Unidad de Contenido

[Ciberseguridad]

Proyecto: B-SAFE
Número: 2018-1CZ01-KA204-048148
Nombre del autor: EDIT VALUE®
Última fecha de procesamiento: 02.09.2020

Funded by the
Erasmus+ Programme
of the European Union

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

Ciberseguridad

Introducción

¿Has experimentado algún ataque malicioso en el que, por ejemplo, alguien intentara crear un documento importante o información privada a través de un enlace presente en un correo electrónico? Si te sucediera algo así, serías una víctima de la ciberseguridad.

Hoy en día, la ciberseguridad es una gran preocupación. La ciberseguridad implica la prevención y detección de ataques digitales, la protección de sistemas, hardware y software. También está relacionada con la prevención, detección, respuesta y recuperación de incidentes de ciberseguridad que pueden ser intencionales o no. Por lo general, los ataques cibernéticos tienen como objetivo acceder, cambiar, robar o destruir datos/información, extorsionar dinero o interrumpir negocios normales e infraestructuras críticas. ¿Sabías que según estudios recientes el coste total del cibercrimen para cada empresa es de alrededor de 12.000.000 €?

Por lo tanto, la ciberseguridad es un debate actual que necesita incorporar a la sociedad en su conjunto, ya que cada persona tiene un papel importante en la protección de su propia información digital.

Relevancia práctica: esto es para lo que necesitarás el conocimiento y las habilidades

Los ciberataques ocurren todo el tiempo, lo que significa que mantener el software, el hardware y los datos seguros y protegidos es más importante que nunca. A pesar de esto, solo hay unas pocas personas con estas habilidades, por lo que aprender a iniciarse en la ciberseguridad puede ayudarlo con su propia seguridad personal en Internet.

Después de aprender esta unidad de contenido, entrarás en contacto con el término ciberseguridad y con por qué la ciberseguridad es tan importante hoy en día. Además, en esta unidad de contenido sabrás lo que puedes hacer para tomar algunas medidas de seguridad cibernética en tu vida cotidiana.

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

Construye conocimiento – Ciberseguridad – definición y legislación

La protección de datos y la ciberseguridad se están convirtiendo en valores esenciales para la sociedad. Debido a eso, estas dos áreas han experimentado recientemente un desarrollo legal significativo y ahora están más consolidadas en la UE. Sin embargo, eliminar las amenazas y los ciberataques es casi imposible, por lo que es mandatorio utilizar medidas de ciberseguridad y fortalecer las capacidades de ciberseguridad.

La implementación de medidas efectivas de ciberseguridad es particularmente desafiante hoy porque hay más dispositivos que personas y los piratas informáticos se están volviendo más innovadores. En el mundo conectado de hoy en día, todos se benefician de medidas avanzadas de ciberseguridad. A nivel individual, un ataque cibernético puede resultar en cualquier cosa desde robo de identidad, intentos de extorsión, hasta la pérdida de datos importantes.

Pero, ¿qué entendemos exactamente por "ciberseguridad"?

Definición
La **ciberseguridad** es la práctica de defender ordenadores, servidores, dispositivos móviles, sistemas electrónicos, programas, redes y datos de ataques maliciosos, daños o acceso no autorizado. No existe una definición estándar de ciberseguridad, que sea especialmente aceptada universalmente. En otras palabras, la ciberseguridad está relacionada con todas las salvaguardas y medidas adoptadas para defender los sistemas de información y su uso contra el acceso no autorizado, los ataques y los daños para garantizar la confidencialidad, integridad y disponibilidad de datos.

1. Aplica conocimiento

Ejercicio OPCIÓN MÚLTIPLE

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

Objetivo específico asociado: OE_Medidas de ciberseguridad_O1_O1

Situación: ¿Cuál es el significado de ciberseguridad?
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- La ciberseguridad incluye la defensa de hardware y software.
- Los ataques cibernéticos están aumentando y ahora todo el mundo es más vulnerable a este tipo de incidentes.
- Las medidas efectivas de ciberseguridad incluyen la aplicación de múltiples medidas de ciberseguridad.
- La formación en ciberseguridad debe brindarse lo antes posible debido a la necesidad de la aplicación de múltiples acciones de ciberseguridad.

