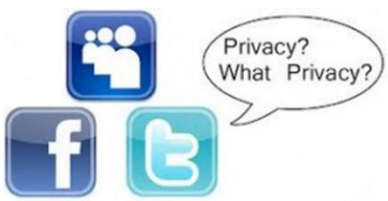
Proyecto IDCAP: Mejorar la Competencia Digital en Personas Adultas

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

¿Cómo proteger mis datos personales?

Area de competencia: Protegiendo datos personales y privacidad



Introduccion

El módulo cubre temas clave en el área de datos personales y protección de la privacidad. Los objetivos del módulo son:

- discutir los principios de seguridad en un entorno digital e informar sobre posibles amenazas – robo de información, correos electrónicos falsos y otros;
- para presentar los principios básicos de seguridad del uso de la tecnología - ¿deben seguirse las reglas del sombrero cuando se utiliza Internet en redes Wi-Fi disponibles públicamente, ¿qué es la conexión segura y qué son los archivos adjuntos de correo electrónico no seguros?
- para explicar el uso de contraseñas seguras - que son los principios que debe seguir al crear contraseñas? ¿Cómo usar contraseñas de forma segura en la vida cotidiana?

1.Introduccion a la seguridad en un entorno digital

1.1. Seguridad del Ordenador

La seguridad informática significa que nuestro equipo está protegido contra el acceso no autorizado, uso, divulgación, interferencia, alteración o destrucción. Es posible y necesario cuidar de su propia información y seguridad informática. La información almacenada en un ordenador y publicada en Internet puede afectar al bienestar personal, a la salud e incluso a la vida. Hay muchas amenazas - amenazas de privacidad, descifrado de contraseñas o piratería, divulgación de información personal, virus, carga, descarga y envío de archivos maliciosos, y personas maliciosas que quieren daño.

En Internet, tenemos acceso a redes sociales, chats online, foros, programas de chat especiales (como Skype), juegos y más. Si no se cumplen los estándares de seguridad necesarios, las personas con malas intenciones no solo pueden enterarse de sus datos privados, sino también utilizar su identidad (suplantarle).

Los virus informáticos se han convertido en un "valor clásico". Diferentes métodos se utilizan, por ejemplo, el usuario recibe un correo electrónico con un enlace a un sitio web popular como Youtube o Facebook con una película o imagen atractiva. Tratar de verlo infecta el ordenador indefenso de un usuario con un solo clic del ratón.

Los archivos adjuntos de correo electrónico son particularmente peligrosos porque pueden contener virus y otro software malicioso. Abrir un archivo adjunto en un correo electrónico puede instalar automáticamente malware en su ordenador y ni siquiera lo notará. Este tipo de malware puede afectar a los archivos de la computadora, robar contraseñas, o espiar a usted,

por lo que debe tener mucho cuidado al recibir mensajes con archivos adjuntos de destinatarios desconocidos.

Consejos para tratar archivos adjuntos no deseados

Consejo	Explicacion
Nunca abra archivos adjuntos de correo electrónico sospechosos	Incluso si recibes un correo electrónico de alguien que conoces, no hay garantía de que la persona realmente lo haya enviado. El malware puede enviarle automáticamente mensajes que contengan virus. Al recibir un correo electrónico con un archivo adjunto, es mejor pedirle al remitente que se asegure de que ha enviado un correo electrónico.
Actualizar el programa de antivirus	Si el programa antivirus no se actualiza, no puede proteger su equipo de virus.
Deje el *cortafuegos* del equipo encendido	Un firewall informático ayuda a evitar que las personas o el malware accedan a su ordenador a través de Internet.
Si es posible, antes de descargar los archivos adjuntos de correo electrónico, compruebe si hay virus	Muchos proveedores de correo electrónico en línea comprueban automáticamente los archivos adjuntos antes de descargarlos. Si el equipo le pide que compruebe si hay

Consejo	Explicacion
	virus descargando archivos adjuntos, hála por sí mismo.

1.2. Seguridad de datos – phishing

El phishing es un tipo de ciberdelincuencia que combina un conjunto de herramientas técnicas e ingeniería social para robar información sensible, personal y financiera de una víctima. Un atacante intenta pretender ser una organización real, una autoridad de confianza o una persona conocida.

La mayoría de las víctimas de phishing se animan a hacer clic en los correos electrónicos con los siguientes temas:

- ✓ Aviso formal de fuga de datos
- ✓ Aviso de entrega de UPS 1ZBE312TYI00015011B23
- ✓ Recordatorio de IT: Su contraseña caducará en menos de 24 horas
- ✓ Debe cambiar su contraseña inmediatamente
- ✓ Porfavor lea el aviso de su administrador

Cómo reconocer el phishing:

Demasiado bueno para ser verdad. Estos son mensajes, cartas, llamadas que te dicen que has ganado la lotería o que has sido seleccionado al azar para recibir un premio o servicio.

