Content Unit

Unidad de Comprobación

Proyecto: B-SAFE
Número: 2018-1CZ01-KA204-048148
Nombre del autor: UDIMA
Última fecha de procesamiento: 24.8.2020

Funded by the
Erasmus+ Programme
of the European Union

1. Las diez mayores amenazas de Internet para los usuarios

Es fácil acceder a Internet en esta era digital y este ofrece muchas formas de explorar el mundo virtual donde, a diferencia del mundo real, todo es fácilmente accesible. Abre un mundo nuevo y viene acompañado de muchas ventajas pero también de muchos riesgos.

1. *Contenido inapropiado*

Hay toneladas de contenidos en Internet y no todos estos contenidos son socialmente aceptables ni están clasificados por edad o área. Algunos contenidos pueden ser ilegales, inapropiados, ofensivos o inadecuados para algunos grupos de edad. Cualquiera puede encontrar contenido inapropiado, perturbador o explícito, incluso niños pequeños sin supervisión.

Muchos sitios web perturbadores no son "ilegales", lo que significa que nadie supervisa ni gestiona su contenido. Algunos de estos contenidos son pornografía, violencia, productos peligrosos (como armas), racismo u odio, sitios pro-ana (promueven la anorexia) u otros sitios con contenido extremista.

2. Robo de datos

La información financiera o personal se roba mediante el uso de ordenadores, servidores y otros dispositivos electrónicos con el fin de obtener algún beneficio o dañar a la víctima. Los ladrones cibernéticos pueden atacar bancos, corporaciones e individuos. Es un acto ilegal de obtener datos confidenciales, que incluyen también números de tarjetas de crédito sin cifrar, detalles de cuentas bancarias de personas, contraseñas, información almacenada en empresas, secretos comerciales, propiedad intelectual, código fuente, información de clientes o registros de empleados.

El ciberdelincuente puede acceder a los ordenadores de estos usuarios a través del software espía, que es un software que permite a un usuario obtener información sobre las actividades informáticas de otra persona.

3. Robo de identidad

El robo de identidad es la acción de robar información de identificación personal para cometer actos ilegales. En la primera fase, el delincuente adquiere una identidad informática extranjera. Esto se hace con mayor frecuencia robando datos electrónicos (contraseñas, datos de acceso, etc.), generalmente mediante copia no autorizada (skimming), phishing engañoso o piratería.

En la segunda fase, el agresor hace un mal uso de la identidad en beneficio propio para dañar a la víctima. Por ejemplo actuando bajo su nombre en redes sociales como Facebook. Es el acto de robar información de identificación personal para cometer actos ilegales, tales como: abrir una línea de crédito, alquilar una casa, comprar bienes o servicios, fraude o extorsión relacionada con subastas y salarios.

4. Atención no deseada

Este tipo de atención podría provenir de alguien que simplemente está obsesionado con la víctima (ciberacecho/ciberintimidación) o alguien cuya intención es dañar a la víctima (acoso cibernético/ciberacoso).

Por un lado, el *ciberacecho* es una atención obsesiva no deseada a una persona específica a través de Internet. Se comete a través de la tecnología en línea, como el correo electrónico, las redes sociales, la mensajería instantánea, los datos personales disponibles en línea; los acosadores cibernéticos pueden usar todo lo que hay en Internet para establecer un contacto inapropiado con sus víctimas. Algunas formas son seguir a la persona en línea, buscar información personal de manera obsesiva, observar en secreto (en línea), llamar y enviar mensajes de texto persistentes para manipular, y otros medios diferentes para acercarse a la víctima inesperadamente.

Por otro lado, el ciberacoso es un delito que ocurre cuando las personas utilizan las redes sociales o Internet para intimidar, acosar, amenazar o menospreciar a otros.

5. Estafas y engaños

Un tipo de estafa o engaño sería el phishing. Es la práctica de enviar comunicaciones fraudulentas que parecen provenir de una fuente de confianza, generalmente a través del correo electrónico.

Estas comunicaciones pueden incluir malware (spyware, ransomware, virus y gusanos), lo que generalmente ocurre debido a clics peligrosos o archivos adjuntos de correo electrónico que luego instalan software peligroso.

6. Información no deseada

Usando Internet podemos terminar encontrando información que no estábamos buscando o información o perfiles falsos. Puedes encontrar información engañosa en lugar de lo que estabas buscando o sin solicitarla.

El medio de comunicación en línea más popular es el correo electrónico. Es muy común usarlo en nuestra rutina diaria y por eso este es uno de los medios favoritos para el spam. Los correos electrónicos falsos son una amenaza común, pero también puedes recibir este tipo de información engañosa a través de mensajes de redes sociales o diferentes sitios web.

Además, las noticias falsas se pueden encontrar en todas partes, no solo cuando se usa el correo electrónico. En las redes sociales es muy común encontrar no solo noticias falsas sino también identidades falsas.

7. Fácil propagación y larga duración

La información como fotos, noticias, etc., se puede cargar en cualquier momento, en cualquier lugar y por cualquier persona. Una vez que la información está en línea, permanece allí para siempre, por lo que debes tener mucho cuidado con la información que compartes en línea.

También es muy fácil difundirlo por todo el mundo y en poco tiempo.

8. Destrucción o modificación de datos

Los datos importantes pueden destruirse o modificarse en el ordenador del usuario con el fin de hacer daño.

Una forma podría ser a través de virus, que son programas de ordenador diseñados para infectar otros programas, destruyendo datos esenciales del sistema y haciendo que las redes no funcionen.

