibido ningún correo electrónico del banco o no es cliente hasta ahora (Verbraucherzentrale, 2021).

Referencias

Carretero, S.; Vuorikari, R. y Punie, Y. (2017). *DigComp 2.1: El marco de competencia digital para los ciudadanos con ocho niveles de competencia y ejemplos de uso*. doi:10.2760/38842

Michaud, Katelyn. (2021). *¿Qué es el robo de datos?* https://safety.lovetoknow.com/personal-safety-protection/what-is-data-theft

MOZ (2022). *Operadores de búsqueda de Google.* https://moz.com/learn/seo/search-operators

Norman, C.; Skinner, H. (2006). eHealth Literacy: Essential Skills for Consumer Health in a Networked World. *J Med Internet Res* 8(2):e9. DOI: 10.2196/jmir.8.2.e9

Norton. (2020). *¿Qué es un virus informático?* https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

Malwarebytes. (2020). *Definición de hacking: ¿Qué es el hacking?* https://www.malwarebytes.com/hacker

Verbraucherzentrale (2021). *Spam: E-Mail-Müll im Internet.* https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/spam-emailmuell-im-internet-10757

WebsiteSetup (2021). https://websitesetup.org/evaluating-online-resources

Organización Mundial de la Salud [OMS]. 2017. *Digital Health Literacy.* https://www.who.int/global-coordination-mechanism/working-groups/digital_hl.pdf