¿Qué son los ataques de ransomware?

Las ciberamenazas están a la orden del día, y entender cómo funcionan es vital para protegerse de ellas. Un caso especial es el ransomware, un tipo de malware que secuestra y roba la información de tu computadora, dejándola incluso inutilizable hasta que pagues un rescate. Aparecieron como una novedad en el mundo de la ciberseguridad, pero no tardaron en convertirse en una de las amenazas más importantes. Estos ataques afectan a individuos, gobiernos, y empresas de todos los tamaños, robando información sensible a menudo por grandes sumas de dinero.

¿Cómo operan los ciberdelincuentes con ransomware?

Los grupos de ciberdelincuentes están constantemente ideando formas de hacer los ataques de ransomware más peligrosos y difíciles de resolver. Utilizan diversas entradas para infectar los equipos, tales como:

* **Correos electrónicos:** Documentos adjuntos maliciosos.
* **Software o videojuegos piratas:** Pueden ocultar ransomware en programas descargados de fuentes no confiables.
* **Sitios web maliciosos:** Un simple clic puede desencadenar la infección.

La naturaleza impredecible de estos ataques resalta la importancia de estar siempre alerta y protegerse proactivamente.

¿Cuáles son las cifras detrás de los ataques de ransomware?

Cualquier búsqueda en Internet puede revelar cientos de casos documentados donde el costo del rescate asciende a millones de dólares. Además, se invierten otras sumas significativas en investigación para mitigar estos ataques y recuperar los datos. Sin embargo, pagar el rescate nunca asegura la recuperación de la información, lo que muchas veces deja a las víctimas sin otra opción más que aguantar las pérdidas.

¿Cómo protegerse contra un ataque de ransomware?

Adoptar medidas proactivas es crucial para proteger tu información:

1. **Escanear archivos de origen dudoso:** Antes de utilizarlos, verifica cualquier archivo que venga de fuentes no confiables.
2. **Utilizar software confiable:** Descarga software solamente de fuentes oficiales.
3. **Prestar atención a las alertas de seguridad:** Haz caso a las advertencias de tus herramientas de seguridad.

**¿Qué hacer en caso de ser atacado por ransomware?**

Si un ataque de ransomware te afecta, apaga inmediatamente el equipo y llama a un experto en ciberseguridad. Evita manipular el dispositivo hasta que llegue un profesional, minimizando así el riesgo de mayores pérdidas.

**¿Por qué es importante realizar respaldos de seguridad?**

Asegurar copias de seguridad de tus datos es una medida preventiva esencial. Mantener tus datos replicados en otras computadoras o discos duros externos te protege en caso de ser víctima de ransomware. Así, aunque el ransomware ataque, puedes recuperar tu información sin necesidad de pagar un rescate.

La denuncia: un paso crucial en la ciberseguridad

Denunciar siempre es importante, tanto a autoridades competentes, empresas de antivirus como a especialistas de ciberseguridad. Estas acciones ayudan a mitigar futuras amenazas y proporcionan información valiosa para prevenir nuevos ataques. Tu denuncia podría significar una diferencia crucial en la lucha contra el ransomware y otras ciberamenazas.

La ciberseguridad es una responsabilidad personal y colectiva. Mantente informado y sigue aprendiendo sobre las mejores prácticas para proteger tus datos y equipos de futuros ataques.

¿Por qué evitar el software pirata?

El uso de software y contenidos piratas puede parecer una solución tentadora para acceder a programas sin coste. Sin embargo, tras esta apariencia de gratuidad, se esconden numerosos riesgos. Estos archivos suelen ser manipulados por grupos que desean insertar malware, utilizándolos como caballos de Troya para infectar nuestros dispositivos con software malicioso sin que nos demos cuenta. Además de atentar contra la seguridad personal, utilizar software pirata puede poner en peligro a otros usuarios e incluso redes completas, convirtiendo computadoras en "zombies" controlados remotamente por criminales cibernéticos.

