Unidad de Contenido

[Cibercrimen]

Proyecto: B-SAFE
Número: 2018-1CZ01-KA204-048148
Nombre del autor: bit cz training
Última fecha de procesamiento: 26.6.2020

Cibercrimen

Introducción

Seguramente ya hayas recibido un email que te pide que cambies tu contraseña bancaria o solicitando alguna deuda o impago. Generalmente estos emails no parecen creíbles, no hay una identificación clara de la persona o de la institución y el lenguaje es bastante malo. Pero mucha gente quiere cumplir con el requerimiento, ya que a menudo temen haber actuado de forma negligente. La siguiente sorpresa es que la cuenta bancaria ha sido extraída y que la deuda no era válida. El último, pero no por ello menos importante, ejemplo de cibercrimen es piratear el software. Por ejemplo, utilizar una copia ilegal del software que no respeta los derechos de imagen ni su precio. Estos son ejemplos de cibercrimen a los que se enfrenta prácticamente cada persona que está en internet.

El cibercrimen es un fenómeno largamente establecido y unido inseparablemente a la conectividad global. Cualquier actividad criminal que involucre un ordenador ya sea como instrumento, objetivo o medio para perpetrar futuros crímenes pertenece al ámbito del cibercrimen. Una definición generalizada de cibercrimen es: "actos ilegales en los que el ordenador es una herramienta , un objetivo o ambos" (IT Act 2000).

El cibercrimen ha sido utilizado para describir un amplio rango de ataques, incluidos los ataques contra los datos de los ordenadores y de sus sistemas, falsificaciones y fraudes relacionados con las ordenadores y ataques al copyright. Nuestra creciente dependencia de los ordenadores y redes digitales convierten a la tecnología en sí misma en un objetivo; ya sea por la obtención de información o como medio para causar daño y disrupción.

Importancia práctica – ¿Para qué necesitas estos conocimientos y habilidades?
Después de trabajar esta unidad de contenidos, conocerás las definiciones de los principales términos relacionados con el crimen en el ciberespacio, podrás reconocer diferentes tipos y métodos de cibercrimen y cómo protegerte del crimen proveniente de los espacios virtuales. También estarás familiarizado con los aspectos peligrosos no solamente para los adultos, sino también para los niños.

1. Construye **conocimiento – El rol del cibercrimen en internet**

El cibercrimen es la cara B de la ciberseguridad. Un amplio espectro de actividad dañina e ilegal llevada a cabo utilizando ordenadores e internet. Esta unidad te ayudará a comprender el cibercrimen y cómo defenderse personalmente, a tus hijos y a tu organización contra ello.

Sobre todo, aunque no siempre, el cibercrimen es cometido por cibercriminales o hackers que quieren ganar dinero. Algunos cibercriminales se organizan, utilizan técnicas avanzadas y tienen elevados conocimientos técnicos. Otros son hackers novatos. Rara vez, el cibercrimen persigue dañar ordenadores por razones ajenas al dinero. Estas pueden ser políticas o personales.

¿Qué significa el cibercrimen? El cibercrimen se define como un crimen en el que el ordenador es el objeto del crimen (hacking, phishing, spamming) o se utiliza como herramienta para cometer algún delito (pornografía infantil, delitos de odio).

Aquí hay unos cuantos ejemplos de los diferentes tipos de cibercrimen:

- Fraude por email y por internet.
- Fraude identitario (en el que la información personal se roba y utiliza)
- Robo de la tarjeta bancaria o del medio de pago.
- Robo y venta de información corporativa.
- Ciber Extorsión (solicitar dinero para evitar una amenaza de ataque).
- Ataques de ransomware (un tipo de ciber extorsión).
- Crypto Hacking (los hackers hacen minería de criptomonedas utilizando recursos que no poseen).
- Ciberespionaje (los hackers acceden a datos del gobierno o de empresas).

Cuando hablamos de cibercrimen siguiendo los ejemplos de arriba, normalmente nos referimos a dos categorías de delito:

1. Un ordenador conectado a una red es el objetivo del delito – este es el caso de ataques sobre la confidencialidad, integridad o disponibilidad de la red.
2. Un ataque cometido mediante la asistencia de ordenadores conectados a una red y relacionados con las tecnologías de la información y de la comunicación: este es el caso de ataques como el robo, el fraude y la falsificación.

El siguiente texto se enfoca en los diferentes delitos cometidos con la asistencia de ordenadores.

El cibercrimen consiste en varios grupos o categorías. Estas categorías ponen el foco en el objeto de protección legal: "delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas del ordenador; delitos orientados al contenido; y delitos orientados al copyright. La cuarta categoría de "delitos orientados al ordenador" no se enfoca en el objeto de protección legal, sino en el método utilizado para cometer el crimen. Esto puede llevar a solapamientos entre categorías.

Categorías de cibercrimen

Vamos a ver ahora cada una de estas categorías

Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas del ordenador All
Todos los delitos de esta categoría están relacionados directamente contra uno de los tres principios legales de confidencialidad, integridad y disponibilidad.

- Acceso ilegal (hacking, cracking)
- Intercepción ilegal (sin derechos)
- Interferencia en los datos (añadiendo códigos maliciosos. Por ejemplo, virus)
- Interferencia en los sistemas (añadiendo, transmitiendo, dañando, borrando, deteriorando, alterando o suprimiendo datos del ordenador. Por ejemplo, virus que frenan o ralentizan los sistemas)

Ejemplo

En 2017, el ataque del WannaCry, presuntamente lanzado por Corea del Norte, liberando un tipo de ransomware que no solamente bloquea el contenido en los dispositivos del usuario, sino que también se expande rápidamente. El virus infectó 300.000 ordenadores alrededor de todo el mundo y los usuarios fueron requeridos a pagar cientos de dólares para descifrar y recuperar sus datos.

Delitos relacionados con el ordenador
Esta categoría cubre muchos delitos que necesitan un ordenador para ser cometido. Al contrario que en las categorías precias, estos delitos no son a menudo tan estrictos en la protección de los principios legales.

- Fraude relacionado con el ordenador
- Falsificación relacionada con el ordenador
- Phishing
- Robo de identidad
- Uso indebido de dispositivos

Ejemplo

Entre 2013 y 2016, Yahoo experimentó una brecha que tuvo como consecuencia el robo de tres mil millones de cuentas de usuario. En algunas de esas cuentas, los atacantes fueron víctima del robo de

información privada y de contraseñas, que podían ser utilizadas para acceder a las cuentas de usuario en otros servicios online. Muchos de estos datos están disponibles todavía hoy, de manera gratuita o pagada, en la dark web.

Delitos relacionados con el contenido

Esta categoría cubre:

- Material erótico o pornográfico
- Pornografía infantil
- Material xenófobo - racismo, delito de odio, exaltación de la violencia
- Insultos relacionados con símbolos religiosos
- Apuestas y juegos online ilegales
- Difamación e información falsa
- Spam y amenazas relacionadas

El desarrollo de instrumentos legales a tener en cuenta en esta categoría está muy influenciada por los enfoques nacionales, que pueden tener en cuenta fundamentalmente principios legales y culturales. Para contenido ilegal, sistemas de valores y sistemas legales que difieren mucho entre las distintas sociedades.

Ejemplo

Un conocido pedófilo, Matthew Falder, quien fue un académico del Reino Unido con un Doctorado de la Universidad de Cambridge University, fue considerado en 2017 culpable de 137 delitos cometidos contra 46 individuales, incluyendo violación y actividad sexual con un niño de la familia, incitación a la explotación sexual de un menor y posesión y distribución de pornografía infantil, entre otros delitos (Dennison, 2018; Vernalls y McMenemy, 2018). Él chantajeó a sus víctimas para cometer actos abusivos y degradantes contra ellos mismos (p.e., autodañarse y lamer una escobilla del baño manchada) y contra otros, y recoger estos actos en imágenes y vídeos (Davies, 2018; Dennison, 2018). Él entonces compartió las imágenes y vídeos en sitios dañinos (como Hurt 2 the Core, ahora extinto), que se especializan en violaciones, asesinatos, sadismo, tortura y contenido pedófilo (McMenemy, 2018).

Delitos relacionados con el copyright

La digitalización ha abierto la puerta a nuevas violaciones de los derechos de imagen. Las más comunes incluyen el intercambio de canciones, archivos y software protegidos por copyright a través de servicios de compartición, obviando el copyright. Este es el tipo de cibercrimen más frecuente y generalmente se encuentra tolerado por el conjunto de la sociedad, pero deberíamos asumir que se trata de una actuación illegal que acarrea consecuencias.