Oferta rápida. Frases: "última oportunidad", "sólo 1 hora", "solo hoy" y así sucesivamente indica un caso de phishing. Los estafadores utilizan la manipulación que crea un sentido de urgencia. Al recibir este tipo de mensaje, es aconsejable comprobar la veracidad de la información directamente con la empresa o proveedor de servicios.

Enlaces ocultos con otras palabras clave. Cualquier estafador utiliza palabras clave simples, frases que le llevarán a un sitio fraudulento. Estos enlaces a menudo ocultan un sitio completamente diferente de lo que piensas. Una muy buena manera de asegurarse de que lo que está abriendo es hacer clic en el botón derecho del ratón y seleccionar la opción Inspeccionar. Vea qué vínculo está asociado a ese enlace o palabra clave. ¿Qué esconde? Tenga cuidado porque las imprecisiones ortográficas a menudo ocultan enlaces falsos.

Extraños apegos. Si no espera ninguna información específica, no debe mirar los archivos adjuntos de correo electrónico. Uno de los métodos de la ciberdelincuencia es adjuntar un archivo que puede contener malware a un mensaje inocente. Es aconsejable comprobar el remitente, el propósito del mensaje antes de abrirlo. El único formato seguro que puede abrir un archivo. texto.

How to avoid phishing:

Consejo	Explicacion
Estese alerta	Siempre lea cuidadosamente los correos electrónicos de amigos y extraños
Tenga cuidado con los diversos canals de comunicacion	Preste atención a diferentes tipos de comunicación: correos electrónicos, anuncios, llamadas telefónicas y otros tipos de comunicación que soliciten cualquier información financiera.
Haga clic con cuidado	Evite hacer clic en "habilitar contenido", que le permite habilitar la vinculación adicional entre diferentes documentos.
No haga clic en los enlaces sospechosos	Evite hacer clic en enlaces en correos electrónicos, aplicaciones de mensajería o anuncios. Explore los enlaces individualmente, utilizando todos los recursos disponibles.

Verifique la confiabilidad del remitente	Asegurese de que el correo electrónico sea de una Fuente confinable.

Si usted es víctima de phishing:

1) Cambie las contraseñas de sus aplicaciones y cuentas en línea con otro teléfono u ordenador.
2) Analiza tu ordenador en busca de virus y comprueba si hay software malintencionado.
3) Denunciar el robo de datos a la policía y guardar una copia de la solicitud.
4) Informe a su organización / banco o la autoridad competente.

1.3. Seguridad del usuario del ordenador – informacion publicada en las redes sociales

Hay dos maneras de ver el concepto de seguridad del usuario del equipo. Es posible hablar del potencial de un ordenador para poner en peligro la salud de su usuario, como la posibilidad de una descarga eléctrica, aunque sea leve. Sin embargo, el riesgo más común para una persona es el riesgo de información autopublicada.

A menudo hay una falta de conciencia de cuántas amenazas variadas plantean las redes sociales.

Las redes sociales son una parte importante de la vida cotidiana de hoy en día - están acostumbrados a:

- Comunicar;
- Obtener información;
- Publicar y compartir información, etc.

Existen dos tipos de amenazas a las redes sociales: las amenazas **tecnológicas** y organizativas**.**

Las amenazas tecnológicas están relacionadas con diversas tecnologías y su uso en las redes sociales. **Las amenazas organizativas** están relacionadas con el comportamiento del usuario de Internet, acciones y actividades del propio usuario. Un ataque de amenaza organizacional suele ser causado por otra persona en la red social.

Las amenazas más comunes en las redes sociales son:

- ✓ varios tipos de malware o virus;
- ✓ ataques de phishing - mensajes de phishing o correos electrónicos que contienen enlaces a sitios web que están infectados con malware;
- ✓ envío de spam;

- ✓ clics ocultos que hacen que el usuario haga clic en algo que no sea el usuario previsto originalmente;
- ✓ varios tipos de perfiles forjados, algunos de los cuales son semiautomáticos o totalmente automatizados y otros son artificiales;
- ✓ los ataques de inferencia son técnicas de minería de datos e información que analizan los datos disponibles para obtener información adicional sobre la víctima. En las redes sociales, se utilizan para hacer referencia e identificar la información personal y sensible de los usuarios que el usuario no ha optado por compartir, como las creencias religiosas y la orientación sexual. El ataque a la red social se basa en la información disponible en los perfiles de la víctima y sus amigos.
- ✓ cibermobing - humillación emocional utilizando la tecnología moderna. Ejecución hipotecaria, humillación, sexting, acoso, envío de fotos desagradables, burlas, mentiras sobre la identidad para obtener información personal, acceder a la información de otras personas, rastrear, etc.

