One does not simply add MFA

It’s not just a walk into Mordor, good MFA is a journey

@christine@ruby.social

Art by Maja Vonge Cornils

What you will learn

- ✓ What is MFA
- ✓ How to secure your accounts
- ✓ What are the MFA types
- ✓ How to protect users and secure an application
- ✓ Potential testing steps
- ✓ MFA implementation best practices

"Its black gates are guarded by more than just orcs."

Things you don't need to worry about

Taking notes or pictures 📝

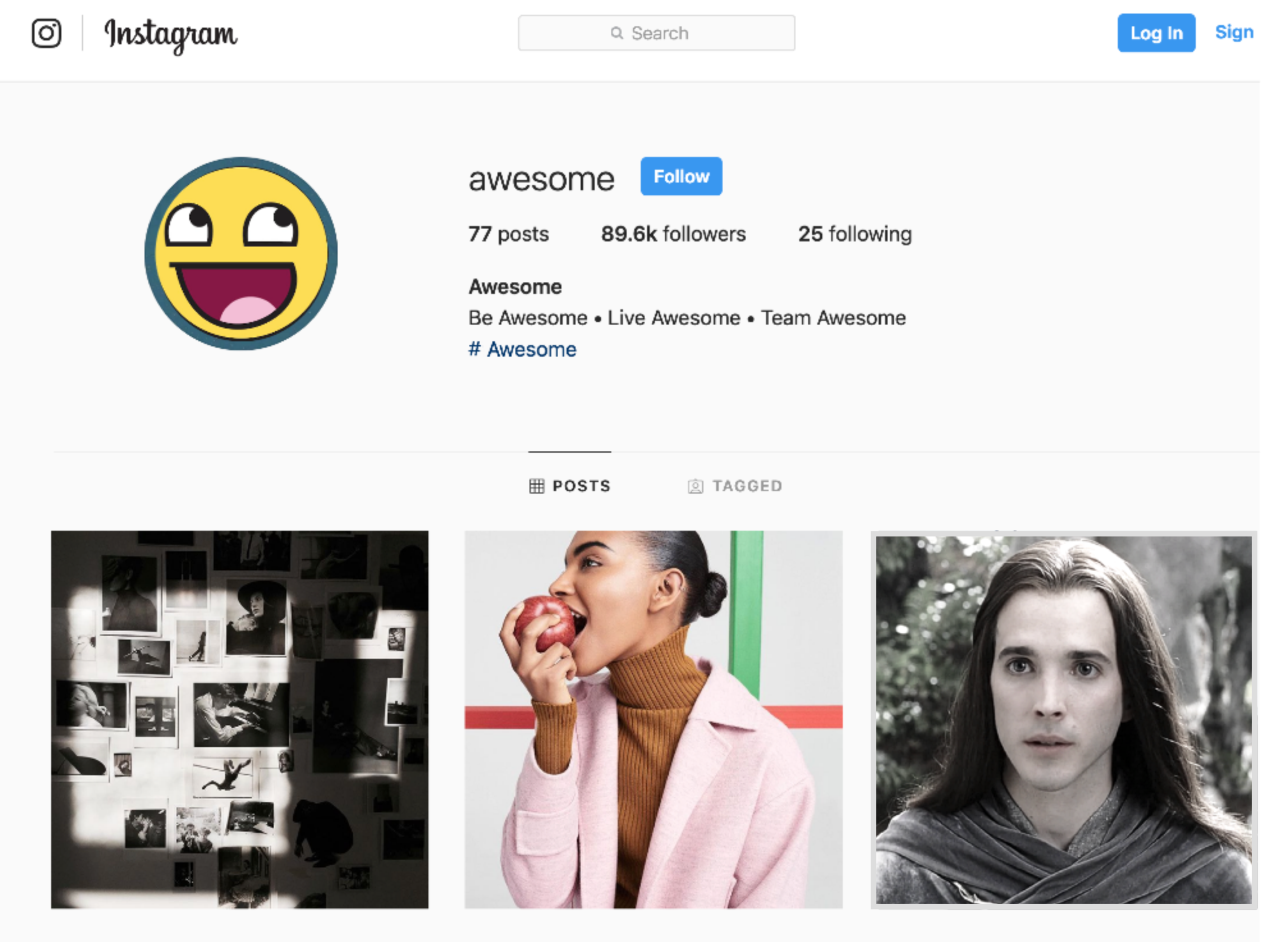
Asking foolish questions 🤔

Slides QR code

"There is evil there that does not sleep, and the Great Eye is ever watchful"

