PREVENCIÓN RAMSOMWARE

CIBER CRACKING

NO HAGAS CLIC EN ENLACES NO VERIFICADOS

Evita a toda costa hacer clic en enlaces de sitios web sospechosos, la mayoría de las infecciones de ramsomware provienen de aquí.

NO ABRAS ARCHIVOS ADJUNTOS DE CORREOS ELECTRÓNICOS QUE NO SEAN DE CONFIANZA

Nunca ejecutes un adjunto de algún correo electrónico que no sea de confianza, si tienes dudas puedes subir los archivos adjuntos a www.virustotal.com para comprobar si se trata de un archivo malicioso.

DESCARGA SOLO DESDE SITIOS EN LOS QUE CONFÍAS

Para reducir el riesgo de descargar ransomware, no descargues software ni archivos multimedia de sitios web desconocidos.

EVITA PROPORCIONAR DATOS PERSONALES

Los cibercriminales que planifican un ataque de ransomware pueden intentar obtener datos personales antes de un ataque. Pueden utilizar esta información en correos electrónicos de phishing para dirigirse específicamente a ti.

UTILIZA EL ANÁLISIS Y FILTRADO DEL CONTENIDO DEL SERVIDOR DE CORREO ELECTRÓNICO

El uso del análisis y filtrado del contenido en los servidores de correo electrónico es una forma inteligente de prevenir el ransomware.

NUNCA UTILICES DISPOSITIVOS USB DESCONOCIDOS

Nunca insertes dispositivos USB u otros dispositivos de almacenamiento extraíbles en el ordenador si no sabes de dónde proceden.

MANTÉN EL SOFTWARE Y EL SISTEMA OPERATIVO ACTUALIZADOS

Mantener el software y el sistema operativo actualizados te ayudará a protegerte del malware. Porque cuando ejecutas una actualización, te aseguras de que te beneficias de los parches de seguridad más recientes, lo que dificulta que los cibercriminales aprovechen las vulnerabilidades de tu software.

UTILIZA SOFTWARE DE SEGURIDAD Y MANTENLO ACTUALIZADO

Un buen software de seguridad o antivirus puede prevenir que ejecutes el ramsomware una vez descargado detectándolo y poniéndolo en cuarentena, mantén este software actualizado para que sea más eficiente.

TEN SEGMENTADA TU RED

Una red segmentada y con los permisos bien estructurados evitaría que el ramsomware se extendiese por toda tu red aislándolo solo en el lugar que ha tenido lugar la infección evitando así su propagación.

REALIZA COPIAS DE SEGURIDAD DE LOS DATOS + COPIA EXTERNA EN OTRA UBICACIÓN

Si sufres un ataque de ransomware, tus datos permanecerán seguros si realizas una copia de seguridad de estos. Aparte de esta copia de seguridad deberemos de disponer de otro sistema de backup en una ubicación diferente y aislada de la primera para minimizar al máximo la perdida de datos.