Proyecto IDCAP: Mejorar la Competencia Digital en Personas Adultas

Numero de Proyecto: 2018-1-PL01-KA204-051003

¿Como proteger mi dispositivo?

Area de competencia: dispositivos de proteccion

Introduccion

Este módulo cubre los temas más importantes que vale la pena prestar atención cuando se trabaja con dispositivos digitales a diario: su teléfono inteligente, tableta, ordenador portátil y ordenador de escritorio.

Los objetivos del módulo son:

- explicar los métodos para proteger los dispositivos de ser accedidos físicamente por otros - PIN, entrada de contraseña, huellas dactilares, reconocimiento facial;
- enseñar cómo proteger los dispositivos digitales de ser accedidos de forma remota por otros usuarios – instalación y uso de programas antivirus y aplicaciones. Descarga segura de aplicaciones y documentos al dispositivo;
- explicar los beneficios de respaldar la información sobre el dispositivo digital y ofrecer posibilidades tehnicales.

1. Seguridad física de los dispositivos

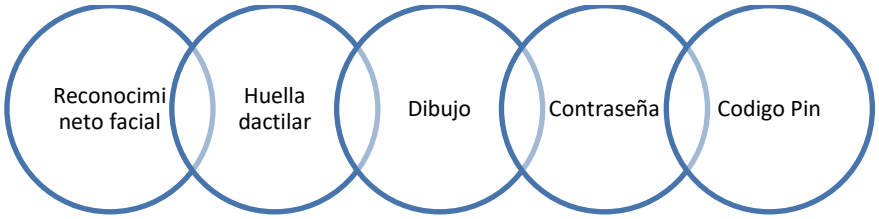
Muchas personas hoy en día tienen un ordenador, un teléfono móvil y algún otro dispositivo que quieren proteger de los daños. Las amenazas son: actividad física humana (imprudencia,descuido, fallo, mal funcionamiento), malware (virus), hackers, fenómenos naturales / catástrofes, fallos técnicos, etc. Como cualquier cosa importante, queremos mantener los datos seguros. Hay muchas maneras de proteger su dispositivo: mediante el cifrado de su dispositivo, usando un código pin, utilizando bloqueos de huellas dactilares, reconocimiento facial, la función “encontrar mi dispositivo",bloquear y eliminar sus datos.

Factores que pueden aumentar la seguridad fisica de su pispositivo

- contraseñas / PIN;
- dispositivos especiales/sotware;
- seguro de los locales;
- uso adecuado del equipo (de acuerdo con los manuales de instrucciones);
- proteccion contra el fuego o mojado.

Cuando se utilizan contraseñas / PIN y / o software especial/ huellas dactilares,el dispositivo no se puede utilizar en caso de robo. Hay programas disponibles para rastrear un dispositivo robado.

Ejemplos para desbloquear su teléfono :



Proteccion de la informacion mediante el uso de un almacenamiento de datos externo:

- Copiar archivos a / desde un almacenamiento de datos externo (como CD, DVD o unidades flash USB) para tareas específicas,
- Al conectar el almacenamiento de datos externos al ordenador, escanee con un programa antivirus,
- Tenga mucho cuidado al usar el almacenamiento de datos externo proporcionado por amigos y conocidos,
- No almacene información importante y sensible en sus dispositivos innecesariamente.

2. Cifrado

El cifrado es el proceso de cifrado de información legible para que solo pueda ser leída por alguien que tenga un código secreto o una clave de descifrado. Esta es una manera de ocultar / bloquear la información hasta que se introduce el código y la información se convierte de nuevo en texto legible. Muchas personas utilizan el cifrado de datos para la seguridad de los datos confidenciales.

Tiene la capacidad de cifrar tanto los datos que almacena en sus dispositivos como los datos que envía. Hay varios métodos de cifrado. Por ejemplo, FDE es un cifrado de disco completo que se utiliza para cifrar todo el disco del sistema. Esto significa que toda la información,está oculta.

El cifrado en línea HTTPS se utiliza para proteger los datos que se envían. Esto significa que la información se cifra en el camino desde el navegador a la página de inicio. Los correos electrónicos y otros programas de comunicación también ofrecen métodos de cifrado que debe establecer usted mismo. La clave para un cifrado exitoso es mantener su clave o contraseña segura y hacerla lo mas compleja posible. Puede utilizar el administrador de contraseñas para recordar contraseñas.