@christine@ruby.social

Let our journey begin…



awesome

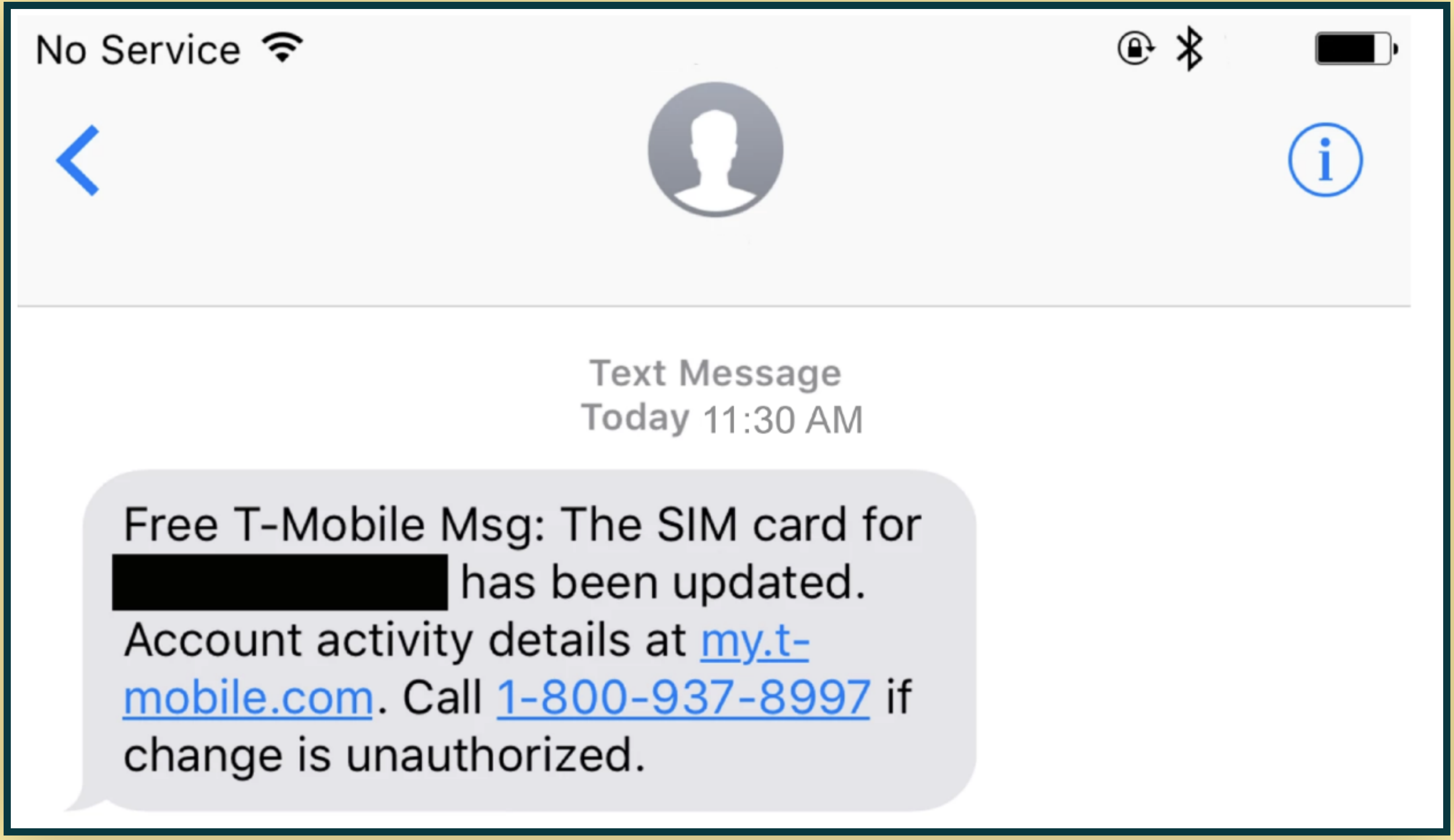
77 posts 89.6k followers 25 following

Awesome

Be Awesome • Live Awesome • Team Awesome

Awesome

@christine@ruby.social

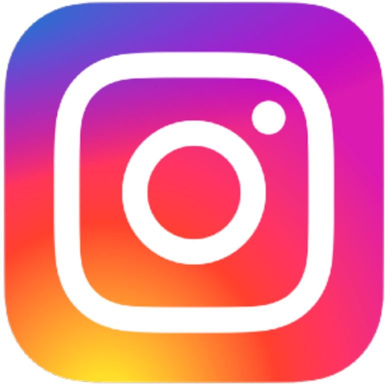


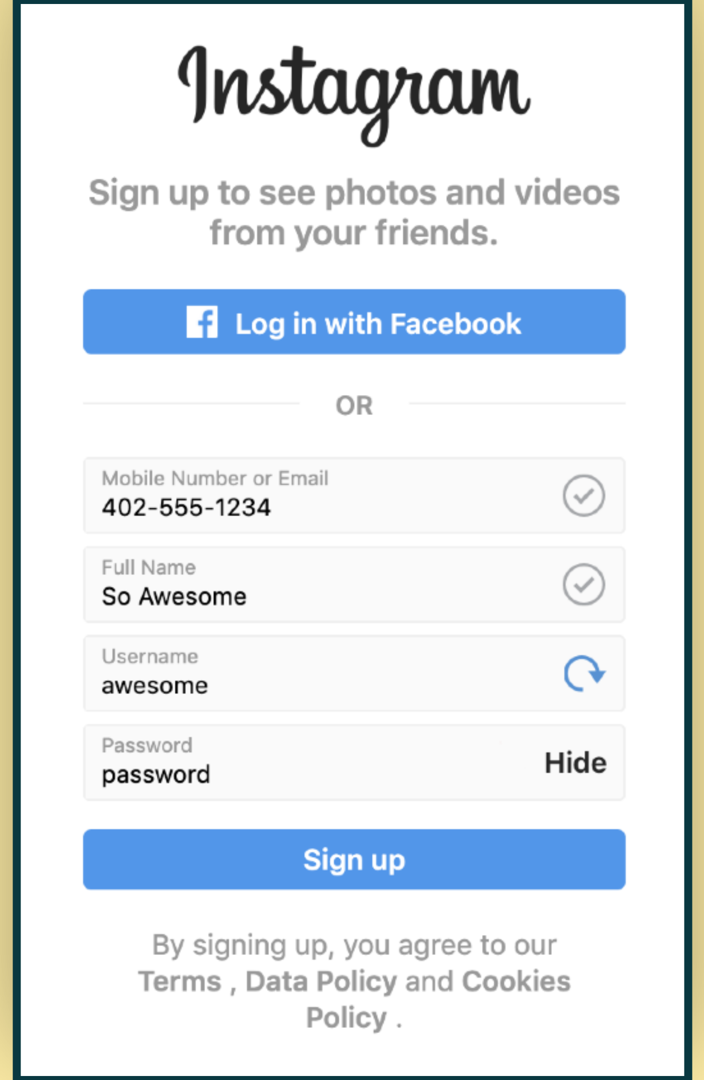
Text Message
Today 11:30 AM

Free T-Mobile Msg: The SIM card for [redacted] has been updated. Account activity details at my.t-mobile.com. Call 1-800-937-8997 if change is unauthorized.

Back to the beginning…

To when you signed up for





Sign up to see photos and videos from your friends.

Mobile Number or Email
402-555-1234 ✓

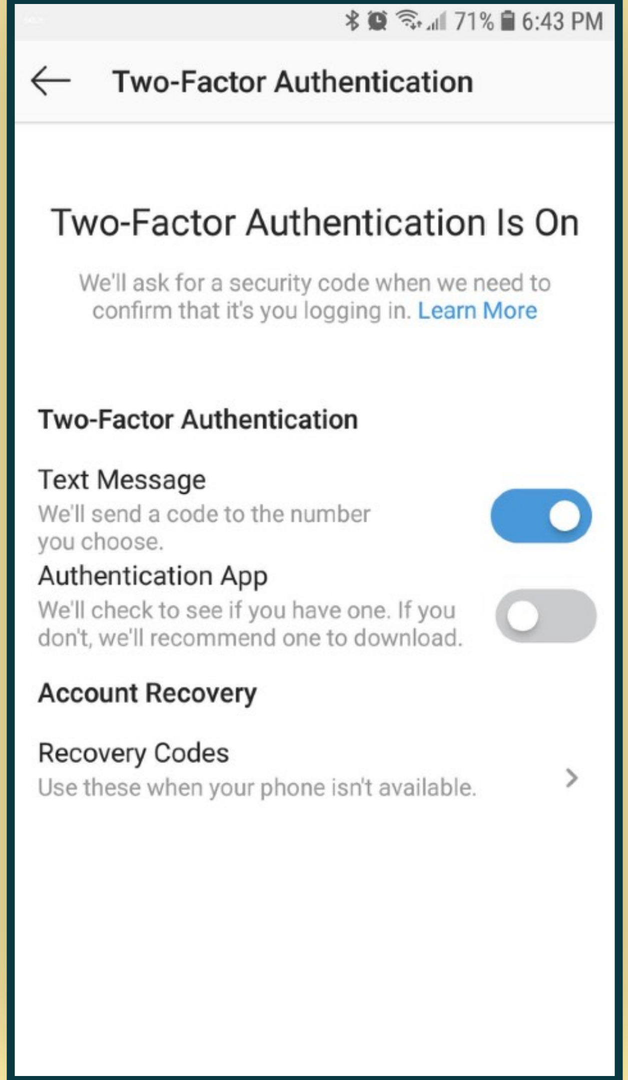
Full Name
So Awesome ✓

Username
awesome

Password
password

By signing up, you agree to our **Terms** , **Data Policy** and **Cookies Policy** .

@christine@ruby.social



71% 6:43 PM

Two-Factor Authentication

Two-Factor Authentication Is On

We'll ask for a security code when we need to confirm that it's you logging in. Learn More

Two-Factor Authentication

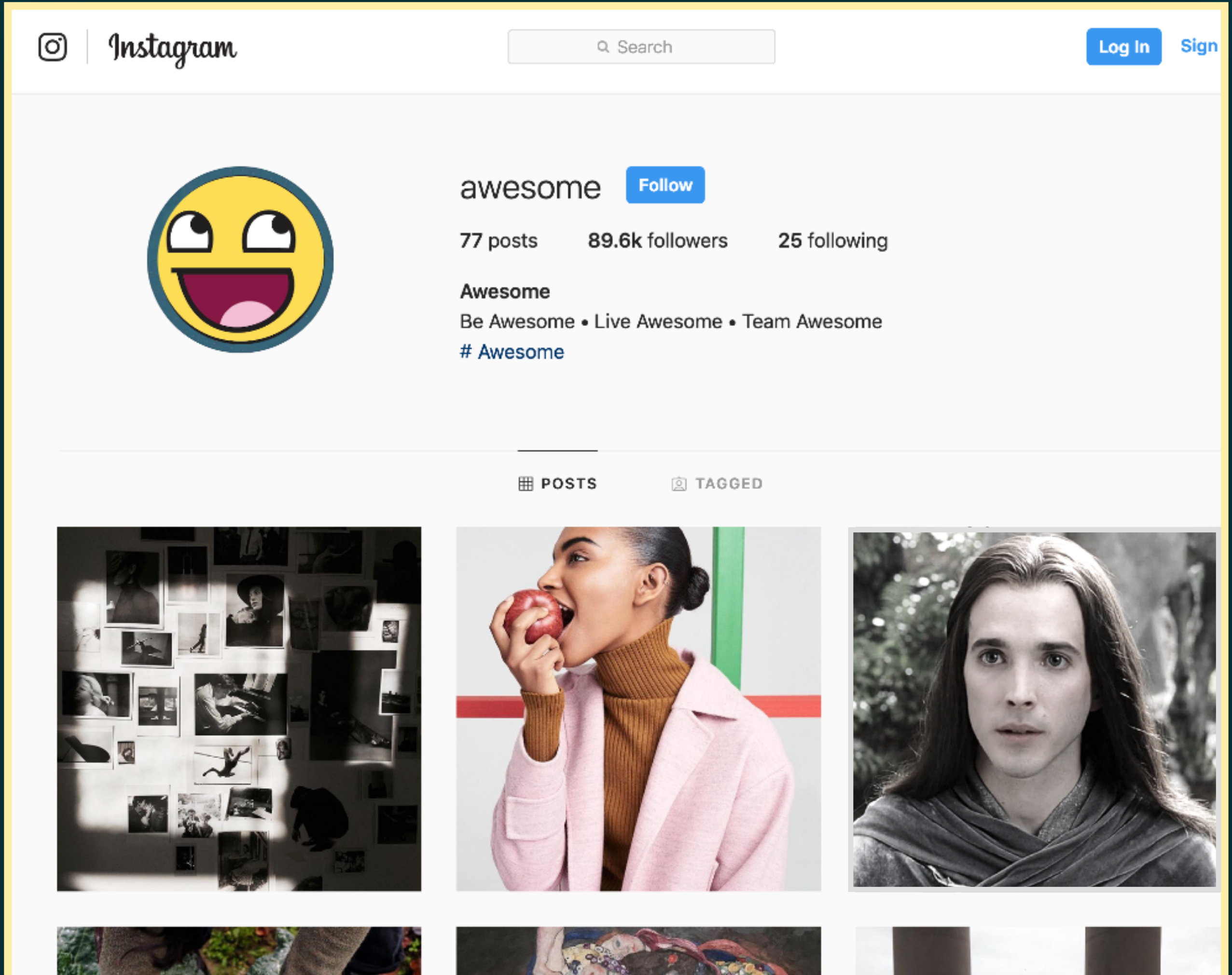
Text Message ●
We'll send a code to the number you choose.

Authentication App ○
We'll check to see if you have one. If you don't, we'll recommend one to download.

Account Recovery

Recovery Codes ›
Use these when your phone isn't available.

