Activen en segundos esta función gratuita de Gmail

Google ha desarrollado una función en Gmail que pretende brindar una capa adicional para la protección de ciberataques a sus usuarios de Gmail, su plataforma de correo electrónico, que puede activarse en cuestión de segundos.

Esto es como consecuencia de que la seguridad en línea se ha vuelto una preocupación central para millones de usuarios que, diariamente, envían y reciben correos electrónicos, siendo una de las principales amenazas: el phishing.

Esta técnica la usan los ciberdelincuentes para engañar a las personas con el fin de obtener información sensible, como contraseñas, números de tarjetas de crédito o datos personales.

Por qué es muy peligroso el phishing

Es una de las formas más comunes de ciberataque. Los delincuentes envían correos electrónicos que parecen legítimos, imitando a empresas o instituciones conocidas, para engañar a los usuarios.

Al hacer clic en enlaces o descargar archivos adjuntos maliciosos, las víctimas son dirigidas a sitios web falsos que solicitan información personal o instalan programas dañinos en sus dispositivos.

Este tipo de fraude ha evolucionado con el tiempo, y los estafadores se han vuelto cada vez más sofisticados. En la actualidad, un correo electrónico fraudulento puede ser casi indistinguible de una comunicación oficial, lo que hace que las medidas preventivas sean más necesarias que nunca.

Cuál es la función de Google para evitar estafas en Gmail

Con el objetivo de reducir los riesgos y ofrecer una experiencia más segura, Google ha implementado una nueva función en Gmail que realiza un análisis de seguridad en tiempo real.

Esta herramienta, de activación rápida y gratuita, detecta y bloquea posibles amenazas en el momento en que un usuario abre un correo electrónico, o intenta acceder a un enlace sospechoso.

Cuando se detecta un intento de phishing, Gmail alerta al

usuario inmediatamente, evitando que acceda a sitios web maliciosos o descargue archivos dañinos. Además, La función se actualiza constantemente para mejorar su capacidad de identificar amenazas emergentes y proteger a los usuarios de las nuevas tácticas que se puedan desarrollar.

Qué ofrece esta función de Google en la seguridad en línea

Una de las grandes ventajas de esta nueva función es su simplicidad. Google ha diseñado el sistema para que los usuarios puedan activarlo en menos de un minuto, brindando una defensa rápida y eficaz contra los ataques cibernéticos.

No requiere conocimientos avanzados en tecnología, por lo que cualquier persona, sin importar su experiencia en informática, puede configurar la protección en cuestión de segundos.

Además, Google recomienda a los usuarios activar la autenticación en dos pasos (2FA). Este método añade una capa adicional de seguridad al solicitar una verificación adicional cada vez que se intenta acceder a la cuenta desde un nuevo dispositivo. Estas dos herramientas refuerzan la protección contra accesos no autorizados y posibles estafas.

Cómo activar la función de protección mejorada en Google Chrome

Para los usuarios que navegan por internet utilizando Google Chrome, es posible activar una opción de protección más avanzada que funciona en conjunto con Gmail y otros servicios de Google. Esta configuración mejora la defensa frente a ataques de phishing y otro tipo de amenazas, como programas maliciosos o intentos de suplantación de identidad.

Esta función, conocida como “Protección mejorada”, brinda un análisis más detallado y exhaustivo de las páginas web que se visitan, los archivos que se descargan y las extensiones que se instalan.

Activar la “Protección mejorada” es un proceso sencillo. Solo es necesario ingresar el comando chrome://settings/security en la barra de direcciones del navegador y seleccionar la opción correspondiente.

Mientras que la “Protección estándar” ofrece una seguridad básica, la “Protección mejorada” analiza activamente las actividades en línea del usuario para detectar comportamientos

sospechosos y bloquea de forma preventiva sitios o archivos potencialmente peligrosos.

Con información de Infobae