El cifrado puede funcionar si el dispositivo es seguro. La consideración principal es asegurarse de que el dispositivo no está comprometido, libre de virus, o no

comprometido de ninguna otra manera. Asegúrese de que el dispositivo no sea accesible para personas no deseadas. Recuerde, si la aplicación o programa que desea utilizar no necesita cifrado, a continuación, considere otras opciones. Es importante utilizar aplicaciones seguras o software que no le ponen en peligro.

3. Codigo Pin/ dibujo

Un Código pin es un mecanismo de seguridad especial que se aplica para autorizar su cuenta bancaria, dispositivo o cualquier información confidencial. El código pin no debe ser revelado a nadie. Se recomienda cambiarlo de la misma manera que cambia su contraseña. Debe recordar su código Pin.

Para protegerse, no realice pagos desde ordenadores públicos o desde dispositivos desconocidos. Hay programas que pueden leer todo lo que el usuario introduce utilizando el teclado - incluyendo códigos pin. Por lo tanto, utilice el código PIN solo en su dispositivo privados. **Los códigos pin de tipo dibujo** también están disponibles, así que ten cuidado, ya que las personas tienden a crearlos demasiado simple, estándar, y la pantalla del dispositivo necesita ser limpiada regularmente para evitar que sea rastreado por líneas de arrastre. Al introducir un pasador o dibujo, es aconsejable cubrir una mano con la otra a medida que escribe, y asegurarse de que la pantalla del dispositivo no es demasiado brillante y claramente visible desde otros ángulos.

4. Huella dactilar

El sensor de huellas dactilares está disponible para varios dispositivos. Es un dispositivo biométrico que ayuda a identificar rápidamente a una persona. Se puede configurar en casi todos los dispositivos inteligentes que tienen un sensor de huellas dactilares incorporado. La huella digital puede ser menos segura que

un código PIN complejo, una combinación o una contraseña. Hay varias maneras de eliminar físicamente su huella digital de su dispositivo. Tenga en cuenta que la eliminación de la huella digital también se puede hacer de otras cosas cotidianas. Si su dispositivo no es seguro, su huella digital se puede leer como cualquier información de su dispositivo.

Se utiliza un proceso de autorización de dos factores para el tipo de autenticidad de huellas dactilares. Esto significa que normalmente también se utiliza el código PIN. Si los dispositivos no pueden reconocer o leer la huella digital, entonces se utiliza el código pin. Además, después de las actualizaciones o el encendido, el código PIN se utiliza por motivos de seguridad.

Si eliges usar tu huella digital como método para desbloquear el dispositivo, ve a la configuración de tu dispositivo y sigue los pasos adecuados. La primera configuración es muy importante - sus dedos son escaneados. Es aconsejable mantener el teléfono en una posición natural y asegurarse de que siga todos los pasos requeridos.

Puede haber problemas con su uso si el sensor está dañado, sucio o no se ha realizado la actualización del dispositivo necesaria. Varias empresas prefieren reemplazar su huella digital con una herramienta de reconocimiento facial.

5. Reconocimiento facial

El reconocimiento facial es un tipo de autenticación que requiere una cámara. Es una opción para desbloquear el dispositivo o para conectarse a aplicaciones específicas mostrando su cara en la cámara. Los expertos que trabajan en inteligencia artificial durante muchos años reconocen ahora que el reconocimiento facial es una de las formas más seguras de conectarse al sistema.

Para configurar el reconocimiento facial, necesitas un dispositivo, una cámara y una configuración facial adecuados: tendrás que escanear tu cara desde todos los lados para ser reconocida por tu dispositivo.

En la mayoría de los casos, el sistema de reconocimiento facial de un teléfono barato utiliza sólo una cámara orientada hacia adelante y algunos algoritmos no tan sofisticados - y tal vez incluso un flash para tomar una mejor foto. Sin embargo, una cámara 2D convencional sin sensor infrarrojo y un proyector de punto se puede engañar fácilmente mediante la visualización de una fotografía.

