

**El Ramsonware** es de las amenazas más peligrosas hoy en día y por esta razón debemos estar muy atentos para no ser parte de este círculo vicioso que han creado los hackers, su único cometido es de encriptar (secuestrar) tus archivos importantes y luego pedir el pago de un rescate por ellos en criptomonedas, a la larga pierdes dinero y no recuperas tu información.

# RANSOMWARE

## ¿Qué es?

Software o programa que restringe el acceso a aplicaciones, archivos o al sistema infectado, pidiendo un rescate a cambio de eliminar dicha restricción.



## ¿Cómo se propaga?



- Web
- Correos electrónicos
- Almacenamiento externo (USB/Disco duro)
- Aplicaciones

## ¿Cómo evitar el contagio?



No abras links o archivos recibidos por email de origen desconocido.



Asegúrate de tener instalado un antivirus y que esté siempre actualizado.



Solo descarga aplicaciones desde sitios seguros.



No ejecutes archivos recibidos que vengan de personas desconocidas.

**El Phishing** es otra de las practicas maliciosas de los hackers para llegar a ti mediante correos electrónicos para tratar de engañarte y así poder sacarte información y usarla en tu contra, así como también poder acceder a tus datos de accesos a cuentas bancarias para robarte.

## Pistas para identificar un correo de *phishing*



- 1** Es un **correo inesperado** y que no has solicitado.  
Tu paquete será enviado **después del pago.** X
- 2** El asunto parece **importante, urgente o llamativo.**  
Necesitamos qe nos facilites esta información **lo antes posible.** X
- 3** Te piden facilitar **datos personales, credenciales y bancarios** bajo alguna excusa.  
Introduce **aquí tus datos bancarios.** X
- 4** Contiene algún **archivo adjunto** o facilita un **enlace** para realizar alguna gestión, la cual te va a causar una **consecuencia**, probablemente económica.
- 5** El mensaje contiene **faltas de ortografía** o está mal redactado.  
Eres elegido para recibir un **nuevo** regalo. X