KLAR TECH

TECNOLOGÍA + CONSULTORÍA + AUTOMATIZACIÓN

Jul 2022

CIBERCRIMEN ¿QUÉ ES?

TIPOS DE CIBERCRIMEN

3 CONSEJOS

PARA PROTEGERTE DEL CIBERCRIMEN

+ *ADEMÁS*

¿Qué es Whaling?

Editorial

¿Alguna vez te haz preguntado si tus datos están seguros? Si es así, entonces, entender lo que es el cibercrimen, cómo funcionan los distintos tipos de cibercrimen y cómo puedes protegerte ante estos, es fundamental para que conserves la calma.

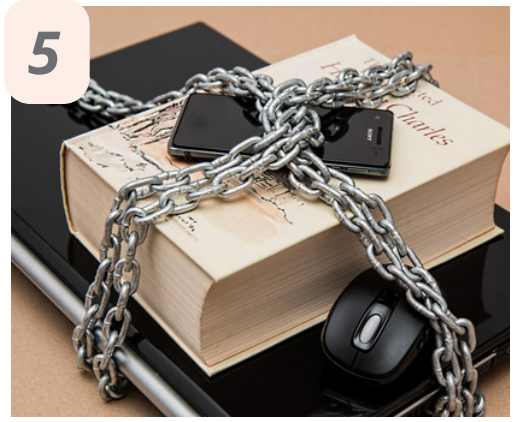
El cibercrimen es una actividad delictiva dirigida a un ordenador, un teléfono móvil, un televisor "smart TV", una red informática o simplemente un dispositivo que se encuentre conectado a una red.

La mayor parte del cibercrimen, está cometido por cibercriminales o hackers que desean obtener dinero de otras cuentas. Estos ataques los cometen personas u organizaciones secretas. La otra parte de hackers se encargan de recabar información muy importante y confidencial, puede ser información proveniente de un banco, una empresa, o simplemente de una persona en específica, con el fin de hacerla salir a la luz, o para extorsionar.

Algunos cibercriminales están organizados, utilizan técnicas avanzadas y cuentan con grandes habilidades técnicas (las cuales han sido adquiridas desde hace muchos años). Mientras que otros son hackers novatos. En otras ocasiones, el cibercrimen tiene como objetivo dañar los ordenadores por motivos distintos ala obtención de dinero. Estos pueden ser políticos o personales.

Laura Figs

LAURA FIGS
Editora



TECNOLOGÍA

Tipos de cibercrimen

¿Por qué seguirlos?

Tipos de cibercrimen

En la actualidad existen muchos tipos de cibercrímenes, algunos catalogados por su nivel de riesgo hacia la persona u organización que es atacada. A continuación, te mencionaremos algunos de los ataques más comunes, empleados por los hackers o cibercriminales.

DEFINICIÓN

Los ciberataques dirigidos a los ordenadores suele implicar virus y otros tipos de malware.

Los cibercriminales pueden infectar ordenadores con virus y malware para obtener datos o que estos dejen de funcionar. También pueden eliminar o robar datos.

Ataques de malware

Un ataque de malware es aquel en el que un sistema informático o una red están infectados con un virus informático u otro tipo de malware.

Los cibercriminales pueden utilizar un ordenador infectado por malware con varios fines. Por ejemplo, robar datos confidenciales, utilizar el ordenador para llevar a cabo otros actos delictivos o dañar los datos.

Phishing

Un ataque de phishing es aquel en el que se envían de manera masiva correos electrónicos de spam u otras formas de comunicación con la intención de engañar a los destinatarios para que hagan algo que debilite su seguridad o la de la organización para la que trabajan.

Los mensajes de los ataques de phishing pueden contener archivos adjuntos o enlaces a sitios maliciosos infectados, o bien pueden pedir al destinatario que responda con información confidencial. Estos ataques suelen estar bien hechos, porque se copian de correos de empresas, por lo que si no estás atento, puedes caer en la trampa.

Ataques DoS distribuidos

Los ataques DoS distribuidos (DDoS) son un tipo de ataque que utilizan los cibercriminales para destruir un sistema o una red. A veces se utilizan dispositivos IoT (del inglés "Internet of Things", internet de las cosas) conectados para lanzar ataques DDoS.

El ataque satura un sistema mediante el uso de uno de los protocolos de comunicación estándar que utiliza para enviar spam al sistema con solicitudes de conexión. Envía tantas solicitudes que el equipo es capaz de colapsar a tal punto de quedar inutilizable.

Otros tipos de ataques son los siguientes:

- *Actividad delictiva que utiliza ordenadores para cometer otros delitos.*
- *Ciberespionaje (en el que los hackers acceden a los datos gubernamentales o empresariales).*
- *Robo y venta de datos corporativos.*

¿SABÍAS QUÉ...

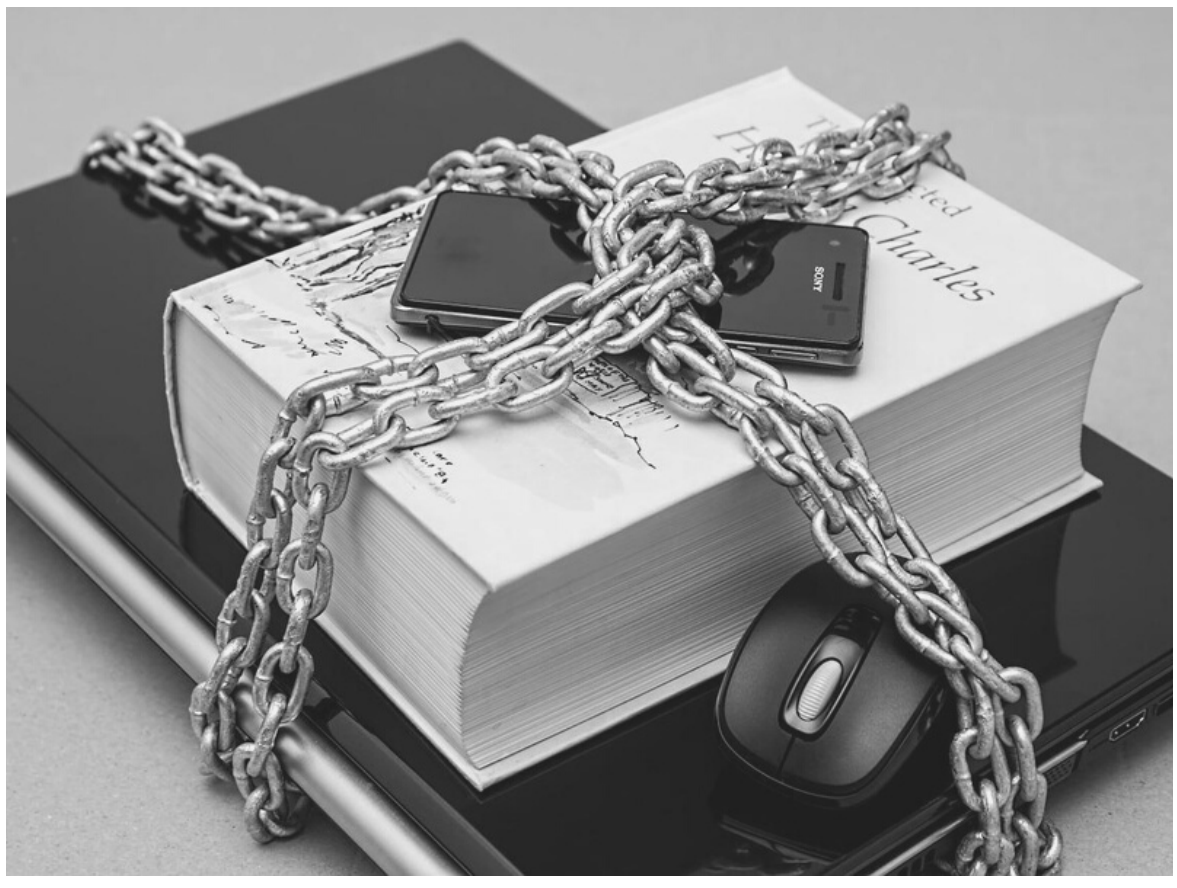
en el 2017 se produjo el ataque de ransomware WannaCry, 230.000 ordenadores se vieron afectados en 150 países. Se estiman pérdidas financieras por valor de 4.000 millones de dólares en todo el mundo?

FUENTE: DELOITTE.COM

HERRAMIENTAS DE REDES

3 consejos para protegerte del cibercrimen

Existen diversos consejos que te pueden servir para mejorar tu seguridad y así protegerte de los ciberataques, de los cuales pueden obtener tus datos o hasta incluso borrarlos.



Ahora que ya sabes la amenaza que representa el cibercrimen, Hazte la siguiente pregunta: ¿Cuáles son las mejores formas de proteger tu ordenador y tus datos personales? Estos son los principales consejos:

Mantén el software y el sistema operativo actualizados

Hacer esto te garantiza que podrás beneficiarte de los parches de seguridad más recientes para proteger tu ordenador o tu teléfono móvil.