@christine@ruby.social



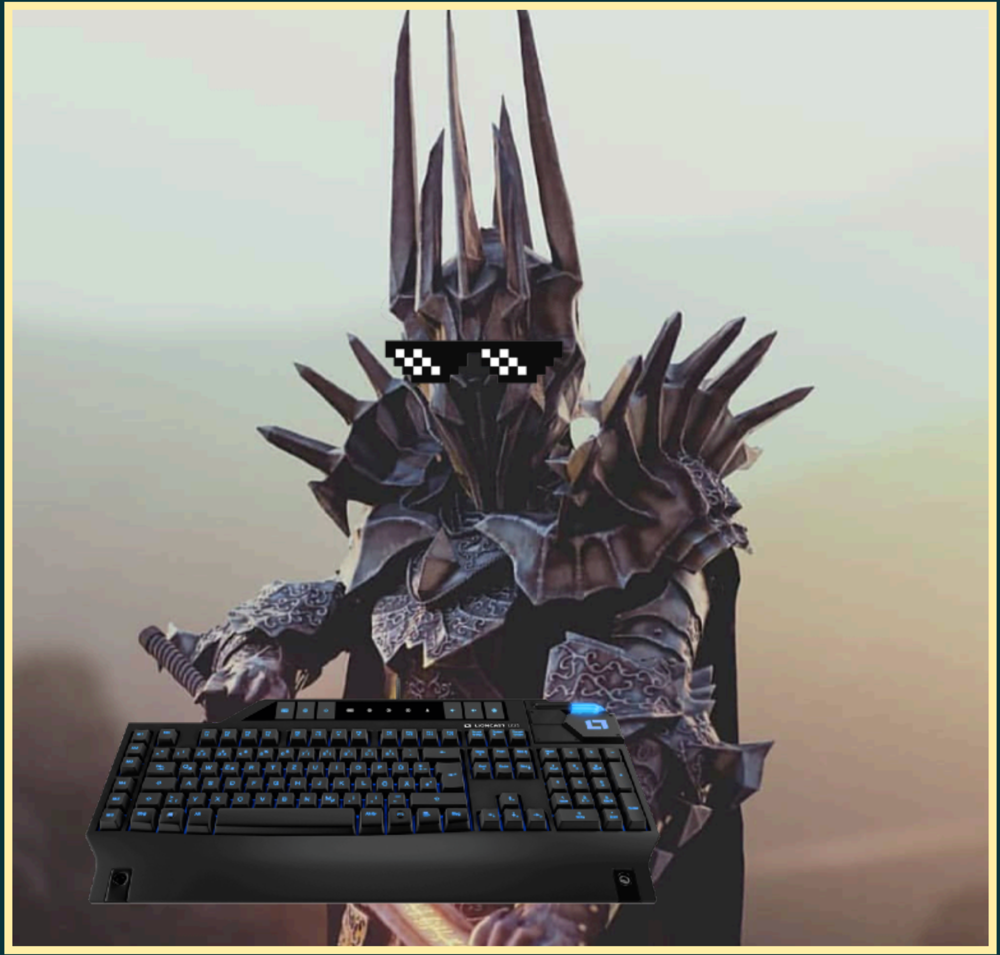
awesome

77 posts 89.6k followers 25 following

Awesome

Be Awesome • Live Awesome • Team Awesome

Awesome



What was the hacker up to?

