[PDF Database Document] - BTCC Cryptocurrency Exchange

Original:
https://www.btcc.com/en-US/academy/research-analysis/how-your-phone-guesses-your-seed-phrase-and-puts-your-cryptocurrency-at-risk

How Your Phone Guesses Your Seed Phrase – and Puts Your Cryptocurrency at Risk

On Reddit, one user says predictive text could be a crypto investor's worst enemy — making it easy for thieves and criminals to gain access to victims' digital assets.

If you ever type your seed phrase into your phone, you might want to read this.

A user on Reddit claims his Android phone managed to guess his seed phrase — and this could be advantageous to hackers.

Seed phrases consist of 24 random words — and they need to be repeated in order for users to access their digital assets.

Although this is meant to ramp up security for crypto investors, u/Divinux on Reddit warned smartphones could end up being the enemy. They wrote:

"Predictive typing remembers your used words and will suggest the second word as soon as you type the first one, especially if it's a word you don't commonly use."

He expressed fears this might embolden criminals to steal phones and start typing words off BIP 39 lists to see what the phone suggests next.

BIP 39 lists consist of a specific 2,048 words — and while it might take a little work to find the starting phrase, it would be far from impossible.

How to Keep Safe

According to u/Divinux, a top tip includes clearing your predictive text cache — preventing the smartphone from remembering distinctive words.

This can be achieved on both Samsung and Apple devices.

Some Reddit users were more concerned that the crypto apps he was using were asking him to type out his entire seed phrase in the first place.

He explained that this wallet now asks him to confirm two words from the list in a random order — such as the 4th and 18th — adding:

"It is likely I generated a wallet, wrote the seed down, deleted the wallet, and restored it from the written down seed to make sure I wrote it down correctly before transfering funds into it."

As for the best way to determine if you're at risk?

He encouraged people to type out "I love eating bicycles at midnight" into their browser address bar — and then hit search, adding:

"Now close your browser, go into say, whatsapp, and start typing 'I love' into a chat. Note the next word it suggests. Keep following the phrase to the end. It's fun!"

Some of those commenting on the thread argued that password fields should be safe — and the real danger comes when someone is typing a seed phrase in a less-secure environment.

They warned that copying and pasting seed phrases is a bigger problem — especially because the clipboard can be snooped on by malicious applications.