Para evitar amenazas, se pueden utilizar diferentes soluciones ofrecidas por las redes sociales:

- ✓ mecanismos de autenticación,
- ✓ bloqueando a los usuarios,
- ✓ ajustes personales de los usuarios,
- ✓ Opción "usuario de informe".

Las soluciones enumeradas se pueden utilizar con éxito para proteger al usuario de perfiles falsos, abuso emocional, comportamientos ingenuos y de riesgo.

Varias empresas de soluciones de seguridad - AVG, Avira, Kaspersky, Panda, McAfee, Symantec - ofrecen soluciones de seguridad de Internet a los usuarios de redes sociales. Su software por lo general incluye un programa antivirus y firewall, a veces ofreciendo protección anti-spam y anti-phishing para los usuarios de Internet. Este tipo de software ayuda a los usuarios de redes sociales

a proteger sus computadoras personales de amenazas como malware, clics ocultos y phishing.

Consejos para redes sociales seguras

Tipo	Ejemplo
Destino	Piense cuidadosamente antes de obtener información sobre la observación. Todo lo que publiques es probable que se vuelva público en algún momento y puede afectar negativamente tu reputación y futuro. Tenga cuidado - otros también pueden publicar sobre usted. Es posible que incluso necesite pedirle a alguien que elimine la información que han publicado sobre usted.
Privacidad	Prácticamente todas las redes sociales tienen opciones de privacidad adicionales - configurarlas siempre que sea posible. Por ejemplo, ¿realmente necesita el sitio web conocer su ubicación? Verifique las opciones de privacidad regularmente y asegúrese de que funcionan de la manera en que usted piensa.
Contraseñas	Proteja sus cuentas de redes sociales con una contraseña o frase de contraseña lo suficientemente larga y única. Una frase de contraseña es una contraseña que consta de varias palabras, por lo que es fácil de recordar y escribir, pero mucho más difícil de adivinar para los delincuentes cibernéticos.
Fraude	Al igual que los correos electrónicos, las notificaciones de redes sociales se pueden utilizar para varios intentos de fraude. Por ejemplo, una persona malintencionada podría intentar colarse en la contraseña o la información de tu tarjeta de crédito. Tenga cuidado con los enlaces que recibe.
Contactos	No se ponga en contacto con extraños y personas sospechosas. Crear perfiles falsos es muy simple, y muchas

Tipo	Ejemplo
	personas lo utilizan para mentir sobre su identidad. El propósito de estos perfiles es engañar, ganar su confianza y utilizarlo en su contra.
Terminos de uso	Familiarizese con los términos de las redes sociales – cualquier cosa que publique puede convertirse en una propiedad de una red social
Trabajo	Si desea publicar algo sobre su trabajo, primero averigue si es aceptable para su gerencia

Fraude personalizado

La nueva forma de ciberdelincuencia - fraude personalizado - se está volviendo cada vez más popular. Los ciberdelincuentes recopilan o compran información sobre millones de personas y luego usan esa información para personalizar los ataques. Cuanto más sepas sobre estos ataques, más fácil será detectarlos y detenerlos.

Las estafas por correo electrónico y teléfono no son nuevas, los ciberdelincuentes han estado tratando de engañar a la gente durante años. Algunos ejemplos son "Has ganado la lotería" o el famoso fraude del Príncipe de Nigeria. Pero en estos ataques tradicionales, los ciberdelincuentes no saben con qué van a lidiar. Simplemente hacen un correo electrónico general y lo envían a millones de personas. Debido a que estas estafas son tan genéricas y uniformes, por lo general son fáciles de reconocer. El fraude personalizado es diferente, el delito cibernético se investiga primero, y se prepara un correo electrónico adecuado para cada víctima. Lo hacen recopilando información o comprando una base de datos de nombres de personas, contraseñas, números de teléfono y otra información. Esta información es fácilmente accesible gracias a muchos sitios web hackeados. También a menudo está disponible gratuitamente en los

sitios de redes sociales y en los recursos disponibles al público de las autoridades públicas.

El ataque funciona así: encuentran o compran información sobre los nombres de usuario y contraseñas de las personas obtenidas de sitios web hackeados, luego encuentran su dirección de correo electrónico e información relacionada con usted en tal base de datos y se la envían a usted (así como a todos los demás en esta base de datos) - un correo electrónico con información sobre usted, incluyendo la contraseña que utilizó en el sitio web hackeado. Los delincuentes cibernéticos le dan esta contraseña como "prueba" de que su ordenador o dispositivo ha sido hackeado, lo que obviamente está mal. Los ciberdelincuentes también afirman que usted ha estado escabulléndose en el material pornográfico en Internet después de la piratería. El correo electrónico amenaza con que, si usted no paga el rescate, evidencia de sus actividades en línea vergonzosas serán enviados a su familia y amigos.