🤔

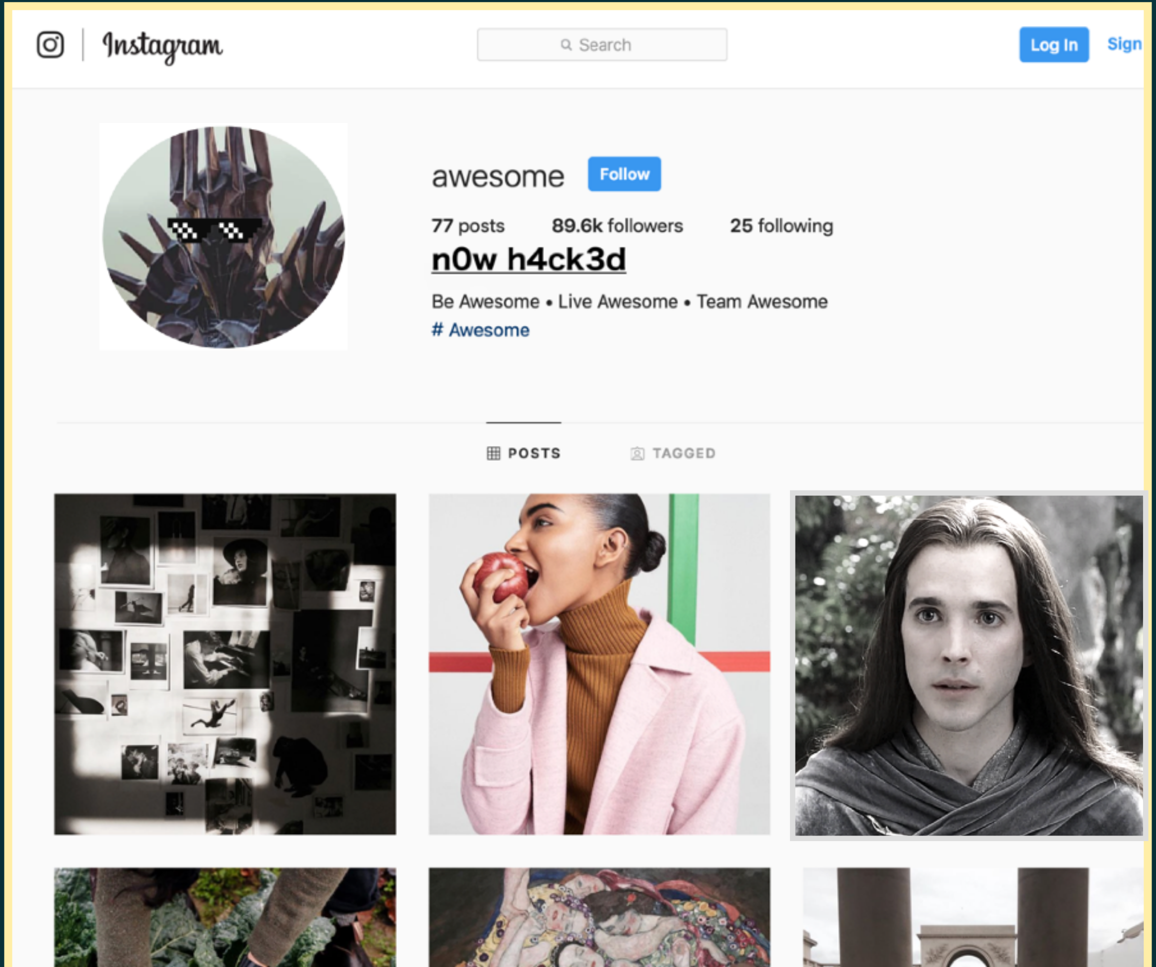
Calling your mobile provider

On the phone with your mobile provider…

Using social engineering

Now they have all the access…

Sim swap/sim hijacking



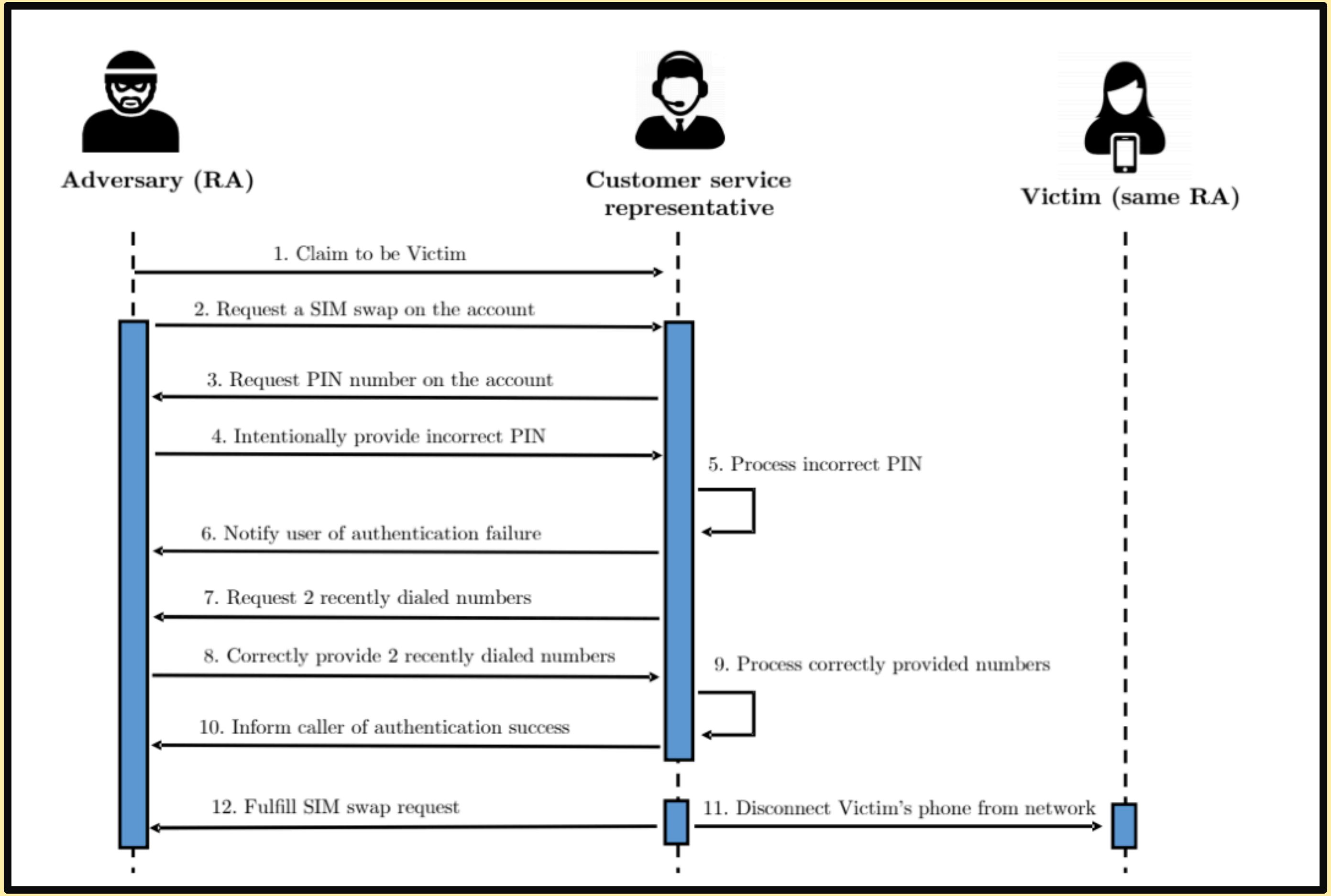
awesome

77 posts 89.6k followers 25 following

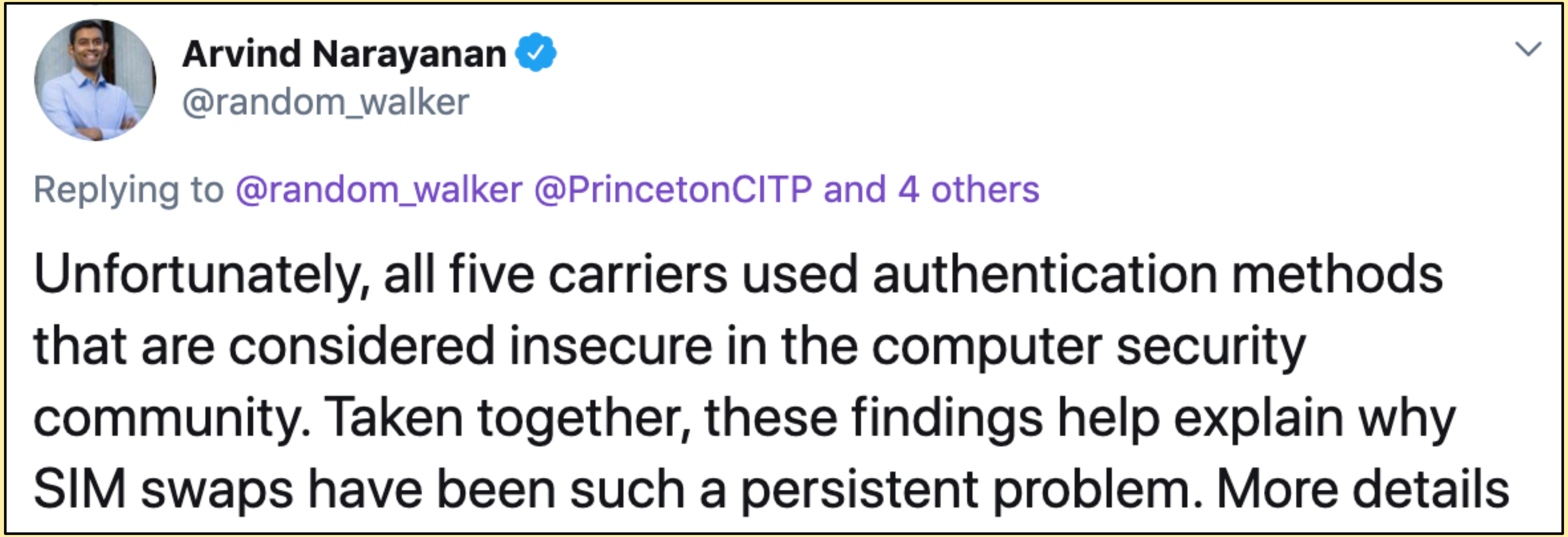
n0w h4ck3d

Be Awesome • Live Awesome • Team Awesome

Awesome


Adversary (RA)
Customer service representative
Victim (same RA)
1. Claim to be Victim
2. Request a SIM swap on the account
3. Request PIN number on the account
4. Intentionally provide incorrect PIN
5. Process incorrect PIN
6. Notify user of authentication failure
7. Request 2 recently dialed numbers
8. Correctly provide 2 recently dialed numbers
9. Process correctly provided numbers
10. Inform caller of authentication success
11. Disconnect Victim's phone from network
12. Fulfill SIM swap request

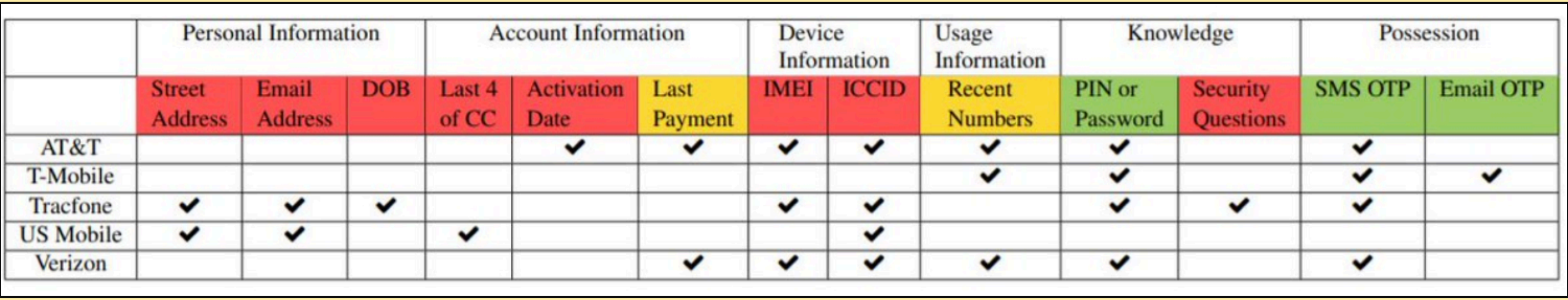
issms2fasecure.com/assets/sim_swaps-01-10-2020.pdf



Arvind Narayanan
@random_walker

Replying to @random_walker @PrincetonCITP and 4 others

Unfortunately, all five carriers used authentication methods that are considered insecure in the computer security community. Taken together, these findings help explain why SIM swaps have been such a persistent problem. More details



	Personal Information			Account Information			Device Information		Usage Information	Knowledge		Possession	
	Street Address	Email Address	DOB	Last 4 of CC	Activation Date	Last Payment	IMEI	ICCID	Recent Numbers	PIN or Password	Security Questions	SMS OTP	Email OTP
AT&T					✓	✓	✓	✓	✓	✓		✓	
T-Mobile									✓	✓		✓	✓
Tracfone	✓	✓	✓				✓	✓		✓	✓	✓	
US Mobile	✓	✓		✓				✓					
Verizon						✓	✓	✓	✓	✓		✓	

@christine@ruby.social

Let’s check on some Aussie Telcos

Telstra

vodafone

OPTUS

22 September 2022

optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack

@christine@ruby.social

> We learned that SMS-based authentication is not nearly as secure as we would hope, and the main attack was via SMS intercept

Christopher Slowe
Reddit chief technology officer and founding engineer
August 2018

What is authentication?

The process of verifying that someone or something is the actual entity that they claim to be.

- OWASP.org

(these people know what they are talking about when it comes to security)

… but what are the different factors of auth?

- Factor is knowledge (i.e. your password)
- Is the other method choice
  - Possession (token/soft token)
  - Identity (biometrics)

What about all those other acronyms…

2FA = 2SV = MFA = 2F

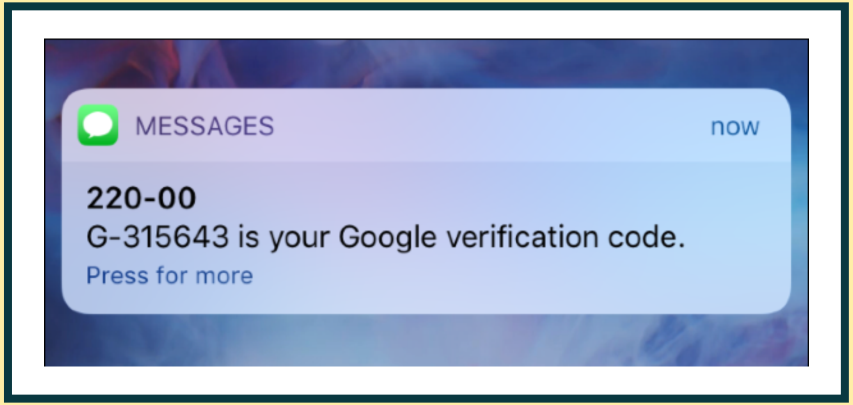
Why didn't MFA help?

- SMS was used
- For most users MFA won’t even be enabled

Let's travel deeper to discover all of our factor choices

SMS

- Most common
- Most compromised
- Not recommended by NIST since 2016



220-00
G-315643 is your Google verification code.

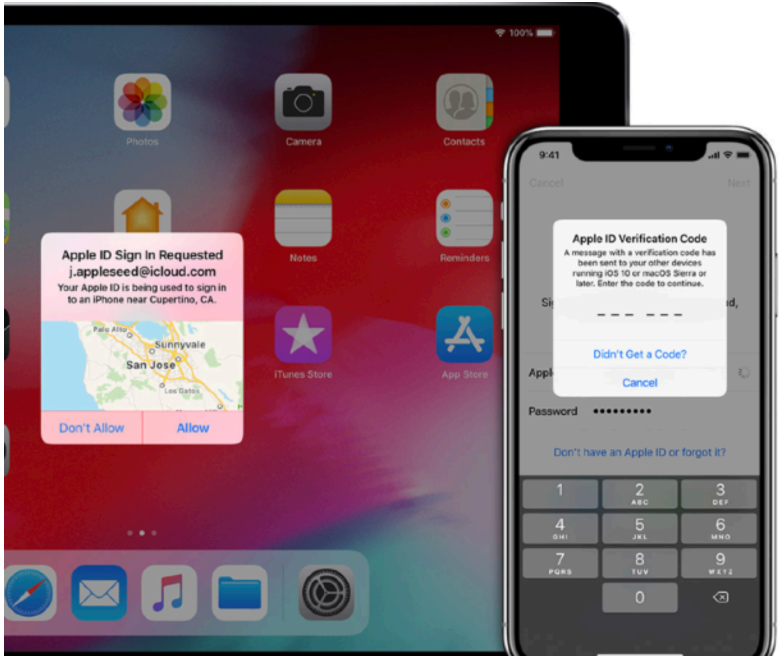
If SMS wasn't bad enough

- SS7 (network shared by every telecom) has it's own vulnerabilities
- Text messages that are sent can be intercepted

Let's figure out all the ways to hack it...

1. Sim-swap (aka what just happened to us)
2. Port-out scam
3. Brute force on the application itself
4. Exploit SS7 weakness

Push Based



Apple ID Sign In Requested
j.appleseed@icloud.com
Your Apple ID is being used to sign in to an iPhone near Cupertino, CA.

Apple ID Verification Code
A message with a verification code has been sent to your other devices running iOS 10 or macOS Sierra or later. Enter the code to continue.