Si elige el reconocimiento facial como mecanismo de seguridad, se recomienda utilizar un dispositivo de alta calidad. Asegúrate de que funcione. Los expertos todavía están trabajando en la mejora de este sistema. Reconocen que el reconocimiento facial se utilizará en el futuro para acceder a sitios web específicos, artículos de tienda y otras actividades.

6. Encontrar tu teléfono

Los programas están diseñados para localizar y administrar su teléfono en cualquier momento. Esta función se utiliza si el teléfono se pierde o es robado. Puede localizar, eliminar datos, ver la carga de la batería y conectarse a una red Wi-Fi. Aunque tenga en cuenta que las características pueden variar dependiendo del sistema operativo.

Hay ambos programas integrados que le ayudan a realizar un seguimiento de la actividad de su teléfono y hay otros que se pueden descargar por separado y están disponibles para la compra.

Para utilizar esta función, debe activarla (en su dispositivo) y explorar las capacidades del dispositivo. Utilice la búsqueda en Internet para averiguar todo acerca de su dispositivo o consulte a la persona que puede ayudarle a hacerlo.

Google, también, es un servicio que te permite bloquear, llamar, cerrar sesión, etc, de forma remota. Su dispositivo se puede encontrar a través de Internet. La práctica muestra que esta característica se utiliza principalmente para bloquear el dispositivo y cerrar sesión en ciertos perfiles, pero no siempre es posible encontrar físicamente el dispositivo. Hay varios programas que cobran por esta función. El programa de Apple se llama "**Find My iPhone**", el programa de

Microsoft es "**Mi Windows Phone**" y Google ofrece "**Buscar mi dispositivo**". Estos son sólo algunos de los muchos programas.

7. Uso Seguro de las aplicaciones móviles

Es importante obtener aplicaciones móviles de una fuente segura y confiable. Los delincuentes han aprendido a crear y distribuir aplicaciones móviles infectadas que se parecen a las reales. Si instala una aplicación infectada de este tipo, los delincuentes pueden tomar el control de su dispositivo.

Para dispositivos Apple, solo puedes descargar aplicaciones para iPad y iPhone desde la App Store de Apple. En esta tienda, Apple ha llevado a cabo exámenes de seguridad en todas las aplicaciones móviles antes de su lanzamiento. Apple no puede "capturar" todas las aplicaciones infectadas, pero un entorno administrado reduce drásticamente el riesgo de infección. Si Apple encuentra una aplicación infectada en su tienda, se eliminará inmediatamente de la tienda. Windows Phone adopta un enfoque similar para administrar aplicaciones.

Android te da la opción de descargar la aplicación desde cualquier lugar en Internet. Usted necesita ser más cauteloso acerca de la aplicación que está instalando como no todos ellos se prueban. Google mantiene una tienda de aplicaciones: Google Play y sus aplicaciones tienen al menos una comprobación de seguridad básica. Se recomienda a nosotros el uso de aplicaciones sólo de Google Play. Evitar aplicaciones de otros sitios web, ya que es relativamente fácil de distribuir aplicaciones maliciosas que infectan su dispositivo móvil. Para obtener más protección, instale el software antivirus en su dispositivo móvil.

Permisos. Una vez que haya instalado la aplicación desde una fuente de confianza, configúrela de acuerdo con sus preferencias y necesidades de privacidad. Siempre tenga en cuenta antes de dar permiso a una aplicación - ¿quieres darle permiso y realmente necesita la aplicación? Si dejas que la aplicación siempre sepa tu ubicación, puedes permitir que el desarrollador de la aplicación realice un seguimiento de tu movimiento, o incluso vender esa información a otros.

Actualizaciones. Las aplicaciones móviles deben actualizarse regularmente. Los delincuentes siempre buscan vulnerabilidades en las aplicaciones. La mayoría de los dispositivos le permiten actualizar las aplicaciones automáticamente. Si esto no es posible, comprueba si hay actualizaciones de aplicaciones al menos una vez cada dos semanas. Por último, cuando se actualiza una aplicación, revise siempre qué cambios se realizan en los permisos de la aplicación.

8. Bloquear y limpiar

Bloquear su dispositivo es una manera muy simple de protegerse de daños o divulgación de información. Además, conectando físicamente el dispositivo al escritorio, el lugar de trabajo tiende a disuadir a los ladrones de obtener el dispositivo. Sólo una llave especial puede desbloquearlo.

