El ciberpatrullaje en la Red ha detectado un envío masivo de correos electrónicos que suplantan a una multinacional logística estadounidense dedicada al comercio electrónico. El email recibido indica que su cuenta personal ha sido bloqueada por motivos de seguridad al haber detectado accesos ilegítimos, debiendo el usuario introducir sus credenciales para poder recuperarla. El objetivo de los ciberdelincuentes es conocer nuestras credenciales de acceso y, además, hacer uso de la tarjeta bancaria vinculada a nuestra cuenta.

La Policía Nacional alerta de una tentativa viral de fraude a través de phishing, realizada mediante el envío masivo de email supuestamente enviados por una multinacional logística estadounidense dedicada al comercio electrónico. Los ciberdelincuentes utilizan los logos de la mercantil para dar apariencia de autenticidad y utilizan en la cabecera del mensaje una dirección que induce a engaño sobre la cuenta de correo que desde la que realmente se está enviando el mensaje. De este modo pretenden engañar al usuario con el fin de obtener sus credenciales de acceso y los datos de la tarjeta bancaria vinculada a nuestra cuenta, con el objetivo de realizar un uso fraudulento.

Ciberpatrullaje de la Red

Desde la entrada en vigor del Estado de Alarma, el hecho de que los ciudadanos permanezcan confinados en sus viviendas hace que aumente el uso de Internet, sobre todo para realizar compras. Por ello, los especialistas en ciberdelincuencia de la Policía Nacional han intensificado la vigilancia y monitorización de los movimientos presumiblemente ilícitos por la Red y las redes sociales.

Fruto de ello, recientemente se ha detectado una tentativa viral de fraude a través de phishing, mediante el envío masivo de correos electrónicos que suplantan la identidad de una multinacional logística. El email recibido por la víctima indica que su cuenta ha sido bloqueada por motivos de seguridad, al haber detectado accesos ilegítimos, instando al usuario a que pinche en un enlace para “desbloquear la cuenta”.

Al pulsar el enlace se abre una nueva ventana en el navegador, también con la estética de la empresa original, que ofrece dos opciones: “crear una cuenta nueva” o “iniciar sesión”. En cualquiera de los dos casos, los ciberdelincuentes tendrán acceso a los datos introducidos –nuestros credenciales- y, además, a la tarjeta bancaria vinculada a la cuenta de usuario.

Especial precaución con esta modalidad de phishing

La Policía Nacional advierte de la viralidad de esta modalidad de estafa y aconseja tener una especial precaución, desconfiando de todos aquellos correos procedentes de direcciones desconocidas y verificando que nos encontramos en la página auténtica antes de introducir nuestras credenciales.

---

* Texto remitido en el que se respeta el contenido íntegro, la redacción y la ortografía, con excepción del titular y de la entradilla del artículo