Password ••••••••••

Push Based

- Associated with certain authorized devices

- Not visible on a locked phone screen

Push Based Has Drawbacks

September 15th, 2022

Security Questions

Security Questions

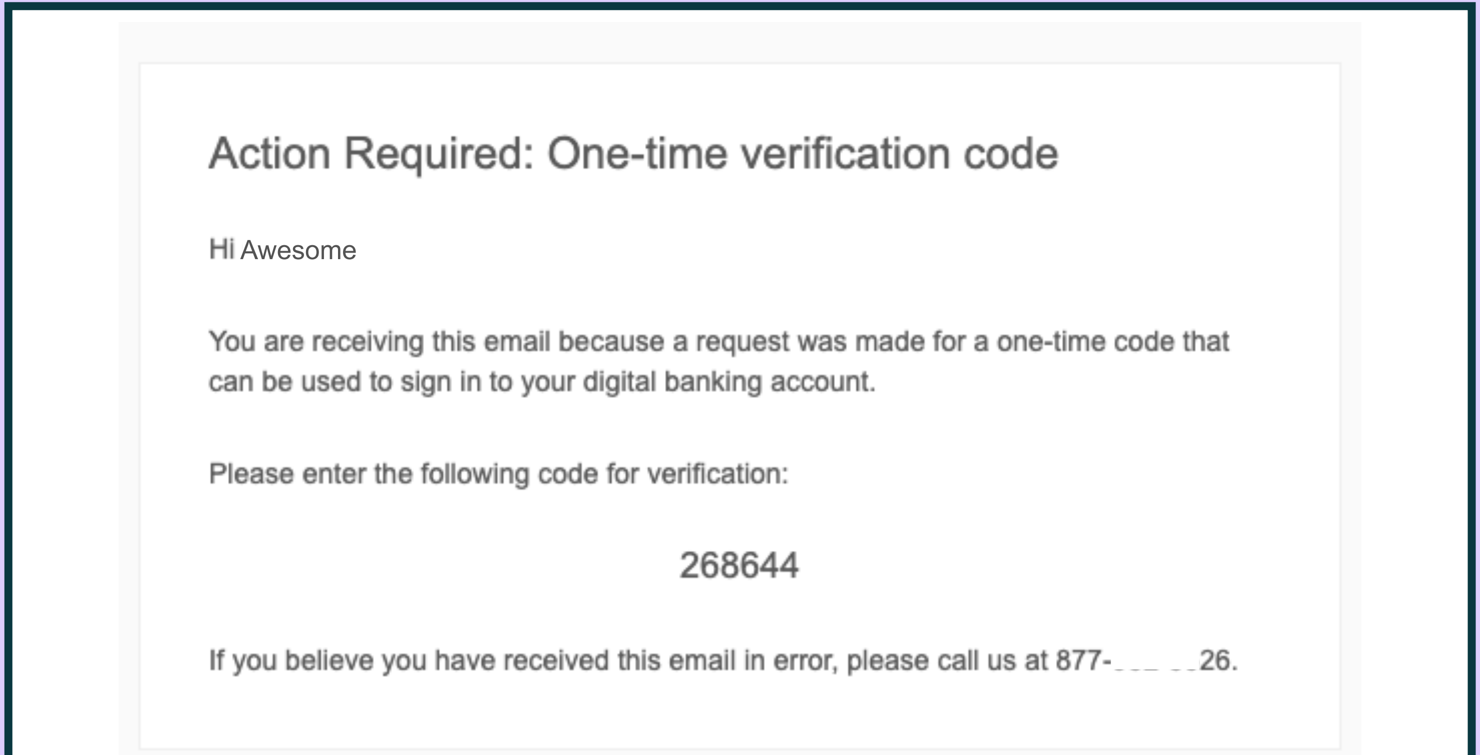
- User answers a set of questions during sign-up
- For example
  - Merry’s mother’s maiden name?
  - What is the shire’s address?

Email

Email

- At login time, an email with verification code is sent to user
- Convient
- Should only be used with verified emails

Example email verification step



Action Required: One-time verification code

Hi Awesome

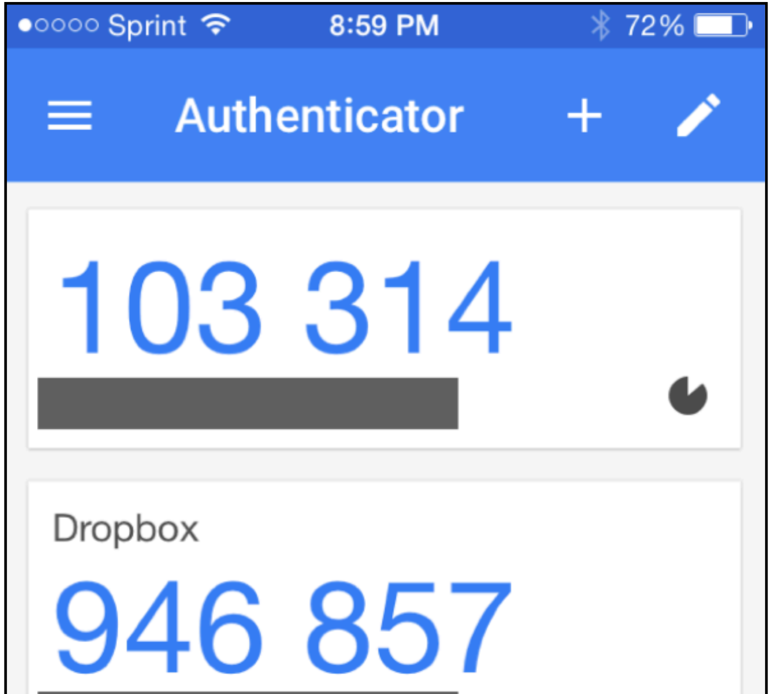
You are receiving this email because a request was made for a one-time code that can be used to sign in to your digital banking account.

Please enter the following code for verification:

268644

If you believe you have received this email in error, please call us at 877-[redacted]26.

TOTP



103 314

Dropbox

946 857

TOTP

Time-based One Time Password

aka app based

aka soft token

- Authy
- Google Authenticator
- 1Password

Token Based

Token Based

Physical keys that can authenticate

- FIDO2/WebAuthn
- USB drive
- Near-field communication
- Many use U2F (Universal 2nd Factor)

OTP vs U2F

OTP

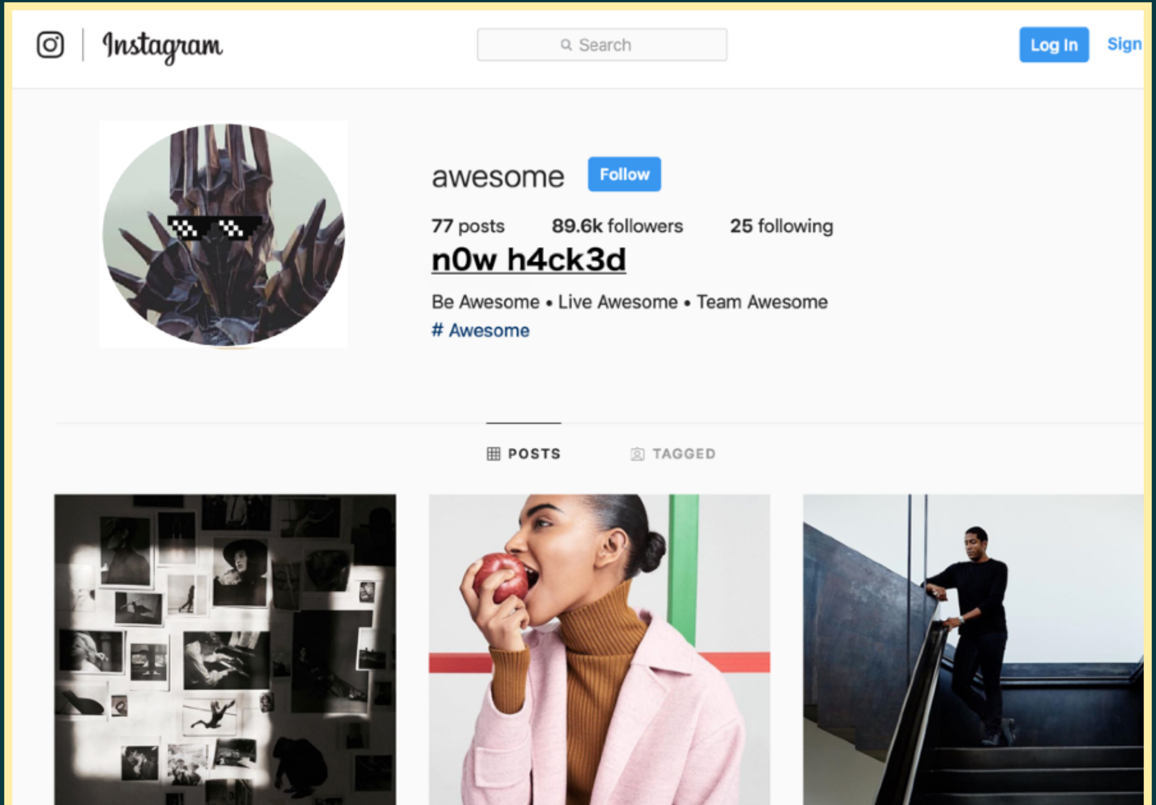
- Users type in codes
- Set up and provision required
- Secrets stored, providing a single point of attack

U2F

- User has physical device
- Strong security from public key cryptography
- No personal information associated with a key

@christine@ruby.social

What would you change now?



awesome

77 posts 89.6k followers 25 following

n0w h4ck3d

Be Awesome • Live Awesome • Team Awesome

Awesome

Secure Your Account

1. Use long password/ passphrase
2. Secure with alternate authentication method
3. Use a VOIP number
4. Don't reuse passwords
5. Pin/password protect phone provider

Keep on being **@awesome**

… now let’s put a twist on our story

@bestlotrmemes
CAST IT INTO THE FIRE! DESTROY IT! ISILDUR!
OH DUDE GOOD IDEA, THAT'S ACTUALLY WAY BETTER THAN WHAT I WAS THINKING
DIRECTED BY
PETER JACKSON

