



Estafa sofisticada relacionada con Bitcoin involucra a personalidades como Carlos Slim

Una campaña masiva de estafa referente al Bitcoin ha estado involucrando personalidades Amancio Ortega, el chef Jamie Oliver, Richard Branson, Bill Gates y últimamente el magnate mexicano Carlos Slim.

Se trata de una estafa sofisticada que se ayuda de anuncios en Facebook, Google y otros sitios importantes, haciendo parecer que la información es legítima y confiable.

Hoy apareció un anuncio en el popular sitio web TechCrunch, bajo el título «*Carlos Slim hace su mayor inversión*». Al acceder a dicho anuncio, se abre un artículo en el sitio web Thinkamaze, que es un scam de alguna página web de CNN referente a tecnología.



En este artículo se puede leer información sobre un proyecto secreto de Carlos Slim que brindaría parte de las ganancias de los multimillonarios de Wall Street a los mexicanos, con una pequeña inversión en su nuevo software.



Dentro de este sitio pirata, todos y cada uno de los enlaces apuntan al sitio pensting-disical.com/click que podría ser un sitio web dedicado al phishing.

Entre los software y páginas web mágicas que ofrecen estos sitios web, destacan The Bitcoin Code, Bitcoin Revolution o Bitcoin Trader. Todos pidiendo un depósito supuestamente reembolsable de 250 dólares que serviría para ganar mucho dinero.

Se trata de una variante de la famosa estafa nigeriana, que por décadas se ha utilizado para estafar a la gente por medio de correo electrónico.

Según Verne, el fundador y consejero delegado de Alto Data Analytics, Alex Romero, esta variante de la estafa se ha remontado al menos a 2017. La compañía detectó tres picos en la estafa, que son en febrero, septiembre y noviembre, siempre utilizando la imagen de personajes conocidos.



Estafa sofisticada relacionada con Bitcoin involucra a personalidades como Carlos Slim

En noviembre pasado, este timo logró un alto nivel de sofisticación cuando los estafadores lograron hackear cuentas verificadas de redes sociales y cambiaron los nombres por personajes como Elon Musk, Donald Trump, entre otros, para pagar por anuncios que dirijan a los sitios web falsos.

La sofisticación y el engaño en la confianza de los usuarios al ver anuncios en sitios legítimos, ha hecho que miles de usuarios caigan en la trampa y pierdan mucho dinero. Lo más recomendable en estos casos, es siempre verificar la autenticidad del sitio web que se está visitando, revisar que la dirección sea la correcta. Si el sitio web tiene logos de CNN y su misma apariencia, pero el URL es thinkamaze.com, definitivamente se trata de un Scam, aunque tenga un certificado SSL válido.

También es necesario tener sentido común, si te ofrecen un software mágico para ganar miles de pesos al día, algo debe andar mal.