Hay varias maneras que pueden proteger nuestro dispositivo no sólo físicamente. Un usuario no debe salir de su lugar de trabajo con un lugar de trabajo no segura: para ausencia temporal - Bloquear **ordenador; (Windows + L), más tiempo desactivado - Cerrar sesión o Apagar**. Para teléfonos y tabletas, puede configurar el dispositivo para que se bloquee automáticamente después de un cierto número de segundos. La mayoría de los dispositivos tienen un botón de apagado único y fácil de acceder que facilita el proceso.

Si no apagas el dispositivo, es posible que otras personas interfieran con el dispositivo. Cuando termines con tu trabajo, es más seguro apagar el dispositivo

por completo. La pérdida de su conexión a Internet impide que los piratas informáticos accedan al dispositivo. Mantener el dispositivo encendido siempre aumenta el riesgo.

Limpiar es la acción de hacer que la información del disco duro sea ilegible. Esto significa que los datos se eliminan, pero es posible recuperarlos con la ayuda de un programa adecuado. Al reemplazar un dispositivo, el disco duro, es aconsejable limpiarlo tanto como sea posible. Sin embargo, la forma más segura es destruir físicamente su disco duro para asegurarse de que sus archivos no se restauran.

9. Virus y antivirus

La ciberdelincuencia gana el control mediante la instalación de malware en ordenadores o dispositivos. Esto permite al criminal monitorear su actividad en línea, robar contraseñas o archivos, y utilizar su sistema para atacar a otros.

El malware es básicamente software informático utilizado con fines ilegales. El término proviene de la combinación de las palabras "software" y "malicioso". Los ciberdelincuentes instalan malware en ordenadores o dispositivos para obtener el control sobre ellos. Una vez instalado, el malware permite al criminal para supervisar su actividad en línea, robar contraseñas o archivos, y utilizar su sistema para atacar a otros. Malware puede infectar cualquier dispositivo, desde ordenadores Apple hasta cámaras de seguridad.

Los virus de cifrado son un tipo especial de malware que ahora se está extendiendo activamente en Internet, amenazando los documentos de las víctimas y otros archivos.

¡Protéjase – Detener el malware!

Desafortunadamente, los programas antivirus no pueden detener todo el software malicioso. Los ciberdelincuentes están constantemente desarrollando software nuevo y sofisticado que puede evadir los antivirus. Por supuesto, los

desarrolladores de antivirus están mejorando constantemente sus soluciones también. Los ciberdelincuentes explotan vulnerabilidades en su software. La versión de software más reciente o actual que tiene la menor vulnerabilidad. Por lo tanto, se recomienda:

- Mantener actualizados sus sistemas operativos, aplicaciones, navegadores, extensiones y otras aplicaciones. La solución más sencilla suele ser tener instaladas actualizaciones automáticas.

Una forma común en la que los ciberdelincuentes infectan ordenadores y dispositivos móviles es a través del desarrollo de software falso o aplicaciones móviles, haciéndolos disponibles en Internet, y engañando a las personas para que los instalen voluntariamente.

- Descargar e instalar programas sólo de tiendas en línea de confianza, y estudiar comentarios de programas y evitar aquellos que son poco utilizados o tienen sólo unas pocas críticas positivas.
- Elimine una aplicación que ya no necesite.
- Los ciberdelincuentes a menudo manipulan a las personas para configurar su propio malware, por ejemplo, pueden enviarle un correo electrónico que contiene un archivo adjunto o enlace en el texto y puede parecer que proviene de un amigo o su banco. Desafortunadamente, al hacer clic en un enlace o descargar un archivo adjunto, el malware se instala en su sistema.
- Realice copias de seguridad periódicas de sus sistemas y archivos, ya sea en la nube o sin conexión, como en un disco duro externo.

10. Pragramas con y sin licencia

Si el programa tiene un precio, debe ser comprado y descargado legalmente. También debe prestar atención a dónde descargar sus programas. No haga esto en sitios web sospechosos - puede poner en peligro su dispositivo y otro software

en tu ordenador. Los usuarios de ordenadores deben tener en cuenta las leyes de derechos de autor que se aplican a libros, discos de vídeo y música y casetes, y software. Copiar, distribuir o utilizar programas informáticos sin el permiso del propietario de los derechos de autor se denomina piratería.

