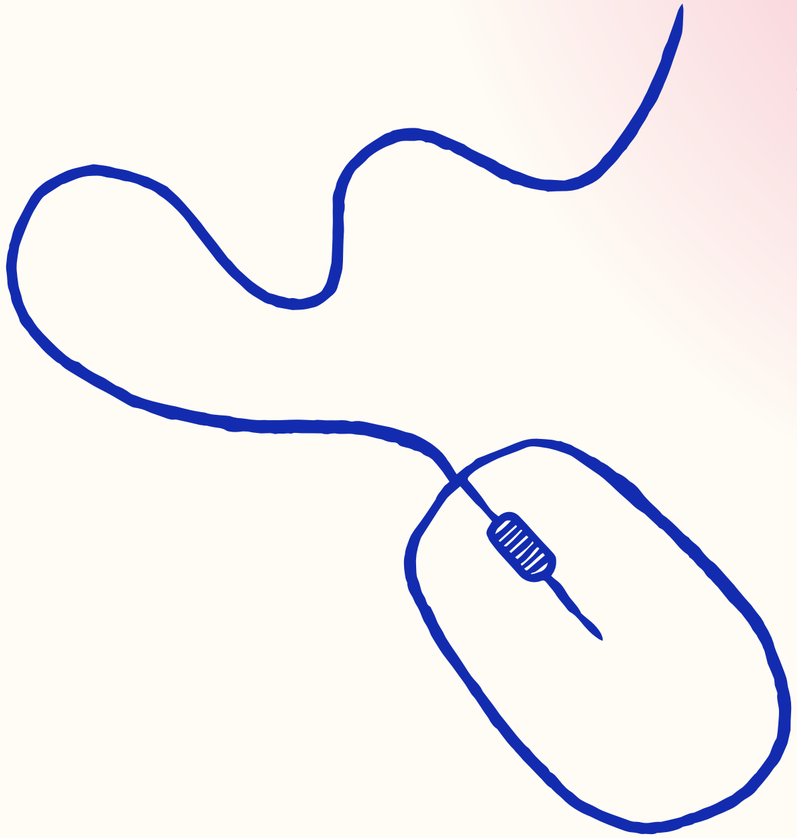
INFORMÁTICA

moral pia
savio victoria
noguera aitana



amenazas informáticas

1_ phishing

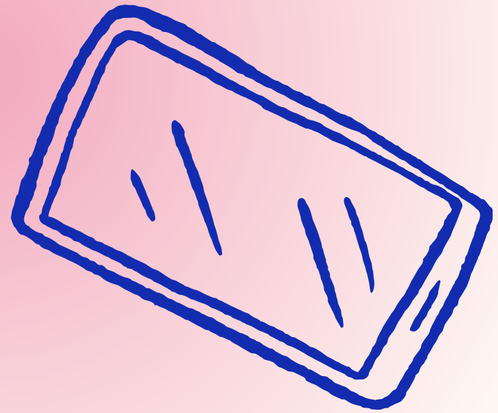
Es un tipo de ataque cibernético que utiliza correos electrónicos, mensajes de textos y llamadas para obtener información de los usuarios
Nunca respondas a un mensaje de spam: al hacerlo los estafadores detectan tu direccion de correo electrónico y recibiras mas spam

2_escaneo de puertos

Es una técnica que los piratas informáticos utilizan para descubrir los puntos debiles en una red.Un ataque de escaneo de puertos ayuda a los ciberdelincuentes averiguar si están recibiendo datos.

Funciona enviando diferentes puertos de un sistema o red. Estas respuestas ayudan a determinar si un puerto está abierto o cerrado.

Para prevenir esto es necesario contar con información sobre amenazas actualizadas que este en linea en constante evolución



3_ criptografia

Es una disciplina de la ciberseguridad qu se encarga de proteger la información y las comunicaciones mediante el uso de algoritmos, codigos y firmas.
Los primeros mensajes cifrados datan del siglo v a.c, cuando los espartanos usaban una especie de vara en la que se desarrollaba una cinta con letras gracias a esta vara se podía descifrar mensajes.