9. Deshabilitar el dispositivo

El dispositivo del sistema operativo del ordenador puede ser atacado por un troyano. Es un programa de computadora que obtiene acceso a un ordenador o sistema.

Los troyanos se camuflan en forma de software normal para dañar los procesos del sistema, los datos del disco duro, etc. Se introducen principalmente a través de archivos adjuntos de correo electrónico.

10. Terrorismo cibernético

El ciberterrorismo es siempre más severo que otros comportamientos que se llevan a cabo en o a través del ciberespacio.

Este tipo de delito es un ciberataque que tiene como objetivo generar miedo o intimidar a la sociedad con un objetivo ideológico. Para este propósito, el terrorista usa ordenadores o redes de comunicación para causar suficiente destrucción o interrupción.

2. Las diez reglas más importantes para un comportamiento seguro en Internet

1. Contraseñas

Muchos servicios en Internet están protegidos con un código de acceso, para proteger la privacidad de la información. Si esta contraseña es simple o común (muy fácil entre los usuarios) se podría adivinar con facilidad accediendo de forma inapropiada a la cuenta como si fuera el usuario real. Por este motivo, se recomienda el uso de contraseñas seguras, con más de 8 caracteres en combinación con letras (mayúsculas y minúsculas), dígitos y caracteres especiales; evita información personal como el número de identidad nacional, nombres de familiares o conocidos y nunca use patrones muy simples o palabras de diccionario. Para mayor seguridad, se recomienda modificar las contraseñas periódicamente. Las contraseñas nunca deben registrarse en cuadernos o archivos no cifrados.

2. Tecnologías de seguridad

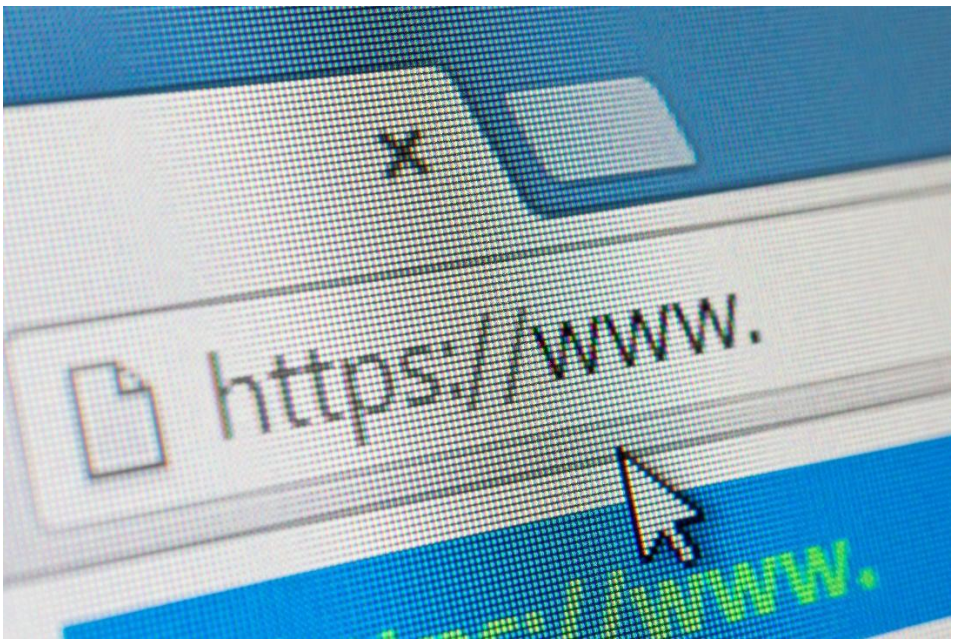
Crea varias copias de seguridad de todos tus datos importantes y asegúrate de que no estén todos almacenados en el mismo lugar. Mantén siempre tu software actualizado. Instala un filtro/software de phishing en tu aplicación de correo electrónico y también en tu navegador web.

Las soluciones antivirus, cortafuegos y antispam representan las aplicaciones más importantes para proteger el equipo contra las principales amenazas que se propagan por Internet. El uso de estas tecnologías reduce el riesgo y la exposición a amenazas. Para protegerse contra los virus, ejecuta análisis programados regularmente con tu software antivirus y asegúrate de que tu software antivirus y antispyware sean compatibles.

3. Páginas de confianza

A través de técnicas de Ingeniería Social, muchos sitios web a menudo se promocionan con datos que pueden atraer la atención del usuario, como descuentos en la compra de productos (o incluso ofertas gratuitas), primicias o materiales exclusivos para noticias de actualidad, material multimedia, etc. Para una navegación segura, se recomienda que el usuario sea consciente de estos mensajes y evite acceder a páginas web con estas características.

Verifica las credenciales SSL del sitio web y nunca uses información personal/confidencial en sitios que no tengan un certificado SSL válido instalado.



A través de las técnicas de Black Hat SEO, los atacantes suelen colocar sus sitios web entre los primeros lugares en los resultados de los motores de búsqueda, especialmente en los casos de búsquedas de palabras clave ampliamente utilizadas por el público, como actualidad, noticias extravagantes o temas populares (como deportes y sexo). En el caso de estas búsquedas, el usuario debe estar atento a los resultados y verificar qué sitios web se están enlazando.

Si no queremos dejar nuestra huella en Internet, una de las formas más seguras es a través de una red virtual privada o mediante un servidor proxy que actúa como intermediario en la comunicación con el sitio web que visitamos.