**¿Cuáles son los riesgos de usar software pirata?**

* **Malware oculto**: Los archivos pirata pueden contener cracks o binarios que no solo cumplen la función de eludir la licencia, sino también instalan malware perjudicial.
* **Infecciones persistentes**: Algunos malware pueden permanecer inactivos en el sistema hasta que sean activados para llevar a cabo funciones cibercriminales sin conocimiento del usuario.
* **Impacto en el dispositivo**: Cambios inusuales en el dispositivo, como ralentización, cambios en configuraciones o conexiones sospechosas, pueden indicar una infección.
* **Redes maliciosas**: Los dispositivos infectados pueden transformarse en parte de una botnet, utilizada para realizar ataques coordinados.

**¿Cómo puedo protegerme si decidí utilizar software pirata?**

Aunque la recomendación principal es evitar el consumo de software pirata o no autorizado, si decides seguir adelante, hay acciones para mitigar riesgos:

1. **No desactivar el antivirus**: Es esencial mantener el antivirus activo.
2. **Escaneos periódicos**: Siempre escanea archivos descargados antes de abrirlos.
3. **Atención a alertas del antivirus**: No ignores las advertencias del sistema de seguridad.
4. **Observación continua**: Monitorea tu dispositivo buscando los signos mencionados de posibles infecciones.

**¿Cuál es la mejor alternativa al software pirata?**

La mejor alternativa al software pirata es optar por el software legítimo, ya sea mediante la compra de licencias, el uso de software libre o versiones gratuitas desde el proveedor oficial. No solo se protege el dispositivo, sino también se apoya a los desarrolladores que crean estas herramientas.

* **Software libre y gratuito**: Muchas empresas y comunidades desarrollan software libre que puede reemplazar programas comerciales.
* **Sitios de análisis en línea**: Empresas como VirusTotal ofrecen servicios para analizar archivos sospechosos antes de su ejecución.

**¿Cómo validar la legitimidad de mi software?**

Mantener un sistema operativo legítimo es crucial. A continuación se presenta cómo verificar la validez de una licencia de Windows 11, que sigue un proceso similar en otras versiones:

# Comando para verificar el estado de la licencia en Windows

slmgr.vbs /dli

Este comando muestra un resumen del estado de la licencia, ayudándote a confirmar su autenticidad.

**¿Qué hacer si soy víctima de malware?**

1. **Contacta a un experto en ciberseguridad**: Es fundamental buscar ayuda profesional si sospechas de un ataque.
2. **Notifica a tu proveedor de antivirus**: Informar a proveedores de software sobre potenciales amenazas ayuda a mejorar las defensas globales.

Promover la seguridad digital es crucial en un mundo interconectado, donde nuestras acciones pueden impactar no solo en nuestra seguridad, sino también en la de nuestra comunidad digital. Por eso, el primer paso siempre será optar por software seguro y legítimo.

¿Por qué es crucial mantener actualizados los sistemas operativos?

El entorno empresarial actual enfrenta desafíos complejos relacionados con la seguridad informática. Muchas organizaciones aún operan con sistemas obsoletos simplemente porque "funcionan". Sin embargo, mantener sistemas desactualizados puede ser un riesgo significativo, ya que los parches de seguridad son esenciales para protegerse contra ataques potencialmente devastadores.

* **Vulnerabilidades y parches:** Cada sistema operativo o software tiene potenciales fallas que pueden ser explotadas. Los parches son actualizaciones que cierran estas brechas de seguridad.
* **Riesgo económico:** Un fallo de seguridad puede llevar a pérdidas económicas severas. Empresas grandes han sufrido costos millonarios debido a la falta de actualizaciones.
* **Caso Clorox 2023:** Un ejemplo reciente es Clorox, que perdió miles de millones de dólares y un 20% de sus ventas totales por un ataque cibernético que desestabilizó sus operaciones.

¿Qué implica no actualizar el software?