- confidencialidad : la información solo esta disponible para usuarios autorizados
- integridad: la información se ha manipulado
- autenticacion : se confirma la autenticidad de la informacion de un usuario
- vinculación: se vincula una acción a un sistema de gestión autorizado
- privacidad: se protege la privacidad de las comunicaciones personales

4_ backdoors

• comprometen la cadena de suministro, afectando dispositivos o 'software' antes de llegar a los usuarios finales. Un ejemplo son los dispositivos para televisiones anteriormente mencionados o los 'routers' de 'WiFi'

.

•Aunque es difícil detectar un backdoor, especialmente cuando un ciberdelincuente ya lo está explotando, los siguientes métodos le ayudarán a identificar este tipo de ataques para así adoptar las medidas de seguridad necesarias.

Una puerta trasera o Backdoor es un método utilizado para sortear las barreras de autentificación y encriptación de un ordenador y crear un acceso secreto que permita acceder y controlar un equipo o dispositivo sin que el usuario se dé cuenta.

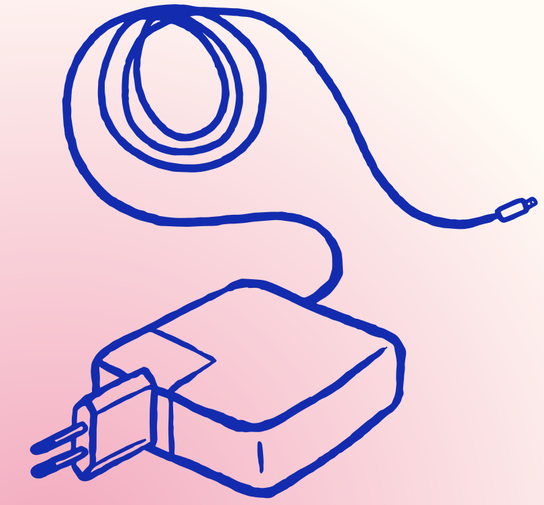
Una puerta trasera permite al intruso crear, eliminar, renombrar, editar o copiar cualquier archivo, ejecutar diferentes comandos, cambiar cualquier configuración del sistema, borrar el registro de Windows, ejecutar, controlar y terminar aplicaciones, o instalar nuevo

6_ransomware

es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.[1] Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate

Para protegerte contra el ransomware, usa el Wi-Fi público con cautela. Cuando te conectas a una red pública, tu dispositivo es más vulnerable de lo normal. Para evitar riesgos, cada vez que uses una red pública, abstente de hacer operaciones confidenciales o utiliza un servicio de VPN

un tipo de malware que impide el acceso a su dispositivo y a los datos almacenados en él, generalmente cifrando sus archivos



7_ troyano

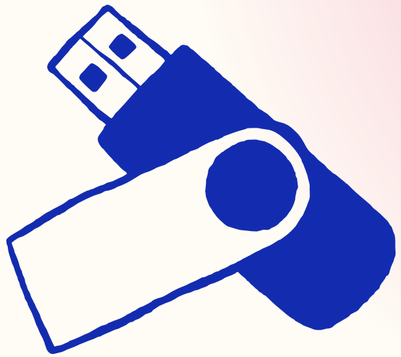
es un tipo de malware que se presenta como un programa legítimo, pero que en realidad es software malicioso

Disfrazado de programa legítimo
Ejecución de tareas
Acceso al sistema
Robo de información
Capacidad de comunicarse con servidores

El método de entrega suele hacer que un atacante utilice la ingeniería social para ocultar código malicioso dentro del software legítimo para intentar obtener acceso al sistema de los usuarios con su software.
Nunca descargues ni instales software de una fuente en la que no confíes por completo . Nunca abras un archivo adjunto ni ejecutes un programa que te hayan enviado en un correo electrónico de alguien que no conoces

8_sniffing

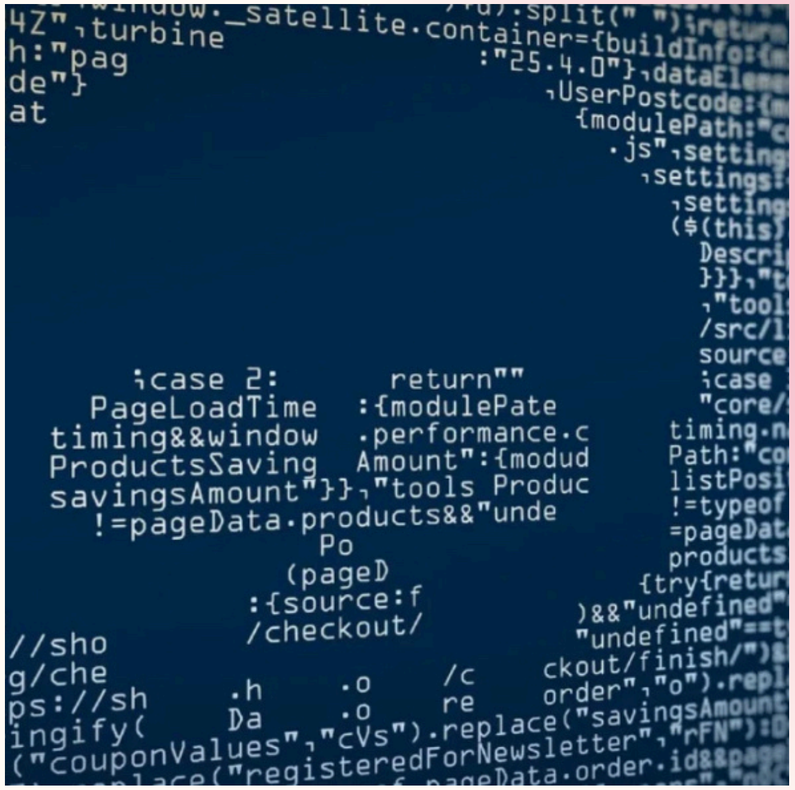
Es un ciberataque que consiste en interceptar y analizar los paquetes de datos que se envian a través de una red .
consiste en interceptar y analizar paquetes de datos qué viajan por una red.el objetivo es obtener información confidencial como datos personales para utilizarla en ataques.



Se utiliza para obtener paquetes de datos no cifrados que contienen información sobre contraseñas . Se trata de un tipo de ataque de intermediario en el que el hacker roba datos que se mueven entre el dispositivo y su destino

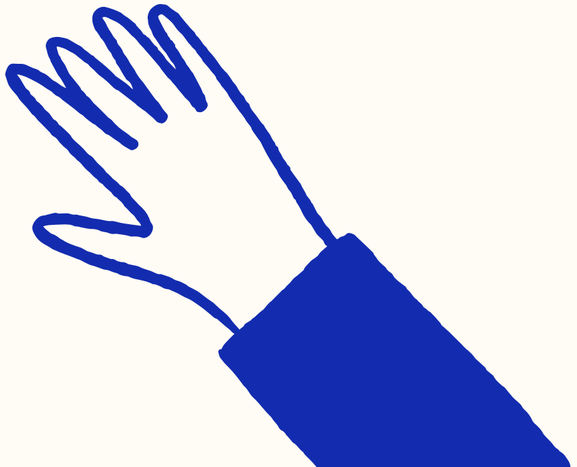
Es cualquier software corrupto, dañino, nocivo o no autorizado diseñado para infiltrarse y dañar un sistema informatico

Entre sus principales características podemos identificar las siguientes: - Se presentan como archivos ejecutables, o han adherido su código malicioso a imágenes, hojas de cálculo o documentos.
- No pueden reproducirse por sí mismos, es decir para infectar otras computadoras es necesario que el usuario intervenga



No Uses Temas o Plugins Pirata. ...
Mantén las Actualizaciones al Día.
...
Usa Contraseñas Seguras Siempre. ...
Comprueba tu Ordenador Habitual de Acceso a la Web. ...