Ejemplo

El más común de los delitos relacionados con el copyright es utilizar una copia ilegal de software en el ordenador de casa o descargar música o películas de sitios online como ShareRapid o MegaRapid.

1. Aplica conocimiento

Ejercicio VERDADERO/FALSO

Asociado al objetivo específico: OE_ conocerás el rol del cibercrimen en internet_01_01: puedes reconocer las diferencias entre los distintos tipos de cibercrimen.

Situación: Si la música o el cine están colgados en Internet, puedo descargarlos legalmente.
Tarea: Elige si la respuesta correcta es verdadero o falso:

- Verdadero
- Falso

Ejercicio OPCIÓN MÚLTIPLE

Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: más respuestas podrían ser verdaderas.
Marque las categorías correctas de ciberdelito

- **Delitos informáticos**
- **Robo físico de una computadora, tableta o teléfono**
- Delitos relacionados con el contenido
- **Delitos relacionados con los derechos de autor**

Ejercicio EMPAREJAR PREGUNTAS Y RESPUESTAS

Tarea: Relaciona las respuestas - Elige las opciones correctas seleccionándolas desde el menú desplegable hasta el texto exacto.

_____ cubre muchos delitos que necesitan un sistema informático para cometerse. A diferencia de las categorías anteriores, estos delitos generales a menudo no son tan estrictos en la protección de los principios legales.
_____ incluye violaciones de instrumentos legales más influenciados por enfoques nacionales, que pueden tomar en cuenta principios culturales y legales fundamentales. Los sistemas de valores y los sistemas legales difieren ampliamente entre sociedades.
_____ incluyen el intercambio de canciones, archivos y software protegidos por derechos de autor en sistemas de intercambio de archivos o mediante servicios de alojamiento compartido y la elusión de los sistemas de gestión de derechos digitales (DRM)

Delitos relacionados con la informática, *Delitos relacionados con los derechos de autor,* ***Delitos relacionados con el contenido***

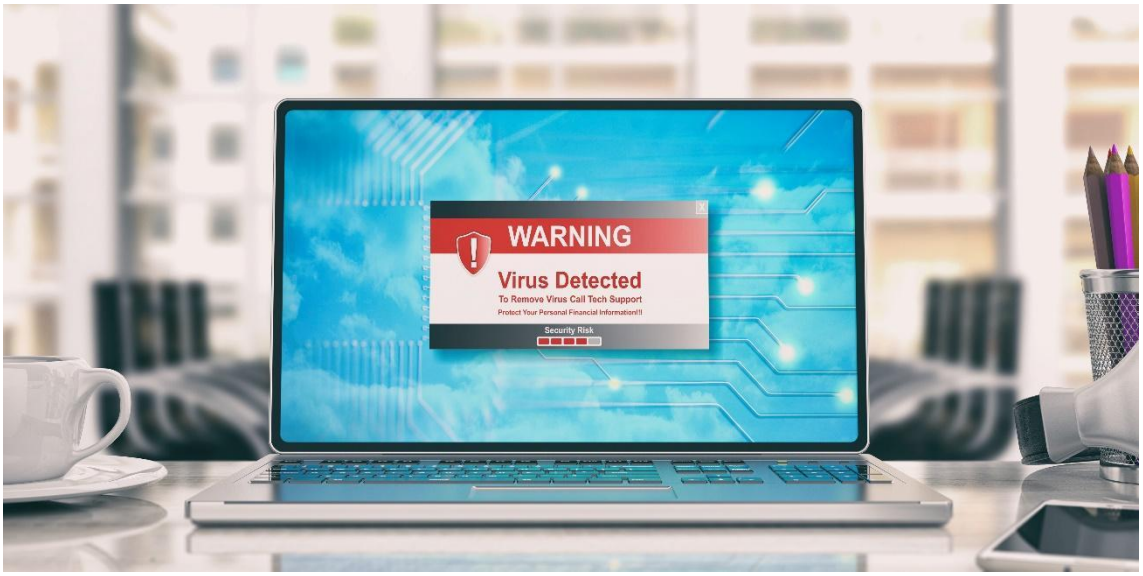
2. Construye conocimiento - Los métodos y ejemplos del cibercrimen

Ya hemos visto las cuatro categorías que se distinguen cuando se trata de cibercrimen. Ahora vamos a realizar una Mirada en profundidad a los roles de los ordenadores en el cibercrimen y los métodos para atacar en el ciberespacio:

Los ordenadores cumplen con cuatro roles en los crímenes: sirven como **objetos, sujetos, herramientas y símbolos**. Los ordenadores son objetos de crimen cuando son saboteados o robados. Juegan el rol de sujetos cuando son el espacio en el que se cometen los crímenes. Los ataques mediante virus caerían bajo esta categoría. Cuando los crímenes mediante automatización se llevan a cabo, los ordenadores se convierten en el sujeto de los ataques. El tercer rol de los ordenadores en los crímenes como herramientas, permitiendo a los criminales producir información falsa y controlar crímenes. Finalmente, los ordenadores se utilizan como símbolos para embaucar a las víctimas.
El más común es el cibercrimen en el que el ordenador se utiliza como sujeto. Los principales métodos para utilized un ordenador como elemento criminal son:

- malware
- hacking
- spam
- phishing
- Ataques DoS Distribuidos (DDoS)

Los principales métodos para atacar



Definición

> ***Malware*** es una etiqueta general para hablar de software malicioso que se propaga entre ordenadores y que interfiere en las operaciones de los mismos. Puede ser destructivo, por ejemplo borrando archivos o causando caídas del sistema, pero también puede utilizarse para robar datos personales.

Hay **muchas formas de malware**. Algunas de ellas son las siguientes:

- Los **virus** pueden causar una leve disfunción informática, pero también pueden tener efectos más graves en términos de dañar o eliminar hardware, software o archivos.
- Los **gusanos** son programas que se reproducen a sí mismos, pero pueden propagarse de forma autónoma, dentro y entre los ordenadores, sin necesidad de un ordenador central ni de ninguna acción humana. Por lo tanto, el impacto de los gusanos puede ser más severo que el de los virus, destruyendo redes enteras.
- Los **troyanos** son una forma de malware que parecen ser programas legítimos pero que facilitan el acceso ilegal a una computadora. Pueden realizar funciones, como el robo de datos, sin el

conocimiento del usuario y pueden engañar a los usuarios realizando una tarea rutinaria mientras realizan acciones ocultas y no autorizadas.

- El spyware es un software que invade la privacidad de los usuarios reuniendo información sensible o personal de sistemas infectados y vigilando los sitios web visitados.

Definición
El pirateo es un proceso común que resulta en la violación de la privacidad y la información confidencial de una persona. Se identifican las debilidades de un sistema o las lagunas en una red y se accede a los detalles privados. Por lo tanto, el hacking también se conoce como una intrusión no autorizada.

Sin embargo, la piratería informática no siempre se percibe como un robo y se puede utilizar para causas productivas. Este tipo de piratería que implica buenas intenciones se conoce como piratería ética. S realiza para asegurar el sistema operativo.

Los hackers pueden clasificarse en diferentes categorías como sombrero blanco, sombrero negro y sombrero gris, según su intención de piratear un sistema.

Hackers de sombrero blanco o hackers éticos

Nunca tienen la intención de dañar un sistema, sino que tratan de averiguar las debilidades de una computadora o un sistema de red para evaluar su vulnerabilidad. La piratería ética no es ilegal y es uno de los trabajos más exigentes de la industria de la informática. Numerosas empresas contratan a hackers éticos para pruebas de penetración y evaluaciones de vulnerabilidad

Hackers de sombrero gris
Son una mezcla de hackers de sombrero negro y de sombrero blanco. Actúan sin intención maliciosa pero para su diversión, explotando los fallos en la seguridad de un sistema o red informática sin el permiso o conocimiento del propietario. Intentan llamar la atención de los propietarios sobre la debilidad y obtener el aprecio o una pequeña recompensa por parte de los propietarios.

Hackers de sombrero negro o crackers
Hacen piratería para obtener el acceso no autorizado a un sistema y dañar sus operaciones o robar información sensible. La piratería de los Black Hat es siempre ilegal por sus malas intenciones, que incluyen el robo de datos corporativos, la violación de la privacidad, el daño al sistema operativo, el bloqueo de la comunicación de la red, etc.

