NEWSLETTER

1 ALERTA EN ANDROID: FALSA ACTUALIZACIÓN DE CHROME QUE DA ACCESO A TU INFORMACIÓN BANCARIA

El enigma de la caja de Shein puede resultar atractivo, pero detrás de este supuesto premio se oculta un engaño diseñado por ciberdelincuentes para sustraer tus datos personales.

Shein, una de las tiendas en línea más grandes de ropa en China, ha ganado popularidad internacional desde su creación desde 2008, con una gran variedad de prendas a precios accesibles, lo que la ha posicionado como la opción preferida de muchos compradores en los últimos años.
Sin embargo, con la fama también llegan los peligros, y Shein no es inmune a ellos. La empresa lanza periódicamente promociones y ofertas tentadoras para sus clientes, pero lamentablemente, estos eventos también captan la atención de hackers que buscan explotar la confianza de los usuarios para perpetrar fraudes.

El engaño de la caja misteriosa de Shein es un ejemplo de esto. En esta modalidad de estafa, sutil pero peligrosa, los usuarios reciben un correo electrónico que parece ser de Shein y que promete una caja misteriosa como premio exclusivo.

Pero al abrir esta caja, en lugar de descubrir un regalo, los usuarios son redirigidos a un sitio web falso que solicita información personal y datos bancarios con el pretexto de reclamar el premio.

Esta es claramente una técnica de phishing, donde los ciberdelincuentes se aprovechan de la popularidad de la tienda en línea para hackear a los usuarios, principalmente con el fin de obtener sus datos para suplantar su identidad o vender la información a terceros.

Ante esta situación, es crucial estar alerta y tomar medidas para protegerse de este tipo de estafas. Si recibes un correo de Shein con una caja misteriosa o un cupón de descuento, no lo abras.

Además, es crucial siempre confirmar la autenticidad de los correos electrónicos y mensajes que recibes, prestando especial atención a la dirección del remitente y a posibles errores de gramática o de ortografía que puedan indicar un intento de fraude.

Igualmente, es aconsejable evitar hacer clic en enlaces que parezcan sospechosos y no proporcionar información personal a través de sitios web que no estén verificados. Si tienes alguna duda, lo más seguro es ponerse en contacto con la empresa directamente a través de sus canales oficiales para verificar la legitimidad de la promoción.

Al ingresar tus datos en la página web falsa, estás entregando toda tu información a los defraudadores. Ellos pueden utilizarla para suplantar tu identidad, realizar compras fraudulentas, sustraerte dinero o incluso acceder a tus cuentas bancarias.

2 FORO INTERNACIONAL DE CIBERSEGURIDAD 2024

Foro Internacional Ciberseguridad y protección de datos personales 2024

FECHA: **20 Y 21 de Mayo 2024**

MODALIDAD: **Presencial y en linea**

SEDE: **Escuela Juridica del Estado de Mexico**

3 ¿QUÉ ES UN PARCHE DE SEGURIDAD Y POR QUÉ CASI TU VIDA DEPENDE DE ELLOS?

Con la creciente complejidad de las aplicaciones y programas utilizados en la actualidad, es comprensible que ninguno sea perfecto y que existan errores. Aquí es donde los parches, y en particular los parches de seguridad juegan un papel crucial.

Hoy en día, la sociedad está a solo un clic de posibles ataques cibernéticos. Aunque tu seguridad en Internet pueda parecer una fortaleza impenetrable, tiene sus debilidades, ventanas y puertas, por donde, lamentablemente, pueden infiltrarse amenazas.

Por esta razón, se crean los parches de seguridad, que buscan cubrir todas las brechas, proteger tus datos e información y garantizar que todo funcione y esté protegido como debería.

Un parche de seguridad, en su esencia, es una modificación aplicada al software con el objetivo de corregir o "parchear" vulnerabilidades presentes en un sistema operativo, aplicación o dispositivo. Estas vulnerabilidades pueden surgir por diversas causas, como fallos en la programación, errores de diseño o la detección de nuevas amenazas por parte de expertos en ciberseguridad.

Su origen se remonta a los tiempos en que los datos se almacenaban en tarjetas perforadas, donde se utilizaban parches para "reparar" agujeros individuales hechos en dichas tarjetas.

En la actualidad, dada la complejidad de las aplicaciones y programas que se utilizan, es comprensible que casi ninguno sea perfecto y que existan fallos. Estos fallos de software, también conocidos como errores, pueden dar lugar a resultados incorrectos o inesperados, o a comportamientos no deseados.

Por ejemplo, si Google Chrome de repente deja de funcionar correctamente, se emite un parche; si se descubre una vulnerabilidad en Android 13, se emite un parche; si no puedes acceder a una aplicación en Android Auto, se emite un parche. Son tan frecuentes que incluso grandes empresas como Microsoft tienen el conocido "Martes de parches", donde el segundo martes de cada mes lanzan una lista de cambios y mejoras.

El punto crítico aquí es cuando estos fallos pueden ser explotados para eludir las medidas de seguridad, creando lo que se conoce como vulnerabilidades. Aquí es donde entra en juego el parche de seguridad. La situación se vuelve más tensa para las empresas responsables del fallo, ya que los ciberdelincuentes pueden aprovechar estas vulnerabilidades para obtener acceso no autorizado a un sistema, robar datos, instalar malware o extorsionar a las empresas.

Aquí es donde surge la confusión, ya que las actualizaciones y los parches suelen agruparse cuando se lanza una nueva versión de la aplicación de software que ha sido actualizada y parcheada. Cuando se lanza una nueva versión de Android para tu teléfono móvil, por lo general, incluye una variedad de elementos.

El problema surge cuando los usuarios ven los parches de seguridad como una interrupción que perturba su flujo de trabajo y les obliga a reiniciar sus dispositivos. Como resultado, a menudo retrasan su instalación tanto como sea posible, lo cual es un error crítico, ya que no se puede enfatizar lo suficiente la importancia de los parches de seguridad.

Como se mencionó anteriormente, las grandes empresas, debido a la gran cantidad de aplicaciones, software y demás que gestionan, están constantemente tratando de solucionar los problemas que surgen en el camino.
Por ejemplo, Apple lanzó recientemente dos parches importantes para iOS. Estos resuelven más de 40 problemas, incluyendo dos que ya están siendo explotados en ataques. Uno de los errores afecta al kernel del iPhone, mientras que el otro afecta al sistema en tiempo real utilizado en dispositivos como los AirPods.

Por su parte, Google también ha estado trabajando en la corrección de vulnerabilidades en Chrome. En marzo de 2024, lanzaron varios parches, incluyendo algunos para problemas críticos que podrían permitir a un atacante ejecutar código de forma remota.

Microsoft no se queda atrás, lanzando parches para más de 60 vulnerabilidades. Sin embargo, mencionar a esta empresa también implica hablar de graves retrasos en el lanzamiento de parches de seguridad para problemas críticos.

En marzo de 2024, los ciberdelincuentes robaron respaldados del gobierno de Corea del Norte, logrando un gran triunfo al explotar una vulnerabilidad en el sistema operativo Windows, conocida como CVE-2024-21338, que mantuvo a Microsoft en jaque durante un tiempo excesivo, específicamente seis meses hasta que aparentemente lo solucionaron.