Más allá de la seguridad, la obsolescencia tecnológica implica una serie de desafíos que pueden afectar gravemente a una empresa.

* **Riesgo de operaciones:** Los sistemas obsoletos suelen ser menos eficientes, lo que afecta la productividad.
* **Falta de soporte:** Los sistemas sin soporte oficial no reciben actualizaciones ni soluciones a problemas nuevos, incrementando el riesgo de vulnerabilidades.
* **Crisis de imagen:** Un ataque cibernético puede dañar la reputación de una empresa, especialmente si afecta los datos de los clientes.

¿Cuáles son las mejores prácticas para protegerse de ataques?

Adoptar medidas proactivas garantiza que, ante un eventual ataque, los daños sean mínimos y se pueda reaccionar rápidamente.

* **Actualizar regularmente:** Mantener todos los sistemas y aplicaciones al día con las últimas versiones y parches.
* **Evaluaciones de seguridad:** Realizar auditorías periódicas para identificar y corregir posibles vulnerabilidades.
* **Capacitación del personal:** Asegurar que todo el equipo esté informado sobre prácticas de seguridad cibernética y protocolos a seguir ante posibles incidentes.
* **Alternativas modernas:** Si un software ya no cuenta con soporte, es recomendable buscar alternativas con respaldo oficial para minimizar riesgos.

Recuerda, la seguridad y la modernización tecnológica son inversiones, no gastos. Al adoptar estas prácticas, las empresas no solo protegen sus activos, sino que también garantizan su continuidad y competitividad en el mercado global. ¡Sigue aprendiendo y fortaleciendo tus estrategias de seguridad!

¿Por qué son cruciales las actualizaciones de software para la ciberseguridad?

La era digital en la que vivimos está marcada por constantes avances tecnológicos y, como consecuencia, por crecientes amenazas en ciberseguridad. Las actualizaciones de software se han convertido en una de las armas más eficaces a nuestra disposición para contrarrestar estas amenazas. Sin embargo, aún existen usuarios y empresas que desactivan las actualizaciones automáticas por razones que podrían parecer válidas a corto plazo, como evitar gastos adicionales por nuevas licencias. Pero ¿qué costo podría tener esto a largo plazo para la seguridad de los sistemas? Veámoslo en detalle.

**¿Qué beneficios ofrecen las actualizaciones de software?**

Algunos de los beneficios más destacados de mantener el software actualizado incluyen:

* **Mejoras en funcionalidad**: Las actualizaciones suelen traer nuevas características que optimizan la experiencia del usuario.
* **Corrección de errores**: Cada actualización corrige errores reportados que pueden afectar el rendimiento.
* **Parches de seguridad**: Son esenciales para proteger los sistemas contra nuevas vulnerabilidades.

**¿Qué riesgos existen al no actualizar?**

La ciberseguridad es una carrera armamentista donde el tiempo es crítico. Cada día surgen nuevas amenazas y vulnerabilidades que pueden ser explotadas por ciberdelincuentes. Estas son algunas de las amenazas más comunes:

* **Ataques de día cero**: Aprovechamiento de vulnerabilidades no conocidas por la comunidad antes de ser explotadas.
* **Cibercrimen organizado**: Desde pequeñas bandas hasta grandes mafias que buscan explotar vulnerabilidades no parchadas.
* **Riesgos económicos y estratégicos**: Nacionalidades enteras enfrentan riesgos cuando grupos organizados buscan dañar economías.

Cada parche y cada actualización proporciona una capa adicional de defensa para prevenir estos riesgos.

¿Cómo garantizar que las actualizaciones estén activas?

**¿El sistema operativo tiene soporte oficial?**

Utilizar un sistema operativo con soporte del fabricante es fundamental. Un ejemplo claro es Windows XP, un software obsoleto que muchos todavía usan en sistemas críticos. Para garantizar la seguridad:

* **Invierta en mantenimientos regulares**: Si por razones específicas no puedes abandonar un sistema viejo, un experto en ciberseguridad debería auditar y corregir vulnerabilidades.
* **Busque el soporte del fabricante**: Esto garantizará que las actualizaciones de seguridad estén disponibles para tu sistema.