Definición

El Spam es un email no solicitado o email basura enviado típicamente a multitud de receptores alrededor del mundo y a menudo relacionador con productos farmaceúticos o de pornografía. Los emails de spam se utilizan también para enviar emails de phising o malware y puede ayudar a maximizar el retorno potencial para los criminales.

La delincuencia se aleja de los métodos tradicionales como la violencia, las drogas o el robo, y la delincuencia basada en Internet es cada vez más frecuente. Esto va de la mano de la tendencia resultante del aumento de los negocios y las comunicaciones en línea. Las víctimas de la delincuencia pueden perder cualquier cosa que tenga valor: la seguridad, la paz, el dinero o la propiedad.

Paréntesis

El primer estudio que examina el impacto emocional de los delitos cibernéticos muestra que las reacciones más fuertes de las víctimas son de enfado (58%), molestia (51%) y engaño (40%), y en muchos casos, se culpan a sí mismos por ser atacados. Sólo el 3% no cree que les pueda suceder, y casi el 80% no espera que los ciberdelincuentes sean llevados ante la justicia, lo que lleva a una irónica reticencia a tomar medidas y una sensación de impotencia.

Definición

Phishing Una campaña de phishing es cuando se envían masivamente correos electrónicos de spam, u otras formas de comunicación, con la intención de engañar a los destinatarios para que hagan algo que socave su seguridad o la de la organización para la que trabajan. Los mensajes de las campañas de "phishing" pueden contener archivos adjuntos infectados o enlaces a sitios web maliciosos. O pueden pedir al receptor que responda con información confidencial.

Ejemplo

Un ejemplo famoso de estafa de phishing de 2018 fue el que tuvo lugar durante la Copa del Mundo. De acuerdo con los informes de Inc, la estafa de phishing del Mundial involucró a correos electrónicos que fueron enviados a los aficionados al fútbol. Estos correos spam trataban de atraer a los aficionados con viajes gratis falsos a Moscú, donde se estaba celebrando el Mundial. A las personas que abrían y hacían clic en los enlaces contenidos en estos correos electrónicos les robaban sus datos personales.

Definición

Los ataques DoS distribuidos (DDoS) son un tipo de ataque cibernético que los ciberdelincuentes utilizan para hacer caer un sistema o una red. A veces se utilizan dispositivos de IO (Internet de las cosas) conectados para lanzar ataques DDoS. Un ataque DDoS sobrecarga un sistema utilizando uno de los protocolos de comunicación estándar que usa para enviar spam al sistema con solicitudes de conexión.

Ejemplo

Un ejemplo famoso de este tipo de ataque es el ataque DDoS 2017 en la página web de la Lotería Nacional del Reino Unido. Consiguió tirar la página web de la lotería y la aplicación móvil, impidiendo a los ciudadanos del Reino Unido jugar.

Los cibercrímenes más frecuentes incluyen:

Suplantación online

Este delito es uno de los ciberdelitos más comunes que existen. Para este acto delictivo es típico utilizar el nombre, la dirección de dominio, el número de teléfono o cualquier otra información de identificación de otra persona sin su consentimiento y causar daño o cometer fraude, lo cual constituye delito.

Ejemplo

Claire ha comenzado a ser acosada por extraños después de que alguien publicara un mensaje en Internet ofreciendo servicios sexuales en su nombre. El mensaje incluía información privada, como su número de teléfono y la dirección de su casa.

Ciberstalking

El acecho físico puede incluir el seguimiento en persona, la vigilancia secreta, el envío de llamadas y mensajes de texto persistentes para manipular, y otros medios diferentes para acercarse a la víctima de forma inesperada. Lo que diferencia al ciberstalking es que se comete con tecnología en línea como el correo electrónico, las redes sociales, la mensajería instantánea, o los datos personales disponibles en internet. Todo en Internet puede ser utilizado por los acosadores cibernéticos para realizar un contacto inapropiado con sus víctimas.

Ejemplo

Después de que John y su novia rompieran, empezó a acosarla colocando un móvil de prepago con GPS debajo de su coche. John rastreó los movimientos de su ex-novia, y la siguió ingresando a la cuenta del teléfono. John también llamaba a su ex más de 200 veces al día.

Cyberbullying

Podemos denominar este crimen como el uso de los medios sociales o de Internet para intimidar, acosar, amenazar o menospreciar a los demás. En general, si una persona utiliza Internet o cualquier otra forma de comunicación electrónica para amenazar, acosar o asustar a otra persona, esta conducta puede constituir un delito.

Ejemplos

Mientras viaja con su equipo juvenil, uno de los jugadores toma una foto embarazosa de una chica que conoció en la pista. Luego publica la foto en Facebook y la envía a todos los demás jugadores del equipo. La foto posteriormente se distribuye.

Tres de los compañeros de Paul le envían mensajes de texto, culpándole de la pérdida del equipo y diciéndole que no sabe cómo jugar. Paul tiene miedo de contarles a su entrenador y a sus padres que lleva aguantando el acoso durante toda la temporada de hockey. No volverá a jugar al hockey la próxima temporada.

¿Cuál es la diferencia entre ciberbullying y ciberstalking?

Ciberbullying	Ciberstalking
El ciberbullying es el contacto constante con la persona; diciendo cosas hirientes a la misma o contándoles a otros información falsa sobre ella. Por ejemplo, el agresor crea el grupo de Facebook titulado "Odio a..." e invita a todos sus amigos a unirse a él.	El ciberstalking o acoso cibernético es una obsesión por averiguar todo lo que puedas sobre otra persona (sin preguntarle). Por ejemplo, el delincuente averigua dónde nació la persona, si está casada, etc.

Robo de identidad y de datos

El *robo de identidad* 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 relacionados con subastas y salarios, etc.
El *robo de datos* es el acto de poseer ilegalmente datos sensibles, que incluyen información no codificada de tarjetas de crédito almacenada en empresas, secretos comerciales, propiedad intelectual, código fuente, información de clientes o registros de empleados.

Ejemplo

El Marriott fue hackeado en 2018, cuando se robaron 383 millones de registros de huéspedes y más de 5 millones de números de pasaporte. Las violaciones de datos han aumentado en frecuencia y gravedad. Esos datos podrían venderse en el mercado negro y cualquiera podría hacer uso de ellos y utilizar la otra identidad.

Crímenes financieros

Esta categoría incluye actividades que generan riqueza de manera deshonesta para quienes participan en la conducta en cuestión. Consiste en la explotación de información privilegiada o en la adquisición de bienes ajenos mediante el engaño para obtener un beneficio material. Se considera comúnmente que los delitos financieros abarca, entre otros: fraude, blanqueo de dinero, soborno, cohecho y corrupción y muchos otros.

Ejemplo

Uno de los delitos financieros recientes más sonados es el escándalo de Enron, cuando se descubrió que la compañía de energía cometía fraude y la corrupción se encontraba generalizada, y el escándalo de inversiones de Bernie Madoff, donde Madoff aparentaba tener una empresa de inversiones exitosa, pero en realidad sólo robaba dinero de nuevos clientes y se lo daba a clientes más antiguos (Esto es lo que se llama un esquema Ponzi, y Madoff dirigió el más grande de la historia). Madoff fue condenado por numerosos delitos, incluyendo el lavado de dinero y muchos tipos diferentes de fraude..

El cibercrimen es a menudo cometido por alguien cercano, por ejemplo en tu empresa. Este tipo de delito cibernético se denomina fraude interno y se refiere a un tipo de fraude que comete un individuo contra una organización. En este tipo de fraude, el autor del mismo participa en actividades diseñadas

para defraudar, apropiarse indebidamente de la propiedad o eludir las normas, las leyes o las políticas de una empresa. Por ejemplo, el fraude interno comprende actividades como la no notificación de las transacciones de forma intencionada, la realización de transacciones no autorizadas y el marcado erróneo intencionado de los números.
El fraude interno puede clasificarse en dos grandes categorías: la malversación de fondos y el robo de identidad. En el caso de la malversación, el dinero en efectivo se coge directamente de las organizaciones y, en el caso del robo de identidad, la información personal de un cliente es objeto de apropiación indebida por parte del empleado para obtener un beneficio. Entre los ejemplos de fraude interno más comunes se incluyen:

- El robo del dinero de un cliente
- Abuso del crédito de un consumidor
- Lavado de dinero
- Fraude de adquisición
- Robo de datos

Por otro lado, las actividades fraudulentas de personas ajenas a la compañía se denomina fraude externo. Incluye el robo de dinero o acciones por parte de personas ajenas al negocio. Algunos ejemplos de fraude externo son:

- Robo de identidad: tomar control de la identidad virtual de la persona
- Falsificación de la información de una factura (modificando el número de cuenta del beneficiario)
- Falsificación de la información de un pedido, por lo que los bienes son enviados a un destinatario incorrecto
- Falsificación de la voz o de la firma de otra persona
- Falsificación de emails

Existen varias finalidades de los ciberataques en el ciberespacio, que van desde las más moderadas hasta las más despiadadas. Los 4 propósitos más típicos son:

- vandalismo (ataques comunes a los sitios web de gobiernos)
- propaganda (diseminación de información política principalmente a través de internet)
- Denegación de acceso (por ejemplo, ataques contra fuerzas armadas que utilizan ordenadores y satélites para la comunicación)
- ataques de red contra la infraestructura (ataques a los sistemas de transmisión de las empresas de ingeniería eléctrica, industria del gas, industria de la calefacción, industria petrolera e infraestructura de comunicaciones, que son sensibles a los ciberataques, etc.)

