Getting Phished
It Can Happen To You

by Aaron Grothe

Introduction

You can fool yourself

…

It can happen to you
It can happen to me
It can happen to everyone eventually

Yes - "It Can Happen"

What does my Email inbox look like?

Typical week

- 2-3 emails “from” Square/Stripe
  - No Stripe or Square account
- 4-5 emails - my Amazon merchant/user account suspended
  - Email not associated with my amazon account
  - No Amazon merchant account
- 6-8 Emails “from” Email provider - account is going to be disabled

Pretty easy to dismiss

Multi-Factor Authentication

Turn it on if you don't have it turned on for everything important

I use google-authenticator and authy

Highly recommend

Drawback of MFA

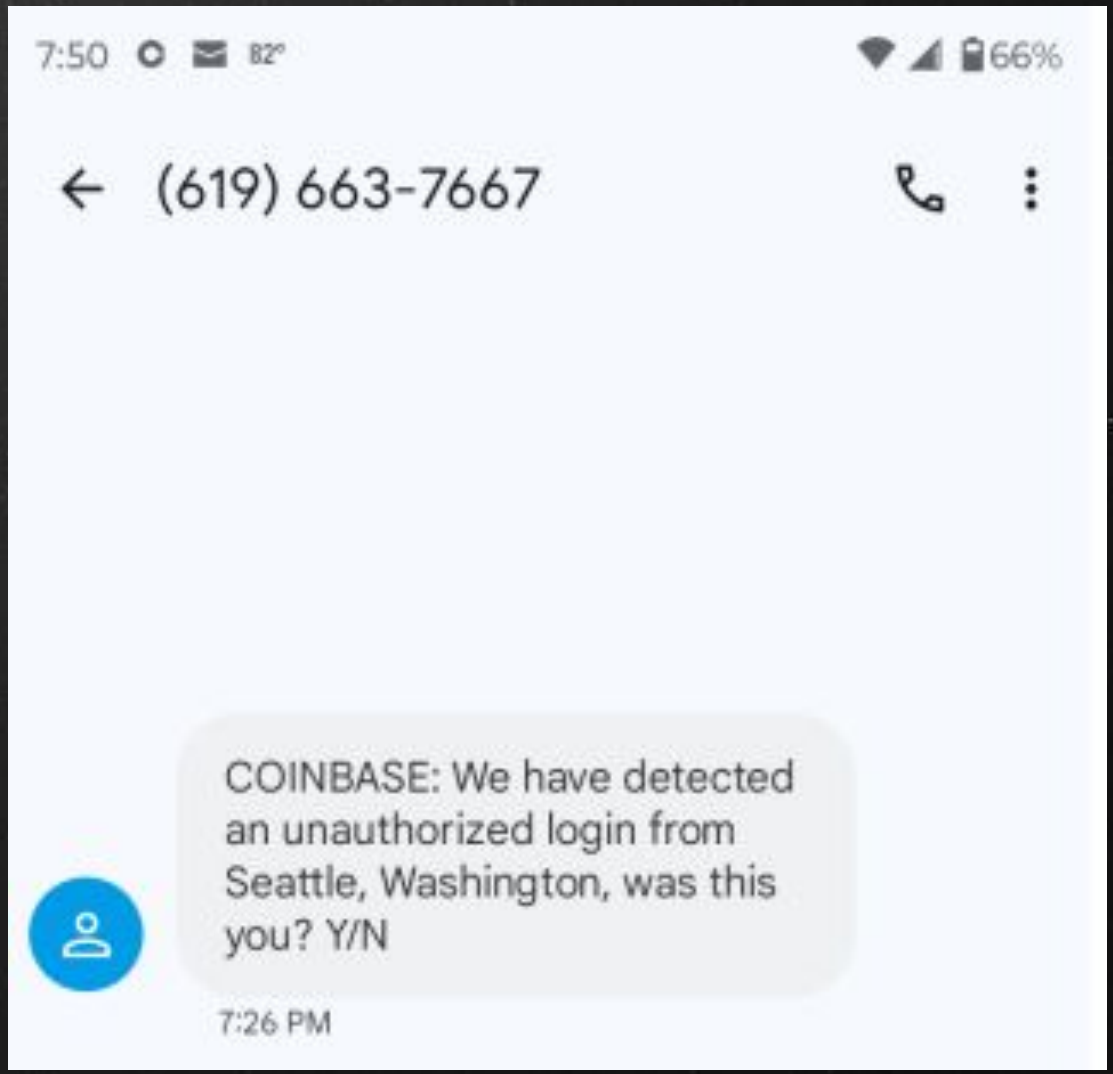
There are multiple MFAs I use

Authenticator apps - Google Authenticator/Authy
SMS Texts
Voice Calls with code

Multiple MFA requests a day

Different ways it is requested
Get a handful of false requests as well

