Qué es el ransomware y cómo evitar el secuestro de tus datos

Raúl Ramírez, encargado de **ciberseguridad** de **NIC México**, entidad del **Tec de Monterrey** y responsable de recursos de Internet, compartió **consejos** para proteger a tu empresa del **ransomware**, o el **secuestro de datos informáticos.**

El **experto** explica que el **ransomware** es un tipo de **malware (software malicioso)** que infecta dispositivos, burla **sistemas** de **seguridad** o engaña al usuario para **robar** información sensible y pedir un pago por el rescate de las mismas.

*"Un **ciberataque** es un **delito informático** que pretenden o llevan a cabo los delincuentes, entre los que se encuentra el **ransomware, el phising, entre otros**"*, menciona.

En las últimas semanas, **Colonial Pipeline**, uno de los oleoductos más grande de Estados Unidos, y la empresa de carnes **JBS Foods** sufrieron este tipo de ataques. En México, la **Lotería Nacional** fue víctima de este tipo de ataque.

El experto compartió con **CONECTA** consejos para evitar los **tipos más frecuentes** de **ciberataques** en tu compañía, o incluso, en tus dispositivos personales.


width="900" loading="lazy">

1.- Haz respaldos de seguridad

Ramírez añade que el ***ransomware*** **secuestra tu información** al bloquear el acceso a tu **computadora** o **dispositivo**.

“Una manera de ***cuidarse*** *es tener* ***procesos de respaldo****, no solo de los* ***equipos,*** *sino incluso de los* ***servidores****”*, menciona Ramírez.

Copias de información sensible en la **nube** o en **dispositivos como discos duros** protegen al usuario quien puede elegir restaurar su equipo sin perder su información respaldada.

2.- Mantener el software actualizado.

Cuando el virus ***WannaCry*** causó estragos en el 2017, las empresas más vulnerables al ***ransomware*** son las que desatendieron las actualizaciones de sus sistemas operativos.

"Hay que mantener activas *las* ***actualizaciones*** *automáticas del sistema operativo",* recomendó el experto.

3.- Activa el doble factor de autenticación

El experto aconseja activar **mecanismos** llamados **“de doble factor**” que tienen algunos sitios web y aplicaciones como por ejemplo ***Amazon*** o ***Facebook***.

Para **ingresar** o **hacer una compra** en ellos no solo basta con ingresar tu **usuario** o **contraseña,** sino que te mandan un **mensaje** o **código** a un teléfono o correo como **medida extra de seguridad**.

4.- Instala un buen antivirus

*“La **herramienta** que no debe faltar es un buen **antivirus**. La mayoría de los antivirus del mercado son buenos”*, comenta Ramírez.

Kaspersky, **Norton**, **McAffee** e incluso algunos gratuitos como **Avast** y **AVG** para versiones en computadora y para teléfono móvil, son algunas de las que sugiere.

El experto menciona que tener antivirus y además **mantenerlo actualizado** ayuda significativamente a evitar ciberataques a tus **dispositivos** o a los de tu **equipo** de **trabajo**.

width="900" loading="lazy">

5.- Observa las señales del engaño

El ***phishing*** es un ciberataque en el que un **delincuente** se hace **pasar por alguien más**, como una empresa, una tienda departamental o hasta una entidad bancaria.

Raúl menciona que **observar a detalle** el nombre de quien envía el **correo electrónico** o el **mensaje** es el primer paso.

*“Por lo general, si es **phishing** no te envían correos con **tu nombre**. También en algunos casos si pones el **cursor** encima de un **link sin darle click** te aparece la **página** a la que te envía.*

*“**Siempre revisa antes de dar click** que el dominio o la dirección corresponda a la dirección correcta”,* comenta Ramírez.

6.- Utiliza el “cifrado”

También el experto comenta que hay otro tipo de **ataque** conocido como **MITM** o ***Man In The Middle*** en el que el delincuente interviene la comunicación entre 2 equipos.

Usar **mecanismos de cifrado** es lo que Ramírez recomienda para hacer frente a esta amenaza, los cuales **no evitan** que la **información** sea **vista** por el **delincuente,** pero si la vuelven **ilegible para él**.

*“Se **encripta** el canal y aun si el atacante esté monitoreando la transferencia de datos será ilegible”*, afirma Raúl.

Además añade que algunos **proveedores** de los **más conocidos** para brindar **mecanismos de cifrado** son **Symantec**, **GoDaddy**, **Digicert**, **Comodo** y **Let’s Encrypt**.

7.- Revisa que los sitios web sean seguros

Como usuario, Ramírez comenta que para no ser **víctimas** de **ataques MITM**, antes de ingresar **contraseñas**, **información sensible** o hacer un **pago** en un **sitio web**, deberás revisar que la conexión sea segura.

Un **ícono** de un **candado verde** o **cerrado** en la parte superior de los navegadores, usualmente colocado al lado de la dirección web, es una **señal** de que es un **sitio seguro**.

8.- Usa VPN en redes públicas.

Si tienes que **utilizar** tu **equipo de cómputo** o **móvil** en lugares con **redes públicas** de Internet, tu conexión puede ser vulnerable por lo que Ramírez recomienda usar una **conexión VPN**.

Este tipo de conexiones llamadas ***“Virtual Private Network”*** o **red privada virtual**

Aeropuertos, **hoteles** y **cafeterías** permiten conectarte a Internet sin necesidad de estar conectado con los demás dispositivos de la red.

Además con una **VPN** podrías conectarte a una **red de trabajo** sin estar dentro de una oficina; **Proton VPN** y **OPENVPN** son un par que el experto menciona.


width="900" loading="lazy">

9.- Usa servicios confiables en la nube

Existe otro tipo de **ataque** llamado **DDoS** en el que un **delincuente** intenta **afectar la capacidad de un sitio web** para que no pueda dar servicio a los clientes o usuarios.

Ramírez comenta que existen **servicios** en **Internet** que brindan **protección** contra este tipo de ataques.

Google Cloud, **Microsoft Azure**, **Amazon Web Services** y **Cloud Flare** son algunos de estos proveedores especializados en brindar protección contra ataques DDoS.

10. Usa plataformas especializadas para tiendas en línea

Si tienes un **negocio** o **tienda en línea** y buscas que tus procesos de pago sean seguros para tus clientes, Ramírez recomienda usar **plataformas** que **brindan esa protección**.

*“**Shopify** y **Akky** en alianza con **epages** son algunas que cumplen con las **regulaciones** de **pago** y **uso de tarjetas**”*, señala.

11.- Capacita a tu personal

La firma de seguridad **Kaspersky** recomienda a las empresas que deben tener un **protocolo de seguridad** que informe a sus empleados determinar si son de confianza los archivos, los vínculos o los correos electrónicos que reciben.

*"Hay que capacitar en prácticas como **jamás** escribir las **contraseñas** en papel o **apagar la computadora** de trabajo al final de cada jornada laboral"*, recomendó el experto.

Además, recomienda que las empresas deben de contar con un **plan de respuesta** ante el caso de un ciberataque.

¿Qué hago si me infectó un ransomware?

De acuerdo con la firma Kaspersky, hay dos tipos **ransomware:** de **bloqueo,** que impide el acceso a la pantalla del equipo; y de **cifrado**, que encripta archivos individuales.

En ambos casos, quienes sufren este tipo de ataques pueden realizar una de las siguientes opciones:

- **Buscar eliminarlo** con alguna herramienta especializada.

- Restablecer el dispositivo como si fuera recién comprado.

- **Pagar el rescate** y arriesgarse a que los ciberdelincuentes cumplan su palabra.

LEE MÁS: