Paranoid Mode: On

In this lesson, we'll learn that it's better to be overly cautious than to risk a security breach.

We'll cover the following

- It’s better to be safe than sorry
- An example

It’s better to be safe than sorry

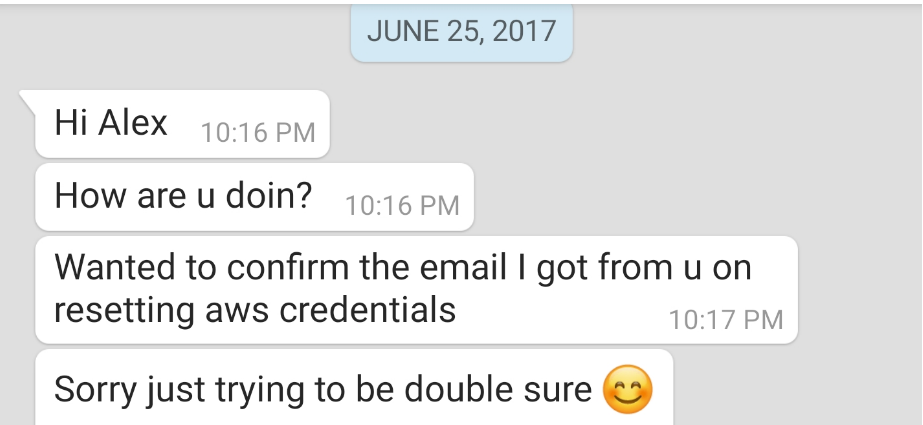
Remember, being paranoid might trigger a scoff or an eye-roll from one of your colleagues, but don’t let that deter you from doing your job and making sure the correct precautions are in place.

Some users do not appreciate enforcing 2FA on their account, or might not like to CC their manager in an email to get an approval, but your job is to make sure the ship is tight and secure, even if that means having to implement some annoying checks along the way.

An example

I still remember being locked out of an AWS account (I stupidly let my password expire) and having to ask our Lead System Administrator for a password reset with an email along the lines of “*Hi X, I’m locked out of my AWS account, can you reset my password and share a new, temporary one here?*”

The response? A message on WhatsApp:



JUNE 25, 2017

Hi Alex 10:16 PM

How are u doin? 10:16 PM

Wanted to confirm the email I got from u on resetting aws credentials 10:17 PM

Sorry just trying to be double sure 😊

it's better to be safe than sorry! Make your security fool-proof by asking for confirmation of on another medium

This was the right thing to do, as a person with malicious intentions could have just gotten hold of my email account and try to steal credentials by posing as me. Again, being paranoid is often a virtue.

In the next lesson, we’ll learn about assigning domains safely.