SEGURIDAD DE DATOS: ¿CUÁLES SON LOS MÉTODOS DE CIBERATAQUE MÁS COMUNES?

En la era de la nube, es necesario conocer los principales ciberataques para que puedas protegerte contra el robo de tus datos.

Pero, primero, ¿qué es un ciberataque? Un **ciberataque** se puede definir como un **acto de mala intención contra los sistemas informáticos**. El ataque implica apuntar a diferentes dispositivos informáticos. Esto puede realizarse a través de computadoras o servidores, aislados o en redes, equipos periféricos como impresoras, o incluso dispositivos de comunicación como teléfonos móviles, smartphones o tabletas.

Descubre en este artículo los **6 métodos más comunes de ciberataques** y algunos consejos prácticos para protegerte de cada uno de ellos.

1. El “Phishing”

El phishing consiste en **hacer creer a la víctima que se está comunicando con un tercero de confianza para extraer información personal** (número de tarjeta de crédito o contraseña). El Phishing se realiza generalmente a través falsos sitios web (tiendas online, pop-ups, y sitios de dudosa procedencia) mediante la creación de copias perfectas de marcas conocidas utilizando logotipos y los colores empresariales de estas empresas.

El phishing también lo puedes encontrar en tu buzón de correo electrónico, generalmente al abrir un correo electrónico reclamándote por no haber pagado un monto específico o bien ser acreedor a un premio por parte de alguna institución. Los hackers en ocasiones pueden utilizar información pública difundida en las redes sociales para llevar a cabo phishing dirigido.

Consejos para protegerte:

- Para comprar en línea, siempre comprueba que el sitio web sea seguro, cuya dirección empieza por **"https".**
- Si un correo electrónico parece sospechoso, **nunca hagas clic en los archivos adjuntos** o enlaces que contiene.
- Siempre que ingreses una contraseña, trata de acceder mediante al sitio web mediante la barra de direcciones, **nunca dentro de un hiper vínculo**.
- **Actualiza tus antivirus** para maximizar la protección contra el malware.
- Utiliza el **filtro de suplantación de identidad del navegador web**: la mayoría de los navegadores existentes ofrecen una función de advertencia de suplantación de identidad.
- Utiliza un **software de filtrado de spam o correo no deseado**.

2. *Ransomware* o Secuestro de datos (pedir dinero)

¿Recibiste un **mensaje cuestionable con archivos adjuntos**? ¿Encontraste una memoria USB? ¡Cuidado con el *ransomware*! Tus datos pueden cifrarse y tomarse como rehén para pedir un rescate.

Consejos para protegerte:

- Haz **copias de seguridad de tus datos con regularidad**, mueve físicamente la copia de seguridad de tu red y colócala en un lugar seguro.
- **No abras mensajes cuyo origen o forma sea dudoso**. El hacker puede haber recuperado algunos de tus datos (los nombres de tus clientes por ejemplo) y crear direcciones de correo electrónico similares a las de tus interlocutores.
- **Aprende a identificar extensiones de archivo cuestionables**. ¿Sueles recibir archivos .doc o .mp4 y el archivo de mensaje del que no está seguro termina con algún otro tipo de extensión? ¡No los abras especialmente! Ejemplos: pif; .com; .murciélago; .exe; .vbs; .lnk. Ten especial cuidado al abrir archivos adjuntos **.scr o .cab**.
- **Actualiza tus herramientas habituales**: Windows, antivirus, lector de PDF, navegador.
- **Usa una cuenta de usuario** en lugar de una cuenta de administrador.

3. Robo de contraseña

El robo de contraseñas consiste en **utilizar software destinado a intentar tantas combinaciones posibles como sea posible para encontrar tu contraseña**. También se puede hacer multiplicando las pruebas en función de la información obtenida por ejemplo en las redes sociales o ingeniería social.

Consejos para protegerte:

- **No utilices como contraseña los nombres de tus hijos, tu mascota** u otros elementos que puedan aparecer en tus redes sociales.
- **Cree contraseñas estrictas** con letras, mayúsculas y caracteres especiales.
- **No uses la misma contraseña** en todas partes.
- **Siempre usa un antivirus** y un *antispyware*.

4. *Malware* o Software malicioso

El *malware* o software malicioso es un **programa que se desarrolla con el único propósito de dañar un sistema informático**. Puede ocultarse en un software de descarga gratuita o en una memoria USB.

Consejos para protegerte:

- **Instala solo software de fuentes confiables u oficiales**. Si el software normalmente pagado se ofrece de forma gratuita, quédate atento.

- **No conectes una memoria USB encontrada sin conocer su origen**, puedes quedar infectado sin saberlo.

5. La red WiFi falsa

Cuando estás en un lugar público, pueden aparecer multitud de **redes WiFi abiertas**. Ten mucho cuidado con algunas de estas redes porque **son simulaciones y pueden tener la intención de robar toda tu información**.

Consejos para protegerte:

- **Asegúrate de que la red en cuestión sea original**. Si es posible, pida confirmación a uno de los responsables de la red abierta (Ejemplo: el servidor del restaurante, etc.).
- Si tienes que crear una contraseña para acceder al WiFi, **nunca uses la contraseña de una de tus cuentas**.
- **Nunca te conectes a sitios web bancarios o importantes** (bandeja de entrada, documentos personales) a través de una de estas redes.
- **Nunca compres en línea** a través de las redes abiertas.
- **Nunca instales una actualización supuestamente "obligatoria"** para acceder a este tipo de WiFi.

6. El USB "encontrado"

Si encuentras un USB, nunca lo conectes a tu computadora. Este **puede haber sido abandonado con el único propósito de robar o encriptar tus datos para obtener un rescate.**

Consejos para protegerte:

- **Simplemente evite conectarlo a tu computadora**. Llévalo al lugar donde lo encontraste (biblioteca, universidad) o tíralo.