2. Construye conocimiento - Ciberseguridad - seguridad de contraseña

¿Conoces la forma más fácil para que un ciberdelincuente tenga acceso a tu banco, redes sociales, correo electrónico y otros datos privados? Es una contraseña débil. De hecho, la mayoría de las contraseñas se descifrarán en un "abrir y cerrar de ojos". Según el Centro Nacional de Seguridad Cibernética, las cinco contraseñas más comunes en 2019 fueron "123456", "123456789", "qwerty", "contraseña" y "1111111". Entonces, si tiene algunas de esas contraseñas o similares, eche un vistazo al siguiente ejemplo.

Example	
Amount of Time to Crack Passwords	
*****	
123456	0,29 ms
potato	1,37 ms
Potato	3,28 s
P0tat0	1h 23m.27s 0.10ms
P0tat0!	1 month, 3 weeks, 5 days and 21h 54min, 40s 8ms
lAtE27P0taT0s!	47623938 millenniums, 8 centuries, 73 years and 8 months

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

Uno de los problemas más comunes con las contraseñas es que generalmente son fáciles de adivinar. Muchas personas piensan que una contraseña corta con muchos tipos de caracteres diferentes es segura cuando, de hecho, la realidad es que la única forma de garantizar una contraseña verdaderamente segura es hacer que contenga al menos 14 algo arbitrarios. Además, como puedes ver, cuanto más compleja es tu contraseña, más difícil es adivinarla. Una contraseña segura es una combinación de letras (mayúsculas y minúsculas), números y símbolos. Una buena manera de nunca olvidar tu contraseña única es elegir una oración en lugar de palabras, mezclandola con caracteres alfanuméricos: ¡la mayoría de los sitios web incluso permiten espacios entre palabras!
Sin embargo, hay más aspectos a considerar al crear nuevas cuentas y perfiles digitales para tu seguridad y protección cibernética. A continuación puedes observar algunas cosas que "HACER" y "NO HACER" muy comunes con respecto a las contraseñas. Si sigues estas "reglas de oro", tus contraseñas son casi indescifrables para los piratas informáticos.

NO HACER: Use la misma contraseña para cada cuenta
HACER: Cree contraseñas únicas para cuentas y perfiles únicos

Una forma sencilla y usada a menudo para recordar las contraseñas es almacenarlas en una hoja de cálculo, disco duro o en notas personales. ¡Intenta memorizar tus contraseñas! También puedes configurar preguntas de seguridad en tus cuentas como medida de precaución. Sin embargo, en lugar de formular preguntas comunes como "¿Cómo se llama tu madre?" o "¿De dónde eres?" usa preguntas que solo tú puedas responder.

NO HACER: Guarda tus contraseñas en otra fuente
HACER: Memoriza tus contraseñas y configura las preguntas de seguridad en tus cuentas

Todos sabemos que hoy en día casi todos los sitios web requieren una cuenta y casi todos usan las mismas contraseñas para diferentes cuentas. Sin embargo, las personas a menudo olvidan que estas cuentas contienen información de identidad o financiera sobre ellas que puede ser robada o comprometida y al usar solo una contraseña se convierten en un blanco fácil para los ataques cibernéticos.

NO HACER: Compartir contraseñas con otros
HACER: **Sé reservado con tus contraseñas**

Inmediatamente después de usar la misma contraseña para cada cuenta, otro error común está relacionado con el hecho de que las personas comparten sus contraseñas con otros por correo electrónico, mensajes de texto o redes sociales.
Para mantener tus contraseñas seguras, debes cambiar las contraseñas con regularidad. Recuerda que en algún lugar del mundo hay un pirata informático que sigue intentando robar las contraseñas de los usuarios y, cuanto más tiempo tienen, mayor es el riesgo de que tengan éxito.