2. Aplica conocimiento

Ejercicio de RESPUESTA SIMPLE

Asociado al objetivo específico: OE_ conocerás el rol del cibercrimen en internet_01_02: puedes nombrar los métodos para atacar en el ciberespacio.

Situación: ¿Qué son los ataques DoS distribuidos? (DDoS)?
Tarea: Elige la opción correcta en este test de selección múltiple. Solamente una respuesta es verdadera.

- Emails de spam u otras formas de comunicación enviados masivamente
- Un tipo de ataque cibernético que se utiliza para tumbar una red
- Emails no deseados enviados a un sin número de receptores alrededor del mundo
- El uso no autorizado, o el acceso a los recursos de una red, que explotan las vulnerabilidades en la seguridad de las identificaciones en las redes

Ejercicio de RESPUESTA SIMPLE

Tarea: Elige la opción correcta en este test de selección múltiple. Solamente una respuesta es verdadera.

¿Cuál de las siguientes actividades realiza un hacker de sombrero gris?

- Es la persona que difunde información no verdadera sobre otra persona.
- Es la persona que intenta robar la información de la identificación personal.
- Es la persona que accede a un sistema sin permiso, solamente por diversión.
- Es el responsable de muchos crímenes financieros a través de internet.

Ejercicio de RESPUESTA SIMPLE

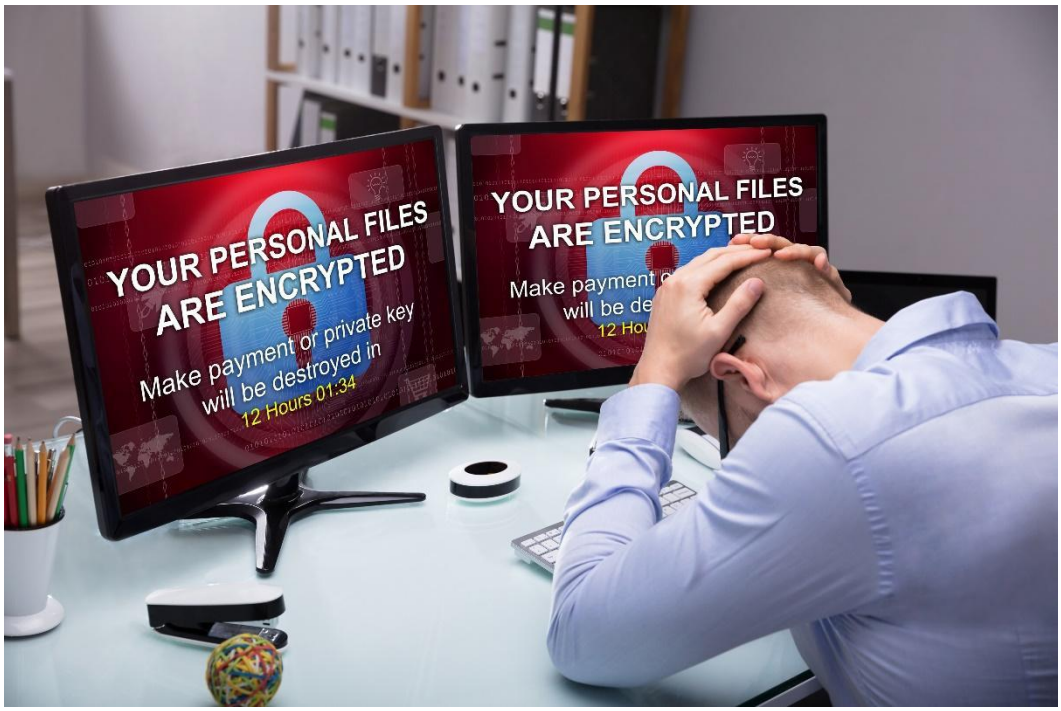
Asociado al objetivo específico: OE_ conocerás el rol del cibercrimen en internet_01_03: puedes describir el fraude interno y externo

Situación: ¿Qué significa el fraude interno?
Tarea: Elige la opción correcta en este test de selección múltiple. Solamente una respuesta es verdadera.

- El fraude interno es cometido por los proveedores en el caso de robo del dinero de la compañía.
- El fraude interno incluye actividades como el ciberacoso o el grooming.
- El fraude interno es cometido por los empleados en caso de realizar transacciones no autorizadas.
- El fraude interno es cometido por los clientes de la empresa.

3. Construye conocimiento – Impacto del cibercrimen

Los ordenadores también pueden ser utilizados para atacar y cometer crímenes en el mundo real (violaciones de los derechos de propiedad intelectual, fraudes con tarjetas de crédito, fraudes en la transferencia de fundos electrónicos, pornografía, etc.) e incluso terrorismo. Los terroristas suelen utilizar las tecnologías de la información para planificar y ejecutar sus actividades delictivas. Cuando esto ocurre, se le llama ciberterrorismo. El aumento de la interacción internacional y el uso generalizado de la tecnología de la información ha facilitado el crecimiento de la delincuencia y el terrorismo. Gracias a los avances en la tecnología de las comunicaciones, no es necesario que las personas estén en un país para organizar ese tipo de delitos. Por lo tanto, los terroristas y los delincuentes pueden encontrar lagunas de seguridad en el sistema y pueden funcionar desde lugares inusuales en lugar de en su país de residencia.



La mayoría de los incidentes internacionales futuros, ya sean militares o de espionaje, tendrán una dimensión cibernética. Por lo tanto, resulta muy oportuno considerar la evaluación de estos ataques. En la actualidad se debate la posibilidad de que los incidentes se conviertan en un conflicto bélico insostenible, en el que puedan producirse muertes, destrucción, daños personales o daños a la propiedad. El problema es que atribuir las acciones a un estado en particular es casi imposible. Es difícil reconocer a un atacante particular sin la cooperación precisa del Estado en cuyo territorio se encuentra el atacante.

El impacto del cibercrimen

Los impactos del cibercrimen pueden ser devastadores debido al elevado riesgo de pérdida de datos y al impacto financiero.

En individuos

Violación de datos, robo de identidad, problemas con dispositivos… El cibercrimen puede tener un gran impacto sobre los individuos. Puede que te encuentres con cargos sospechosos en tu tarjeta de crédito como resultado de un robo de identidad, un ataque que exige un rescate de cientos o miles de euros para liberar tus archivos, o costosos cargos en datos o electricidad por parte del criptojacking o las redes de bots. Los costes pueden ser más graves que monetarios cuando el ciberacoso incluye el acoso sexual.

En empresas y gobiernos

Las empresas, así como las organizaciones de salud y los gobiernos, también pueden sufrir la pérdida de datos confidenciales, ingentes pérdidas financieras y daños a la marca. El ransomware contra las pequeñas y medianas empresas en 2019 exigió 5.900 dólares para desbloquear sus archivos o sistemas. Y lo que es mucho peor, el tiempo de inactividad durante estos ataques, les costó a las empresas afectadas un promedio de 141.000 dólares. Estop or no hablar del ransonware contra los gobiernos, como el que hizo que el condado de Jackson, Georgia, pagara 400.000 dólares para restaurar sus sistemas e infraestructura de TI.

Otro término que se utiliza en este context es el de ciberguerra. Echemos un vistazo en profundidad a los dos términos.