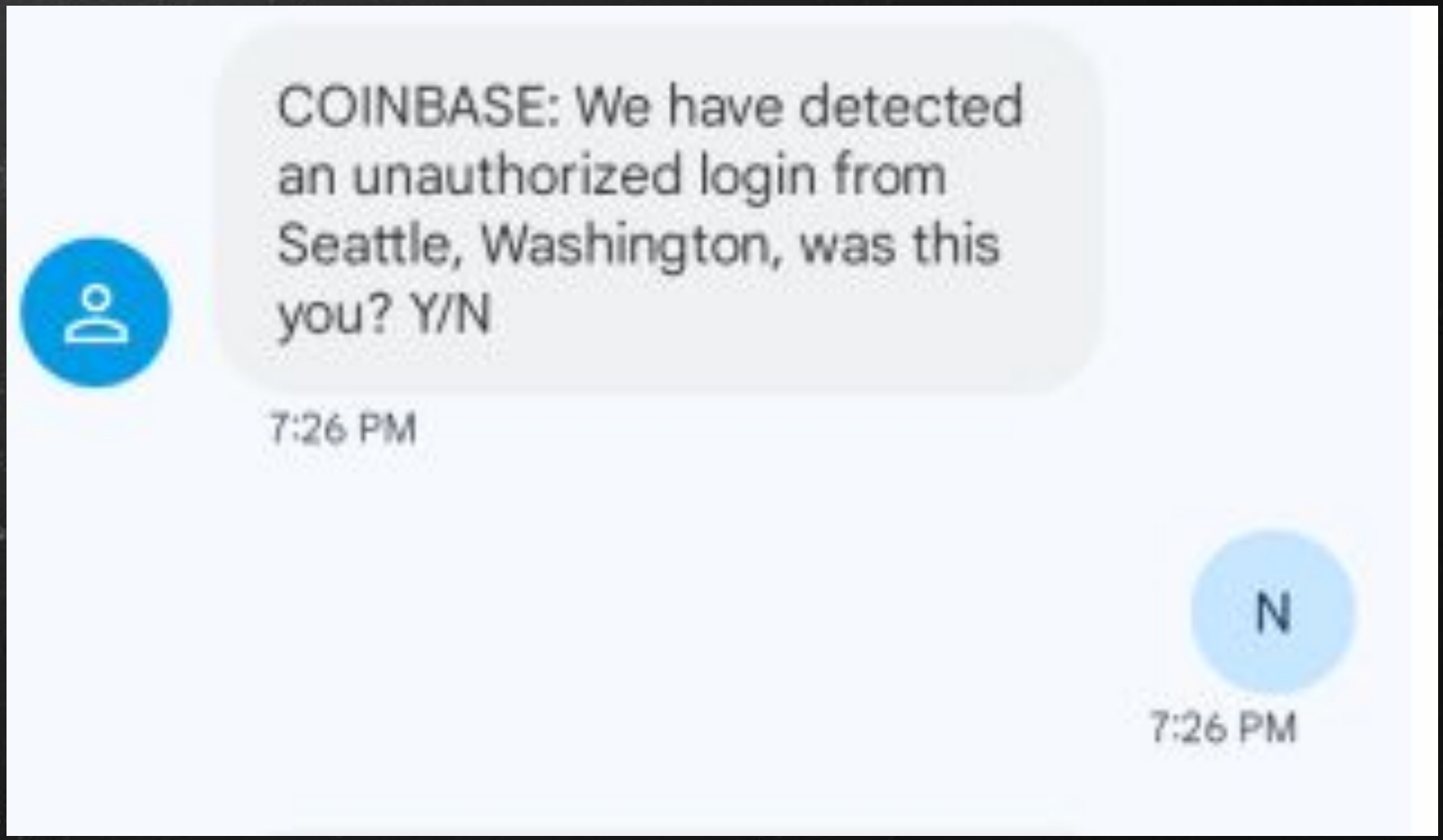
So this got my attention



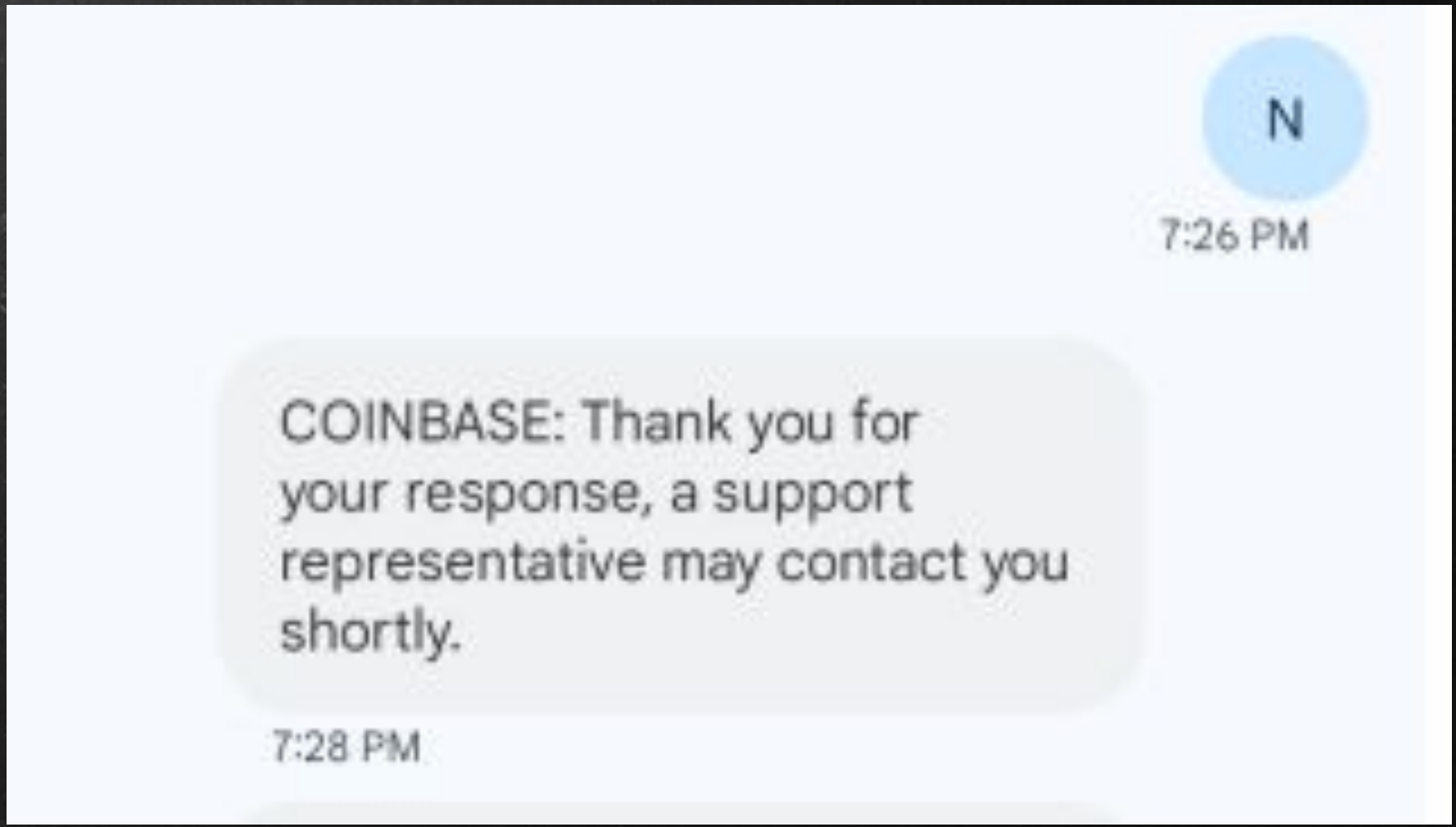
Why?

- I have a Coinbase account
- I am always concerned about anything Crypto
- Lot of exchanges are being hacked
- My Coinbase account is tied to my bank account and they won't let me unattach it

Mistake #1


COINBASE: We have detected an unauthorized login from Seattle, Washington, was this you? Y/N
7:26 PM
N
7:26 PM

Now I Messed Up!!!



