Borcelle Company

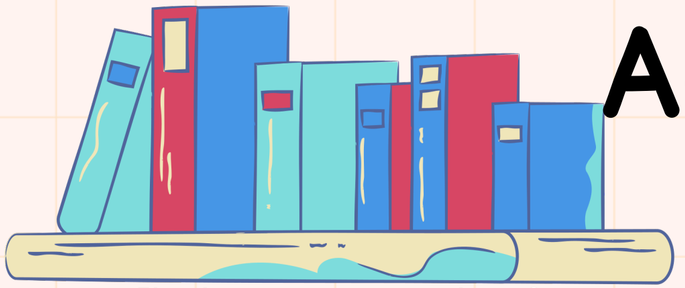
Seguridad informática

19	Adware
20	Control Remoto de Equipos (forma maliciosa)
21	Trashing

Prof: Andrea Gómez

3A

integrantes:Leonel Ortiz, Joaquín Calivar y Thiago Carrizo

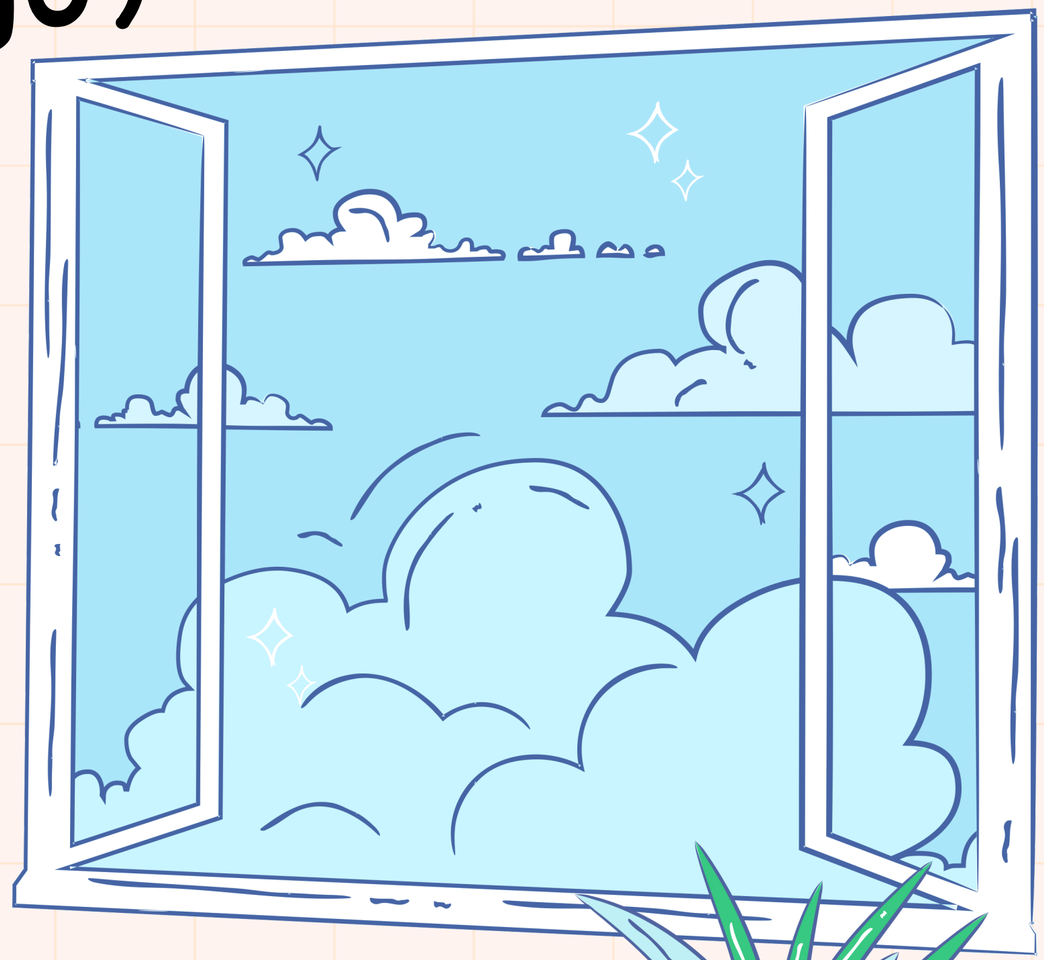


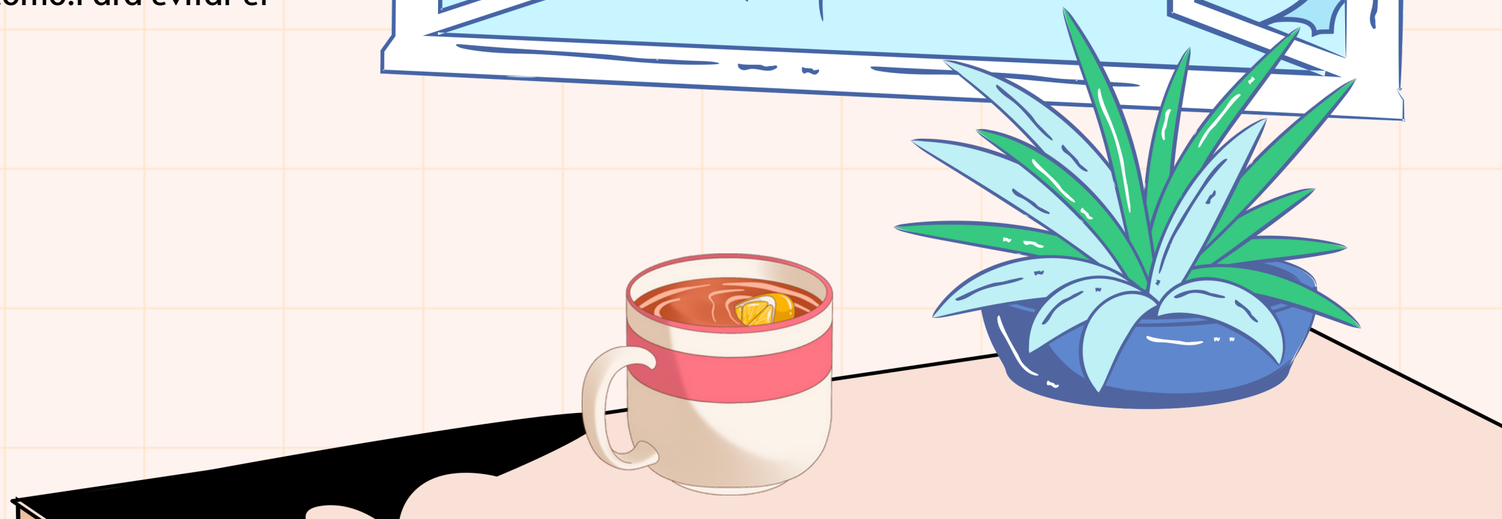
Adware(Thiago)

El adware es un tipo de software que muestra anuncios no deseados en la pantalla de tu dispositivo, ya sea una computadora o un móvil. A