**Aumento de ataques cibernéticos a dispositivos inteligentes ponen en riesgo a los usuarios**

* *En el marco del mes de concientización sobre ciberseguridad, se destacan nuevas amenazas dirigidas a dispositivos inteligentes, como redes Wi-Fi falsas y estaciones de carga comprometidas. Es crucial que tanto usuarios como empresas refuercen sus medidas de protección para evitar posibles ataques.*

**Ciudad de Guatemala, 15 de octubre del 2024 -** Durante el mes de octubre se conmemora el mes de la concientización sobre ciberseguridad en el mundo, por lo que [Palo Alto Networks](https://www.paloaltonetworks.com/), empresa líder en ciberseguridad que se dedica a proteger a organizaciones y consumidores contra amenazas digitales, comparte los más recientes hallazgos en ataques a dispositivos inteligentes que pueden afectar a cualquier persona.

Aunque los consumidores y las empresas han ganado conciencia de tácticas como el phishing o el malware, existen muchos métodos menos conocidos y también dispositivos que los ciberdelincuentes utilizan. Esto se produce en un contexto en el que se documenta un aumento drástico en el número de ataques y las personas usan cada vez más dispositivos inteligentes en su cotidianidad, lo que hace vital que tanto las empresas como los usuarios tomen en serio la ciberseguridad.

*"Es vital que las personas tomen las medidas adecuadas para garantizar la seguridad de todos sus dispositivos inteligentes, no solo de sus teléfonos y computadoras, ya que los ciberdelincuentes pueden causar desde el robo de identidad hasta pérdidas financieras. Al mismo tiempo, las empresas tienen una responsabilidad crucial en la protección de los datos de sus clientes, ya que muchas de las violaciones que comprometen la información del consumidor podrían evitarse con una configuración adecuada de ciberseguridad," comentó Ramón García, District Sales Manager para Centroamérica y el Caribe en Palo Alto Networks.*

El potencial para que los consumidores se conviertan en víctimas de ciberdelitos se ha disparado a medida que la velocidad de un ataque avanza rápidamente. En casi el 45% de los casos de ciberseguridad registrados por Palo Alto Networks este año, los atacantes exfiltraron datos en menos de un día después del abordaje, lo que significa que solo hay unas pocas horas para detenerlos.

Para los usuarios, las vías de ciberdelitos se están diversificando apresuradamente. Aunque Palo Alto Networks encontró que los ataques de phishing se redujeron 17% en 2023, muchas más rutas se han abierto a través de los nuevos dispositivos inteligentes que han salido al mercado.

**Estos son los nuevos tipos de ataques que han sido detectados**

Sobre los diversos tipos de ataques que los consumidores deben conocer, desde redes Wi-Fi falsas hasta altavoces inteligentes, los investigadores de Palo Alto Networks han proporcionado la guía definitiva para saber cómo protegerse y mantener sus dispositivos personales seguros.

* **Ataques de gemelo malvado**: Configuran una red Wi-Fi falsa en lugares públicos como restaurantes o aeropuertos, engañando a los usuarios para que se conecten a ella. Esto permite interceptar datos como contraseñas, correos electrónicos e información de tarjetas bancarias.
* **Juice jacking:** Los atacantes intervienen estaciones de carga públicas, como las que se encuentran en aeropuertos o cafeterías, para robar datos. Cuando los usuarios conectan sus dispositivos a estas estaciones, se puede inyectar algún software malicioso.
* **Cryptojacking**: Secuestran dispositivos de los usuarios para minar criptomonedas sin su conocimiento. Esta actividad no autorizada puede llevar a un aumento en los costos de electricidad, un rendimiento reducido del dispositivo y posibles daños al hardware.
* **Electrodomésticos inteligentes:** Apuntan a los consumidores con mucho más que solo su teléfono o computadora. Desde refrigeradores hasta cafeteras y otros electrodomésticos conectados pueden ser puntos de entrada para acceder a sistemas más críticos.
* **Dispositivos wearables portátiles:** Los electrónicos de fitness y otros dispositivos portátiles como relojes pueden exponer datos personales y de salud, lo que puede generar vulneraciones para consumidores o empresas.
* **Sistemas de automóviles:** Los autos con sistemas de entretenimiento conectados a Internet también pueden ser objetivos para los hackers. Estos podrían acceder a los datos personales del usuario, rastrear su ubicación o incluso interferir con las funciones del sistema.

El año pasado se vio un aumento del 72% en las violaciones de datos desde 2021, que tenía el récord de todos los tiempos. Con los atacantes cada vez más creativos en las formas en que están apuntando a las personas, y con un aumento registrado del 49% interanual de víctimas publicadas en sitios de filtración de ransomware, nunca ha sido más importante para los consumidores y las empresas tomar medidas de ciberseguridad.

