Don't Fry Your Brain On Cryptocurrencies

cyber security mobile banking cryptocurrencies

Summary: Digital wallets, where cryptocurrency sits, and the exchanges on which they can be traded, present vulnerabilities that have already publicly been exploited. What can your bank do to stay safe?

Too much technology can fry your brain. At least that is what a new study seems to point out. Canadian researchers have released the results of a 10Y study on how children's brains develop over time and found kids that spend less than 2 hours each day watching screens scored better on cognitive tests than those who spent more time watching screens. Take care.

As you ponder how much screen time you can handle, we continue our discussion on blockchain and cryptocurrencies, along with some tips to help safeguard your bank and customers.

When it comes to digital wallets that some of your customers or employees may be using, note that the emergence of cryptocurrencies has made it more difficult than ever to control the impact of a cyberattack. This is because security relies almost entirely on the digital wallet's private key staying secure.

Digital wallets, where cryptocurrency sits, and the exchanges on which they can be traded, present vulnerabilities that have already publicly been exploited.

Case in point: The hacking of a crypto-exchange in 2013 actually caused a dramatic drop in the value of Bitcoin. Also, 93% of mobile (or 'digital') wallets, which can hold crypto-currency information alongside traditional payment card data, have been found to contain at least three medium risk vulnerabilities and 90% contain at least two high-risk vulnerabilities, according to research from High-Tech Bridge. Caution is clearly needed.

In the face of cryptocurrencies' fast and continuous rise and the equally sharp increase in potential risk, what can community banks do to mitigate risk?

Monitor who's on third: Third-party hardware and software developers typically make the mobile or digital wallets that hold these digital currencies. Like third-party relationships in general, banks must be aware of which companies are developing these wallets and how they are managing and mitigating potential risks and vulnerabilities. What that typically means is that the private key used in the encryption process needs to be kept safe.

Owning the digital asset: Many banking customers may not understand the concept of 'owning' a digital asset, especially a monetary one. While the blockchain technology underlying cryptocurrency seems very secure, the currency is just a balance on a ledger. The user really holds a cryptographic private key, which enables them to make transactions from their wallet. If that private key is stolen or compromised, that 'money' is stolen.

Harden up: So-called hardware wallets may be cryptocurrency users' best bet to secure the all-important private key that allows transactions. These hardware wallets are offline so they can't be hacked. They also often use multi-factor authentication to access the key. If you discuss this option with any of your business

customers, make sure that they find one that also uses the FIDO Alliance's protocol to protect cryptocurrency. FIDO is the world's largest ecosystem for standards-based authentication, so it is a good place to start.

CECL SOLUTION - WITH YOU, EVERY STEP OF THE WAY

CECL is one of the biggest challenges for community bankers these days. Our experts are ready to guide you every step of the way through this integration with no software to maintain. Learn more about our CECL Solution.