La clavees, en esto y casi todos estos casos, los ciberdelincuentes no han hackeado su dispositivo. Ni siquiera saben quién eres o qué sitios web visitas. Los estafadores simplemente están tratando de usar algunas de las cosas que saben acerca de usted para intimidar y hacerle creer que han hackeado su máquina y hacerle pagarlos. Recuerde, los malos pueden utilizar las mismas técnicas para llamadas telefónicas fraudulentas.

¿Qué hacer? Reconocer tales correos electrónicos y llamadas telefónicas como fraudulentas. Es natural sentir miedo cuando alguien tiene su información personal. Pero recuerda, ¡el remitente está mintiendo! Un ataque es parte de una campaña masiva automatizada, no un intento de atacarte. Hoy en día, cada vez es más fácil para los delincuentes encontrar o comprar información personal, así que prepárate para ataques más personalizados en el futuro.

Signos para reconocer un ataque:

- Siempre sospeche cuando reciba un correo electrónico, mensaje o llamada telefónica muy urgente. Cuando alguien usa emociones como el miedo o la urgencia, tratan de hacerte prisa.
- Cualquier persona que solicite el pago en *criptomoneda BitCoin,* tarjetas de regalo u otros instrumentos de pago no rastreables.
- Si recibes un correo electrónico sospechoso, haz una búsqueda en Google para ver si alguien ha reportado un ataque similar.

Siempre trate de usar contraseñas largas y únicas para cada una de sus cuentas en línea. ¿No recuerdas todas las contraseñas? Utilice el administrador de contraseñas. Además, utilice la autenticación de 2 pasos siempre que sea posible.

1.4 . Huellas digitales

La huella digital es información que dejamos consciente o sin saberlo en el entorno virtual: información visual, de audio y escrita. También hay cierta información que no es autogenerada, sino creada por padres, amigos, trabajo, etc. No tener una huella digital hoy en día puede ser imposible l pero ser demasiado activo en las redes sociales también puede tener consecuencias negativas.

La huella digital se basa en su actividad en Internet: hábitos de compra, medios de comunicación, uso de dispositivos, plataformas que elija.

2. Principios basicos de seguridad

2.1. Conexión a internet

Para evitar que otras personas usen los datos de autenticación de otra persona, como el nombre de usuario y la contraseña, **¡debes asegurarte de que estás navegando de forma segura!**

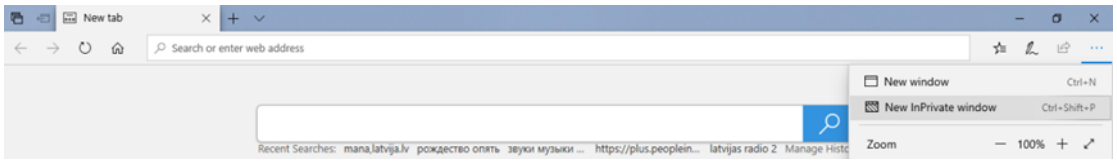
Durante la navegación, el navegador web almacena información sobre las páginas web que visita en el disco duro del usuario, que se puede dividir en tres tipos:

1) Una lista de las páginas que visita o el Historial de las páginas que visita.
2) Información contenida en páginas web, que normalmente se almacena en una llamada *Cachememory*. Normalmente se trata de una carpeta llamada *Archivos temporales* del nternet.
3) Cookies - pequeños archivos de texto. Estos archivos registran, las contraseñas, una lista de páginas visitadas y las fechas en que se vieron. Los navegadores transfieren esta información a los servidores de Internet. Por lo general, cuando abre un sitio web en su navegador, se le da la opción de aceptar / rechazar el uso de cookies. Se recomienda que acepte el uso de cookies en los sitios web a los que planea volver.

Cuando utilice un ordenador público, tenga en cuenta que otras personas podrán ver el historial del navegador de los sitios que el cliente ha visitado, así como los archivos descargados. Se recomienda que borre el historial de su navegador **Ctrl + H** y cookies para evitar cualquier situación desagradable. En muchos navegadores, puede hacerlo pulsando **Ctrl** + **Mayús** + **Eliminar** en el teclado.

Si no desea que su navegador registre su historial de actividad y nombres de usuario y contraseñas, le recomendamos que utilice la navegación privada. La navegación privada puede tener un nombre diferente en cada navegador, pero su esencia es la misma en todos los navegadores. Las siguientes imágenes muestran algunos ejemplos de cómo abrir una ventana de navegación privada.

Microsoft Edge



Google Chrome

Recuerde proteger su identidad, contraseñas y códigos de seguridad. Estos datos pueden ser utilizados por personas no autorizadas.