The Phone Call

This is when things goes really wrong

Get a phone call immediately afterwards (What are the Odds???)

The Phone Call

Caller asks for my email address to confirm account.

Does several very smart things

- Says he can put a freeze on my account - only for 30 minutes though
- Says someone is currently trying to access my account and transfer money
- Mentions an 800 number to call if I want to call back into Coinbase
- Asks if I share this password with any other accounts

The Phone Call

- Says he can put a freeze on my account - only for 30 minutes though
  - Ticking Clock
- Says someone is currently trying to access my account and transfer money
  - Active Threat
- Mentions an 800 number to call if I want to call back into Coinbase
  - If they're giving me an 800 number they must be legit
- Asks if I share this password with any other accounts
  - Do I? If so maybe that is how it got hacked. Transfers responsibility to me

The Phone Call

I start asking questions

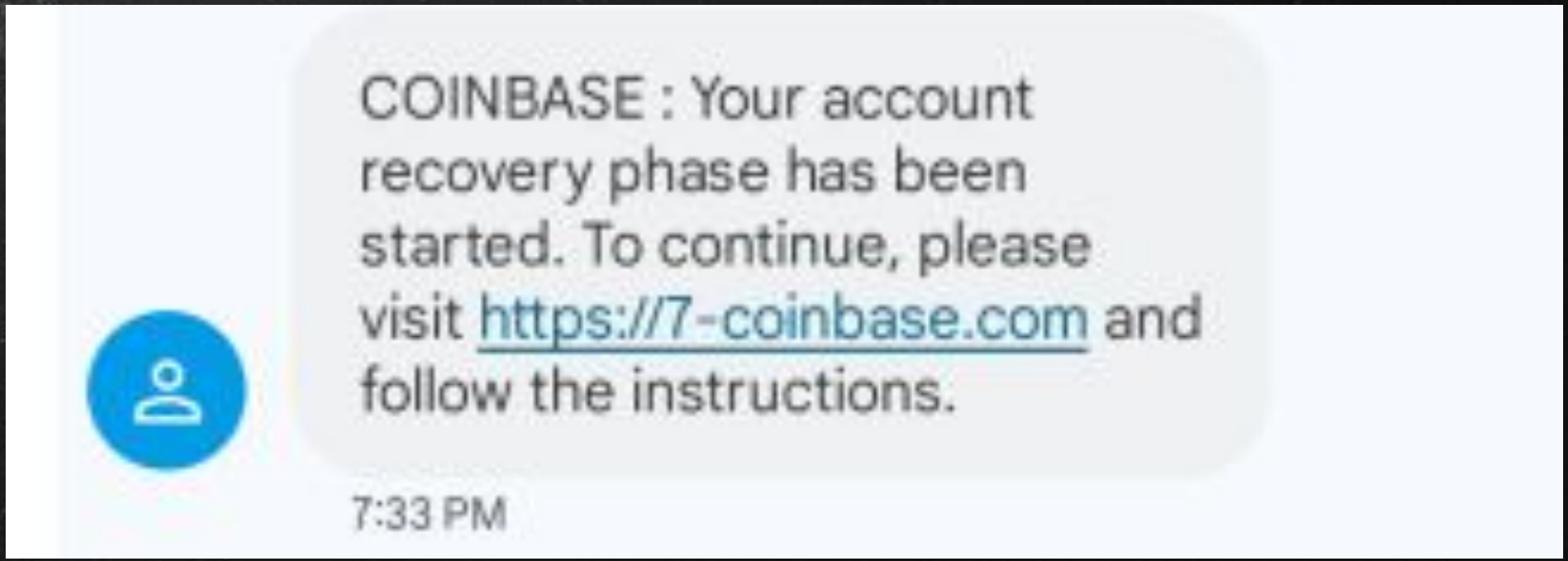
- Why can you only lock the account for 30 minutes?
- I have MFA on the account how can this be happening?
- Can you tell me the size of the transactions they're attempting?

What Saved Me?

- The tech support guy is asking me to do things on my phone.
  - I fortunately suck at doing things on my phone
- I'm home and able to access my PC
  - Start a chat session with Coinbase tech support to confirm that this is valid
  - Takes a lot of steps to validate
- I tell the "tech support" guy that I'm having trouble with my phone and trying to be on the phone and using the internet on my phone slowing things down

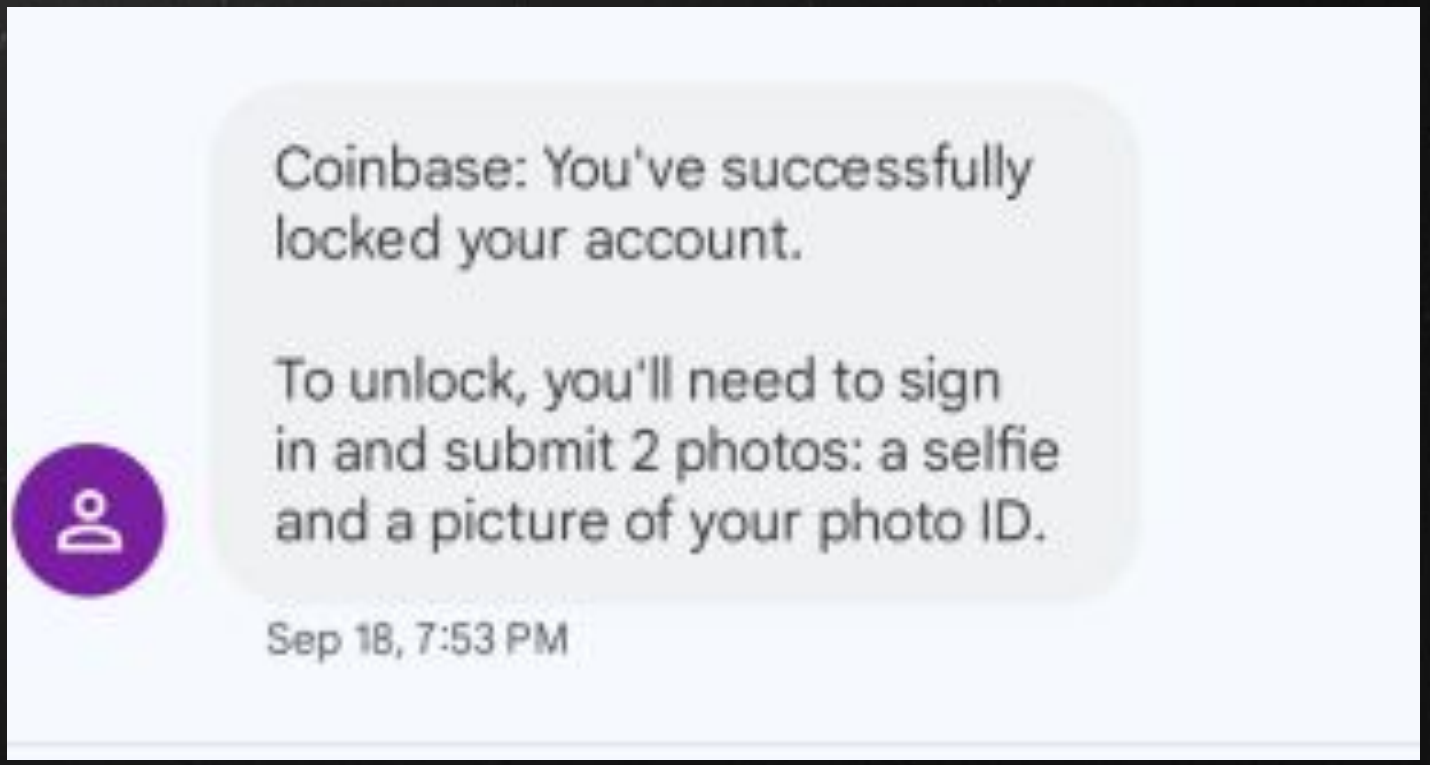
What Saved Me?

- The "tech support" guy is getting frustrated that I haven't been able to get into my account and everything.
- So he sends me the following and moves on to next target



What Saved Me?

- Fortunately the link https://7-coinbase.com isn't valid
- I slow walked it enough I got an update from Coinbase it is an invalid request
- I am able to really lock my account



How close was I?

I was really close to falling for it?

If this had happened at work, where I had less access to the internet I might have fallen for it.

The potential for financial impact is very large for this, because of the way the account is setup.

Takeaways

- Have MFA turned on everywhere
- Turn off/inactivate accounts you don't need to access
- Independently try and validate anything like this that comes to you
- Stop, breathe and think