SEGOB
SECRETARÍA DE GOBERNACIÓN

COMISIÓN NACIONAL DE SEGURIDAD

POLICÍA FEDERAL

NO TE DEJES SORPRENDER!!!

Si recibes un correo electrónico o al prender tu computadora aparece una leyenda en la que te amenazan con multarte o intervenir tu equipo de cómputo, porque supuestamente ingresaste a páginas no seguras o por descargar programas, música, juegos de videos on line, **¡No es verdad!** y podrías ser víctima de fraude. **Se trata de un virus conocido como *Malware* que ha infectado tu equipo y podría provocar daños irreparables.**

La **Comisión Nacional de Seguridad**, a través del **Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX)**, realiza patrullajes continuos en la red pública de internet a fin de identificar este tipo de virus también conocidos como "ransomware" que bloquean completamente los equipos de cómputo y tienen la capacidad de borrar la información.

La Comisión Nacional de Seguridad (CNS) recomienda:

- Nunca realices pagos o depósitos en ningún establecimiento o centro de conveniencia ya que ninguna instancia gubernamental o privada realiza este tipo de operaciones o cobros, **¡Es falso!**
- Utiliza un software antivirus que evite la instalación no consentida de éste tipo de programas maliciosos.
- En caso de haber sido infectada tu computadora, para poder desinfectarla se requiere de seguir los siguientes pasos.

1) Ubica otra computadora con conexión a internet.
2) Descargar en una memoria USB la herramienta de PoliFix, desde la página **http://www.infospyware.com/antimalware/polifix**
3) Una vez guardado este programa en USB, reinicia la computadora infectada, pulsa F8 para entrar al menú de opciones avanzadas de Windows.
4) Selecciona la opción modo seguro e inicia el sistema operativo.
5) Inserta la memoria USB y ejecuta la herramienta PoliFix, desde la memoria, no la instales.
6) De inmediato se desplegará una ventana con tres opciones. Presiona analizar y espera alrededor de 20 minutos, al terminar desplegará una segunda pantalla en la que advierte que se creó un reporte con terminación .txt. Dale aceptar.
7) Reinicia el equipo y reestablece la conexión a internet.
8) Baja las actualizaciones críticas e importantes de Java que ofrece Microsoft, a través de la página **http://www.microsoft.com/es-xl/security/resources/ransomware-whatis.aspx.**
9) Instala o actualiza el antivirus de tu computadora.
10) Evita bajar programas desconocidos o videos de la red que tengan un dominio dudoso o que provengan de un correo electrónico no familiarizado.

La Coordinación para la Prevención de Delitos Electrónicos de la División Científica de la Policía Federal realiza patrullajes en la red, que permite identificar este tipo de virus o programas maliciosos, los puntos anteriores sirven casi en todos los sistemas operativos de Windows. Sin embargo, en algunos casos es inoperante por la versión del sistema operativo que manejan (eliminar), por lo que se pide a los usuarios se pongan en contacto con nosotros a través del Centro de Atención al Comisionado (CEAC).

En caso de haber sido o estás siendo víctima de algún malware o de alguna extorsión a través de la red, comunícate de inmediato al **CEAC al 088** (teléfono gratuito y nacional que opera las 24 horas del día, los 365 días del año), donde uno de los asesores te ayudará a resolver tu problema y le dará seguimiento a tu caso a través de un número de expediente, de forma anónima si fuera el caso.

También nos puedes contactar a través de la cuenta de Twitter **@CEAC_CNS**, en Facebook **CEAC CNS** y a través del correo electrónico **ceac@ssp.gob.mx**.