menudo, se instala junto con otros programas gratuitos o se obtiene a través de descargas sospechosa

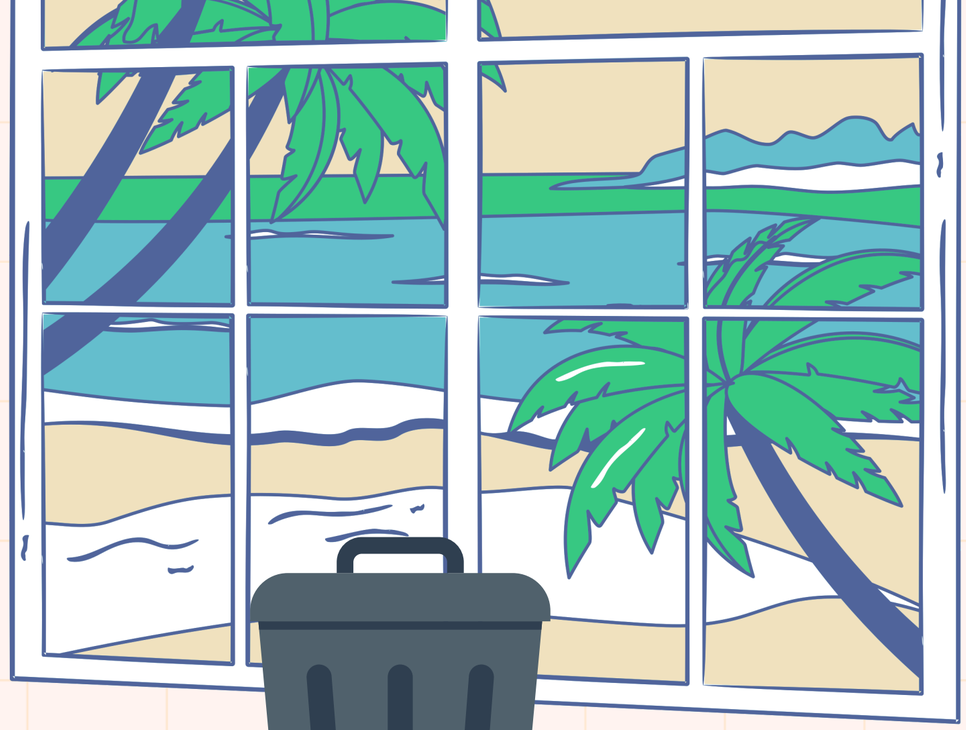
Su objetivo principal es generar ingresos para sus desarrolladores mostrando publicidad.
Tiene la capacidad de mostrar anuncios publicitarios de manera constante, incluso cuando el usuario no está navegando en internet.
Causar molestias: Estos programas tienden a generar anuncios de poca calidad, que resultan irritantes para el usuario.