Se recomiendan las siguientes pautas básicas cuando se utiliza Internet:

- No proporcione su documento de identidad, códigos PIN y otros datos de acceso a otras personas;
- No publicar en Internet y enviar copias de documentos (pasaporte, documento de identidad, licencia de conducir) a través de correo electrónico, aplicaciones de comunicación o redes sociales;
- No reenvíe contraseñas y otra información privada en el-correos o mensajes de aplicaciones de comunicación (WhatsApp, Viber, Messenger, etc.) y redes sociales (Facebook, Twitter, etc.);
- No abra archivos adjuntos al recibir correos electrónicos sospechosos;
- No le cuentes demasiado a los demás sobre tu vida en Internet y las redes sociales, especialmente tu situación financiera, cosas nuevas, salir de casa, etc.;
- Piense cuidadosamente acerca de qué fotos publicar en Internet y cómo su publicación podría afectar algún día a la vida de una persona, como las relaciones con amigos, familiares, colegas, empleadores actuales o futuros;

1. Al recibir un correo electrónico de una autoridad pública o banco pidiéndole que envíe sus datos personales a la autoridad, nunca debe

hacerlo, ya que la autoridad nunca le pedirá los datos en forma de correo electrónico;

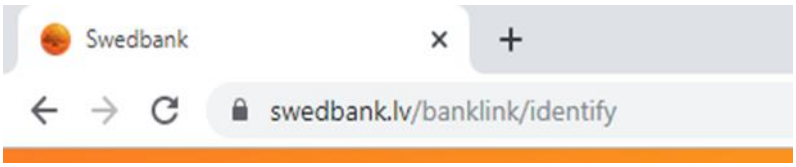
2. Al conectarse a los servicios electrónicos, asegúrese de que otras personas no puedan ver los datos de acceso introducidos y la información obtenida como resultado del servicio electrónico;
3. Asegúrese de que tiene un programa antivirus instalado en su ordenador conectado al internet;
4. Apague el ordenador durante la noche no sólo para ahorrar electricidad, sino también para reducir el riesgo de que el equipo sea hackeado y utilizado ilegalmente.

2.2. Coneccion segura – paginas web con certificado de seguridad

Seguridad significa la protección de los datos almacenados en redes informáticas y sistemas informáticos contra daños, pérdidas o accesos no autorizados. Hoy en día, la rápida disponibilidad de las redes informáticas, y especialmente de Internet, pide que este problema se aborde cada vez más. El principal problema de seguridad en las redes informáticas es su protección contra el uso no autorizado, por ejemplo, al realizar pagos electrónicos, existe la posibilidad de que los datos sean robados y mal utilizados.

El cifrado se utiliza para proteger los datos o el contenido de los mensajes contra el uso no autorizado. El cifrado es el proceso de procesamiento de datos y mensajes por parte del originador o del remitente del mensaje. Para utilizar dichos datos o el contenido del mensaje, debe descifrarse. La clave de cifrado se utiliza para cifrar y descifrar los datos.

Los sitios web que intercambian mensajes cifrados se denominan **sitios web seguros.**



Una connexion segura es usualmente representada por un icono 

Riesgos asociados a las actividades enlínea:

- divulgación involuntaria de información personal. Para utilizar los servicios ofrecidos en los sitios web, a menudo necesita registrarse con su información personal, como nombre, fecha de nacimiento, dirección. Antes de proporcionar esta información, asegúrese de que el sitio sea confiable y seguro;
- acoso o intimidación mediante la difusión de rumores maliciosos o mediante el envío de mensajes de amenaza;
- violencia potencial. Mediante el uso de redes sociales como Facebook.com y hacer nuevos contactos, se encuentra con un posible abusador, acosador, etc. Por lo tanto, es necesario pensar en qué información proporcionar sobre usted, y evaluar críticamente las ofertas realizadas.

En casos de fraude, acoso y humillación emocional, informar a los organismos encargados de hacer cumplir la ley, como la policía.

Seguridad infantil en Internet

Se recomiendan las siguientes medidas para proteger a los niños de los efectos negativos al usar Internet:

- Coloque la computadora en una habitación donde las actividades del niño en la web pueden ser monitoreadas;
- Cree cuentas de usuario secundarias con derechos de usuario de equipo limitados;

- Restringir la navegación activando filtros que prohíben el acceso a sitios web que contienen contenido de niños (drogas, pornografía, discursos de odio, armas, etc.);
- Restringir el uso de juegos dañinos prohibiendo juegos sobre ciertos temas;
- Limite el uso del equipo estableciendo una programación para el uso del equipo;
- Por ejemplo: **Cuentas** de usuario y seguridad familiar.

2.3. Wi-fi

Si su computadora, tableta o teléfono inteligente es compatible con WiFi (Internet inalámbrico),puede usar Internet sin tener que conectar un cable adicional a su dispositivo.

WiFi se puede utilizar tanto en casa como fuera de él. Si desea utilizar WiFi fuera de su casa, a menudo puede ver diferentes redes WiFi en sus dispositivos, pero no todos tendrán acceso porque la red puede estar protegida por contraseña.