El uso ilegal de programas informáticos es, por ejemplo:

1. Instalación de un CD de software adquirido legalmente en varios equipos, si la licencia o acuerdo indica que puede instalarse en un solo equipo;
2. Copiar el programa para su instalación y distribución sin el permiso del autor;
3. Instalación de software desde un disco comprado ilegalmente.
4. Poseer copias ilegales de programas informáticos de Internet.

El software y otros tipos de archivos (textos, imágenes, etc.) se ofrecen para ser descargados de forma gratuita a través de Internet. Sus editores no siempre tienen el derecho de distribuirlos para su uso por otros. Por lo tanto, debe asegurarse de que está legalmente permitido hacer copias antes de descargar.

11. Descargas

La descarga es el proceso de almacenar archivos desde un servidor de red a un dispositivo de almacenamiento. La descarga de archivos es necesaria si el usuario desea obtener los archivos ofrecidos en el sitio web, como documentos, imágenes, música, vídeos y software.

Para guardar un archivo o imagen en su ordenador o dispositivo, descárguelo. El archivo se guardará en la ubicación de descarga predeterminada.

Puede descargar diferentes tipos de archivos:

Tipo	**Formato**	**Ejemplo**
Texto	Docx, txt	Kopsavilkums.docx

Tipo	Formato	Ejemplo
Imagen	Jpg. Gif, png.	IMG0034.jpg
Audio	Mp3, wma	Voice.mp3
Video	Avi, mpg, mpeg	Ceplis.avi
Programas	Exe	Skype.exe
Archivo	Zip, rar	Arhivs.zip

La opción de descarga de archivos se puede especificar de diferentes maneras, pero normalmente se caracteriza por un enlace o el botón de descarga (Descargar).

12. Navegadores

Un navegador una una aplicacion para ver páginas web. Para ver una pagina web, primero se descarga o se transmite desde el sevidor web global al ordenador del Usuario antes de abrirse.

Para utilizar los servicios de Internet, necesita:

- Dispositivo programable con capacidad de conexión de red;
- Un proveedor de servicios de Internet (ISP) que garantiza que el dispositivo se puede conectar a Internet (puede ser necesario hardware adicional);
- Navegador de Internet.

Algunos ejemplos de navegadores incluyen:

No es seguro abrir ninguna página porque hay riesgos de que la página contenga virus, que también pueden abrir páginas fraudulentas que suplantan información.

Hay signos por los que puede suponer que una página web es segura. Las dos características más sencillas que indican la seguridad de una página se muestran en la barra de direcciones:

1. **https** antes de la dirección (indica que la información se transmite al ordenador de forma cifrada);
2. El símbolo de "bloqueo" normalmente bloqueado (el símbolo de bloqueo puede variar en diferentes navegadores de Internet).

La descarga de una página se detiene si:

- La descarga se retrasa;
- Detecta durante la descarga, falta la información necesaria para la página.

La página necesita actualizarse si:

- No se pudo cargar la página. Por ejemplo, algunas imágenes tienen cuadrados con cruces rojas en la página o no toda la información está disponible;
- La página no ha sido vista por el usuario durante algún tiempo y la información de la página ha cambiado durante este tiempo (la página no se actualiza automáticamente).

13. Copias de datos

Es importante almacenar datos no sólo en un ordenador, sino también en algún otro lugar. En este caso, siempre es posible restaurar datos importantes en caso de cualquier problema con el ordenador.

Datos generalmente almacenados en el ordenador:

- fotos;
- documentos de trabajo;

- programas importantes, software;
- proyectos de vídeo y audio;
- archivo de correo electrónico y correos electrónicos de amigos.

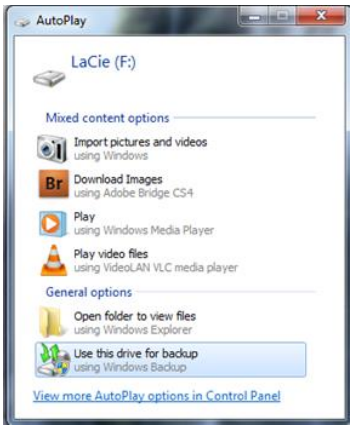
Si cree que no necesita copias de datos, recuerde que hay muchas maneras de perder documentos importantes.