@christine@ruby.social

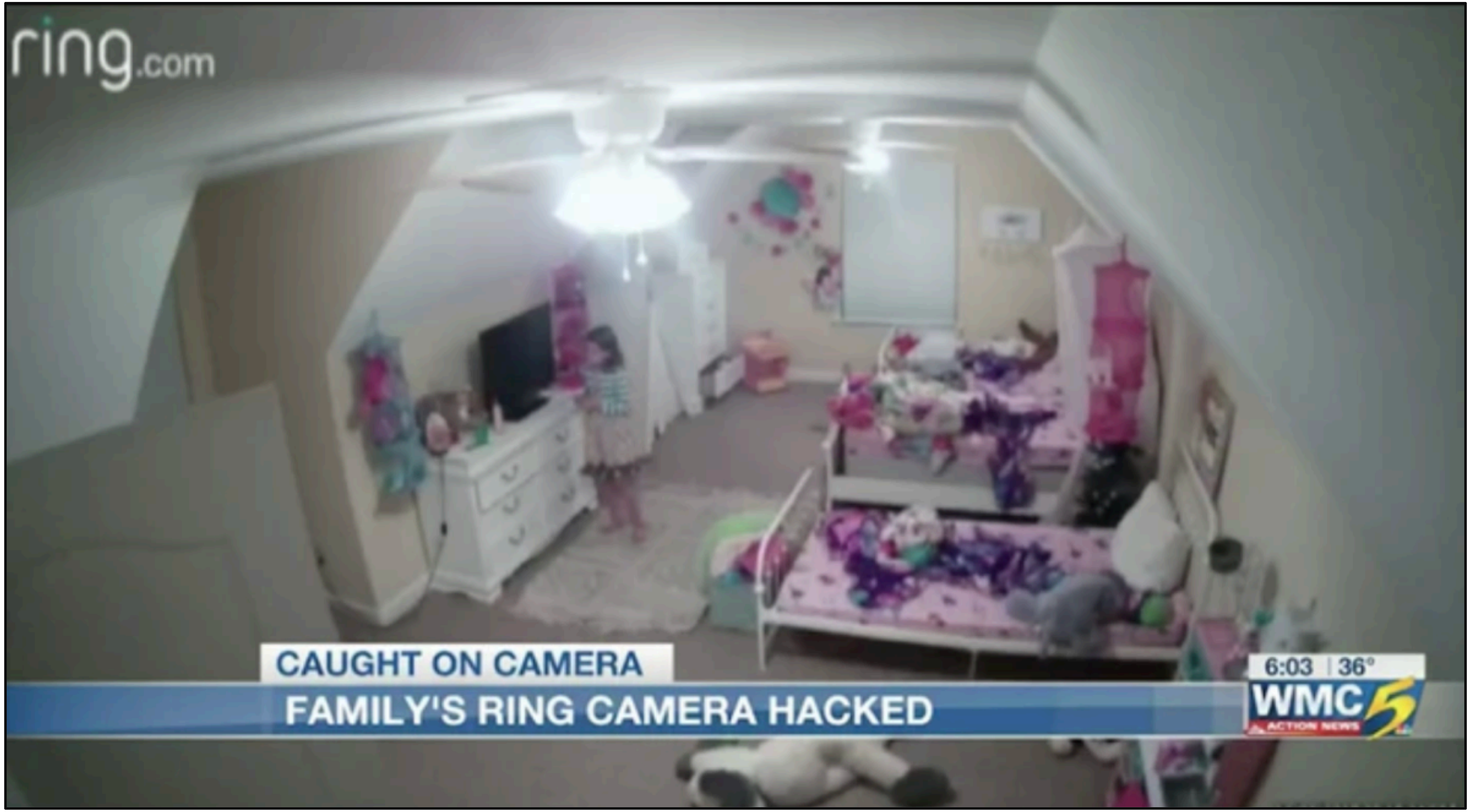
Not that twist...

- Now you are the engineer at **shiregram** (an insta rival)
- How do you secure your users from all the bad stuff out there?

Security is everyone's job

Security is everyone's job

- Engineers
- Designers
- Infrastructure
- Managers
- Not just info sec!



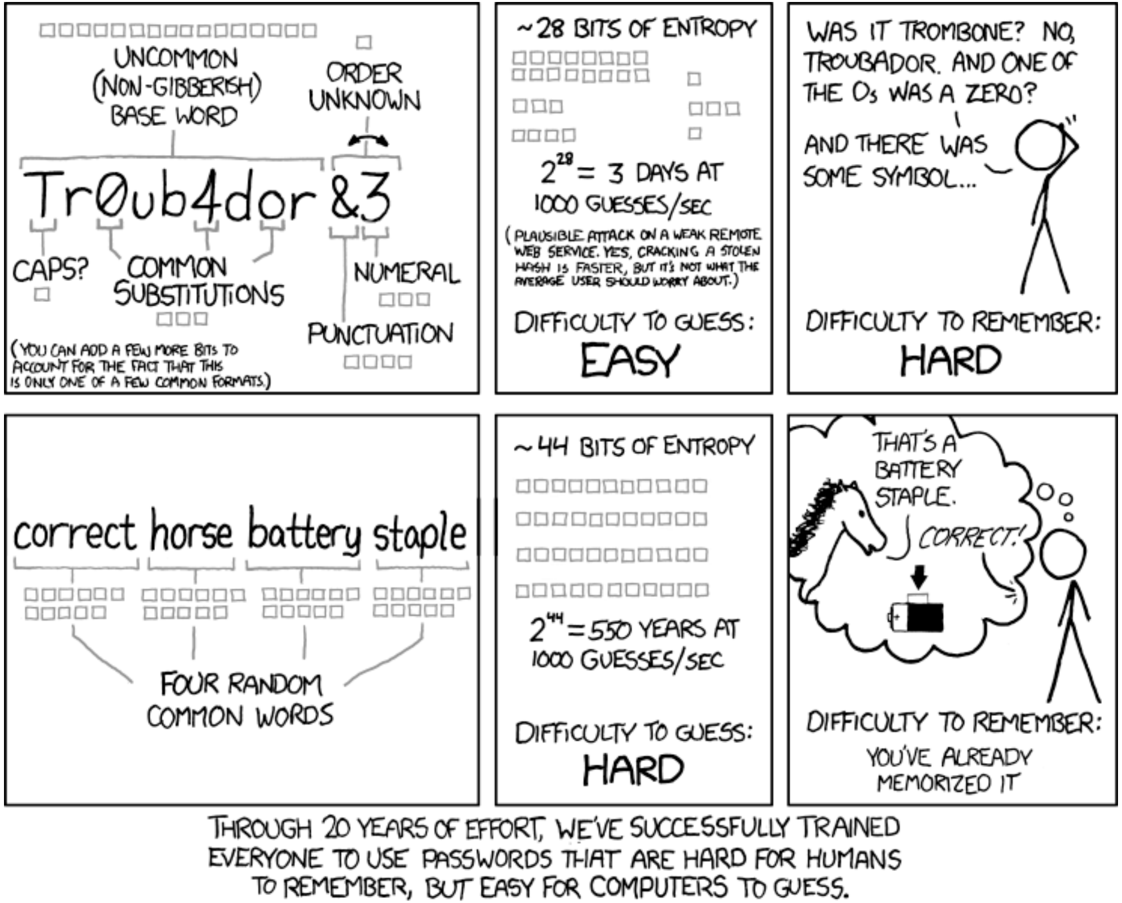
wmcactionnews5.com/2019/12/11/family-says-hackers-accessed-ring-camera-their-year-old-daughters-room

nbc-2.com/story/41428183/stranger-spews-racial-slurs-over-familys-hacked-ring-camera

Back to your security basics

- Strong passwords/passphrase 💪🏾
- Don't make them be rotated 🔁
- Store the hash securely 🔒
- Only store sensitive data that you need ⛔

