

Golpe que promete alta rentabilidade em Bitcoins

Tem crescido o golpe digital das falsas “trade forex, binary e cryptocurrencies”, no qual os bandidos digitais monitoram redes sociais e grupos de investidores e fazem amizade ou contato com potenciais vítimas para aplicar o golpe. Comumente chegam às vítimas preferenciais com base em postagens das próprias “presas”, que indicam se elas possuem algum patrimônio ou valor a investir.

Aí vem a “engenharia social” ou a arte de “enganar pessoas”, os criminosos, fazem um contato com a vítima, prometendo altíssima rentabilidade para seu dinheiro. Para tanto, conduzem a vítima a criar uma conta em uma corretora de bitcoins e comprá-los. Neste momento, para ganharem confiança, pedem que a pessoa acesse o “site” da corretora, que é um site falso, e a induzem a criar uma conta e depositar apenas um pequeno valor para ver a rentabilidade. Assim é feito, em questão de dias os valores em bitcoins rendem 5 a 10% na “conta virtual”, o que “desarma” o investidor, fazendo com que este transfira grandes quantias de criptomoedas para a corretora falsa.

Assim, os criminosos mantêm o painel por aproximadamente 30 (trinta) dias, com simulações falsas de rentabilidade. As vítimas demoram até 60 (sessenta) dias para descobrirem e só percebem quando solicitam o “resgate do investimento”. Então, começam as desculpas, as evasivas, até que chega um momento em que a corretora simplesmente some, para de responder, tira o site do ar (site, aliás, registrado anonimamente) e o golpe se consuma.

Geralmente, a vítima tem pouquíssimos registros, não consegue mais acesso ao seu “painel administrativo” no site falso da corretora e pode ter apenas alguns prints dos endereços de

destino dos bitcoins, registrados na sua própria corretora.

É possível investigar e rastrear o dinheiro, porém, não significa necessariamente saber quem está por trás de uma carteira eletrônica. Isso vai depender da cooperação da exchange, wallets e aplicações. Não é um procedimento simples e rápido e pode envolver outros continentes. A recomendação para quem é vítima é preservar todas as mensagens e contatos recebidos e imediatamente buscar apoio para apuração da identidade dos fraudadores. Ainda que o número de WhatsApp usado para mensagens pelo fraudador seja internacional, a rede guarda registros de aplicação, o que pode indicar pessoas do Brasil, apenas usando um número internacional para dificultar a apuração da autoria.

O golpe tem se mostrado extremamente eficaz tendo em vista o momento ruim dos investimentos no Brasil, sobretudo em renda fixa, onde pessoas físicas buscam alternativas na Bolsa de Valores e nas Criptomoedas.

Para não se tornar mais uma vítima, basta uma simples pesquisa no Google para se ter uma dimensão se a corretora tem boa reputação ou é um scammer (qualquer esquema ou ação enganosa e/ou fraudulenta que, normalmente, tem como finalidade obter vantagens financeiras). Um site muito útil é o <https://www.scamadviser.com/> responsável por checar qualquer site indicado e pode informar se trata de um site confiável ou não, muitas vezes indicando se o site oferece serviços de criptomoedas de alto risco. Se o risco apontado pelo ScamAdviser for alto, fuja! E mais uma dica: jamais revele seus investimentos em redes sociais!