4. Compartir información

Toda la información que subimos a Internet sobre nosotros mismos, las imágenes que compartimos en las redes sociales dejan un rastro digital que conforma lo que se conoce como nuestra "identidad digital". Por ello, es necesario estar atentos sobre todo a la identidad digital que creamos y solo subir información sobre nosotros mismos que consideramos cien por cien pública.

No des acceso a tu ubicación, cámara o micrófono para evitar dar información adicional. No uses el GPS para mostrar en tus publicaciones dónde te encuentras.

Tanto en clientes de mensajería instantánea como en redes sociales, se recomienda aceptar e interactuar solo con contactos conocidos. Esto evita acceder a los perfiles creados por los atacantes para comunicarse con las víctimas y exponerlas a diversas amenazas como malware, phishing, cyberbullying u otras.

5. Redes WiFi gratuitas

Si utilizas una red Wifi gratuita para navegar por páginas públicas, el riesgo es mínimo. No obstante, debemos evitar navegar por páginas web que nos pidan añadir datos personales, como contraseñas o nombres de usuario, ya que el Wifi podría verse comprometido y por tanto alguien podría interceptar nuestros datos personales. Debemos prestar la misma atención cuando nos conectamos a Wifis conocidas.

6. Enlaces sospechosos

Uno de los medios más utilizados para dirigir a las víctimas a sitios maliciosos son los hipervínculos o enlaces. Evitar hacer clic en estos nos protege del acceso a páginas web que tienen amenazas capaces de infectar al usuario. Los enlaces pueden estar presentes en un correo electrónico, una ventana de chat o un mensaje en una red social: la clave está en analizar si se ofrecen en alguna situación sospechosa que te haga dudar (una

invitación a ver una foto en un idioma diferente al tuyo , por ejemplo), provienen de un remitente desconocido o hacen referencia a un sitio web de poca confianza.

7. Descarga de archivos

Una de las mayores brechas de seguridad proviene de la descarga de archivos. Si no estás completamente seguro del origen de lo que estás descargando, evítalo o verifícalo antes de descargar. Muchos sitios fingen ofrecer programas populares que son alterados, modificados o suplantados por versiones que contienen algún tipo de malware y descargan el código malicioso en el momento en que el usuario lo instala en el sistema. Por ello, se recomienda que al descargar aplicaciones siempre lo hagas desde las páginas web oficiales.

Por otro lado, la propagación del malware suele realizarse a través de archivos ejecutables. Se recomienda evitar la ejecución de archivos a menos que se conozca la seguridad de los archivos y su procedencia sea de confianza (ya sea de un contacto de mensajería instantánea, un correo electrónico o un sitio web).

8.Actualización del sistema operativo y las aplicaciones

Tener el sistema operativo (Windows, Linux, Apple ...) y todas las aplicaciones instaladas correctamente actualizadas es una de las principales garantías para no dejar puertas abiertas a tu ordenador que puedan explotar los ciberdelincuentes. Aunque actualizar los ordenadores lleva tiempo y, a veces, requiere reiniciar, es esencial corregir las vulnerabilidades de seguridad en el software instalado.

Si ya estás tomando las precauciones al navegar desde tu ordenador de escritorio o portátil, no olvides tu móvil, es muy importante que tengas en cuenta las mismas reglas para este caso. A través de dispositivos como teléfonos inteligentes, los propietarios de otros tienen más probabilidades de violar los elementos de seguridad que tu sistema operativo puede ofrecerte.

9. Evita añadir información personal en formas dudosas

Cuando el usuario se enfrenta a un formulario web que contiene campos con información sensible (por ejemplo, nombre de usuario y contraseña), se recomienda verificar la legitimidad del sitio. Una buena estrategia es verificar el dominio y el uso del protocolo HTTPS para garantizar la confidencialidad de la información. De esta forma, los ataques de phishing que intentan obtener información sensible se pueden prevenir simulando una entidad de confianza.

10. Cookies

Una cookie es un archivo creado por un sitio web que contiene pequeñas cantidades de datos que se envían entre un remitente y un receptor, con el fin de conocer las preferencias del usuario y facilitar su experiencia en el sitio. Sin embargo, es probable que la información que se comparte llegue a terceros, por lo que es conveniente evaluar el tráfico de estos datos y en cualquier caso, desde el navegador podemos decidir eliminar estas cookies para evitar sustos innecesarios.

Aplica conocimiento

Cibercrimen

1. ¿Cuál es la definición de ciberdelito?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: podría haber más de una respuesta correcta

a) El cibercrimen consiste en ver contenido inapropiado en Internet.
b) El cibercrimen es un acto ilegal en el que el ordenador es una herramienta, un objetivo o ambos.
c) El cibercrimen es el seguimiento de los correos electrónicos laborales de los empleados por parte de los empleadores.
d) El cibercrimen es obtener información pública en Internet.

2. ¿Cuál de los siguientes ejemplos es phishing?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: podría haber más de una respuesta correcta

a) Recibiste un correo electrónico celebrando que ganaste un i-Phone y debes enviar cierta información personal para recibir el premio.
b) Recibiste un correo electrónico con una oferta con productos para comprar.
c) Recibiste un correo electrónico requiriendo que cambies la contraseña a tu cuenta bancaria y con el enlace directo para hacerlo.
d) Recibiste un correo electrónico con información sobre algún evento cultural en tu ciudad.

3. Verdadero o Falso?

La piratería también puede percibirse como un acto productivo y útil.

V □ **F** □

4.Emparejar respuestas - puedes arrastrar y soltar las respuestas correctas en una parte determinada del texto

_____es el acto de robar información de identificación personal para cometer actos ilegales, tales como: abrir una línea de crédito, alquilar una casa, comprar bienes o servicios, fraude o extorsión relacionado con subastas y salarios.