NO HACER: Elija una contraseña segura y quédese con ella

HACER: Cambia tus contraseñas cada tres meses

La mayoría de los navegadores y aplicaciones permiten a los usuarios guardar sus credenciales para que no tengan que insertarlas cada vez que desean iniciar sesión. A pesar de ser muy conveniente, ten en cuenta que si pierdes tus dispositivos y un extraño logra descifrar su contraseña de acceso, toda esa información es accesible para dicha persona.

NO HACER: Usa un factor de autenticación
HACER: Añade autenticación de dos factores para cada cuenta digital

Si utilizas la autenticación de dos factores en tus cuentas digitales, les añadirás una capa adicional de seguridad. Cuando alguien inicie sesión en tu cuenta desde una nueva ubicación, dispositivo o navegador, recibirás una contraseña, que deberás ingresar para iniciar sesión en tu cuenta. Aparte de eso, otro tipo de autenticación de dos factores es una huella digital, una huella de voz o un código enviado a tu teléfono. Muchas personas piensan que esto lleva mucho tiempo, pero si estás muy preocupado por tu privacidad, debes usar una autenticación de dos factores para tus cuentas digitales cuando esta opción sea posible. Cuando no tienes la opción de usar una autenticación de dos factores, debes seguir las recomendaciones que se mencionaron anteriormente.

2. Aplica conocimiento

Ejercicio ELECCIÓN ÚNICA

Objetivo específico asociado: OE_Medidas de ciberseguridad_02_01

Situación: por favor, seleccione de entre las siguientes oraciones la correcta.
Tarea: Elige la opción correcta siguiendo el principio de opción múltiple: solo una oración es verdadera.

- Se recomienda elegir una contraseña simple para memorizarla mejor.
- Algunas contraseñas únicas derivan de un nombre de pila, el nombre de un miembro de la familia o el nombre de una mascota.
- Cuantos más caracteres y símbolos contengan las contraseñas, menos difíciles serán de adivinar.
- Una contraseña segura tiene una combinación de letras mayúsculas y minúsculas, símbolos y números, y al menos ocho caracteres de longitud.

Ejercicio ELECCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Medidas de ciberseguridad_O2_O2

Situación: ¿Cuáles son algunas de las reglas para proteger tus cuentas digitales de los ataques cibernéticos?
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Usa la misma contraseña en múltiples sitios web / cuentas.
- Cambia las contraseñas regularmente.
- Guarda las credenciales de inicio de sesión en el navegador o la aplicación de un ordenador en particular.

- Una huella digital, una huella de voz o un código pin son una buena opción para una autenticación de dos factores.
- Al crear una nueva contraseña, evite las palabras que se encuentran en el diccionario, los pronombres, los nombres de usuario y otros términos predefinidos, así como las contraseñas de uso común.

3. Construye conocimiento – Compras en línea

Como hemos visto antes, la ciberseguridad evoluciona la conexión entre las personas y la aplicación de prácticas que tienen como objetivo proteger la información de ataques maliciosos.

