



VERACRUZ  
GOBIERNO  
DEL ESTADO



SEV  
Secretaría  
de Educación

IEEV

Instituto de Espacios Educativos  
del Estado de Veracruz



# Ransomware



¿Qué es?

Es un tipo de malware que impide a los usuarios acceder a sus sistemas o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.

¿Cómo puede Infectarse?

Uno de los métodos más habituales es a través de spam malicioso que son mensajes no solicitados que se utilizan para enviar malware por correo electrónico. El mensaje de correo electrónico puede incluir archivos adjuntos trampa, como PDF o documentos de Word

## ¿Cómo funciona un ransomware?



Cómo protegerse del ransomware

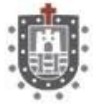


Crear copias de seguridad seguras de sus datos de forma regular. Asegúrese de desconectar físicamente los dispositivos de su computadora después de realizar una copia de seguridad

**¡manténgase informado!**



VERACRUZ  
GOBIERNO  
DEL ESTADO



SEV  
Secretaría  
de Educación

IEEV  
Instituto de Espacios Educativos  
del Estado de Veracruz



# Ciberdelincuencia



La ciberdelincuencia es aquella actividad que, por medio de la red, tenga como objetivo atentar a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y los datos, así como el uso fraudulento de tales sistemas, redes y datos.

Como Opera la  
Ciberdelincuencia



**El ciberdelincuente**  
envía un correo electrónico al usuario  
sobre una **transferencia interbancaria**

Te informamos que ha recibido una transferencia de \$83,000.00 a tu Tarjeta Bancomer

Una vez que el usuario accede dando clic a la liga, envía a un **sitio falso** (idéntico al real) **pedirán** todos los datos, así como:

- ✗ Contraseñas
- ✗ NIP

con esta información, automáticamente:

**tu cuenta  
puede ser  
vulnerada!**

Medidas anti  
Ciberdelincuencia



**1 WIFIS PÚBLICAS**

Conectar los dispositivos lo menos posible a este tipo de redes.



**2 ACTUALIZACIONES**

Realizar actualizaciones periódicas de los sistemas operativos.



**3 WEBCAM**

La cámara del ordenador es mejor mantenerla tapada mientras no se utiliza.



**4 COPIA DE SEGURIDAD**

Aprender a realizar copias de seguridad de nuestro material más sensible garantiza una mayor tranquilidad al usuario



**5 ANTIVIRUS**

Siempre contar con un antivirus, y si es de pago mejor



**6 SMARTPHONE**

Mantener las funciones bluetooth y GPS desconectadas cuando no se usen.



**7 DISCO DURO EXTERNO**

Trasladar los archivos más importante al disco duro externo dificulta en el robo de información.



VERACRUZ  
GOBIERNO  
DEL ESTADO



SEV  
Secretaría  
de Educación

IEEV

Instituto de Espacios Educativos  
del Estado de Veracruz



# PHISHING



Es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

¿Como trabaja en Phishing?

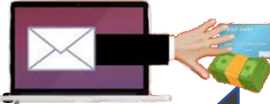


RECOMENDACION



**NUNCA ABRAS**  
CORREOS ELECTRÓNICOS  
DE DUDOSA PROCEDENCIA  
Y mucho menos contestes información  
que sólo tú debes conocer!

# Pharming



Es un tipo de cibercrimen, en el que el tráfico de un sitio web es manipulado para permitir el robo de información confidencial.

Por ejemplo: Tarjetas de crédito u otra información Bancaria.

## Proceso del Pharming.

1

El usuario abre una página o ejecuta un archivo "dudoso" recibido por correo electrónico o messenger, infectando su máquina sin saberlo.



2

El usuario visita cualquier sitio, por ejemplo: **www.gmail.com**

SITUACIÓN  
...NORMAL...  
EQUIPO  
...INFECTADO

La máquina normalmente se debe enlazar al portal "www.gmail.com"



Una máquina infectada con PHARMING se conecta directamente al portal establecido por el archivo HOST, pero este no es el verdadero de "www.gmail.com"



3

El servidor web entrega la **PÁGINA FALSA** al usuario.



## Recomendaciones



**NO** abras o ejecutes archivos "dudosos" aún cuando el título del mensaje parezca normal

**NO** ingreses a páginas recibidas por Messenger o correo desde el primer clic, se puede infectar tu equipo