_____ es el contacto constante con la persona; decirle cosas hirientes a la persona o dar a otros información falsa sobre la persona. Por ejemplo, el delincuente crea el grupo de Facebook titulado "Odio ..." e invita a todos sus amigos a unirse.
_____incluye actividades que generan riqueza deshonestamente para quienes participan en la conducta en cuestión. Consiste en la explotación de información privilegiada o la adquisición de la propiedad de otra persona mediante engaño para asegurar un beneficio material. Se considera comúnmente que los delitos financieros abarcan lo siguiente: fraude, blanqueo de dinero, soborno, soborno y corrupción y muchos otros.

_____es una obsesión por averiguar todo lo que pueda sobre la persona (sin preguntarle). Por ejemplo, el delincuente averigua dónde nació la persona, si está casada, etc.

Cyberbullying, Cyberstalking, Identity theft, Financial crimes,

5. Completa la oración con la palabra correcta – completa el espacio en blanco.

El ciberataque que utiliza o explota redes informáticas o de comunicación para causar suficiente destrucción o interrupción para generar miedo o intimidar a una sociedad hacia un objetivo ideológico se denomina (_____).

Protección contra contenido inapropiado

1. Empareja las respuestas- puedes arrastrar y soltar las respuestas correctas en una parte determinada del texto

_____ se describe como una imagen explícita o descriptiva destinada a estimular sentimientos sexuales.
_____ es la promoción o incitación al odio contra personas o grupos por motivos de origen étnico, religión, discapacidad, edad, nacionalidad, condición de veterano, orientación sexual, género, identidad de género o cualquier otra característica.

_____son los sitios web que entienden la anorexia como un estilo de vida, no como una enfermedad.

_____ proporcionan información atractiva, como eventos históricos, pero los hechos están distorsionados y se refieren a otras fuentes de información ya manipuladas por una percepción cambiante del mundo.
Racismo u odio, pornografía, sitios web pro-ana, sitios con contenido extremista

2. ¿Qué clasificación puede ayudarme a reconocer los sitios web con contenido inapropiado?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: podría haber más de una respuesta correcta
a) Clasificación de la Asociación de imágenes en movimiento (p.ej. PG)
b) LT Int. Escala (p. ej. clasificaciones de familias corporativas LT)
c) Escala Nacional (p.ej. NSR)
d) Clasificación PEGI online (p.ej. PEGI 7)

3. ¿Cuál de las siguientes herramientas es útil para el control parental del contenido en línea?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: podría haber más de una respuesta correcta

a) Protection online app
b) iWebfilter
c) K10 Web Protection
d) Anti-game

4. *¿Qué habilidades son necesarias para enseñar a los niños a minimizar los riesgos del contenido inapropiado?*

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: podría haber más de una respuesta correcta

a) habilidades en IT
b) Pensamiento crítico y resiliencia
c) Habilidades digitales
d) Maneras positivas de usar la tecnología

5. Completa la oración con la palabra correcta - completa el espacio en blanco

Podemos tener herramientas útiles para la protección como las leyes, los controles parentales, la configuración del software, las instituciones de apoyo, pero la clave es el/la (_____) entre tú y el niño.

discurso, confianza, discusión, conversación, comunicación.

Protección de Datos Personales

1. Completa el texto con las palabras correctas - completa el espacio en blanco

_____, también conocida como privacidad de la información, es un aspecto de la seguridad de los datos que se ocupa del manejo adecuado de _____. Protege principalmente los datos personales de los invididuos de _____. El/la _____ de datos personales ha sido un/a _____ derecho en Europe durante años. La protección de datos se ha vuelto cada vez más importante en los últimos años debido a _____ y _____ que facilitan recolección, procesamiento, almacenamiento, difusión y análisis de datos. El/la _____ es un reglamento legalmente vinculante sobre la protección de las personas en lo que respecta al procesamiento de datos personales.

Uso indebido, desarrollos técnicos, RGPD, fundamental, privacidad de datos, datos personales, protección, redes globales

2. Verdadero o Falso?

El RGPD solo se aplica al procesamiento automático de datos personales

V □ F □

Los datos personales se refieren a datos sensibles sobre un individuo.

V □ F □

Los datos sensibles deben estar cada vez más protegidos

V □ F □

Los datos personales incluyen, por ejemplo, nombre, fecha de nacimiento, edad o domicilio, número de cuenta.

V □ F □

La fecha sensible incluye, por ejemplo, número de tarjeta de crédito, creencias religiosas, afiliación sindical, origen racial y étnico.

V □ F □

3. Completa el texto con las palabras correctas - completa el espacio en blanco

El RGPD define _____ principios clave que deben cumplirse estrictamente dentro del _____. Las violaciones de estos principios pueden resultar en _____. Para datos personales _____ el RGDP tiene _____ fundamentos legales disponibles para el procesamiento como el procesamiento de _____ está prohibido en general a menos que se cumplan condiciones específicas. Se aplican requisitos especiales al procesamiento de _____. El procesamiento de datos solo está permitido en _____.

procesamiento de datos, siete, no sensibles, seis, sanciones máximas, datos personales, datos sensibles, casos excepcionales

4. ¿Qué es lo correcto con respecto a las violaciones de datos?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: podría haber más de una respuesta correcta

a) Es deber del controlador de datos informar al procesador de datos inmediatamente de cualquier violación de datos.
b) Si ocurre una violación de datos, el controlador de datos debe cumplir con la obligación de informar y notificar.
c) Si ocurre una violación de datos, el procesador de datos debe cumplir con la obligación de informar y notificar
d) La autoridad de protección de datos debe ser informada dentro de las primeras 24 horas.
e) La autoridad de protección de datos debe ser informada dentro de las primeras 72 horas.
f) Se debe informar a la autoridad de protección de datos si es probable que la violación suponga un riesgo para los derechos y libertades de los interesados.
g) La notificación adicional del interesado no siempre es necesaria si es probable que exista un alto riesgo para los derechos y libertades de los interesados.