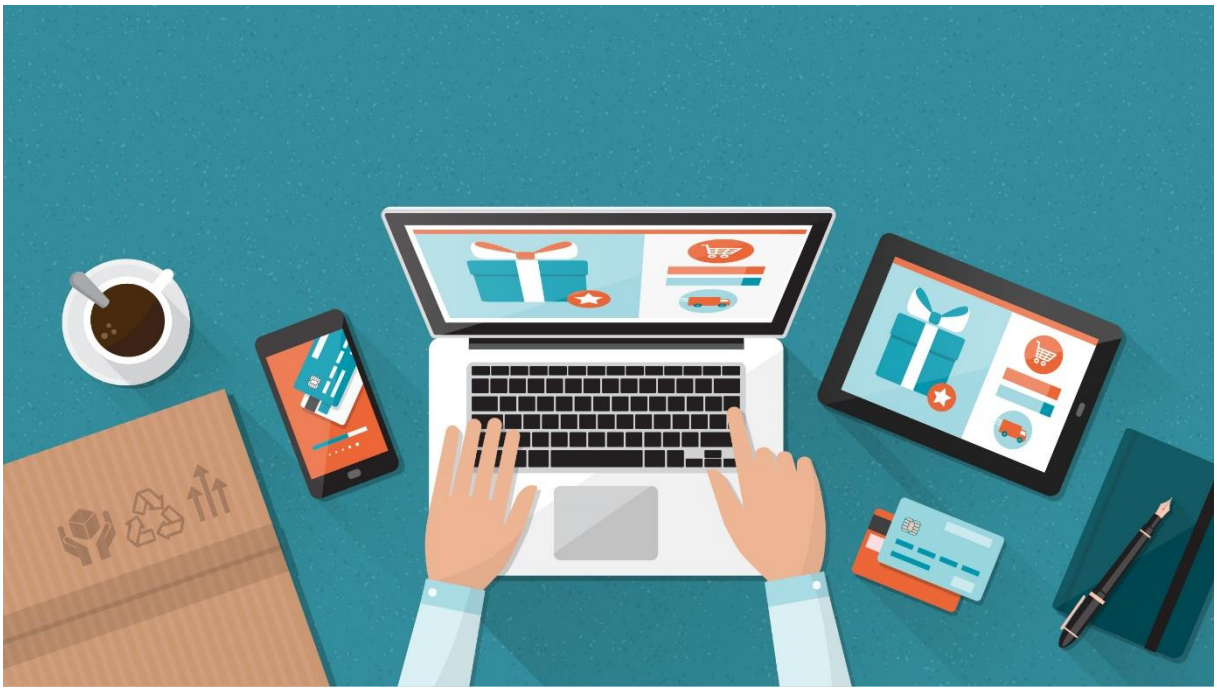
En 2019, el comercio electrónico fue responsable de alrededor de 3.5 billones de dólares en ventas y se espera que alcance los 4.9 billones para 2021. Además, el 21.8% de la población mundial compra en línea y las marcas se están volviendo cada vez más activas en las redes sociales, lo que significa que se están involucrando más con las personas a través de diferentes canales en línea.

Hoy en día, cada vez más personas prefieren las compras en línea a las compras convencionales. Algunas de esas ventajas están relacionadas con la conveniencia, las comparaciones de precios, la comodidad y la accesibilidad. Por lo general, cuando compras en línea, debes crear una cuenta. En consecuencia, estás obligado a proporcionar parte de tu información privada, como "nombre", "dirección", "número de teléfono", "correo electrónico" y un método de pago.

Teniendo esto en cuenta, y dado que se rastrea todo en Internet, no es sorprendente que todos los datos que resultan de la gran cantidad de comercio electrónico e interacciones en las redes sociales signifiquen que es importante conocer más profundamente las posibles consecuencias de estas acciones.

Si deseas evitar las estafas por Internet mientras compras en línea, deberás tomar algunas precauciones. A continuación puedes encontrar algunas sugerencias:

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



Pague con tarjeta de crédito o cargo

Las tarjetas de crédito son generalmente la opción más segura, ya que permiten a los compradores buscar un crédito del emisor si el producto no se entrega o no es lo que se ordenó. Considera usar una tarjeta de crédito virtual única. Las tarjetas de crédito virtuales son tarjetas de crédito únicas que te permiten realizar transacciones en tu cuenta de tarjeta de crédito principal sin usar o exponer tu número de cuenta de tarjeta de crédito principal. Por ejemplo, puedes usar Capital One para crear este tipo de tarjetas de crédito.

Saber con quién estás tratando

Lee las reseñas y mira si otros consumidores han tenido una experiencia positiva o negativa con el sitio web. Asegúrate de que el sitio tenga habilitada la seguridad.

Monitorea tus cuentas financieras

Lee tus estados de cuenta regularmente y asegúrate de que reflejen los cargos que tú autorizaste.

Consulta la política de privacidad

La política de privacidad describe cómo se recopila, utiliza y comparte tu información personal cuando visitas o realizas una compra en una tienda en línea. Debes leer la política de privacidad y ver si estás de acuerdo con la privacidad de la empresa.

