

## **S2 Grupo advierte de la mayor oleada de la historia de ciberataques tipo phishing**

**La empresa española de ciberseguridad S2 Grupo ha advertido de que la llegada del confinamiento ha acarreado un incremento sin precedentes de los ciberataques masivos a particulares y empresas**

De hecho, expertos de la compañía han informado de que, sin duda, se está viviendo la mayor oleada de la historia de ciberengaños tipo phishing. Éstos consisten en suplantar la identidad de una empresa o persona y de forma fraudulenta conseguir información privada de las víctimas como pueden ser contraseñas, datos de tarjetas de crédito, información bancaria o directamente infectar los equipos con malware, por ejemplo.

“Cualquier tipo de situación es buena para un ciberdelincuente, si puede extraer dinero. Ahora que estamos en casa el uso de las redes y de los servicios online es todavía más común. Por eso, aprovechan cualquier noticia destacada para desarrollar métodos de engaño que capten la atención de los usuarios y que se descarguen algún documento, que entren en algún enlace o introduzcan sus credenciales y así conseguir su objetivo: robar nuestros datos, nuestro dinero o la instalación de malware en nuestros equipos”, ha explicado José Rosell, socio-director de S2 Grupo.

“El procedimiento es sencillo. El ciberdelincuente envía mensajes de forma masiva haciéndose pasar por compañías de prestigio y piden pinchar en un enlace, por ejemplo, que hará que se descargue algún virus en nuestro equipo o nos llevará a alguna página falsa en la que, si no nos damos cuenta, introduciremos nuestras credenciales o nuestros datos bancarios y el atacante podrá disponer de ellos”, ha comentado Miguel A. Juan, socio-director de S2 Grupo.

Desde la compañía de ciberseguridad se ha advertido de que estos mensajes están llegando por email, por whatsapp, por SMS o por redes sociales, y se atribuyen a conocidas compañías de agua, luz, bancos, supermercados y servicios de televisión.

Expertos de S2 Grupo han aconsejado tener cautela si se reciben este tipo de mensajes, comprobar bien los emails y no abrirlos si se desconoce el remitente, asegurarse de que la página web en la que se introducen los credenciales es la auténtica de la compañía y, ante cualquier duda, contactar directamente con la empresa para cerciorarse de que el mensaje es oficial. Junto a esto, si se detecta algún tipo de ciberataque se puede informar a la Guardia Civil a través del email [ciberestafas@guardiacivil.org](mailto:ciberestafas@guardiacivil.org).

### **Datos de contacto:**

Luis Núñez  
667574131

Nota de prensa publicada en: [Madrid](#)

Categorías: [Ciberseguridad](#)

---

**NotasdePrensa**

<https://www.notasdeprensa.es>