5. Completa el texto con las palabras correctas - completa el espacio en blanco

Para asegurar la protección de los _____, el problema de _____ es un problema central. En este contexto la _____ y la _____ son palabras clave importantes. _____ se refiere a la protección de datos a través de _____. Esto significa que al desarrollar nuevas tecnologías, se deben garantizar soluciones adecuadas que se ajusten a la protección de datos. _____ significa privacidad a través de _____. La persona responsable debe garantizar, mediante la configuración predeterminada adecuada, que solo aquellos _____ son procesados, que son absolutamente necesarios.

datos personales, seguridad de los datos, datos personales, privacidad por diseño, privacidad por diseño, privacidad por defecto, diseño tecnológico, privacidad por defecto, configuración por defecto

Protección de Teléfonos Inteligentes

1. ¿Qué medida de precaución debes tomar para proteger tu teléfono inteligente y los datos privados almacenados en él en caso de pérdida o robo?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: podría haber más de una respuesta correcta

a) Usa un número de identificación personal y un bloqueo de pantalla
b) Usa un PIN con una combinación de números común para que sea fácil de recordar para ti
c) Anota el número de serie de tu teléfono inteligente
d) No instales una aplicación antirrobo

2. ¿Qué es correcto en la mensajería instantánea?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: podría haber más de una respuesta correcta

a) MI (mensajería instantánea) es un chat fuera de línea para intercambiar mensajes.
b) La mensajería instantánea es una comunicación basada en Internet a través de aplicaciones móviles.
c) La transmisión del mensaje tiene lugar en el llamado procedimiento de extracción.
d) La MI es solo para la transmisión de textos.
e) Ejemplos de mensajería instantánea son WhatsApp, Skype o Facebook Messenger.

3. La mayoría de las aplicaciones de mensajería instantánea son gratuitas. ¿Qué riesgos se avecinan?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: podría haber más de una respuesta correcta

a) La aplicación debe pagarse más tarde, lo que conlleva altos costes
b) Los datos de la persona suelen ser el producto
c) La comunicación está mayoritariamente encriptada
d) Malware de todo tipo está oculto en las aplicaciones.

4. Verdadero o Falso?

No hay ningún problema con el permiso de aplicación sin restricciones
V □ F □

Los productores de aplicaciones están interesados en Tus datos personales
V □ F □

Todo acceso a los datos personales es obvio a través de los formularios de permiso de una aplicación.
V □ F □

La protección de datos es un tema cada vez más importante en relación con la mensajería instantánea y las aplicaciones
V □ F □

Existe riesgo de phishing
V □ F □

No hay ningún problema con la comunicación no cifrada.
V □ F □

5. Complete the sentence with the correct word – fill in the blank

Dado los potenciales _____ de usar aplicaciones en tu teléfono inteligente, probablemente te estés preguntando cómo puedes protegerte mejor y proteger tu privacidad. Aquí hay algunos consejos sobre lo que debes considerar al usar aplicaciones en tu teléfono inteligente: usa siempre la _____ versión de la aplicación, _____ de usar imágenes que no posees como imágenes de perfil, lee la _____ cuidadosamente antes de instalar una aplicación, ingresa solo los datos _____ , usa una _____ que no revele mucho sobre ti y no te moleste cuando se trata de spam, verifica los derechos de _____ de la aplicación y ajústalos si es necesario, ajusta la _____ de las aplicaciones (por ejemplo, la visibilidad de las imágenes de perfil) y _____ contactos no deseados.

bloquea, riesgos de seguridad, abstente, última, acceso, política de privacidad, configuración de privacidad, más necesarios, dirección de correo electrónico adicional

Flujo de información/comunicación en línea

1. El medio de comunicación en línea más común es

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: podría haber más de una respuesta correcta

a) Mensajería instantánea
b) Correo electrónico
c) Páginas web

2. Completa la oración con la palabra correcta - completa el espacio en blanco

Los _____ son correos electrónicos indeseables que te engañan de mala fe con información falsa o te llevan a realizar actos dañinos. Los programas maliciosos, por ejemplo, a menudo se transfieren a correos electrónicos falsos a través de _____. Por lo tanto, es importante conocer las características típicas de los correos electrónicos maliciosos. Por ello, debes tener cuidado con lo siguiente: se promete algo que parece _____ (demasiado bueno para ser verdad), el contenido del correo electrónico de alguna manera no encaja con el (supuesto) _____ de confianza, el correo electrónico contiene ciertas palabras _____ como asunto (por ejemplo, "último recordatorio" o "cuenta bloqueada"), se te pide que reveles _____, el _____ parece extraño, el correo electrónico contiene una gran cantidad de _____ (ortografía o gramática), el correo electrónico se mueve automáticamente a la _____ o se te pide que ejecutes programas con _____ extraños (por ejemplo, jpg.vbs "o" gif.exe ").

Correos electrónicos falsos, errores, archivos adjuntos, carpeta de spam, remitente de correo electrónico, irritante, poco realista, información confidencial, remitente, nombres de archivo.