Gratis puede ser costoso

Los protectores de pantalla gratuitos, tarjetas electrónicas u otros pueden contener virus peligrosos. Mantén tu software antivirus y antispyware actualizado junto con su firewall.

No envíes tu información financiera por correo electrónico.

Las compañías legítimas no solicitan información financiera por correo electrónico o mensaje emergente.

Pague con tarjeta de crédito o cargo

Las tarjetas de crédito son generalmente la opción más segura, ya que permiten a los compradores buscar un crédito del emisor si el producto no se entrega o no es lo que se ordenó. Considera usar una tarjeta de crédito virtual única. Las tarjetas de crédito virtuales son tarjetas de crédito únicas que te permiten realizar transacciones en tu cuenta de tarjeta de crédito principal sin usar o exponer tu número de cuenta de tarjeta de crédito principal. Por ejemplo, puedes usar Capital One para crear este tipo de tarjetas de crédito.

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

3. Aplica conocimiento

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Medidas de ciberseguridad_O3_O1

Situación: ¿Cuáles son algunos de los tipos de información que nunca debes dar mientras compras en línea?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Número de seguridad social.
- Código de seguridad de tarjeta de crédito - PIN.
- Número de tarjeta de débito.
- Número de cuenta bancaria.
- Dirección de correo electrónico.

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Medidas de ciberseguridad_O3_O2

Situación: de la lista, selecciona los comportamientos correctos para evitar ser víctima del delito cibernético
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Antes de dar la información de la tarjeta de crédito, te debes tomar el tiempo suficiente para investigar el sitio web.
- Compra en un sitio web que tenga encriptación.
- Lee la política de devolución del sitio web y otros términos y condiciones, así como la política de privacidad del sitio, antes de pedir cualquier cosa.
- Paga con tarjeta de débito, efectivo o transferencia bancaria.
- Usa un "punto de acceso" para proteger tu confidencialidad.

4. Construye conocimiento - Cloud Computing

Atrás quedaron los días en que guardabas tus archivos en un disco compacto o incluso en un pen drive, siempre con la terrible sensación de que eventualmente extraviarías esos archivos para nunca volver a encontrarlos. Hoy en día, puedes acceder a tus archivos en cualquier ordenador y, de hecho, las soluciones en la nube se están utilizando cada vez más en todo el mundo en las actividades cotidianas. Estás constantemente interactuando con algún tipo de solución en la nube cuando revisas tu correo electrónico o mientras usas tu teléfono para verificar las condiciones del tráfico. Con las soluciones en la nube, tus datos se almacenan con un proveedor y se accede a ellos a través de Internet.
Por lo tanto, la pregunta que surge en este contexto es si nuestros datos están seguros y protegidos en la nube. Por eso, es importante saber más sobre el concepto de computación en la nube.

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

Definición

La **computación en la nube** se puede definir mediante la entrega de recursos de TI a demanda- como almacenamiento, potencia informática o capacidad de intercambio de datos -en Internet, a través del alojamiento en servidores remotos.

En otras palabras, la computación en la nube significa almacenar y acceder a datos y programas a través de Internet en lugar del disco duro de tu ordenador. Estos recursos incluyen herramientas y aplicaciones como almacenamiento de datos, servidores, bases de datos, redes y software. Las soluciones en la nube son una opción muy popular para las personas y las empresas por varias razones, incluidos los ahorros de costes, el aumento de la productividad, la velocidad y la eficiencia, el rendimiento y la seguridad.

La nube, los grandes datos y la digitalización de la industria van acompañados de un crecimiento en la exposición de vulnerabilidades, lo que permite que las personas malintencionadas apunten a más víctimas. La variedad de tipos de ataque y su creciente sofisticación hacen que sea realmente difícil mantener el ritmo. Por eso, es importante implementar algunas precauciones diarias para evitar robos, fugas y/o eliminación de información importante.

Por favor, consulta un breve resumen de algunas medidas que puedes usar para mejorar la seguridad de la computación en la nube.