En muchoslugares, por ejemplo, cafetería, tiendas, parques que tiene la opción de utilizar WiFi públicagratuita. La mejor manera de utilizar de forma segura las conexiones WiFi públicas en la ubicación pública es averiguar la contraseña y utilizar una conexión gratuita a través de un acceso cifrado. WiFi disponible públicamente sigue siendo una de las formas más utilizadas para conectarse ilegalmente a su dispositivo móvil y acceder a sus datos personales.

2.4. Archivos adjuntos de correo electronico, enlaces incluidos y mensajes de Spam

Spam o correo no deseado se llama spam y basura. Los spammers pueden enviar correo electrónico fácil y económico a miles de personas al mismo tiempo. Tales cartas son anónimas.

Cómo luchar contra el **spam**:

a) **Usa un bloqueador de spam. El bloqueador de spam puede reducir significativamente el** spam entrante. La mayoría de los proveedores de correo electrónico como Google Gmail tienen un bloqueador automático de spam. Si es necesario, también se pueden utilizar programas adicionales que bloqueen el spam. Sin embargo, en este caso también, existe la probabilidad de recibirlos.

b) **No responda al spam. Si recibe un mensaje de** spam interesante, puede verse tentado a responder a él o hacer clic en el enlace para optar por no recibir más correos electrónicos. Al responder al spam o al hacer clic en un enlace, usted está indicando sin saberlo que esta dirección de correo electrónico está funcionando, y que el nuevo spam se enviará a esta dirección en el futuro.

c) **Desactive las imágenes.** El correo electrónico puede contener imágenes que el spammer puede rastrear. Cuando abres spam y permites que las imágenes se descarguen en él, indicas que estás listo para recibir spam nuevo.

d) **Desactive el panel de visualización de mensajes**. Al hacer clic en una letra, se muestra automáticamente en el panel de presentación. Ver spam puede hacer que recibas más spam.

9) **Compruebe la carpeta de spam con** regularidad. A veces los bloqueadores de spam bloquean no sólo el spam, sino también los correos electrónicos legítimos. Por lo tanto, debe comprobar su carpeta de spam tan a menudo como sea posible para evitar perderse un mensaje importante. Compruebe la configuración de su cliente de correo electrónico para el que se permitirán los correos electrónicos y cuáles serán bloqueados.

☑	Crear varios correos electrinicos para usarlos para diferentes propósitos
☑	No revele su direccion de correo electrónico privado en redes públicas

	No cree direcciones de correo electrónico cortas. Muchos spammers envían correos electrónicos a correos electrónicos aleatorios. Cuanto más corta sea la dirección, más fácil será de descubrir.
	Si desea colocar un anuncio en Internet, cree una nueva dirección de correo electrónico para este fin.
	Si necesita revelar su dirección de correo electrónico, hágalo de una forma menos comprensible, como firstname.lastname@mail.com escribir como firstname-lastname-et-mail-dot-com.
	No utilice su dirección de correo electrónico privada al registrarse en redes públicas.
	No se arriesgue a utilizar la opción "cancelar suscripción", ya que esto a menudo sólo animará a enviarle más spam.
	Cambie su dirección de correo electrónico privada si fue descubierta y tiene una gran cantidad de spam.

2.5. Contraseñas seguras

Las contraseñas que elija son el escudo más importante y principal para proteger sus cuentas. Utilice una forma sencilla pero segura de crear y almacenar todas sus contraseñas.

Pasos para simplificar las contraseñas:

1. *Frases de contraseña*

La característica más importante de las contraseñas es que deben ser lo suficientemente largos, cuantos más caracteres haya en la contraseña, mejor.

Estas se llaman frases de contraseña, un tipo de contraseña segura que utiliza frases cortas o palabras casuales:

- *Es hora de un café negro fuerte!*
- *Playa de arrastre de caracoles desaparecidos*

Ambas contraseñas son seguras, con más de 20caracteres, y ambas contraseñas son fáciles de recordar, fáciles de escribir, pero difíciles de descifrar. Encontrará sitios web o situaciones que requieran el uso de símbolos, números o letras mayúsculas para la contraseña. ¡Pero recuerde, la clave de la contraseña es la longitud!

2. *Administradores de contraseña*

Necesitas una contraseña única para cada una de tus cuentas. Si usas la misma contraseña para varias cuentas, corres un gran riesgo. Todas las necesidades de un atacante cibernético son hackear el sitio web que está utilizando, robar todas las contraseñas, incluida la suya, y luego utilizar su contraseña para iniciar sesión en todas sus otras cuentas. Sucede más a menudo de lo que te imaginas. Es posible comprobar www.haveibeenpwned.com cuántos sitios web utiliza han sido hackeados y sus contraseñas pueden haber sido comprometidas. En tales casos, una solución es utilizar un administrador de contraseñas. **Password Manager es un programa informático especial que almacena todas sus contraseñas** de forma segura y cifrada. Sólo tiene que recordar una contraseña

- para su administrador de contraseñas.