3. Los foros y las salas de chat son medios muy conocidos y populares para la comunicación en línea y el intercambio de información. ¿Qué afirmaciones son correctas?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: podría haber más de una respuesta correcta

a) Los foros son adecuados para la comunicación en tiempo real
b) Los chats son adecuados para la comunicación en tiempo real
c) Los foros son adecuados para debates en los que no todos los participantes necesitan estar conectados al mismo tiempo
d) Los chats son adecuados para debates en los que no todos los participantes deben estar conectados al mismo tiempo.
e) Los foros están mejor organizados
f) Los chats están mejor organizados
g) Solo los foros requieren un registro con una dirección de correo electrónico válida
h) Los chats y foros permiten el intercambio de mensajes de texto, pero generalmente también se pueden usar para intercambiar imágenes, videos, enlaces o archivos.

4. ¿Cuáles son los principales riesgos de utilizar foros y chats?

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) Identidades falsas
b) Malware
c) Altos costes
d) Enlaces a sitios de phishing
e) Comunicación no cifrada
f) Comunicación cifrada

5. Completa el texto con las palabras correctas - completa el espacio en blanco

En las redes sociales, la asunción de un presunto anonimato puede conducir a un comportamiento irreflexivo al tratar con _____ e _____. Como resultado, las redes sociales se están enfocando cada vez más en las actividades _____. Existe el peligro de ser engañado por _____ o por la diseminación consciente o inconsciente de _____. Por lo tanto, siempre debes considerar los siguientes aspectos al tratar con _____: nunca publiques y discutas la información _____ y _____ en un espacio virtual público, usa el

_____ proporcionado para hacer que la información solo sea accesible para un cierto grupo de personas, se crítico cuando _____ amigos, verifica la configuración de redes sociales para la _____ y ten en cuenta la información _____. Si detectas uso indebido o mala conducta en las redes sociales, debes _____ al proveedor de servicios y _____ y organizaciones apropiadas.

información falsa, redes sociales, confidencial, datos, fraudulentas, engañosa, informar, identidades falsas, información, autoridades, protección de la privacidad, aceptes, personal, filtro

Control Parental

1. Las consecuencias para la víctima del sexting son:

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: podría haber más de una respuesta correcta

a) Humillación y linchamiento social para el protagonista de las imágenes.
b) El menor se enfrenta al insulto público, afectando en primer lugar a su autoestima, en una edad en la que se va formando su personalidad y depende en gran medida de la imagen que perciben los demás ya que la opinión de los demás es importante.
c) También hay sentimientos de impotencia, principalmente cuando se les cuenta el caso a los padres, o educadores, o de culpa por estar en esa situación.
d) No hay consecuencias.

2. Completa el texto con las palabras correctas - completa el espacio en blanco

El grooming se define como _____ llevado a cabo deliberadamente por un _____ para establecer una relación y control emocional sobre un menor a fin de preparar el terreno para _____ sexuales. En algunos casos se realiza entre menores, pero habitualmente con diferencia de edad, donde el mayor suele ser el _____. El objetivo del grooming es ganarse la confianza de los _____, obtener imágenes o videos de contenido _____, e incluso conocernos en persona.

Adulto, acoso cibernético, abusos, sexual, menores, acosador

3. Completa el texto con la palabra correcta - completa el espacio en blanco

Uno de los primeros pasos del _____ suele ser un matón que insulta o amenaza a la _____ diciendo que filtrará información que _____ su _____. La información enviada por el acosador sobre el acosado puede ser cierta, pero en este caso se filtrará adrede por el hecho de ser _____ o perjudicial para los intereses del acosado o puede ser directamente falsa. Si es así, se convierte en _____.

Cyberbullying, reputación, desinformación, negativo, víctima, dañará

4.Completa el texto con la palabra correcta - completa el espacio en blanco

Una forma de saber si el _____ está sufriendo _____ es analizar la cantidad de tiempo que pasa usando los dispositivos _____, la frecuencia y las manifestaciones _____ de no estar conectado. Si el menor parece estar _____, ansioso o agitado cuando no está conectado, o si experimenta cambios frecuentes de _____, el neolismo podría ser la razón.

Menor, emocionales, anímicamente, digitales, netholismo, estado de ánimo

5. Completa el texto con la palabra correcta - completa el espacio en blanco

Se pueden utilizar varias técnicas para la ____ de datos en secreto de un dispositivo digital. A veces, los _____ esconden sus intenciones al vmsotrarse como algo diferente a ellos. Por ejemplo, en los anuncios, requiriendo información para visualizar el contenido o pidiendo la _____ para que disfrutar de un servicio _____. Pero, más a menudo, los _____ comparten sus datos porque no son conscientes del peligro, por lo que se necesita una forma más responsable de actuar en _____.