9_ código malicioso



- Almacenar y transportar de forma segura
- Utilizar las herramientas y técnicas adecuadas
- proteger de descargas electrostáticas
- Mantener alejado de líquidos y humedad
- Evitar el polvo y la suciedad
- Asegurar los cables y alambres

El equipo no se inicia o no funciona correctamente
El equipo tarda en abrir archivos
El equipo muestra mensajes de error de acceso a los datos
El equipo bloquea el sistema con errores
Cuando el sistema accede al disco duro, se escucha un chasquido
Cuando entra en funcionamiento, el disco duro no emite ningún tipo de ruido

10_daños físicos al equipo

Los daños físicos pueden describirse como los daños resultantes de que el recubrimiento magnético de los platos del disco duro se dañe o
se destruya. Estos daños pueden producirse en
cualquier dispositivo de almacenamiento con piezas moviles

11_spoofing

Características del spoofing
Suplantación de identidad. ...
Manipulación de datos. ...
Engaño de confianza. ...
Ataques soterrados. ...
Utilizar autenticación de dos factores.
...
Implementar medidas de seguridad en
el
correo electrónico. ...
Capacitar a los empleados sobre los
riesgos

Utilice contraseñas seguras. ...
Comprueba la configuración de privacidad
de las redes sociales. ...
Evite los correos electrónicos de phishing.
...
Evite el Wi-Fi público. ...
Compruebe regularmente los extractos
bancarios. ...
Utilice siempre sitios web seguros. ...
Actualizar el software de seguridad

es un ciberataque en el que un
atacante se hace pasar por una
persona o entidad de confianza
para obtener información de sus victimas

12_hackers

Utiliza contraseñas seguras y únicas: ...
Habilita la autenticación de dos factores (2FA): ...
Mantén tu software y dispositivos actualizados: ...
Ten cuidado con los correos electrónicos y enlaces sospechosos: ...
Descarga software solo de fuentes confiables: ...
Utiliza una red Wi-Fi segura:

El hacking es el uso de medios no convencionales o ilícitos para obtener acceso no autorizado a un dispositivo digital, sistema o red informática

persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora

13_exploit

el objetivo de un ataque padece un defecto de diseño que permite a ciertas personas crear los medios para acceder a él y utilizarlo en su propio interes

Un exploit es un software, un fragmento de datos o una secuencia de comandos que aprovecha un error o una vulnerabilidad de una aplicación o sistema para provocar un comportamiento involuntario o imprevisto

Las características de un exploit son:
Es un programa malicioso o código que aprovecha las debilidades de un sistema o software
Puede ejecutarse de forma remota, sin que el atacante esté físicamente presente
Puede violar la confidencialidad, integridad y disponibilidad (CIA) de la información
Puede adoptar diversas formas, como un malware exploit, sitios web con anuncios maliciosos, o ataques DDoS
Puede llegar a la máquina objetivo por distintos medios, como un correo o una memoria USB
Requiere la intervención del usuario del lado del cliente, por ejemplo, abriendo un archivo o haciendo clic en un enla

14_ eavesdropping

significa escuchar secretamente, es el acto de escuchar en secreto o sigilosamente conversaciones privadas o comunicaciones de otros sin su consentimiento

características son:

Intercepción de redes

Los atacantes pueden acceder a redes Wi-Fi sin contraseña o con claves débiles, o a redes públicas como las de aeropuertos o cafés.

Software malicioso

Los programas maliciosos, como los keyloggers o el spyware, pueden enviar información personal del usuario.

Ingeniería social

El phishing, smishing o baiting son técnicas que engañan al usuario para que revele información confidencial.

Sniffing

Es una forma de espionaje que consiste en robar datos mientras se transmiten por la red. Puede afectar a cualquier dispositivo conectado,

15_ ataques de contraseña

es cuando los cibercriminales utilizan una lista de contraseñas de uso común para intentar obtener acceso a varias cuentas en un dominio.

Utilizar contraseñas seguras de al menos 8 caracteres
Combinar letras, números y símbolos
Incluir al menos una letra mayúscula
No reutilizar la misma contraseña para varias cuentas
Evitar palabras sencillas, nombres propios, fechas de nacimiento, etc.
No revelar información personal por teléfono, email o redes sociales

Ataque de fuerza bruta
Un atacante intenta adivinar la contraseña de un usuario probando todas las
combinaciones posibles. Esto puede hacerse de manera manual o con software
automatizado.
Ataque de rociado de contraseñas
Un atacante utiliza una lista de contraseñas comunes para intentar acceder a varias cuentas

es un ciberataque que impide que los usuarios legítimos accedan a un sistema de computadoras o red

Consumir recursos computacionales como espacio de disco, ancho de banda o tiempo de procesador.
Alterar la información de estado, como
la interrupción de sesiones TCP.
Alterar la información de configuración, como la información de rutas de encaminamiento.
Interrumpir componentes físicos de red.
Obstruir los medios de comunicación entre la víctima y los usuarios de un servicio

es una estrategia multicapa que pueda proteger sitios web, aplicaciones, API, DNS autoritativo y recursos de red mediante el uso de tecnologías con una sólida trayectoria de bloqueo estos eventos

16_ delegación de servicios

17_ fraude informatico

es una actividad delictiva o fraudulenta que se comete a través de dispositivos digitales, con el objetivo de obtener un beneficio económico ilícito.

Los ciberdelitos se cometen a través de programas maliciosos desarrollados para borrar, dañar, deteriorar, hacer inaccesibles, alterar o suprimir datos informáticos sin tu autorización y con fines económicos y de daño.

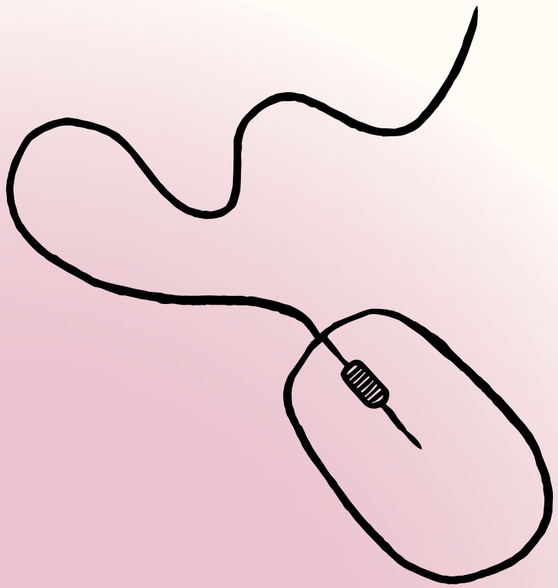
Mantener el software y los sistemas operativos actualizados para protegerse contra vulnerabilidades.

-

Verificar siempre la autenticidad de la persona o entidad antes de compartir información. Es decir, no compartir datos personales o confidenciales a menos que estés seguro de la identidad del destinatario.

18_ malware

software malicioso que puede dañar o alterar el funcionamiento de un dispositivo, servicio o red



puede usar vulnerabilidades de software conocidas para infectar el equipo

Instala un software antivirus/malware.
...
Mantén actualizado tu software antivirus. ...
Ejecuta análisis programados regularmente con tu software antivirus. ...
Mantén tu sistema operativo actualizado. ...
Protege tu red.

20_ software ilegal

Actualizar software y computadora
Mantener el software y la computadora actualizados ayuda a prevenir el software malicioso.
Usar una cuenta no de administrador
Siempre que sea posible, se recomienda usar una cuenta que no sea
Tener cuidado con los archivos

es un programa informático que se copia, distribuye o instala sin la autorización del fabricante.