El adware se ocasiona principalmente a través de descargas de software, tanto legítimo como fraudulento, que incluyen el adware como componente oculto.
Para evitar el adware, es crucial tomar medidas preventivas como:Para evitar el adware, es crucial tomar medidas preventivas como:
Utilizar software de seguridad confiable.
Mantener el software y el sistema operativo actualizados.
Descargar aplicaciones solo de fuentes oficiales
https://youtu.be/3JJB6Jz2NIY?si=OesnBSblHcXUM6in





Trashing (Leonel)



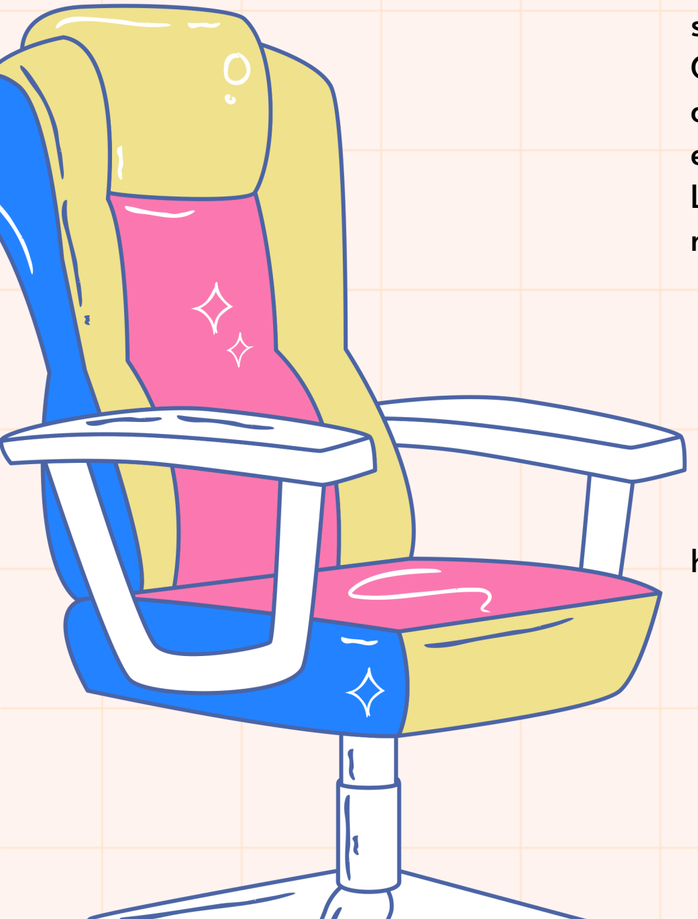
Trashing se refiere a la práctica de buscar información sensible o confidencial en la basura (basureros, papeleras, etc.), con el fin de obtener datos útiles, como: contraseñas, datos personales etc algunas de sus características son Tipo: física y social Nivel técnico requerido: bajo Acceso: a información confidencial Detección: difícil de detectar Puede ser el primer paso de un ataque mayor Puede ocurrir por demasiados procesos activos, falta de memoria física, poca localidad de referencia, algoritmo de reemplazo ineficientes, etc algunas formas de poder evitarlo es aumentar la memoria física, controlar el grado de multiprogramación, usar algoritmos de reemplazo de páginas eficientes ,etc

https://gemini.google.com/app/7412f2e3fa935121?hl=es#:~:text=Evitar%20el%20control,entrantes%20y%entes

Control remoto de equipos (Joaquín)

ControlRemoto de Equipos (Forma maliciosa)
Elcontrolremoto malicioso de equipos se refiere a la capacidad noautorizada que tiene un atacante para acceder y manipular undispositivo (computadora, servidor, smartphone, u otro equipoconectado a una red) a distancia, sin el consentimiento delpropietario legítimo.
El objetivo principal de este tipo de acceso es realizar actividades dañinas o ilegales.
Las características del control remoto malicioso se centran en cómo se logra y qué capacidades le otorga al atacante:
1. Acceso no autorizado
2. Persistencia
3. Ocultamiento y evasión

Este control se logra mediante la instalación de software malicioso (malware) en el equipo de la víctima. Ejemplos: Troyanos de Acceso Remoto (RATs): permiten control total desde una ubicación remota. Backdoors (Puertas Traseras): entradas ocultas en software o hardware para acceso no autorizado. Keyloggers: registran cada pulsación de teclado, capturando contraseñas e información sensible. Spyware: programas que monitorean y recopilan información sobre la actividad del usuario sin su conocimiento. Evitar el control remoto malicioso protege tu privacidad, tus datos y tu seguridad digital. Estrategias: 1. Mantener el Software Actualizado (Sistemas Operativos y Aplicaciones) Importancia: Las actualizaciones incluyen parches de seguridad que corrigen vulnerabilidades que los atacantes podrían explotar. Acción: Habilita actualizaciones automáticas en Windows, macOS, Linux, Android, iOS y aplicaciones (navegadores, programas de oficina, multimedia, etc.).



https://gemini.google.com/app/7412f2e3fa935121?hl=es#:~:text=Evitar%20el%20control,entrantes%20y%20salientes