Contraseñas, online, menores, fugas, perpetradores, internet

Hardware y software

1. *Une las respeustas: puede elegir la respuesta correcta en el menú de desplazamiento para cada parte del texto.*

El hardware se refiere a los elementos _____ de un ordenador. Ejemplos de hardware en un ordenador son _____. El software, comúnmente conocido como _____, consta de todas las instrucciones que le indican al hardware cómo realizar una determinada función. El software es capaz de realizar _____ tareas diferentes con el mismo hardware básico.

monitor y ratón, teclado, físicos, programas o aplicaciones, muchas

2. *¿Qué consejos/trucos puedes hacer con respecto a la protección del software? (opción múltiple: una respuesta no es correcta)*

a) Actualizaciones periódicas de software
b) Crear varias copias de seguridad
c) No instalar firewalls
d) Encriptar la información

3. *Un ejemplo de protección de hardware es evitar la compra de componentes de hardware de países o fuentes de riesgo (elección verdadero/ falso).*

a) Verdaderp
b) Falso

4. *¿Qué medidas puedes implementar para tener una mejor protección del software? (opción múltiple: una respuesta no es correcta)*

a) Instalar un antivirus y mantenerlo actualziado
b) Explorar las herramientas de seguridad que instales
c) Instalar actualizaciones del sistema operativo
d) Inhabilitar el uso compartido de archivos y medios si no lo necesitas

5. *¿Cuáles son los ataques más comunes al hardware? (opción múltiple - dos respuestas no son correctas)*

a) Accidentes físicos
b) Modificación
c) Troyanos
d) Phishing

Datos personales en redes sociales

1. ¿Con qué problemas de seguridad debes tener cuidado cuando usas las redes sociales? (opción múltiple: elige las opciones correctas siguiendo el principio de opción múltiple. Ninguna, una, más de una o todas las opciones pueden ser verdaderas)

a) Si un enlace te redirige a un sitio web, debes prestar atención para ver si hay una dirección física y contactos
b) Mira si el sitio web tiene una política de devoluciones, así como su política de envío.
c) Cuando recibes una solicitud de amistad de alguien que no reconoces, puedes intentar una búsqueda inversa de imágenes.
d) Para evitar un ataque de phishing, deberías ver la URL completa que te ayudará a mostrar si conduce a un sitio web legítimo.

2. Empareja las respuestas: puedes arrastrar y colocar las respuestas correctas en una parte determinada del texto.

La mayoría de los sitios web permiten configurar la información que se publica como información pública o privada mediante la opción de control "_____".

La forma en que se presentan o almacenan los datos personales en una red social en particular es responsabilidad del _____.

El ataque más común en las redes sociales utiliza una estrategia para atraer al usuario, a saber, a través de un _____.

propietario/proveedor de redes sociales; ataque de suplantación de identidad; configuración de privacidad

3. ¿Qué características están relacionadas con las redes sociales? (opción múltiple: una respuesta no es correcta)

a) Interactivas
b)Facilitan la creación o el intercambio de información, ideas, intereses profesionales y otras formas de expresión.
c) Conexión entre dos o más personas
d) Más de 4 mil millones de usuarios activos de redes sociales

4. *¿Cuáles son los riesgos más comunes en las redes sociales? (opción múltiple: una respuesta no es correcta)*

a) Software que utiliza cifrado para deshabilitar el acceso de un objetivo a sus datos, como fotografías o documentos, hasta que se pague un rescate.
b) Tipo de software o código malicioso que parece legítimo pero que puede tomar el control de tu ordenador
c) Forma de malware que es capaz de copiarse a sí mismo y propagarse a otro ordenador
d) Forma de malware que daña físicamente tu ordenador

5. ¿Qué consejos puedes aplicar para estar siempre un paso por delante de un posible ciberdelito en las redes sociales? (opción múltiple: una respuesta no es correcta)

a) No guardes tus credenciales de acceso en tus dispositivos/navegador/ aplicaciones
b) Evita compartir información personal online
c) Ten el último software de seguridad
d) Verifica tu configuración de privacidad

Ciberseguridad

1. *¿Qué es la ciberseguridad? (opción múltiple: una respuesta no es correcta*

a) Prevención y detección de ataques digitales, protección de sistemas, hardware y software
b) Práctica de defensa de ordenadores, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos.
c) La ciberseguridad solo se aplica a software y hardware
d) Técnicas de protección de ordenadores, redes, programas y datos contra accesos no autorizados o ataques destinados a la explotación.

2. *Para mejorar tu ciberseguridad en línea, ¿qué medidas puedes aplicar? (opción múltiple: una respuesta no es correcta)*

a) Crea diferentes contraseñas para diferentes cuentas y perfiles
b) Cambia tus contraseñas de vez en cuando y usa una combinación de letras mayúsculas y minúsculas, símbolos y números
c) Guarda tus contraseñas en una hoja de cálculo en tu ordenador
d) Usa un factor de autenticación de múltiples factores (si es posible) para diferentes cuentas en línea

3. ¿Qué precauciones debes aplicar al comprar online? (opción múltiple: una respuesta no es correcta)

a) Leer reseñas y ver si otros consumidores han tenido una experiencia positiva o negativa en ese sitio web específico.
b) Crear tarjetas de crédito virtuales
c) Mantener actualizado tu software antivirus y antispyware junto con tu firewall
d) No leer los términos y condiciones de diferentes sitios web porque todos son muy similares

4. De la lista, selecciona las frases correctas relacionadas con la definición y aplicación de la computación en la nube. (opción múltiple: una respuesta no es correcta)

a) Práctica de utilizar una red de servidores remotos alojados en Internet para almacenar, administrar y procesar datos en lugar de un servidor local o un ordenador personal
b) Entrega de diferentes servicios a través de Internet, incluidos servidores, almacenamiento, bases de datos, redes, software y análisis.
c) Solo existe un tipo de soluciones de computación en la nube
d) La computación en la nube se puede proveer sin interacción humana

5. ¿Qué medidas puedes utilizar para mejorar la computación en la nube? (opción múltiple: una respuesta no es correcta)

a) Utiliza una autenticación multifactor
b) Establece diferentes niveles de autorización a la información según las necesidades de las personas
c) Garantizar la formación en materia de protección de datos e información privada
d) Haz copias de seguridad de tus datos/información

Internet de las cosas

1. ¿Qué frases de IoT son correctas? (opción múltiple: elige las opciones correctas siguiendo el principio de opción múltiple. Ninguna, una, más de una o todas las opciones pueden ser verdaderas)

a) El IoT mejorará el transporte público
b) El IoT está convirtiendo los objetos físicos en un ecosistema de información compartida entre dispositivos que se pueden llevar, son portátiles e incluso implantables, lo que hace que nuestras vidas sean ricas en tecnología y datos.
c) Las aplicaciones comerciales de IoT son numerosas
d) Los coches inteligentes, los aparatos fitness y rastreadores portátiles, los asistentes de voz y los coches inteligentes son ejemplos de tecnologías de IoT.