Mal funcionamiento: los programas tienen más posibilidad de que sus herramientas o elementos no funcionen correctamente, ya que no cuentan con las actualizaciones más recientes. Soporte técnico: al usar un programa “pirata” no se cuenta con el soporte técnico que brinda el fabricante ante cualquier falla o problema.

21_ adware

es un software que muestra publicidad no deseada o engañosa en la pantalla del usuario, ya sea en un navegador web o en un dispositivo móvil
se instala en un dispositivo de forma oculta para mostrar anuncios y ventanas emergentes no deseados

Ser intrusivo: El adware tiene la capacidad
de mostrar anuncios publicitarios de
manera constante, incluso cuando el
usuario no está navegando en internet.
Causar molestias: Estos programas tienden
a generar anuncios de poca calidad, que
resultan irritantes para el usuario.

22_ trashing

es una técnica utilizada por ciberdelincuentes para obtener información confidencial de personas o empresas. Para ello, buscan en la basura o en otros lugares de descarte de información, como dispositivos electrónicos desechados, datos como contraseñas, números de tarjetas de crédito, direcciones de correo, teléfonos, o cualquier otra información personal relevante.

Para evitar el trashing físico, lo mejor es asegurarte de destruir adecuadamente tus documentos usando destructoras de papel o con empresas especializadas. Lo importante es evitar lo típico de romper un papel a mano en pocos trozos o hacerlo una bola y tirarlo a la papelera, porque cualquiera puede acceder a su contenido.

Los ciberataques son acciones maliciosas que se realizan para vulnerar la seguridad de sistemas informáticos, redes o datos. Los ciberdelincuentes pueden provocar un ataque cibernético de varias formas, entre ellas:

Ejecutar código en el navegador web

Cuando un usuario visita un sitio o aplicación, el código se ejecuta automáticamente en el navegador web, lo que puede robar información o redirigir al usuario a un sitio malicioso.

Ataques de fuerza bruta

Los atacantes pueden adivinar contraseñas si estas están formadas por nombres de mascotas, niños o pasatiempos.

Uso de malware

es un intento intencional de obtener acceso no autorizado a un sistema informático, red o dispositivo digital para robar, modificar o destruir datos

23_ciberataque

24_ whiter wat

El término sombrero blanco en Internet se refiere
a un hacker ético, o un experto de seguridad informática, quien se especializa en pruebas de
penetración y en otras metodologías para detectar vulnerabilidades y mejorar la seguridad
de los sistemas de comunicación e información de
una organización

Son expertos en seguridad informática
Detectan vulnerabilidades en sistemas informáticos
Trabajan de manera legal y ética
No tienen intención de generar daños
Están autorizados por la organización, entidad y/o gobierno
Usan los mismos métodos que los ciberdelincuentes para que la prueba se acerque lo
más posible a la realidad
Ayudan a las organizaciones a resguardarse de los hackers peligrosos

25_ defacement

Defacement es un ataque a un sitio web que cambia la apariencia visual de una página web. Normalmente son producidos por hackers que obtuvieron algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración de esto

se realiza contra un sitio web, en el que se modifica la apariencia de alguna de sus páginas, para llevar a cabo algún tipo de acción fraudulenta o de vandalismo

Actualizaciones regulares: Es esencial mantener actualizado el software del sitio web, incluidos los sistemas de gestión de contenido (CMS) y complementos

El spyware se instala en los ordenadores sin el consentimiento de los usuarios. Se introducen, por ejemplo, cuando se descargan archivos de Internet o de redes peer-to-peer (P2P), con la instalación de software libre o, en ocasiones, simplemente cuando se visitan sitios web poco fiables

es un software malicioso que se instala en un dispositivo sin el consentimiento del usuario para monitorear su actividad y recopilar información personal.

26_spyware

La mejor manera de controlar el spyware es
evitando que se introduzca en el ordenador en el primer lugar, pero no descargar programas y no hacer clic en archivos adjuntos de correo electrónico no siempre es una opción.

muchas gracías!