¿Qué es el ciberterrorismo?	¿Qué es la ciberguerra?
El concepto de ciberdelincuencia se confunde a menudo con el de ciberterrorismo. El ciberterrorismo es siempre más severo que otros comportamientos que se llevan a cabo en o a través del ciberespacio. La OTAN define el ciberterrorismo como "un ciberataque que utiliza o explota las redes informáticas o de comunicación para causar la suficiente destrucción o perturbación como para generar miedo o intimidar a una sociedad con un objetivo ideológico".	La guerra cibernética implica la utilización y el ataque hacia ordenadores y redes en la guerra. Implica operaciones ofensivas y defensivas ante la amenaza de ciberataques, espionaje y sabotaje. La guerra cibernética se ha definido como "las acciones de un Estado-nación para penetrar en las computadoras o redes de otra nación con el fin de causar daño o interrupción".

Ejemplo
La ciberguerra, incluyendo los ataques a la red, han ganado alguna importancia adicional desde el 11 de septiembre. La situación después de los ataques del 11 de septiembre trajo consigo un intenso debate sobre el uso de las tecnologías de la información y la comunicación por parte de los terroristas. Este debate se vio facilitado por los informes de que los delincuentes utilizaron Internet en la preparación de su ataque. Aunque los ataques no eran ciberataques, Internet desempeñó un papel importante en la preparación del delito. En este contexto, se descubrieron diferentes formas en las que las organizaciones terroristas utilizan Internet.

3. Aplica conocimiento

Ejercicio de RESPUESTA SIMPLE

Asociado al objetivo específico: OE_ conocerás el rol del cibercrimen en internet_01_05: puedes nombrar tipos de cibercrimen.

Situación: ¿Cuál es el peor ciberataque que se comete en el mundo real?
Tarea: Elige la opción correcta en este test de selección múltiple. Solamente una respuesta es verdadera.

- Fraudes con la tarjeta de crédito
- Pornografía
- Ciberterrorismo
- Robo de identidad

Ejercicio OPCIÓN MÚLTIPLE

Tarea: Elija las opciones correctas siguiendo el principio de opción única: más respuestas podrían ser verdaderas.
¿Qué impacto puede tener el ciberdelito para las personas?

- Robo de identidad
- Perder el trabajo
- Problemas saludables
- Violaciones de datos

Ejercicio **EMPAREJAR PREGUNTAS Y RESPUESTAS**

Tarea: Elige las opciones correctas seleccionándolas desde el menú desplegable hasta el texto exacto.

_____ también puede sufrir pérdida de datos confidenciales, enormes cargas financieras y daños a la marca.

empresas, empleados, hackers

4. Construye conocimiento - Posibilidades para la prevención y la protección

Todo, desde el dinero robado, el robo de los datos personales y financieros, la pérdida de productividad y el daño y la destrucción de datos críticos corporativos o individuales, se clasifica como ciberdelito. Desafortunadamente, tanto los hackers como los que cometen cibercrímenes, son cada vez más sofisticados.
¿Cuáles son las mejores formas de proteger tu ordenador y tus datos personales?
La mejor manera de protegerse contra el cibercrimen es la prevención. Para contar con seguridad online, es bueno tener en cuenta cinco puntos clave: Precaución, Prevención, Protección, Preservación y Perseverancia.

Para cumplir con estos puntos, es importante llevar a cabo los siguientes pasos:

1. Evitar la divulgación de información personal en Internet y en los correos electrónicos
2. Considera cuidadosamente el envío de cualquier fotografía en línea. Cualquiera puede usarla en cualquier momento en otro contexto
3. Usa contraseñas fuertes
4. Utiliza y actualiza el software antivirus
5. Evita enviar el número de tarjeta de crédito y las contraseñas a través del correo electrónico
6. Vigila los sitios a los que acceden tus hijos
7. Haz una copia de seguridad de tus datos para evitar la pérdida de información debida al ataque de un virus.

8. Usa un programa de seguridad que dé control sobre las cookies
9. Manten actualizados los programas informáticos y el sistema operativo
10. Nunca abras archivos adjuntos en correos electrónicos de spam
11. No hagas clic en los enlaces de los correos electrónicos de spam o de sitios web no confiables
12. Contacta directamente con las empresas cuando hayas recibido una solicitud sospechosa
13. Vigila los extractos de tu cuenta bancaria
14. Ten en cuenta los sitios web que visitas

¿Cómo puedo reconocer los sitios webs seguros?

Los 3 consejos sobre seguridad en los sitios web que aparecen a continuación despejarán las dudas y te enseñarán a identificar si un sitio es confiable o no. Primero, aprenderás un par de controles visuales simples que te darán información útil de un vistazo. Luego, te explicaremos las herramientas de seguridad en los sitios web que debes tener para informarte y guiarte. Por último, te diremos cómo investigar un poco más a fondo en caso de que aún te quede alguna duda. Ahora, seremos más cuidadosos y volveremos a poner el foco en la navegación web.

1 – Controles visuales de seguridad de una web

- Haz una doble comprobación de las URL. Empecemos con el consejo más fácil: no es nada difícil comprobar que la URL parece legítima. Antes de hacer clic en cualquier enlace, pasa el cursor por encima de él y mira en la esquina inferior izquierda de la pantalla en la que se muestra la URL. El primer truco del phishing es parecer lo más auténtico posible. A primera vista, la URL puede parecerse al verdadero McCoy, pero una inspección más detallada puede revelar un 1 en lugar de una l, o .net en lugar de .com. Prepárate para comprobar la validez de todas y cada una de las URL antes de hacer clic o antes de introducir cualquier información personal como puede ser un nombre de usuario y una contraseña.
- Comprueba si hay https. Esas letras que ves al principio de cada URL significan Protocolo de Transferencia de Hipertexto (http). Es la base de cómo se comunican los datos en la web. Y aunque resulte muy útil, también es fácilmente hackeable. Sin embargo, cuando se le añade una "S" como en "https" (y el icono del candado), te indica que el sitio es seguro. Los sitios web con un icono de candado en la barra de direcciones y un prefijo https se encuentran encriptados y tienen un certificado SSL de confianza, que básicamente garantiza una conexión segura entre el sitio web y el navegador. Si no puedes verificar que un sitio web o un enlace es seguro con https, estáte atento y no introduzcas ninguna información personal.

Y ten en cuenta que los ciberdelincuentes harán todo lo que esté en sus manos para presentarse como legítimos, por lo que, aunque los sitios web https sean más seguros, podrías encontrarte en uno dirigido por un ladrón. Así que, si todavía sospechas de un sitio https:, utiliza las otras herramientas de seguridad que se indican a continuación para comprobar si un sitio web es seguro.

2 – Herramientas de seguridad web

- Utiliza las herramientas que incorpora tu navegador. Las primeras herramientas con las que debes familiarizarte son las medidas de seguridad que ya se encuentran en tu navegador. Echa un vistazo a tu configuración de privacidad y seguridad. Lo más probable es que descubras que la configuración predeterminada es más laxa de lo que te gustaría. Ajusta manualmente las reglas y la configuración de la manera que te resulte más cómoda. Bloquea las ventanas emergentes, evita las descargas automáticas y no permitas el seguimiento. Tus opciones variarán dependiendo del navegador que elijas.

- Ejecuta un control de seguridad del sitio web. Hay varios entre los cuales puedes elegir, pero recomendamos VirusTotal por su posición imparcial. Estas herramientas en línea utilizan escáneres antivirus y otras soluciones de seguridad para comprobar si un sitio web se encuentra amenazado. Simplemente introduce la URL que quieras que sea escaneada en la barra de búsqueda del sitio y obtendrás el resultado al instante: introduce una URL, y VirusTotal te dirá si el sitio es sospechoso.

-
- Instala herramientas de seguridad web. Para una total confianza en la seguridad del sitio web, protégete con las mejores suites de seguridad cibernética, (p.e. Avast Free Antivirus, McAfee, AVG, Windows Defender). También puedes añadir el beneficio de la privacidad a la seguridad del sitio web si utilizas una red privada virtual.

3 - Investigación rápida de la seguridad del sitio web

- Comprueba los datos de contacto de la web. Si has hecho todo lo anterior y aún no estás seguro, entonces ve hasta la puerta principal y llama. Es decir, encuentra la información de "Contáctenos" en el sitio y llámales. Dependiendo de cómo (y de si) te respondan, te darán una pista de si se trata o no de una operación legítima.