Usa una autenticación de múltiples factores	La combinación tradicional de nombre de usuario y contraseñas a menudo es insuficiente para proteger las cuentas de usuario de los piratas informáticos y el robo de credenciales es una de las principales formas en que los piratas informáticos obtienen acceso a tus datos/información. Por ello, debes usar no solo contraseñas seguras sino también una autenticación de múltiples factores, también conocida como autenticación de dos factores, para garantizar que solo el personal autorizado pueda iniciar sesión en tus aplicaciones en la nube y acceder a esos datos confidenciales.

	Un factor múltiple es una de las formas más efectivas de evitar que los hackers accedan a tus aplicaciones en la nube. Algunos ejemplos de autenticación multifactor son una contraseña combinada con un código enviado por SMS o un número generado por una aplicación. También es importante que siempre recuerdes cerrar sesión y nunca guardar tus credenciales.
Administra tu acceso de usuario para mejorar la seguridad informática en la nube	La mayoría de las personas no necesitan acceso a cada información, cada aplicación o cada archivo. Por lo tanto, revisar los niveles adecuados de autorización asegura que cada persona solo pueda ver o manipular las aplicaciones o los datos/información necesarios. Si alguien tiene acceso a todo y es engañado por un correo electrónico de phishing y, sin darse cuenta, proporciona su información de inicio de sesión, el hacker tiene acceso a toda la información con mucha facilidad.
Monitorea, registra y analiza las actividades de los usuarios con soluciones automatizadas para detectar intrusos	El monitoreo y análisis en tiempo real de las actividades del usuario pueden ayudar a detectar eventuales irregularidades que se desvían de los comportamientos/patrones normales. Estas actividades inusuales podrían indicar una infracción en el sistema, por lo que detectarlas desde el principio puede detener a los piratas informáticos y permitir solucionar problemas de seguridad antes de que las cosas salgan mal. Puedes encontrar muchas soluciones para la supervisión y administración de redes automatizadas las 24 horas, los 7 días de la semana y pasar a soluciones avanzadas de ciberseguridad. Debido a que cada negocio/persona tiene diferentes necesidades para diferentes niveles de ciberseguridad, asegúrate de obtener una tercera parte para la evaluación de riesgos antes de realizar una gran inversión.
Entrenamiento anti-phishing	Los hackers pueden obtener acceso a información segura robando credenciales a través de algunas técnicas como el phishing, la suplantación de sitios web y el espionaje en las redes sociales. Por eso, ten en cuenta que, por ejemplo, la formación en phishing debe ser un proceso continuo que debe ser administrado por alguien dentro de la organización para que sea efectiva.
Copia de seguridad de archivos en diferentes cuentas en la nube	Independientemente de la escala, la industria, la región y/o las personas, garantizar la disponibilidad de datos es una prioridad para todos. Además, la pérdida de datos/información debido a un error humano es muy alta, así que no coloques todos tus datos importantes en un solo lugar. Ya sea porque estés protegiendo y accediendo a los archivos en tu ordenador portátil personal o seas un proveedor de servicios administrados responsable de una cartera de negocios (y sus crecientes cantidades de datos), las aplicaciones en la nube son esenciales en el mundo digital moderno.

	Por lo tanto, es crucial encontrar más de una solución de respaldo de nube a nube para garantizar una copia de los datos que creas, almacenas y compartes en una ubicación segura.

4. Aplica conocimiento

Ejercicio ELECCIÓN ÚNICA

Objetivo específico asociado: OE_Medidas de ciberseguridad_O4_O1

Situación: con respecto a la computación en la nube, ¿qué afirmación es verdadera?
Tarea: Elige la opción correcta siguiendo el principio de opción múltiple: solo una oración es verdadera.

- En Platform as a Service (PaaS), una empresa de paga a medida que usa para servicios como almacenamiento, redes y virtualización.
- Infraestructura como servicio (IaaS) es un modelo de computación en la nube en el que un proveedor externo entrega herramientas de hardware y software a un Número de cuenta bancaria.
- Software as a Service (SaaS) es un modelo de licencia y entrega de software en el que el software se licencia por suscripción y está alojado de forma centralizada.
- Al usar ordenadores en la nube, los usuarios y las empresas tienen que administrar servidores físicos.