- La forma más sencilla de perder todos sus datos es perder su ordenador o si es robado (esto se aplica más a los portátiles).
- Existe la posibilidad de eliminar datos accidentalmente o copiar sobre otra cosa en documentos importantes.
- Su ordenador puede estar infectado, y el malware puede corromper ciertos datos o incluso dañar su disco duro.
- Puede haber algunos problemas técnicos (incluyendo la rotura del disco duro - nada es eterno) que puede causar la pérdida de algunos datos.

Hacer copias de datos.

A un ordenador Windows:

- **Comprar un dispositivo de almacenamiento** externo. Puede ser cualquier unidad flash USB o disco duro externo. Es deseable comprar un dispositivo que tenga al menos el doble de espacio que la memoria de su computadora.
- La primera vez que conecte un dispositivo de almacenamiento externo a su ordenador, le ofrece la opción de usarlo como un lugar para almacenar datos. Si esta opción no aparece, simplemente escriba el nombre del programa en la ventana de búsqueda "Copia de seguridad".



- Se abrirá la siguiente ventana, donde tendrá que hacer clic en "Configurar copia de seguridad". A continuación, deberá seleccionar el disco externo en el que desea realizar una copia de seguridad de los datos. Al final, tendrá que hacer clic en "Guardar configuración y ejecutar copia de seguridad".
- Después de completar estos pasos, Windows hará la primera copia de seguridad de los datos (la clave es no quitar el disco de almacenamiento externo). Puede seleccionar "Cambiar programación" a continuación y aparecerá la siguiente imagen. La figura muestra que se le da la opción de elegir la programación cuando se restaurarán las copias de datos. Se le ofrece la oportunidad de hacer esto una vez al día, semanal y mensualmente. Lo principal a recordar es que el dispositivo al que está realizando la copia de seguridad debe estar conectado a un ordenador a la hora y día seleccionados.

Hacer copias de datos en un ordenador Mac OS.

Esto es muy parecido a lo que ocurre con un ordenador Windows. Al insertar un disco de almacenamiento externo, podrá usarlo como ubicación de copia de seguridad. Debe elegirlo o pasar por Preferencias del Sistema -> Time Machine. A continuación, seleccione el disco de almacenamiento externo necesario y haga una copia de los datos que contiene.

Hacer copias de datos en un teléfono móvil.

Una forma muy conveniente de hacer una copia de seguridad de tus contactos y calendario es con tu cuenta de Google (correo electrónico de Gmail). Con la configuración de cuenta y sincronización, puede activar la función de copia de seguridad en cualquier momento. Una cuenta de Google debe aparecer junto a tus cuentas si has accedido a ella desde tu teléfono. La ventaja de utilizar dicha copia de contactos es que cuando cambias de teléfono, los datos se copiarán automáticamente en el nuevo dispositivo. En Internet, puedes ver información sobre tus contactos a la izquierda haciendo clic en Gmail. Aparte de las capacidades que ofrece Google, hay otros tipos de software que ofrecen opciones de copia de seguridad. Una opción es simplemente copiar datos importantes conectando su teléfono a un ordenador. También puede encontrar programas individuales en Internet que proporcionan copias de seguridad. Si usted está buscando uno que sea adecuado para usted, es importante asegurarse de que es adecuado para el sistema operativo de su ordenador.

Hacer copias de datos en internet.

De forma gratuita, este servicio suele estar disponible con limitaciones de memoria (aproximadamente 5GB-7GB). El uso de este servicio le permite almacenar sus datos más importantes en Internet, lo que significa que puede acceder a ellos desde cualquier lugar y desde su ordenador. El proveedor de servicios se asegura de que estos datos se almacenan de forma cifrada. Ejemplos de estos proveedores de servicios son www.mimedia.com y www.backup.comodo.com Por supuesto, este tipo de almacenamiento de datos es conveniente en términos de acceso, pero no se excluyen varios problemas de seguridad.

Si hay una pérdida de datos, es fácil de restaurar desde una copia de seguridad. En Windows, escriba "Copia de seguridad" en la búsqueda del menú Inicio y, a continuación, haga clic en "Restaurar mis archivos". En los ordenadores Mac, pulse "Time Machine" y, a continuación, "Enter Time Machine". O, simplemente tome su dispositivo de almacenamiento externo, antes de que haya realizado

una copia de seguridad de sus datos, conéctelos a su computadora y copie los archivos que necesita.