Strong passwords/passphrase 💪🏽


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

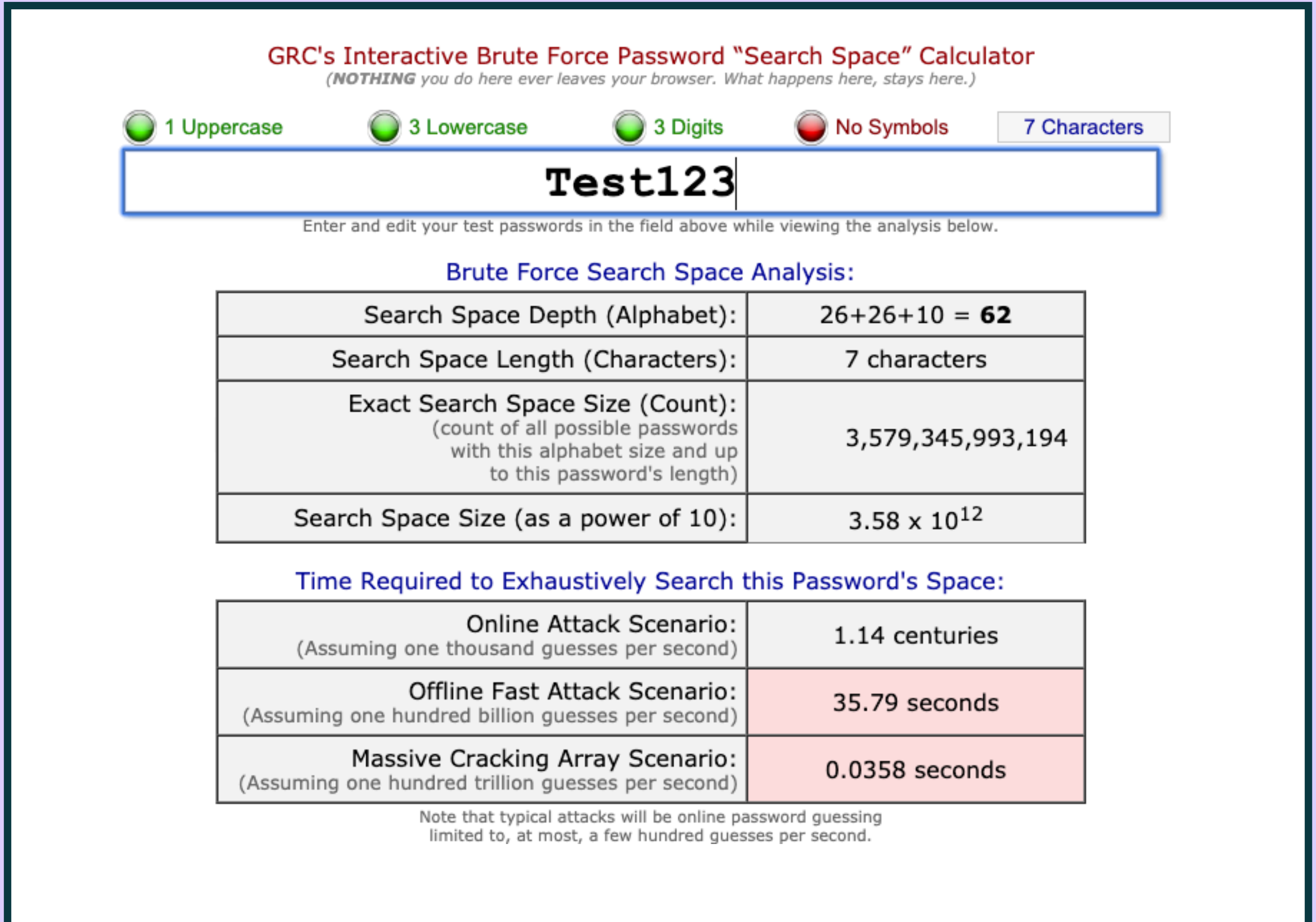
https://xkcd.com/936/

Strong passwords/passphrase 💪🏿

Why this helps

- Greater entropy = harder to brute force the password
- Passwords should be hard to guess, but easy to remember
- Extra length + randomness allows for more entropy

Strong passwords/passphrase 💪



GRC's Interactive Brute Force Password “Search Space” Calculator

(*NOTHING* you do here ever leaves your browser. What happens here, stays here.)

🟢 1 Uppercase 🟢 3 Lowercase 🟢 3 Digits 🔴 No Symbols 7 Characters

Test123

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

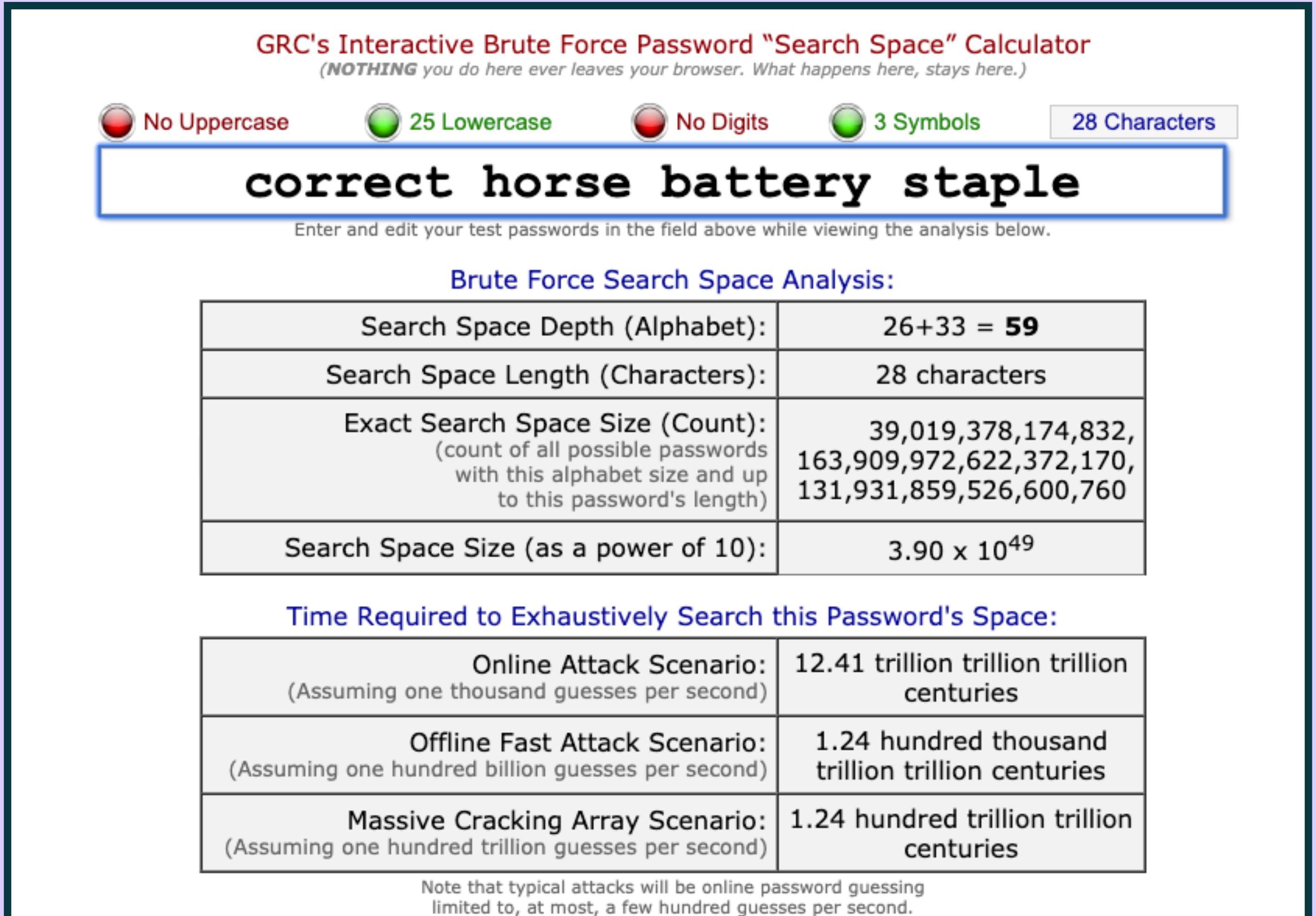
Search Space Depth (Alphabet):	26+26+10 = **62**
Search Space Length (Characters):	7 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	3,579,345,993,194
Search Space Size (as a power of 10):	3.58×10^{12}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	1.14 centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	35.79 seconds
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	0.0358 seconds

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Strong passwords/passphrase 💪



GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

🔴 No Uppercase 🟢 25 Lowercase 🔴 No Digits 🟢 3 Symbols | 28 Characters

```
correct horse battery staple
```

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+33 = **59**
Search Space Length (Characters):	28 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	39,019,378,174,832, 163,909,972,622,372,170, 131,931,859,526,600,760
Search Space Size (as a power of 10):	3.90 x 10^{49}

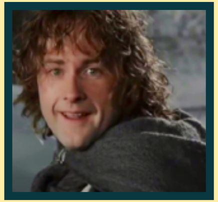
Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	12.41 trillion trillion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	1.24 hundred thousand trillion trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.24 hundred trillion trillion centuries

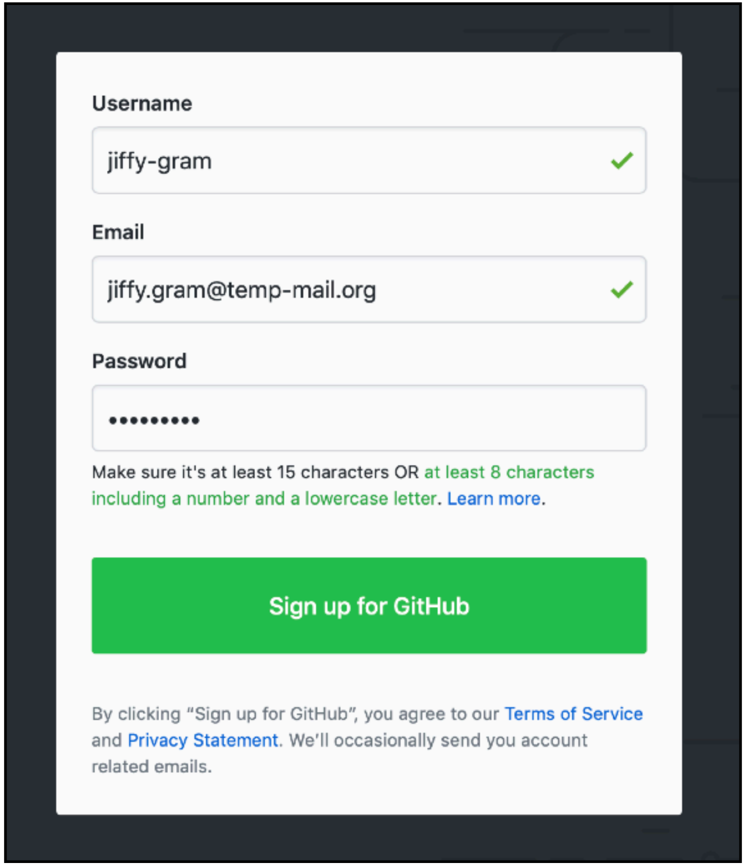
Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Strong passwords/passphrase 💪