Password Manager recupera automáticamente las contraseñas en los sitios adecuados cuando las necesita y le autentica. También tienen otras características, como la capacidad de guardar sus respuestas a preguntas de seguridad, le avisan si reutiliza su contraseña, una función de generador de contraseñas que le permitirá crear y usar contraseñas seguras, y muchas más. La mayoría de los administradores de contraseñas también se sincronizan de

forma segura a través de una variedad de dispositivos, por lo que tiene acceso fácil y seguro a sus contraseñas, sin importar el sistema que utilice.

Anote su contraseña de administrador de contraseñas en papel y guárdela en un lugar seguro en casa. Algunos administradores de contraseñas incluso le permiten imprimir una herramienta de recuperación del administrador de contraseñas. De esa manera, si olvida su contraseña de administrador de contraseñas, tiene un plan de copia de seguridad. Además, en una emergencia, cuando sea necesario, las personas de confianza podrán obtener información en su nombre.

3. *Autenticidad de dos factores*

La verificación en dos pasos (a menudo denominada autenticación de dos factores o autenticación multifactor) proporciona una capa adicional de seguridad. Requiere dos cosas cuando inicias sesión en tus cuentas, tu contraseña y un código numérico que se generaría en tu dispositivo inteligente o se enviaría a tu teléfono. Este proceso garantiza que incluso si los ciber atacantes han obtenido sus contraseñas, no pueden acceder a sus cuentas. La autenticación de dos factores es fácil de configurar y normalmente solo necesita usarla una vez cuando autoriza desde un nuevo dispositivo. Si utiliza un administrador de contraseñas, se recomienda proteger con una frase de contraseña segura y autenticación de dos factores.

La autenticación simplificada **de 2 pasos** significa que, además de introducir algo que conoces (una contraseña), también lo confirmas con algo que tienes (por ejemplo, un código de un teléfono móvil). También hay una autorización de tres pasos donde usted necesita confirmar el acceso con algo que es adecuado para usted - como una huella digital. La ventaja de la autenticación de 2 pasos es que el hacker también necesita acceso a su dispositivo móvil para hackear su cuenta.

3. Usando contraseñas

3.1. Contraseñas: El primer paso en la seguridad

Hay dos tipos de contraseñas: seguras e inseguras. La mayoría de las personas usan contraseñas inseguras: las contraseñas que son cortas, fáciles de recordar, contienen información personal (como nombre, apellidos, año de nacimiento, fecha importante, nombres de mascotas, nombres de familia) o incluso la misma contraseña que se utiliza para varias cuentas.

Hackers a menudo utilizan software de descubrimiento de contraseñas que comprueba muchas contraseñas hasta que encuentran la correcta. Las contraseñas inseguras se pueden descubrir muy rápidamente. La creación de contraseñase cure reduce la probabilidad de que los delincuentes revelen su contraseña y roben información personal y financiera.

Para proteger sus datos, hay principios básicos de seguridad que deben seguirse al usar una contraseña:

- Al introducir su contraseña, tenga cuidado de no permitir que otras personas vean sus dedos moverse en el teclado o la pantalla de su teléfono inteligente;
- Cambie su contraseña cada 3 meses;
- Tenga cuidado de no guardar el acceso automático a la cuenta. Utilice siempre los botones Salir, Cerrar sesión o Finalizar trabajo;
- Evite el uso de contraseñas en sitios de Internet de acceso gratuito.

3.2. Principios de creación de una contraseña segura

Al crear una cuenta de usuario en las redes sociales, utilizando un banco de Internet o cualquier otro portal de autoservicio, debe registrarse con su nombre de usuario, contraseña yother details.

Declaracion	Explicacion
Nunca use informacion personal	No uses nombres, cumpleaños ni nombres de familia como contraseñas. La información personal a menudo está disponible públicamente, por lo que puede adivinar la contraseña muy rápidamente.
Use contraseñas mas largas	La contraseña debe tener al menos seis caracteres. Para que tu contraseña sea más segura, puedes usar 12 o más caracteres para introducir tu contraseña.
Evite escribir sus contraseñas en su blog de notas o télefono	Si todavía desea escribir su contraseña, guárdela en un lugar seguro y no se la muestre a nadie. Se recomienda cifrar las contraseñas y no escribir la contraseña en sí.
Use contraseñas seleccionadas al azar	Las contraseñas aleatorias son las más seguras. En lugar de pensar en sus propias contraseñas, puede utilizar generadores de contraseñas. Las contraseñas aleatorias son más difíciles de recordar porque son creadas por dispositivos.
No use las mismas contraseñas para varias cuentas	Si alguien revela la contraseña de una cuenta, las contraseñas de las otras cuentas también serán vulnerables.
No use palabras que se puedan encontrar en el medio ambiente	Por ejemplo, contraseña *teacher1* será una contraseña insegura.
Incluya numeros, simbolos, y letras minúsculas en las contraseñas	Para crear una contraseña segura, puede reemplazar letras con diferentes símbolos, por ejemplo, basado en la palabra *lunes* y

Declaracion	Explicacion
	reemplazar la letra “o" y “a", puede crear la siguiente contraseña segura M*0nd@y!*

3.3. Estudio de caso y ejercicio practico

El Sr. Berzins, un hombre en sus mejores años, finalmente ha decidido comenzar a utilizar los servicios electrónicos y está listo para inscribirse en el sitio web de la Dirección de Seguridad del Tráfico Por Carretera (CSDD) para que pueda averiguar sobre sí mismo y su coche remotamente en el futuro.

Para crear o activar su cuenta CSDD, la primera vez que inicie sesión en el sitio web debe registrarse con su correo electrónico, crear su propia contraseña e introducirla. Después de que la cuenta se haya creado por primera vez, el acceso a su cuenta CSDD continuará tanto con el acceso establecido como con su acceso a la Banca por Internet.

La tarea de la situación es que el Sr. Berzins obtenga una contraseña para la recién creada cuenta CSDD en su sala de estar en su computadora, para que nadie pueda adivinarlo.

La escena común: el Sr. Berzins está sentado en la sala de estar de su casa de campo detrás de una computadora portátil abierta. En el fondo hay un sofá, en el que duerme un gato persa perezoso llamado Rudis. Mrs. Berzins está en el otro extremo del sofá y tejiendo un sombrero. Berzins tiene un perro negro llamado Poga a sus pies. En algún lugar en el fondo una chimenea está crujiendo cálidamente sobre el trofeo de caza Berzins, una cabeza de alce con cuernos, está colgando. Una pared de la sala de estar está ocupada por una estantería, donde se pueden ver obras reconocibles de diferentes escritores. En las portadas de algunos libros se pueden ver sus retratos, por ejemplo, Shakespeare, Dostoievski, Chéjov, etc. En la otra pared hay una foto de la familia

Berzin, donde se pueden ver a sus hijos adultos y nietos de Berzins y su esposa posando en las Cataratas del Niágara. Un poco más lejos está una hiedra colgando de un estante y un cactus crece en el alféizar de la ventana.

1) Cada uno de los objetos clave (elementos) importantes de la casa de la familia Berzins podría verse como una possible version positive o negative de la contraseña:

- Gato Rudis: *Rudis* / **RuD! $**
- Aficion de la esposa: Knitting /**Kn*tt*ng**
- Planta de interior: Cactus / **sutcac**
- Trafeo: Trophy / **Tr0fhy**
- Perro Poga: Poga / **50g** @
- Grandson12: Grandson12 / **Gr@nds0n**
- Esposa Rosalie: Rosalie / **R0s@lie**
- Chekhov: Chekhov / **Ch3kh0v**
- Dostoevsky: Dostoevsky / **D0$t0j3v$ky**

Summary

Este módulo mantuvo tres temas importantes relacionados con los datos personales y la protección de la privacidad. Como los conceptos básicos para la seguridad de su ordenador y los principios básicos de la protección de datos. Para evitar el phishing, los estudiantes se introdujeron en las formas en que los ciberdelincuentes actúan para robar información. Teniendo en cuenta que uno de los problemas más importantes de la protección de datos personales hoy en día es la publicación y el intercambio de información demasiado personal en diversas redes sociales, este módulo también proporcionó pautas de seguridad de este tema.

Con el fin de utilizar de forma segura dispositivos digitales fuera del hogar, este módulo cubrió los temas de las conexiones a Internet y los principios básicos de un uso seguro de Wi-Fi. También se explicaron los signos de correo electrónico inseguro y spam y se proporcionaron consejos sobre cómo utilizar las contraseñas de forma correcta y segura.

La sección final del módulo examina ejemplos de creación de contraseñas y describe la situación de la e - cómo se crean las contraseñas, que tipo de contraseñas deben ser considerados, ¿y que deben evitarse?

Bibliografia

- *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/
- Pieslēdzies, Latvija! (n.d.). *Esiet sveicināti datorskolā! Mācies pats*. [Online Course]. Tet.lv. https://www.tet.lv/piesledzies-latvija/materiali/start/
- SEB. (n.d.). *SEB privātpersonām*. Seb.lv. https://www.seb.lv/private
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Esidross.lv. https://www.esidross.lv/
- 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/
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Cert.lv. https://www.cert.lv/lv
- Uzdevumi.lv. (n.d.). Uzdevumi.lv. https://www.uzdevumi.lv/
- Latvijas Drošāka interneta centrs. (n.d.). Drossinternets.lv. www.Drossinternets.lv
- Draudzīgs internets. (n.d.). *Interneta Drosības ABC*. Draudzigsinternets.lv. www.draudzigsinternets.lv