- Comprueba si tu antivirus tiene un Certificado Anti-Phishing. No todos lo tienen. Busca plataformas de terceros que realicen pruebas de antiphishing, como AV-Comparatives. Estas plataformas testan los productos antivirus contra URL de phishing (que intentan obtener su información personal) y comprueban si hay falsos positivos cuando se trata de sitios web bancarios legítimos, para asegurarse de que el producto de seguridad conozca la diferencia-
- Comprueba si la URL dispone de política de privacidad. Esto es algo obvio. Si un sitio web no tiene una política de privacidad, es una señal de alerta para tener que comprobar si la empresa es legítima o no.
- Busca al propietario del dominio del sitio web usando WHOIS. También puedes investigar quién es el propietario de un dominio en particular revisando los registros públicos disponibles a través de una búsqueda "WHOIS". Conoce todo sobre el dominio, incluyendo quién lo registró y cuándo lo hizo.

Una respuesta de negocio ante el cibercrimen

Como empresa, la mejor apuesta contra el cibercrimen es preparar un plan sólido que dé respuesta a los posibles incidentes. A menudo, la planificación no es suficiente: hay que contar con el personal de seguridad y las herramientas necesarias para ejecutarla. Un plan de respuesta a incidentes, de acuerdo con el marco del Instituto SANS (una de las organizaciones más fiables sobre estas temáticas), ha de incluir:

- Preparación: codificar la política de seguridad, identificar los tipos de incidentes de seguridad críticos, preparar un plan de comunicación y documentar las funciones, responsabilidades y procesos de cada uno. Reclutar miembros para el equipo de respuesta a incidentes de seguridad informática y entrenarlos..
- Identificación: utilizar herramientas de seguridad para detectar con precisión comportamientos anómalos en el tráfico de la red, las conexiones punto a punto, las aplicaciones o las cuentas de usuario, y recopilar rápidamente pruebas para decidir qué hacer en cada incidente.
- Contener: aislamento del problema.
- Limpiar y volver a poner en marcha los sistemas afectados gradualmente.
- Erradicación: identificar la raíz del incidente y hacer todo lo posible para asegurarse de que el problema no se repita. Arreglar las medidas de seguridad rotas que dejan entrar a los atacantes, reparar las vulnerabilidades y asegurarse de limpiar el malware de todos los puntos de contacto.
- Recuperar: hacer copias de seguridad de los sistemas de producción, teniendo cuidado para evitar otro ataque similar. Testar para asegurarse de que los sistemas están respaldados y funcionan como de costumbre.
- Lecciones aprendidas: hasta las dos semanas después del incidente, repasar con el equipo para entender qué fue bien y qué no, y mejorar el plan de respuesta ante los incidentes.

La UE trata de combatir el cibercrimen a través de una amplia gama de medios. En 2005, el Consejo adoptó la estrategia antiterrorista de la UE para luchar contra el terrorismo y hacer de Europa un lugar más seguro. La estrategia incluye cuatro pilares: prevenir, proteger, perseguir, responder

Para luchar y perseguir el cibercrimen a todos los niveles, la UE ha implementado las siguiente acciones legislativas:

- 2001 – El Marco sobre la Lucha Contra el Fraude y la Falsificación, en la que se definen los comportamientos fraudulentos que los Estados de la UE deben considerar como delitos penales punibles.
- 2002 – Directiva sobre la Privacidad Digital, que define las regulaciones de las comunicaciones electrónicas dentro de la UE, para incrementar la privacidad para los individuales y entidades.
- 2011 – Una Directiva sobre el Combate de la Explotación y la Pornografía Infantil Online, que aborda su evolución en el entorno online, como la captación de menores (delincuentes que se hacen pasar por niños para atraer a menores con fines de abuso sexual)
- 2013 – Una Directiva sobre los Ataques contra los SIstemas de Información, que tiene por objeto hacer frente a los ciberataques a gran escala para reforzar las leyes nacionales sobre delitos cibernéticos e introducir sanciones penales más severas

Las organizaciones activas internacionalmente tratan de contribuir a la lucha contra el delito cibernético. Hay dos organizaciones importantes que operan en la UE:

4. Aplica conocimiento

Ejercicio de SELECCIÓN SIMPLE

Tarea: Elige la opción correcta en este test de selección múltiple. Solamente una respuesta es verdadera.

¿Qué es el Certificado Anti-Phishing?

- Comprueba si hay falsos positivos cuando se trata de sitios web bancarios legítimos, para asegurarse de que el producto de seguridad es capaz de diferenciarlo
- Verifica que una web o enlace es seguro con https

- Verifica el propietario real de un site

Ejercicio VERDADERO/FALSO

Tarea: Selecciona la opción correcta entre verdadero o falso. Solamente una respuesta es la correcta.

Cuando se añade al enlace una "S", como en “https” (y el icono del candado) indica que la web es más segura.

- Verdadero
- **Falso**

---

5. Construye **conocimiento - El impacto del cibercrimen en la vida**

Internet **puede ser un entorno peligroso para los niños y también para los adultos**. Especialmente en esta época digital donde los medios sociales como Facebook, Instagram o Internet en general juegan un papel principal. Proteger especialmente a los niños en Internet requiere concienciarse sobre los riesgos y contar con habilidades informáticas avanzadas. Como padre, tienes que saber qué peligros acechan y cómo protegerte de ellos.

A continuación veremos los seis peligros principals a los que se enfrentan los niños en Internet

- Ciberacoso
- Descargar malware accidentalmente
- Grooming
- Phishing

- Postear información privada
- Las salas de chat

Sin embargo, no sólo los niños se enfrentan a amenazas virtuales. El panorama de la ciberdelincuencia es enorme, y existen varias formas en las que los delitos cibernéticos pueden alcanzarte directamente. Los ciberdelincuentes atacan el desconocimiento y la comodidad humanas, lo que puede deriver en pérdidas financieras y suplantación de identidad. ¿De qué debería tener cuidado la gente? Los criminales diseñan conscientemente sus trampas aprovechando nuestras debilidades y el comportamiento humano, como:

- La predisposición de las personas a confiar en los demás
- La sugerencia de la urgencia o de importancia de un mensaje
- Síntomas de legitimidad o autoridad en un mensaje o individuo (una marca idéntica a la marca oficial de un individuo u organización para sembrar la confianza)
- Miedo a situaciones de alto estrés o donde los individuos pueden estar muy nerviosos
- Comodidad (la decision más sencilla no tiene por qué ser la más segura)
- La tendencia de los individuos a compartir excesivamente datos de su identidad personal en internet (especialmente en formas de medios sociales, como Facebook, Twitter, LinkedIn)
- La falta de familiaridad con las nuevas formas de tecnología que abren a los individuos al riesgo
- La subestimación de estos problemas por parte de los individuos

Si una persona mantiene comportamientos como los mostrados anteriormente, se enfrentará a un mayor riesgo de convertirse en víctima de un robo cibernético. El robo cibernético es un tipo de delito en el que se roba información financiera o personal mediante el uso de ordenadores. Los ladrones cibernéticos son sofisticados y pueden violar las medidas de seguridad de los datos.
En la primera fase, el delincuente debe hacerse primero con una identidad extranjera. Esto se hace sobre todo mediante el robo de datos electrónicos (contraseñas, datos de acceso, etc.), generalmente mediante copias no autorizadas (skimming), phishing engañoso o piratería informática. A esta manera de actuar se la denomina robo de identidad. En la segunda fase, el autor realiza un uso indebido de la identidad. El objetivo es generalmente beneficiarse de su propiedad. En algunos casos, el objetivo puede ser simplemente dañar a la víctima, por ejemplo, actuando bajo su nombre en redes sociales como Facebook.