Ejercicio ELECCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Medidas de ciberseguridad_O4_O2

Situación: de la lista, selecciona los comportamientos correctos para evitar ser víctima del delito cibernético
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Almacena información como direcciones, números de teléfono, información bancaria, etc. en diferentes nubes.
- Crea una contraseña única exclusiva para el servicio en la nube.
- Al usar soluciones en la nube, no es relevante tener un antivirus.
- Por su conveniencia, se sugiere guardar las credenciales de inicio de sesión en la aplicación correspondiente.

Fuentes

Alexandra, Susan (April 04, 2019). 10 Tips for Keeping Your Personal Data Safe on Social Media. Retrieved from https://securitytoday.com/Articles/2019/04/04/10-Tips-for-Keeping-Your-Personal-Data-Safe-on-Social-Media.aspx?Page=2

Cucu, Paul (December 21, 2016). 17 Underused Online Shopping Security Tips. Retrieved from https://heimdalsecurity.com/blog/online-shopping-security-tips/

European Commission (March 2019). Briefing Paper: Challenges to effective EU cybersecurity policy, Briefing paper. European Court of Auditors.

Federal Trade Comission (n.d.). 9 Online Shopping Tips. Retrieved from https://www.yumpu.com/en/document/read/4010016/nine-online-shopping-tips-federal-trade-commission

Kapiswe, Subham (April 23, 2019). NCSC Reveals List Of World's Most Hacked Passwords. .Retrieved from https://en.wikipedia.org/wiki/List_of_the_most_common_passwords#cite_note-NCSCList-15

Kapersky (n.d.). Safer Online Shopping. Retrieved from https://usa.kaspersky.com/resource-center/preemptive-safety/online-shopping

National Cybersecurity Alliance (n.d.). Online Safety Basics: Online Shopping. Retrieved from https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/

Acronis (n.d.). Case study: The Benefits of Cloud-to-Cloud Backup Solutions from Acronis. Retrieved from https://www.acronis.com/en-us/articles/cloud-to-cloud-backup/

D'Silva, Frank (June 15, 2020). 6 Tips for Improving Cloud Computing Security. Retrieved from https://www.ntiva.com/blog/6-tips-for-improving-cloud-computing-security

Afianza conocimiento

La era de internet nos dio la superpotencia de la omnipresencia. Redujo las brechas entre las personas, las empresas y los lugares, permitiendo a las personas estar en cualquier lugar y con cualquier persona con solo un clic.

Como ha aprendido a lo largo de esta unidad de contenido, la privacidad y seguridad en línea de la información personal es una responsabilidad compartida entre todas las partes: gobierno, desarrolladores de software, proveedores de servicios en la nube, empresas y usuarios finales.

Con la implementación del RGPD, los usuarios finales obtienen confianza en su protección de datos, ya que esta regulación tiene como objetivo salvaguardar la privacidad de las personas en Internet. Sin embargo, hay muchos comportamientos que los usuarios finales deben adoptar para desempeñar su papel. Esos comportamientos son comunes a todas las actividades en Internet, desde las redes sociales hasta la nube, y se refieren comúnmente a "las reglas de oro de Internet".

La primera regla se basa en las contraseñas: tener contraseñas únicas y seguras con autenticación de dos factores al iniciar sesión y cambiarlas cada tres meses.

La segunda regla está relacionada con la información privada: no guardes ni compartas información sensible a través de Internet, especialmente cuando compres en línea; Además, si tienes información privada almacenada en un servicio en la nube, asegúrate de no añadir toda tu información en una sola nube.

La tercera regla es practicar la navegación inteligente: no guardes tus credenciales de inicio de sesión en ningún navegador, sitio web o aplicación, y cierra sesión cada vez que salgas de un sitio web. Del mismo modo, no hagas clic en ningún enlace dudoso ni ingreses tu información en sitios web no seguros.