Utiliza un software antivirus y mantenlo actualizado

El software antivirus te permite analizar, detectar y eliminar amenazas antes de que se conviertan en un problema. Disponer de esta protección te ayuda a proteger tu ordenador y tus datos del cibercrimen, para que disfrutes de la máxima tranquilidad. Un antivirus en tu ordenador es una de las principales defensas contra los virus, malwares, entre otros ataques.

Utiliza contraseñas seguras

Asegúrate de utilizar contraseñas seguras que otras personas no puedan adivinar, y no las anotes en ningún sitio a la vista. Las contraseñas más vulnerables son aquellas que solo tienen números, aunque por lo general hay sitios web que te piden contraseñas fuertes para poder ingresar.

Otras formas de proteger tus datos:

- Tenga cuidado con correos electrónicos, mensajes de texto y llamadas telefónicas que usen la crisis para presionarlo y que omita los procedimientos de seguridad habituales.
- Asegure su red doméstica. Cambie la contraseña predeterminada para su red Wi-Fi por una personalizada y segura.
- Evitar conectarte a redes públicas como la de los aeropuertos o los centros comerciales, por lo general son redes vulnerables y que cualquiera puede acceder a ellas.

CONCLUSIÓN

Los equipos vulnerables son aquellos que no poseen contraseñas seguras, no tienen un antivirus como primera línea de defensa, y adicionalmente, no están en una red segura. Recuerda, **la seguridad está en tus manos.**

¿SABÍAS QUÉ...

En 2018 se hackeó el teléfono móvil de Jeff Bezos a través de un video proveniente del teléfono del príncipe heredero de Arabia Saudí, Mohamed bin Salmán ?

FUENTE: ELPAIS.COM

ADEMÁS

¿Qué es Whaling?

Un ataque de whaling es una técnica de cibercrimen que emplea correos electrónicos fraudulentos que imitan mensajes de directivos superiores dirigidos a ejecutivos de alto rango. Como tal, es similar al phishing ejecutivo. Sin embargo, el whaling está orientado a un empleado específico de alto perfil. Con la finalidad de obtener lo datos que él solamente posee y así tener información valiosa de la empresa u organización.

¿Cómo funciona?

Un ataque de whaling es un tipo de ataque phishing en el que se suelen emplear correos electrónicos fraudulentos dirigidos a ejecutivos o gerentes. En tanto que las estafas de phishing se envían de manera masiva, los ataque de whaling se enfocan en individuos considerados de "alto rango" en una organización o empresa valiosa (como director general o ejecutivos).

Al suplantar la identidad del director general (CEO) o de un ejecutivo de alto nivel, los cibercriminales intentan convencer a sus víctimas para que ejecuten acciones desfavorables.

Típicamente intentan obtener grandes transferencias bancarias, información delicada o insertar malware usando enlaces fraudulentos. Las últimas dos implican que esta técnica de ingeniería social puede tener consecuencias a largo plazo, porque los cibercriminales pueden lanzar más ataques con los datos obtenidos de un ataque de whaling.

¿Cómo identificar un correo electrónico de un ataque de whaling?

Los correos electrónicos de whaling pueden exhibir estas características:

- Personalización: el correo electrónico enviado para iniciar un ataque de whaling seguramente incluirá información personalizada.
- Urgencia: las estafas de whaling transmiten una sensación de urgencia, pueden lograr que la víctima actúe antes de pensar en las prácticas de seguridad.
- Lenguaje empleado: con frecuencia se emplea un lenguaje y tono empresariales para convencer a la víctima.
- Firma legítima: los atacantes pueden usar elementos creíbles, como una dirección de correo electrónico, una firma y un enlace que lleve a una página web fraudulenta.
- Archivos y enlaces: los cibercriminales pueden usar archivos adjuntos o enlaces para insertar malware o solicitar información confidencial.

¿Cómo protegerse de un ataque de whaling?

- Compruebe cuidadosamente el correo electrónico, si este proviene de un colega o su jefe, llámelo o póngase en contacto para confirmar la información.
- No haga clic en los enlaces o documentos adjuntos hasta que compruebe que la fuente que envía el correo en verdadera.
- Si ha detectado que el correo enviado es falso, bloquéelo y difúndalo para que otros también estén conscientes.

¿SABÍAS QUÉ...

En 2016, un alto ejecutivo financiero de Mattel recibió un correo electrónico fraudulento de una persona que se hacía pasar por el nuevo director general (CEO). Al caer en el ataque la empresa perdió cerca de 3 millones de dólares?

FUENTE: MAILFENCE.COM