Guatemala aún no ha asignado un presupuesto específico para ciberseguridad en el ejercicio fiscal de 2025, pero los diputados han manifestado la posibilidad de discutir este año la [iniciativa 6347.](https://www.congreso.gob.gt/assets/uploads/info_legislativo/iniciativas/ea912-6347.pdf) Esta ley es fundamental para que el país avance hacia una regulación especializada que permita combatir eficazmente la ciberdelincuencia. Sin esta normativa, Guatemala no podrá integrarse a foros internacionales clave, como el [Convenio de Budapest,](https://www.oas.org/juridico/english/cyb_pry_convenio.pdf) que ha establecido un plazo hasta 2025 para que los países interesados ​​se adhieran a sus principios y accedan a redes globales de expertos en ciberseguridad. [El Observatorio Guatemalteco de Delitos Informáticos (OGDI)](https://ogdi.org/estadisticas) reportó 583 alertas de ciberdelitos hasta julio de 2024, destacándose entre ellos la ciberestafa con 117 denuncias. Además, los principales riesgos en el país incluyen el robo de identidad, las amenazas cibernéticas y el uso de voces clonadas mediante inteligencia artificial. La implementación de la [Ley de Ciberseguridad](https://www.congreso.gob.gt/assets/uploads/info_legislativo/iniciativas/ea912-6347.pdf) permitirá no solo proteger la propiedad intelectual de empresas extranjeras, sino también crear un entorno digital seguro para fomentar la inversión y el crecimiento económico en sectores estratégicos como tecnología, fabricación e investigación y desarrollo.

*“Si bien el número de ataques, el nivel de sofisticación y los métodos utilizados están evolucionando rápidamente, la buena noticia desde la perspectiva del consumidor es que se pueden reducir considerablemente las posibilidades de ser víctima de un hackeo siguiendo algunas buenas prácticas generales.”*, señala García.

Para proteger datos personales, los consumidores deben asegurarse siempre de que sus dispositivos tengan las últimas actualizaciones de seguridad, usar contraseñas fuertes y únicas y habilitar la autenticación de dos factores siempre que sea posible. Adicionalmente, cuidar todo lo que se descargue o desconfiar en lo que hacen clic y considerar el uso de un software antivirus para tener una capa adicional de protección.

Al mismo tiempo, la prevención a la hora de abordar cualquier correo electrónico o mensaje de texto con un nivel de sospecha moderado es importante, ya que el número de ataques en estas modalidades sigue siendo bastante significativo y son cada vez más sofisticados, por lo que mantenerse informados de los más recientes cambios en el mundo digital será clave para evitar ser víctimas de ciberataques.

Finalmente, es recomendable hacer copias de seguridad de todos los datos con regularidad para proteger la información importante en caso de un ataque. A medida que los hackers continúan cambiando sus tácticas, los consumidores también deben estar al tanto de cómo pueden mantenerse alertas y seguros.

**-FIN-**

**Acerca de Palo Alto Networks**

Palo Alto Networks es el líder mundial en ciberseguridad. Innovamos para superar las ciber amenazas, de modo que las organizaciones puedan adoptar la tecnología con confianza. Palo Alto Networks es el líder mundial en ciberseguridad. Brindamos seguridad cibernética de última generación a miles de clientes en todo el mundo, en todos los sectores. Nuestras mejores plataformas y servicios de ciberseguridad en su clase están respaldados por inteligencia de amenazas líder en la industria y fortalecidos por automatización de última generación. Ya sea implementando nuestros productos para habilitar Zero Trust Enterprise, respondiendo a un incidente de seguridad o asociándonos para ofrecer mejores resultados de seguridad a través de un ecosistema de socios de clase mundial, estamos comprometidos a ayudar a garantizar que cada día sea más seguro que el anterior. Es lo que nos convierte en el socio de ciberseguridad preferido.

En Palo Alto Networks, nos comprometemos a reunir a las mejores personas al servicio de nuestra misión, por lo que también nos enorgullece ser el lugar de trabajo de ciberseguridad elegido, reconocido entre los lugares de trabajo más queridos de Newsweek (2021), Comparably Best Companies for Diversity (2021) y HRC Best Places for LGBTQ Equality (2022). Para obtener más información, visite [www.paloaltonetworks.com](http://www.paloaltonetworks.com).

Palo Alto Networks, Prisma y el logotipo de Palo Alto Networks son marcas comerciales de Palo Alto Networks, Inc. en los Estados Unidos y en jurisdicciones de todo el mundo. Todas las demás marcas comerciales, nombres comerciales o marcas de servicio utilizadas o mencionadas en este documento pertenecen a sus respectivos propietarios. Todos los servicios o características no publicados (y cualquier servicio o característica que generalmente no esté disponible para los clientes) a los que se hace referencia en este u otros comunicados de prensa o declaraciones públicas no están disponibles actualmente (o todavía no están disponibles para los clientes en general) y es posible que no se entreguen cuando se espera o en todos. Los clientes que adquieran aplicaciones de Palo Alto Networks deben tomar sus decisiones de compra en función de los servicios y las funciones actualmente disponibles en general.