Beneficios de hacer copia de datos.

1. **Beneficio moral** - usted no tiene que preocuparse de que nada le pase a su orddenador; puede estar seguro de que sus datos importantes no se perderán en ningún lugar!
2. **Beneficio financiero** - Si tiene problemas con su disco duro, puede ser bastante caro tener los servicios de un profesional para restaurar estos datos. Si tiene una copia de seguridad de sus datos importantes, no necesitará dichos servicios.

14. Dispositivo arraigado

El enraizamiento es un proceso que permite a los usuarios de teléfonos inteligentes, tabletas y otros dispositivos que ejecutan el sistema operativo móvil Android para obtener un control privilegiado (conocido como acceso robot) a través de varios subsistemas Android. El propósito de este proceso es superar las restricciones impuestas por los fabricantes en ciertos dispositivos. Por lo tanto, el rooteo le permite cambiar o reemplazar las aplicaciones y la configuración del sistema, ejecutar aplicaciones especializadas que requieren permisos de nivel de administrador o realizar otras acciones que no están disponibles para otro usuario normal de Android. En Android, el rooteo también puede hacer que sea más fácil eliminar y reemplazar completamente el sistema operativo de su dispositivo, por lo general con una versión más reciente de su sistema operativo actual.

Resumen

Al aprender los temas tratados en el módulo, los alumnos saben cómo proporcionar seguridad física de los dispositivos y también entienden los principios del cifrado. Los estudiantes pueden reconocer y utilizar técnicas de protección de dispositivos digitales: reconocimiento facial, entrada de contraseña, dibujo de figuras en una pantalla de dispositivo digital y huellas dactilares.

Mediante el uso de técnicas descritas en el módulo, es posible localizar el teléfono perdido. Los estudiantes son informados sobre diferentes tipos de virus que amenazan los dispositivos y las posibilidades para evitarlos. Para mantener la seguridad de los dispositivos, los usuarios también deben prestar atención a las descargas y utilizar sólo programas legales y con licencia. Después de la información proporcionada los estudiantes pueden dominar los principios del uso de programas antivirus y aplicaciones, decir la diferencia entre los navegadores web y el uso de ellos.

Por último, los alumnos son conscientes de cómo hacer una copia de seguridad de la información en su dispositivo digital y también entienden el propósito del dispositivo rooteado.

Bibliografía

- Pieslēdzies, Latvija! (n.d.). *Esiet sveicināti datorskolā! Mācies pats*. [Online Course]. Tet.lv. https://www.tet.lv/piesledzies-latvija/materiali/start/
- Swedbank. (n.d.). *Swedbank privātpersonām*. Swedbank.lv. https://www.swedbank.lv/private
- Valsts reģionālās attīstības aģentūra. (n.d.). *Valsts pārvaldes pakalpojumu portāls.* Latvija.lv. https://www.latvija.lv/
- *Mana Latvija.lv. Dari digitāli!* (n.d.). Mana.latvija.lv. https://mana.latvija.lv/
- *Drošība internetā.* (n.d.). Mana.latvija.lv. https://mana.latvija.lv/drosiba/
- *E-rīki jeb ceļvedis e-pakalpojumu lietošanā*. (n.d.). Mana.latvija.lv. https://mana.latvija.lv/e-riki/
- *Esiet sveicināti Mācību e-vidē!* (n.d.). [e-learning environment]. Macibas.mana.latvija.lv. https://macibas.mana.latvija.lv/
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Cert.lv. https://www.cert.lv/lv
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Esidross.lv. https://www.esidross.lv/
- Uzdevumi.lv. (n.d.). Uzdevumi.lv. https://www.uzdevumi.lv/
- Baltijas Biroju Tehnoloģijas. (n.d.). *Astoņas digitālās prasmes, kas jāmāca bērniem*. Smartboard.lv. https://smartboard.lv/zinas/astonas-digitalas-prasmes-kas-jamaca-berniem/
- Brečko, B., Ferrari, A. (2016) *Patērētāju digitālo kompetenču sistēma*. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC103155/lfna28133lvn.pdf