LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
WEDNESDAY, SEPTEMBER 27, 2017

PERSPECTIVE

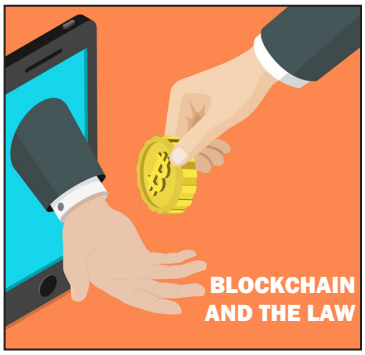
When high-tech cryptocurrencies meet low-tech scammers

By Justin Wales

Most of us have logged into a bank's website, either directly or through a mobile banking app, to transfer or withdraw funds. While most appreciate the convenience of these on-the-go financial management tools, the ease associated with controlling funds online poses a serious threat to account security. Yet most online bank users spend very little time thinking about data security beyond memorizing their password and pin. This is likely because of the perceived difficulty of implementing an always-changing standard of best practices and the relative ease of reversing fraudulent charges without penalty through their bank's customer service departments. But for the growing number of people holding cryptocurrencies, like bitcoin or ether, in mobile wallets or online exchanges, the threat of a security breach is much more dire because of the unwillingness of third-party crypto wallets and exchanges to reimburse funds lost as a result of fraud or theft and the immutability of the virtual currencies themselves.

The reality that cryptocurrencies are susceptible to online theft may surprise those familiar with the security promises associated with the blockchain technology underpinning virtual currencies like bitcoin. Because the blockchain — the public ledger that keeps track of the history of each coin — is decentralized and requires so much computational energy to falsify that it is economically unfeasible to alter, the currencies themselves are widely viewed as "hacker proof."

However, even though a robust blockchain like bitcoin's is itself invulnerable for the foreseeable future (advancements in quantum computing poses serious security concerns), a system is only as vulnerable as its weakest link. Accordingly, while cryptocurrency holders



Shutterstock

can rest assured that the record of their transactions will not be altered to erase the digital currency already in their possession, they still need to be aware of other security threats, including a low-tech scam that has emerged that allows thieves to exploits a weakness in how some of the most popular crypto exchanges and wallets "authenticate" a user via an SMS text message before allowing a password to be reset.

In the "SIM card swap" con, scammers use information obtained through third-party data breaches, phishing emails, social media investigation, or personal knowledge to convince a mobile phone provider's customer service representative that they are an account holder who needs to replace a cellphone's damaged or lost SIM card. Often using as little as the accountholder's name, address and last four SSN digits, the scammer provides the mobile phone provider with a new SIM card to activate, which is then linked by the customer service representative to the accountholder's phone number. Once activated, the scammer is able to receive all calls and text messages sent to the accountholder's number. The thief then goes online and requests a password change for its victim's cryptocurrency wallet or exchange account (but often also their email, social media or traditional bank accounts) at which point the scammer is sent SMS text messages that contain authentication links or codes that allows them to "authenticate" the password change request. Once the password is changed the accountholder is locked out of their account and the scammer is free to do as he or she pleases — including transferring the accountholder's cryptocurrency funds to an anonymous wallet they control with minimal risk of recourse.

Given the increased hype and popularity of cryptocurrencies over the last year, among a wave of adopters who are often less technologically proficient and security-minded than earlier advocates, mobile service providers have seen a significant increase in the number of SIM card swap attempts. Mobile providers have responded with promises to alert their customer service representatives of the scam and better train them to detect attempts, but given the potential harm one could suffer as a result of this scam, it is imperative that mobile users, especially those holding cryptocurrencies, take a proactive role in securing their SIM card and various accounts they do not want breached.

The easiest and best thing a mobile user can do to prevent their SIM card from being surreptitiously swapped is to contact their mobile phone provider and ask that they require anyone who attempts to make a change to their account to recite a verbal passphrase to the customer service representative. For even more security, they can ask their mobile phone provider to disallow any telephonic changes to their account and require that all changes be made only after the accountholder appears in a store with a government-issued ID.

For those new to the cryptocurrency world, perhaps the best advice is to not put too much trust in third-party exchanges or wallets, especially those that integrate text message or email responses as second factor authenticators. At a minimum, disable text or email authentications for your online accounts, and instead set your second factor authentication to be a time-based token generator like Google or Microsoft Authenticator. Ultimately, however, the revolutionary philosophy underlying virtual currencies like bitcoin is that placing trust in a centralized entity, whether a government that issues currencies or a bank, wallet or exchange that holds funds, poses inherent risks to the integrity and security of those assets. Accordingly, a philosophical contradiction develops that runs counter to one of virtual currencies like bitcoin's main characteristics when a crypto holder relies too heavily on the security protocols and business practices of a third-party exchange or wallet to keep his or her assets safe.

For those particularly concerned about the vulnerability of their crypto accounts, or who are holding significant crypto assets, the safest solution is to segregate your funds in an offline wallet stored in a secured home vault or, better yet, safety deposit box. Those unwilling to take this step should take it upon themselves to stay up-to-date on best practices for securing, encrypting, and backing-up their online wallets, and get in the habit of being proactive about data security. Ultimately it is up to you to keep your crypto secure.

Justin Wales *is the co-chair of Carlton Fields' Blockchain Technology and Virtual Currency practice. He can be reached at jwales@carltonfields.com.*


JUSTIN WALES