2. De la lista, selecciona las opciones correctas con respecto al Internet de las cosas. (opción múltiple: una respuesta no es correcta)

a) El IoT solo se puede aplicar a personas y hogares y a la industria del automóvil
b) Sistema de dispositivos de computación interrelacionados, máquinas mecánicas y digitales.

c) Convergencia de múltiples tecnologías, análisis en tiempo real, aprendizaje automático, sensores de productos básicos y sistemas integrados
d) El término IoT abarca todo lo conectado a Internet.

3. ¿Cuáles son las aplicaciones más comunes de Internet de la Cosas? (opción múltiple: elige las opciones correctas siguiendo el principio de opción múltiple. Ninguna, una, más de una o todas las opciones pueden ser verdaderas)

a) Dispositivo portátil que monitorea la glucosa en sangre
b) Un frigorífico que crea automáticamente listas de la compra.
c) Ciudades y hogares inteligentes
d) Venta al por menor y tarjetas conectadas

4. Para protegerte de los ciberataques en todas las capas que componen los dispositivos IoT, ¿qué medidas, de la lista anterior, puedes aplicar? (opción múltiple: elige las opciones correctas siguiendo el principio de opción múltiple. Ninguna, una, más de una o todas las opciones pueden ser verdaderas)

a) Autenticación de dispositivo
b) Instala software de seguridad de Internet de buena reputación en tus ordenadores, tabletas y teléfonos inteligentes
c) Utiliza una solución VPN porque ayuda a proteger los datos transmitidos en tu hogar o Wi-Fi público.
d) Visita el sitio web del fabricante del dispositivo con regularidad para obtener actualizaciones de firmware

5. ¿Cuáles son los pasos más importantes para prevenir una violación de la seguridad cibernética? (opción múltiple: elige las opciones correctas siguiendo el principio de opción múltiple. Ninguna, una, más de una o todas las opciones pueden ser verdaderas)

a) Identificar amenazas y vulnerabilidades
b) Exposición al riesgo de activos a través de diferentes tipos de análisis
c) Desarrollar planes de protección y contingencia
d) Determinar cuándo alertar al equipo de respuesta a emergencias, a los profesionales de ciberseguridad, a los proveedores de servicios y/o proveedores de seguros

Soluciones

Cibercrimen

1b, 2ac, 3V
4: Robo de identidad, Ciberacoso, Delitos financieros, ciberacecho/ciberintimidación
5: Ciberterrorismo

Protección contra contenido inapropiado

1: Pornografía, racismo u odio, sitios web Pro-ana, sitios con contenido extremista

2ad, 3b, 4bd

5: confianza, discusión, charla, communicación, discurso

Protección de Datos Personales

1: privacidad de datos, datos personales, uso indebido, protección, fundamental, desarrollos técnicos, redes globales, RGDP
2: aF, bF, cV, dV, eF
3: siete, procesamiento de datos, sanciones máximas, no sensibles, seis, datos personales, datos sensibles, casos excepcionales
4: b e f
5: datos personales, seguridad de los datos, datos personales, privacidad por diseño, privacidad por diseño, privacidad por defecto, diseño tecnológico, privacidad por defecto, configuración por defecto

Protección de teléfonos inteligentes

1ac 2be 3bd
4: aF, bT, cF, dT, eT, fF
5: riesgos de seguridad, última, abstente, política de privacidad, más necesarios, dirección de correo electrónico adicional, acceso, configuración de privacidad, bloquea

Flujo de Información/Communicación en línea

1b
2: Correos electrónico falsos, archivos adjuntos, poco realista, remitente de correo electrónico, irritante, información confidencial, remitente, errores, carpeta de spam, nombres e archivo.
3: b c e h
4: a b d e
5: datos, información, fraudulentas, false identities, información falsa, redes sociales, personal, confidectial, filtro, aceptes, protección de la privacidad, engañosa, informar, autoridades

Control Parental

1 a b c
2: Acoso cibernético, adulto, sexual, menores, abusos, acosador
3: Ciberacoso, víctima, dañará, reputación, negativo, desinformación
4: Menor, netholismo, digitales, emocionales, anímicamente, estado de ánimo
5: Fuga, perpetradores, contraseñas, online, menores, internet

Hardware y software

1: teclado, monitor y ratón; programas o aplicaciones; físico; muchos
2: g
3: Verdadero
4: g
5: g,h

Datos personales en redes sociales

1: a, b, c, d
2: Propietario/proveedor de redes sociales; Ataque de suplantación de identidad; Configuración de privacidad
3: d
4: d
5: a

Ciberseguridad

1: c
2: c
3: d
4: c
5: d

Internet de las cosas

1: a, b, c, d
2: a
3: b
4: a, b, c, d
5: a, b, c, d