**¿Cómo actualizar Windows 11?**

Asegurarse de que tu sistema operativo esté actualizado es sencillo:

1. **Accede a las configuraciones de Windows**.
2. **Dirígete a Windows Update** para verificar el estado de las actualizaciones.
3. **Instala las actualizaciones pendientes** de inmediato al encontrarlas.

**¿Cómo verificar las actualizaciones de aplicaciones?**

Al igual que el sistema operativo, las aplicaciones también necesitan estar actualizadas para mantener la integridad del sistema. Tomemos como ejemplo Google Chrome:

1. **Abre el navegador y accede a la sección de configuración**.
2. **Selecciona Información de Chrome**, donde la verificación se procederá automáticamente.
3. Si es necesario, actualiza el navegador. La actualización requerirá que el navegador se cierre y se vuelva a abrir.

Consejos finales para mantener la seguridad

Para maximizar la protección que ofrecen las actualizaciones:

* **Habilita las actualizaciones automáticas siempre que sea posible**. Esto garantiza que tu dispositivo esté siempre protegido contra las últimas amenazas.
* **Programa verificaciones mensuales**. Aunque las actualizaciones automáticas son útiles, verificar manualmente cada cierto tiempo puede identificar fallos en el proceso automático.

Mantener todos tus sistemas y aplicaciones actualizados no solo mejora la funcionalidad general, sino que también es un paso crucial hacia una ciberseguridad robusta. En un mundo donde las ciberamenazas están en evolución constante, las actualizaciones son la primera línea de defensa.

¿Qué es el principio de mínimo privilegio en ciberseguridad?

El principio de mínimo privilegio es fundamental en ciberseguridad para proteger información y datos críticos. Se trata de otorgar a los usuarios solo los permisos necesarios para cumplir sus tareas, minimizando así el riesgo de accesos no autorizados. Esto es esencial tanto en empresas como en situaciones personales. En los entornos empresariales, es común que los empleados tengan más permisos de los necesarios, lo que potencialmente abre la puerta a brechas de seguridad.

**¿Por qué es crucial limitar los accesos en un entorno corporativo?**

* **Prevención de ataques internos y externos:** Otorgar solo los permisos necesarios ayuda a prevenir ataques intencionados o accidentales desde cuentas comprometidas.
* **Control de acceso constante:** Asegurarse de que ex-empleados o personas ajenas no mantengan acceso a información o sistemas que ya no deberían.
* **Minimización de errores humanos:** Es común que, por errores o descuidos, los empleados tengan acceso indebido a datos que no les conciernen.

**¿Cómo puede afectar otorgar permisos de más en el plano personal?**

* **Accesos a dispositivos personales:** Cuando prestas tu computadora sin limitar accesos, otras personas podrían ver toda tu información privada.
* **Compartición de enlaces en la nube:** La práctica de compartir documentos sensibles mediante enlaces públicos puede dar acceso a cualquier persona, no solo a quienes fue destinado, a información financiera u otros datos críticos.

¿Cuáles son los riesgos de compartir enlaces de archivos sin restricciones?

Compartir un enlace sin restricciones puede exponernos a múltiples amenazas la exposición de datos confidenciales debido al uso de enlaces públicos es un error común tanto en individuos como en grandes empresas.

**¿Qué ejemplos existen de brechas de seguridad por compartir enlaces?**

* **Exposición accidental:** Una persona trabajando en un café podría compartir accidentalmente un enlace público sin darse cuenta de que cualquiera que tenga acceso al enlace puede ver la información.
* **Fuentes públicas:** Herramientas automáticas o scanners rastrean activamente enlaces en internet, encontrándolos incluso si nunca fueron compartidos intencionalmente, revelando así datos corporativos confidenciales.

