

Two/Multi Factor Authentication

What is it and why do I want it?

From Wikipedia:

- **Multi-factor authentication (MFA)** is a method of [computer access control](#) in which a [user](#) is granted access only after successfully presenting several separate pieces of evidence to an [authentication](#) mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).^{[1][2]}
- **Two-factor authentication** (also known as **2FA**) is a method of confirming a user's claimed identity by utilizing a combination of *two* different components. Two-factor authentication is a type of multi-factor authentication.



Common example of 2 factor authentication

Card (something you have) + PIN (something you know)

But what's the big deal?

Aren't passwords good enough?

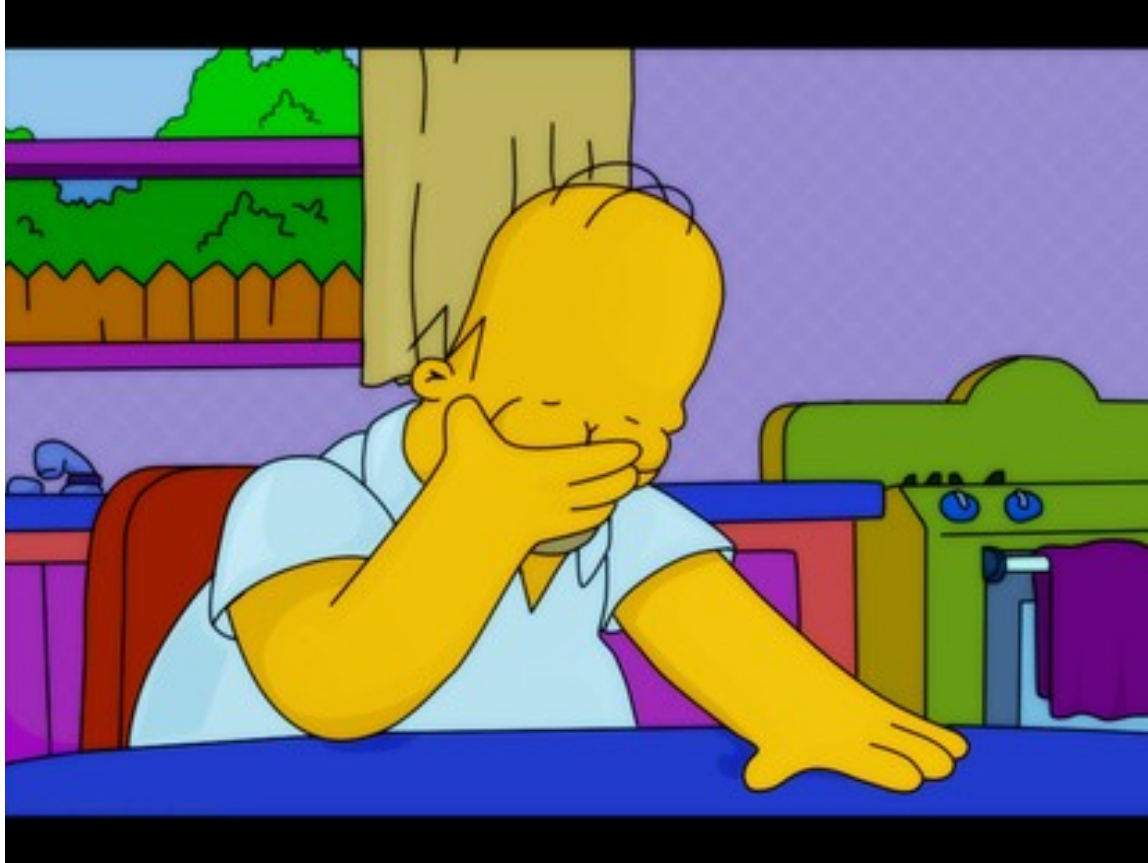
NO!

Why passwords alone are bad:

- They can be guessed
- They can be leaked
- People have trouble remembering complex passwords

**“Security questions” only make
the problem worse.**

Any site that gives you a barrage of
“security questions” should not be
considered too secure.



How I feel after being asked security questions.

The physical component of 2FA is
a strong obstacle/deterrent.

It is important that the physical item
is unique.

When is 2FA not 2FA?

Things to try to avoid



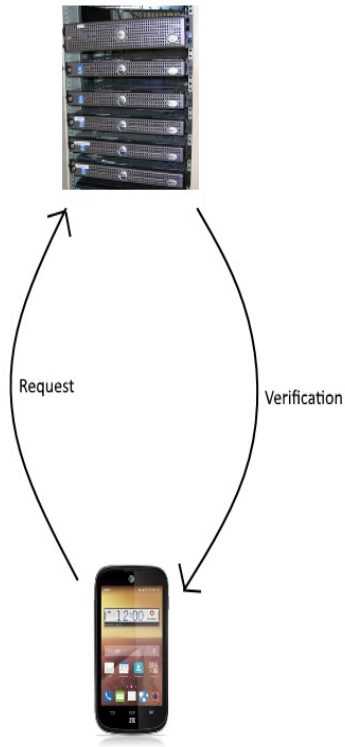
BAAAAAAAAAAAAAD Idea



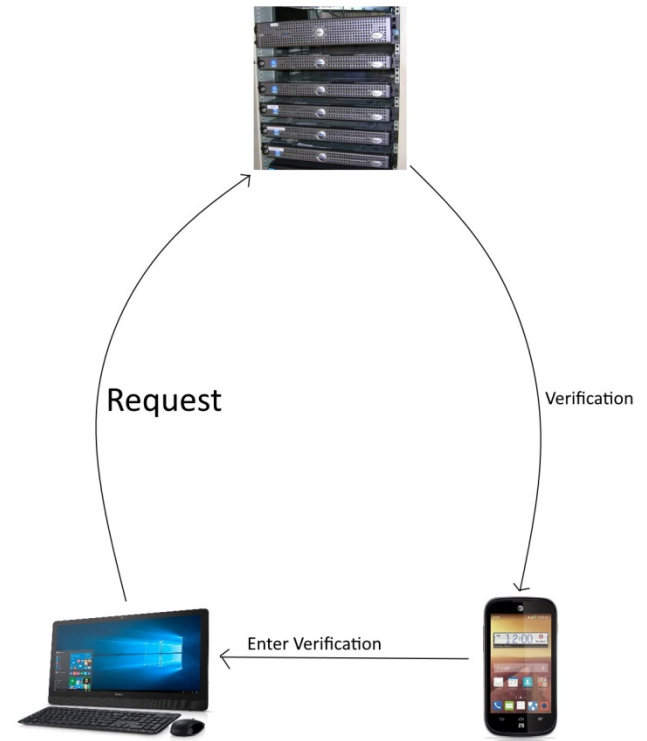
Wait... HUH?

How to and how not to do 2FA

Wrong!



Correct.



Fin