Defenderse no es complicado. Es importante seguir algunas simples reglas:

1. Monitorizar la cuenta
2. Comprar en sitios seguros. Si hay un icono de un candado verde antes del “https” puedes intuir de que se trata de un sitio web seguro
3. Ten cuidado a la hora de abrir emails de los que desconfíes

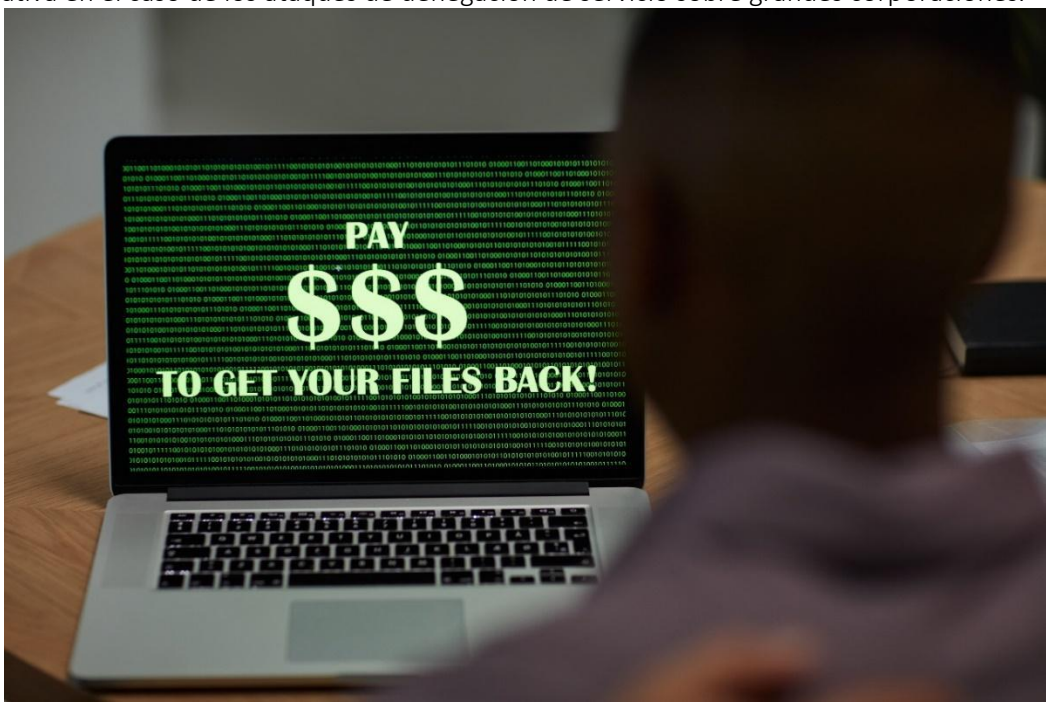
El robo cibernético se lleva a cabo cuando la información financiera o personal es robada mediante el uso de ordenadores. Los ladrones cibernéticos pueden tener como objetivo bancos, corporaciones e individuos.

En la primera fase, el delincuente debe adquirir primero una identidad de computadora extranjera. Esto se hace más a menudo robando datos electrónicos (contraseñas, datos de acceso, etc.), normalmente mediante copias no autorizadas (skimming), phishing engañoso o piratería informática. Esto se denomina robo de identidad.

Impacto en las personas, empresas y en la sociedad

El delito cibernético tiene un impacto directo y significativo en el empleo, la innovación, el crecimiento económico y la inversión. Además, el robo de IP representa al menos el 25% de los costes de los delitos cibernéticos, y supone una amenaza especialmente elevada para la tecnología militar. Dos áreas difíciles de medir dentro del cibercrimen son el robo de IP (dirección IP) y la pérdida de oportunidades.

Los individuos y las empresas pueden sufrir pérdidas financieras significativas debido a los delitos cibernéticos, siendo el impacto más obvio el robo. La pérdida de negocios también puede ser significativa en el caso de los ataques de denegación de servicio sobre grandes corporaciones.



Internet puede hacer la vida más fácil, pero también nos hace más vulnerables a los riesgos. Debido a esto, la seguridad cibernética debe tener la máxima prioridad y afecta enormemente a nuestra vida diaria/trabajo. Las brechas en la ciberseguridad pueden resultar catastróficas para las organizaciones y sus empleados o clientes.

Los daños de los ciberataques y los ciberrobos pueden extenderse desde la víctima inicial a las empresas que se encuentran vinculadas económicamente, aumentando así el daño que supone a la economía. Las empresas comparten comunmente vulnerabilidades cibernéticas, lo que lleva a que las amenazas cibernéticas estén correlacionadas entre las diferentes empresas.

El crimen afecta a todos y en el futuro el cibercrimen (y la ciberseguridad) van a afectar a la gente cada vez más. Nadie se encuentra a salvo y tiene impacto tanto entre los ricos como entre los pobres:

a) Cualquiera con un teléfono en su bolsillo
- Cualquiera que tenga una cuenta bancaria
- Cualquiera que almacene archivos importantes en su ordenador
- Cualquiera cuyo nombre aparezca en una base de datos

El crimen cibernético no algo futurista. Se está comotiendo todos los días, se está produciendo en este preciso momento. Los ladrones cometen crímenes cibernéticos para robar el dinero y la identidad de la gente. Con su identidad, el ladrón puede pedir un préstamo, obtener crédito, acumular deudas y, luego, huir sin dejar rastro. Puede llevar años llegar a rehabilitar su identidad. Un virus puede destruir los

archivos de alguien y una base de datos perdida puede resultar en la recepción de llamadas de ventas no deseadas.

La ciberseguridad es importante para la seguridad nacional.

- Existen secretos de estado que deben permanecer ocultos
- La seguridad personal de nuestros líderes es de gran importancia
- La huella y los datos del Ministerio del Interior deben ser seguras
- Los terroristas no deben poder detener el comercio mediante el robo de bases de datos importantes para la seguridad nacional y mundial

Pero la seguridad nacional no puede pasar por encima de la libertad personal por la que tanto hemos luchado:

- Nuestra libertad de opinión es crucial
- Una prensa libre hace que la gente rinda cuentas
- La privacidad personal asegura la democracia
- Debemos poder disfrutar de hacer cosas en internet sin vigilancia

5. Aplica conocimiento

Ejercicio de OPCIÓN SIMPLE

Tarea: Elige la opción correcta en este test de selección múltiple. Solamente una respuesta es verdadera.

¿Quién puede verse afectado por el cibercrimen?

- a. Cualquiera que tenga un teléfono móvil, una cuenta bancaria o una cuenta online
- b. Solamente los niños
- c. Solamente las empresas
- d. Solo las instituciones públicas

Ejercicio de OPCIÓN SIMPLE

Tarea: Elige la opción correcta en este test de selección múltiple. Solamente una respuesta es verdadera.

¿Qué es el ciberrobo?

- La obsesión por descubrirlo todo sobre otra persona
- Utilizar ordenadores o redes de comunicación para causar miedo o intimidar a la sociedad
- Decir cosas hirientes a alguien o contarles a los otros información falsa sobre dicha persona
- Cuando tu información financiera o personal es robada a través del uso de ordenadores

Fuentes

Source: http://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf
Source: https://study.com/academy/lesson/finance-crime-definition-comparisons-examples.html
Source: https://www.avast.com/c-cybercrime

Source: NATO science for peace and security series, 2008
Source: CLARKE, Richard A. Cyber War, HarperCollins (2010) ISBN 9780061962233
Source: CNN, News, 04.08.2004, available at: www.cnn.com/2004/US/08/03/terror.threat/index.html.
For an overview, see: Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; Gercke, Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007
Source: EU counter-terrorism strategy
Source: https://www.avast.com/c-website-safety-check-guide
Source: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
Source: https://www.enisa.europa.eu/
Source: https://arxiv.org/pdf/1811.06624.pdf

1. Afianza conocimiento

Resumen

El uso de la informática, los sistemas de información y la tecnología de la información y su integración en casi todos los sectores de la actividad humana es un fenómeno actual. No existe casi ningún sector de la actividad humana en el que no se utilice la tecnología de la información o las comunicaciones.

Lamentablemente, a medida que el progreso tecnológico va en aumento, también hay una mayor posibilidad de que se produzcan delitos. El crimen puede ser cometido de muchas maneras. Los ciberdelitos más comunes incluyen:

a) **Malware** - etiqueta general para el software malicioso que se propaga entre laor ordenadores e interfiere con las operaciones informáticas
b) **Hacking** - proceso común que desemboca en la violación de la privacidad y la información confidencial de alguien.
c) **Spam** - correo electrónico no deseado normalmente enviado en masa a innumerables destinatarios en todo el mundo
d) **Phishing** - correos electrónicos spam, u otras formas de comunicaciónenviados masivamente, con la intención de engañar a los destinatarios para que hagan algo que socave su seguridad o la seguridad de la organización para la que trabajan.
e) **Ataques DoS distribuidos (DDoS)** - el ataque tumba un sistema utilizando uno de los protocolos de comunicación estándar enviando spam al sistema con solicitudes de connexion.