**¿Cómo proteger adecuadamente la información al compartir archivos?**

* Pedir el nombre de usuario o correo electrónico de la persona y otorgar permiso de solo lectura a esa persona específica.
* Utilizar servicios de encriptación y herramientas que aseguren que los enlaces compartidos estén protegidos y monitorizados.

¿Qué otros principios pueden ayudar a asegurar nuestros sistemas?

Además del principio de mínimo privilegio, el **concepto de Zero Trust** se está implementando cada vez más en la ciberseguridad moderna.

**¿Qué es Zero Trust y cómo se aplica?**

Zero Trust es un enfoque donde no se confía en ninguna entidad dentro o fuera del perímetro de la red por defecto. Esto implica:

* **Verificación constante:** Todos los accesos a sistemas e información requieren autenticación y autorización.
* **Monitorización continua:** Revisar y validar el comportamiento de los usuarios en la red constantemente para identificar y mitigar riesgos.

Enseñar y aprender a aplicar estos principios es esencial para fortalecer la seguridad de todos los sistemas que utilizamos. Invita a otros a implementar estas prácticas para crear un entorno digital más seguro y protegido para todos.

**Curso de Introducción a la Ingeniería Social: Técnicas, Ataques y Pretexting**

La ingeniería social, en la seguridad de la información es el **proceso de manipular a las personas para que realicen acciones que afecten su medio.** Es lo que tiene de común la guerra de Troya y la historia de Adán y Eva.

**Baiting** es la forma que el atacante **atrae a su víctima con una trampa** y el **Pretexting** es el **engaño a través de un escenario** para que la víctima proporcione información valiosa.

Como surge la seguridad informatica

[Phack](https://es.wikipedia.org/wiki/Phrack) es un foro hacker creado por Legion of Doom(entre 1983 -1985) donde se compartía ideas o temas de seguridad informática y a partir de ahí ***surge el término pretexting gracias al pirateo telefónico (conocido cómo Phreaking).***

En el artículo **More on trashing** es la primera vez que se menciona la ingeniería social, es en 1984 cuando se habla de la técnica de buscar, y no solo de buscar, sino de extraer datos. Este artículo sale a la luz gracias al magazine [2600](https://en.wikipedia.org/wiki/2600:_The_Hacker_Quarterly)

Contribución creada con aportes de: Angie Espinoza

La disciplina que consiste en **extraer datos sin que la víctima se percate** y **lograr la confianza para luego engañarlas** y **manipularlas** para el beneficio propio de quien la implementa, se le conoce como **ingeniería social.**

¿Qué se puede hacer al saber nombres, dirección, número de teléfono y correo?

Diagrama

El contenido generado por IA puede ser incorrecto.

La ingeniería social se usa cuando su fin no es malicioso ni para hacer daño. Por eso las reglas de compromiso se **deben hacer en entornos controlados como pruebas de penetración de red o autorizadas, cuando se realizan investigaciones y en comunicaciones públicas.**

Cuando se realiza la búsqueda de la información **entre más ataques hay, mayor información se obtiene**. El objetivo final de la ingeniería social es llegar a los sistemas de información, prueba este [quiz](https://phishingquiz.withgoogle.com/) para que detectes cuándo te están engañando.

[OSINT](https://ciberpatrulla.com/que-es-osint) significa **Open Source Intelligence** y es muy útil cuando se reúne información.

**Lecturas recomendadas**

[Darknet Diaries](https://open.spotify.com/show/4XPl3uEEL9hvqMkoZrzbx5?si=c82afca2be814572)

Para que la ingeniería social sea efectiva, se necesita tres elementos fundamentales:

* Todos tienen **atención selectiva**
* Todos suelen **distraerse** con algo
* La **confianza**

**Las personas son el eslabón más débil**, es extremadamente **difícil de detectar cuando no existe IDS (Intrusion Detection System) para la falta de sentido de común o ignoracia.**