En general, debes reconocer que son tus datos los que eventualmente podrían verse comprometidos por los ataques cibernéticos y, en consecuencia, debes asegurarte de cumplir con tu parte en la privacidad y seguridad de los datos en Internet.

Las respuestas correctas están en negrita

Situación: ¿Cuál es el significado de ciberseguridad?

Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- La ciberseguridad incluye la defensa de hardware y software.
- Los ataques cibernéticos están aumentando y ahora todo el mundo es más vulnerable a este tipo de incidentes.
- Las medidas efectivas de ciberseguridad incluyen la aplicación de múltiples medidas de ciberseguridad.
- La formación en ciberseguridad debe brindarse lo antes posible debido a la necesidad de la aplicación de múltiples acciones de ciberseguridad.

Situación: por favor, seleccione de entre las siguientes oraciones la correcta.
Tarea: Elige la opción correcta siguiendo el principio de opción múltiple: solo una oración es verdadera.

- Se recomienda elegir una contraseña simple para memorizarla mejor.
- Algunas contraseñas únicas derivan de un nombre de pila, el nombre de un miembro de la familia o el nombre de una mascota.
- Cuantos más caracteres y símbolos contengan las contraseñas, menos difíciles serán de adivinar.
- Una contraseña segura tiene una combinación de letras mayúsculas y minúsculas, símbolos y números, y al menos ocho caracteres de longitud.

Situación: ¿Cuáles son algunas de las reglas para proteger tus cuentas digitales de los ataques cibernéticos?
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Usa la misma contraseña en múltiples sitios web / cuentas.
- Cambia las contraseñas regularmente.
- Guarda las credenciales de inicio de sesión en el navegador o la aplicación de un ordenador en particular.
- Una huella digital, una huella de voz o un código pin son una buena opción para una autenticación de dos factores.
- Al crear una nueva contraseña, evite las palabras que se encuentran en el diccionario, los pronombres, los nombres de usuario y otros términos predefinidos, así como las contraseñas de uso común.

Situación: ¿Cuáles son algunos de los tipos de información que nunca debes dar mientras compras en línea?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Número de seguridad social.
- Código de seguridad de tarjeta de crédito.
- Número de tarjeta de débito.
- Número de cuenta bancaria.
- Dirección de correo electrónico.

Situación: de la lista, selecciona los comportamientos correctos para evitar ser víctima del delito cibernético

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

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- **Antes de dar la información de la tarjeta de crédito, te debes tomar el tiempo suficiente para investigar el sitio web.**
- **Compra en un sitio web que tenga encriptación.**
- **Lee la política de devolución del sitio web y otros términos y condiciones, así como la política de privacidad del sitio, antes de pedir cualquier cosa.**
- Paga con tarjeta de débito, efectivo o transferencia bancaria.
- Usa un punto de acceso para proteger tu confidencialidad.

Situación: con respecto a la computación en la nube, ¿qué afirmación es verdadera?
Tarea: Elige la opción correcta siguiendo el principio de opción múltiple: solo una oración es verdadera.

- En Platform as a Service (PaaS), una empresa de paga a medida que usa para servicios como almacenamiento, redes y virtualización.
- Infraestructura como servicio (IaaS) es un modelo de computación en la nube en el que un proveedor externo entrega herramientas de hardware y software a un Número de cuenta bancaria.
- **Software as a Service (SaaS) es un modelo de licencia y entrega de software en el que el software se licencia por suscripción y está alojado de forma centralizada.**
- Al usar ordenadores en la nube, los usuarios y las empresas tienen que administrar servidores físicos.

Situación: de la lista, selecciona los comportamientos correctos para evitar ser víctima del delito cibernético
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- **Almacena información como direcciones, números de teléfono, información bancaria, etc. en diferentes nubes.**
- **Crea una contraseña única exclusiva para el servicio en la nube.**
- Al usar soluciones en la nube, no es relevante tener un antivirus.
- Por su conveniencia, se sugiere guardar las credenciales de inicio de sesión en la aplicación correspondiente.