Sin embargo, la piratería informática no siempre se percibe como un robo y a veces se utiliza para causas productivas. Este tipo de piratería que implica buenas intenciones se conoce como piratería ética. Este tipo de piratería se hace para hacer más seguro el sistema operativo. Los cibercrímenes más communes son:

- **Suplantación de identidad** – utilizer el nombre de otra persona, su dirección de dominio, número de teléfono o cualquier otro dato de identificación sin su consentimiento
- **Ciberstalking** – obsession con descubrir tanto como sea posible sobre otra persona
- **Ciberacoso** – decir cosas dolorosas a alguien o contarles a los demás información falsa sobre dicha persona
- **Robo de identidad** – robar la información
- de la identificación personal para cometer acciones ilegales

- **Robo de datos** – posesión illegal de datos sensibles, los cuales pueden incluir información no encriptada de las tarjetas de crédito almacenadas en los negocios
- **Crímenes financieros** – incluyen los siguientes: fraude, lavado de dinero, soborno y corrupción entre muchos otros

Los impactos del cibercrimen pueden ser devastadores debido al daño que se realiza contra la reputación, el elevado riesgo de pérdida de datos y el impacto financier para:

- Niños
- Adultos
- Compañías
- Estados/Gobiernos

El ciberdelito puede tener un impacto no sólo financiero, sino también en las personas o empresas. Las empresas, así como las organizaciones sanitarias y los gobiernos, también pueden sufrir la pérdida de información confidencial, así como enormes costes financieros y daños a la marca.

Las acciones sobradamente planificadas del cibercrimen deben ser denominadas ciberterrorismo o incluso ciberguerra. El ciberterrorismo resulta siempre más severo que otros comportamientos que se llevan a cabo en, o a través, del ciberespacio. Se trata de ciberataques aue utilizan o explotan ordenadores o redes de comunicación para causar la suficiente destrucción o la interrupción del servicio con el objetivo de generar miedo o de intimidar a una sociedad con un objetivo ideológico.

La guerra cibernética implica el uso y el ataque de computadoras y redes en la guerra. Comprende operaciones ofensivas y defensivas bajo la amenaza de ciberataques, espionaje y sabotaje.

Una herramienta importante en la lucha contra los delitos cibernéticos es la prevención y la información. Por último, la alfabetización informática es importante como elemento esencial para prevenir en el uso de las tecnologías de la información y las comunicaciones. Debemos preparar no solamente a los niños, sino también a los adultos y a las empresas, para los peligros del ciberespacio y tratar de proporcionarles los conocimientos necesarios para utilizar las tecnologías de la información de manera segura.

Para la seguridad en internet, es importante tener en cuenta los cinco siguientes puntos clave: Precaución, Prevención, Protección, Preservación y Perseverancia.

Estos puntos se incluyen en los siguientes pasos:

1. Evitar divulgar informacion personal en Internet y a través del correo electrónico
2. Pensar cuidadosamente el envío de cualquier fotografía en internet, ya que cualquiera puede utilizarlo en cualquier momento en otro contexto.
3. Utilizar contraseñas fuertes
4. Usar y actualizar software antivirus
5. Evitar enviar información de la tarjeta de crédito o de su contraseña a través del correo
6. Echar un vistazo a los sites a los que acceden tus hijos y utilizar herramientas de control parental
7. Guardar una copia de los datos para prevenir la pérdida de información en caso del ataque de un virus
8. Mantener el software y el Sistema operativo
9. Nunca abrir el contenido adjunto de los correos spam
10. No clicar en los enlaces de correos de spam o de páginas no confiables

11. Contactar directamente a las empresas sobre los requerimientos de los que sospechemos
12. Echar un vistazo a los extractos bancarios
13. Reflexionar sobre las páginas web que visitamos

¿Cómo puedo reconocer las webs seguras?
1 – Controles visuals de seguridad
2 – Herramientas de seguridad web
3 – Rápida investigación sobre la seguridad web

Internet se encuentra repleto de estafas de phishing. Ninguna marca está a salvo de ser falsificada, y ningún usuario está a salvo de ser atacado. Más que nunca antes, necesitamos tomar la responsabilidad de nuestra propia seguridad en internet. Sigue los consejos anteriores y sé inteligente. Has recibido toda la información que necesitas, **pero tu mejor defensor eres tú.**

Las respuestas correctas aparecen marcadas en negrita

Situación: Si la música o el cine están colgados en Internet, puedo descargarlos legalmente.
Tarea: Elige si la respuesta correcta es verdadero o falso:

- Verdadero
- **Falso**

Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: más respuestas podrían ser verdaderas.
Marque las categorías correctas de ciberdelito

- **Delitos informáticos**
- **Robo físico de una computadora, tableta o teléfono**
- Delitos relacionados con el contenido
- **Delitos relacionados con los derechos de autor**

Tarea: Emparejar respuestas: puede arrastrar y colocar las respuestas correctas en una parte determinada del texto.
Delitos relacionados con la informática cubre muchos delitos que necesitan un sistema informático para cometerse. A diferencia de las categorías anteriores, estos delitos generales a menudo no son tan estrictos en la protección de los principios legales.
Delitos relacionados con el contenido incluye violaciones de instrumentos legales más influenciados por enfoques nacionales, que pueden tomar en cuenta principios culturales y legales fundamentales. Los sistemas de valores y los sistemas legales difieren ampliamente entre sociedades.
Delitos relacionados con los derechos de autor incluyen el intercambio de canciones, archivos y software protegidos por derechos de autor en sistemas de intercambio de archivos o mediante servicios de alojamiento compartido y la elusión de los sistemas de gestión de derechos digitales (DRM)

Situación: ¿Qué son los ataques DoS distribuidos? (DDoS)?
Tarea: Elige la opción correcta en este test de seleccion múltiple. Solamente una respuesta es verdadera.

- Emails de spam u otras formas de comunicación enviados masivamente
- Un tipo de ataque cibernético que se utiliza para tumbar una red
- Emails no deseados enviados a un sin número de receptores alrededor del mundo
- El uso no autorizado, o el acceso a los recursos de una red, que explotan las vulnerabilidades en la seguridad de las identificaciones en las redes

Tarea: Elige la opción correcta en este test de selección múltiple. Solamente una respuesta es verdadera.

¿Cuál de las siguientes actividades realiza un hacker de sombrero gris?

- Es la persona que difunde información no verdadera sobre otra persona.
- Es la persona que intenta robar la información de la identificación personal.
- Es la persona que accede a un sistema sin permiso, solamente por diversión.
- Es el responsable de muchos crímenes financieros a través de internet.

Situación: ¿Qué significa el fraude interno?
Tarea: Elige la opción correcta en este test de selección múltiple. Solamente una respuesta es verdadera.

- El fraude interno es cometido por los proveedores en el caso de robo del dinero de la compañía.
- El fraude interno incluye actividades como el ciberacoso o el grooming.
- El fraude interno es cometido por los empleados en caso de realizar transacciones no autorizadas.
- El fraude interno es cometido por los clientes de la empresa.

Situación: ¿Cuál es el peor ciberataque que se comete en el mundo real?
Tarea: Elige la opción correcta en este test de selección múltiple. Solamente una respuesta es verdadera.

- Fraudes con la tarjeta de crédito
- Pornografía
- Ciberterrorismo
- Robo de identidad

Tarea: Complete la respuesta correcta al espacio en blanco sin opciones, respuesta libre.

empresas, negocios, negocios, organizaciones, gobiernos, institutos también puede sufrir pérdida de datos confidenciales, enormes cargas financieras y daños a la marca.

Tarea: Elige la opción correcta en este test de selección múltiple. Solamente una respuesta es verdadera.

¿Qué es el Certificado Anti-Phishing?

- Comprueba si hay falsos positivos cuando se trata de sitios web bancarios legítimos, para asegurarse de que el producto de seguridad es capaz de diferenciarlo
- Verifica que una web o enlace es seguro con https
- Verifica el propietario real de un site

Tarea: Selecciona la opción correcta entre verdadero o falso. Solamente una respuesta es la correcta.

Cuando se añade al enlace una "S", como en “https” (y el icono del candado) indica que la web es más segura.

- Verdadero
- Falso

Tarea: Elige la opción correcta en este test de selección múltiple. Solamente una respuesta es verdadera.

¿Quién puede verse afectado por el cibercrimen?

- a. Cualquiera que tenga un teléfono móvil, una cuenta bancaria o una cuenta online
- b. Solamente los niños
- c. Solamente las empresas
- d. Solo las instituciones públicas

Tarea: Elige la opción correcta en este test de selección múltiple. Solamente una respuesta es verdadera.

¿Qué es el ciberrobo?

- La obsesión por descubrirlo todo sobre otra persona
- Utilizar ordenadores o redes de comunicación para causar miedo o intimidar a la sociedad
- Decir cosas hirientes a alguien o contarles a los otros información falsa sobre dicha persona
- Cuando tu información financiera o personal es robada a través del uso de ordenadores