Do this



Strong passwords/passphrase 💪



Username

jiffy-gram ✓

Email

jiffy.gram@temp-mail.org ✓

Password

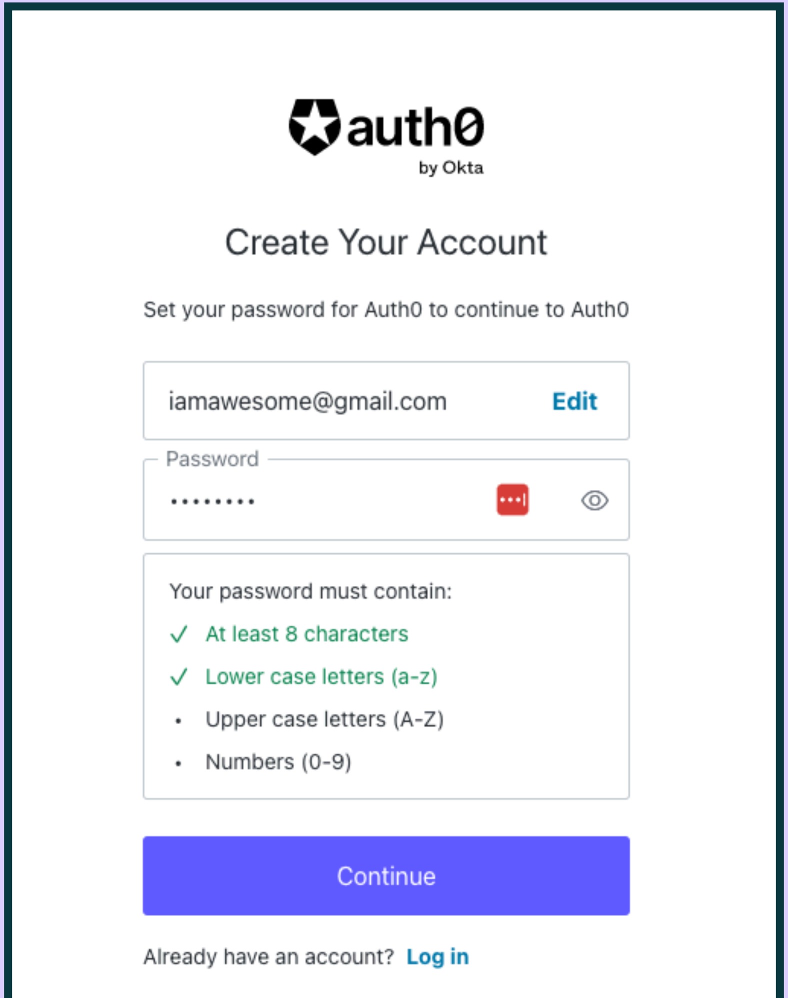
••••••••••

Make sure it's at least 15 characters OR at least 8 characters including a number and a lowercase letter. Learn more.

By clicking "Sign up for GitHub", you agree to our Terms of Service and Privacy Statement. We'll occasionally send you account related emails.

@christine@ruby.social

Strong passwords/passphrase 💪



Create Your Account

Set your password for Auth0 to continue to Auth0

iamawesome@gmail.com Edit

Password

•••••••••

Your password must contain:

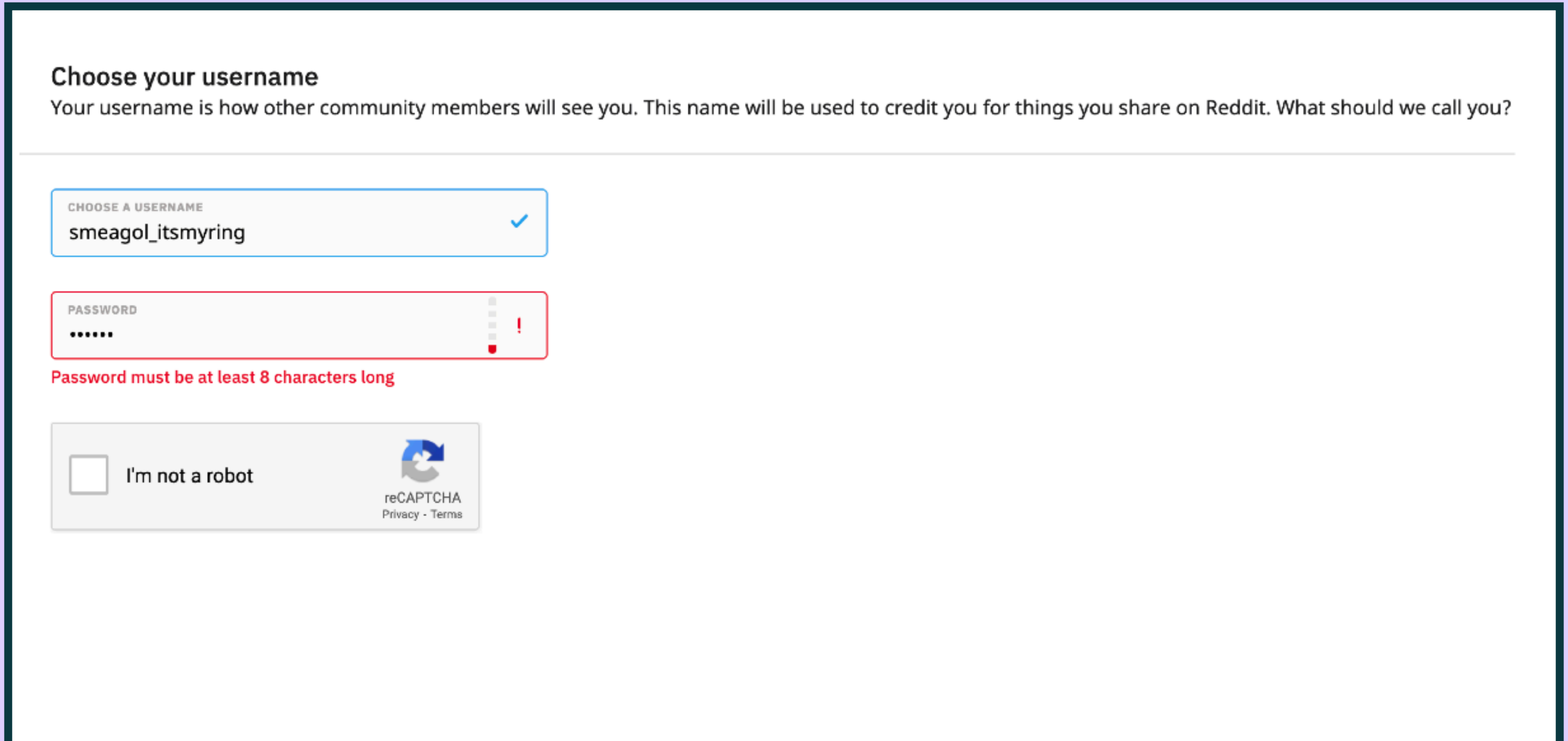
- ✓ At least 8 characters
- ✓ Lower case letters (a-z)
- Upper case letters (A-Z)
- Numbers (0-9)

Already have an account? Log in

@christine@ruby.social

Strong passwords/passphrase 💪

Reddit



Choose your username

Your username is how other community members will see you. This name will be used to credit you for things you share on Reddit. What should we call you?

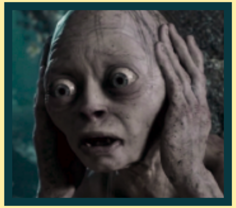
CHOOSE A USERNAME
smeagol_itsmyring ✓

PASSWORD
•••••• !

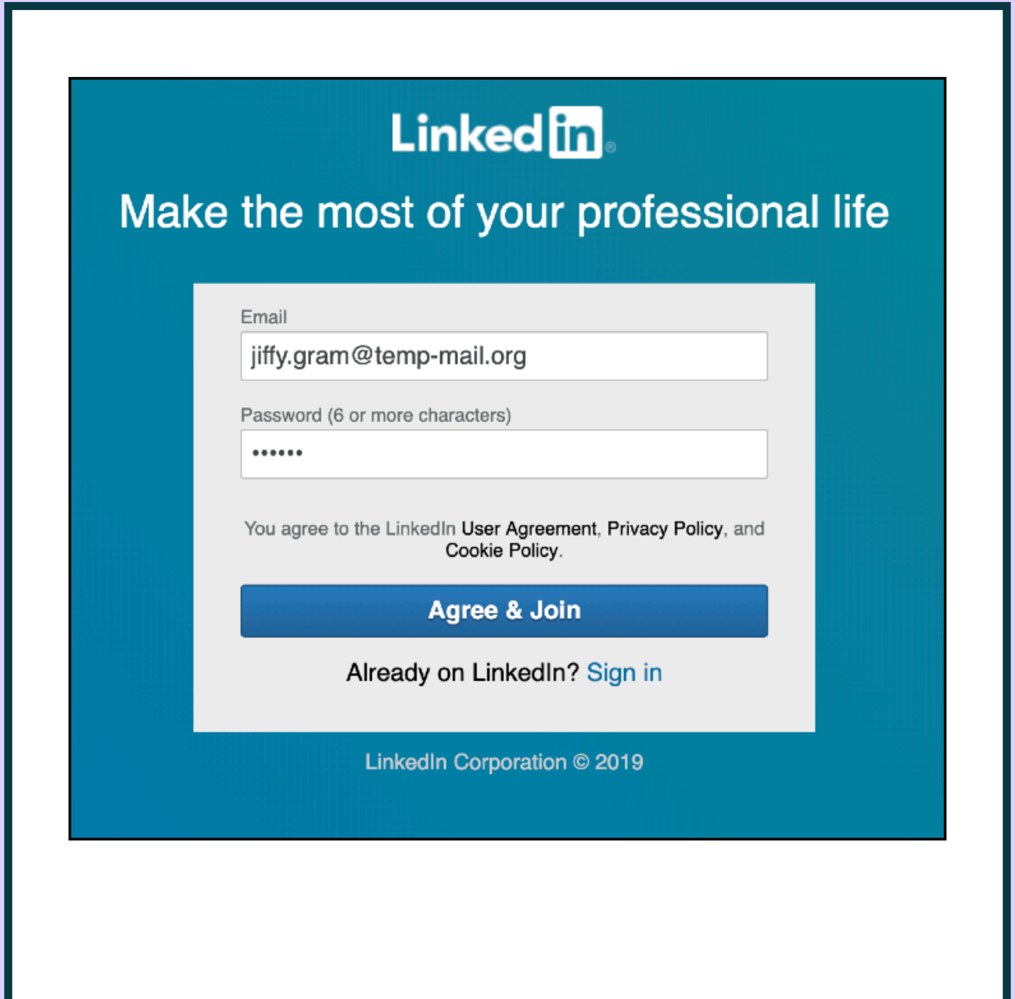
Password must be at least 8 characters long

□ I'm not a robot

Strong passwords/passphrase 💪

Not this 

Strong passwords/passphrase 💪



Make the most of your professional life

Email

jiffy.gram@temp-mail.org

Password (6 or more characters)

••••••

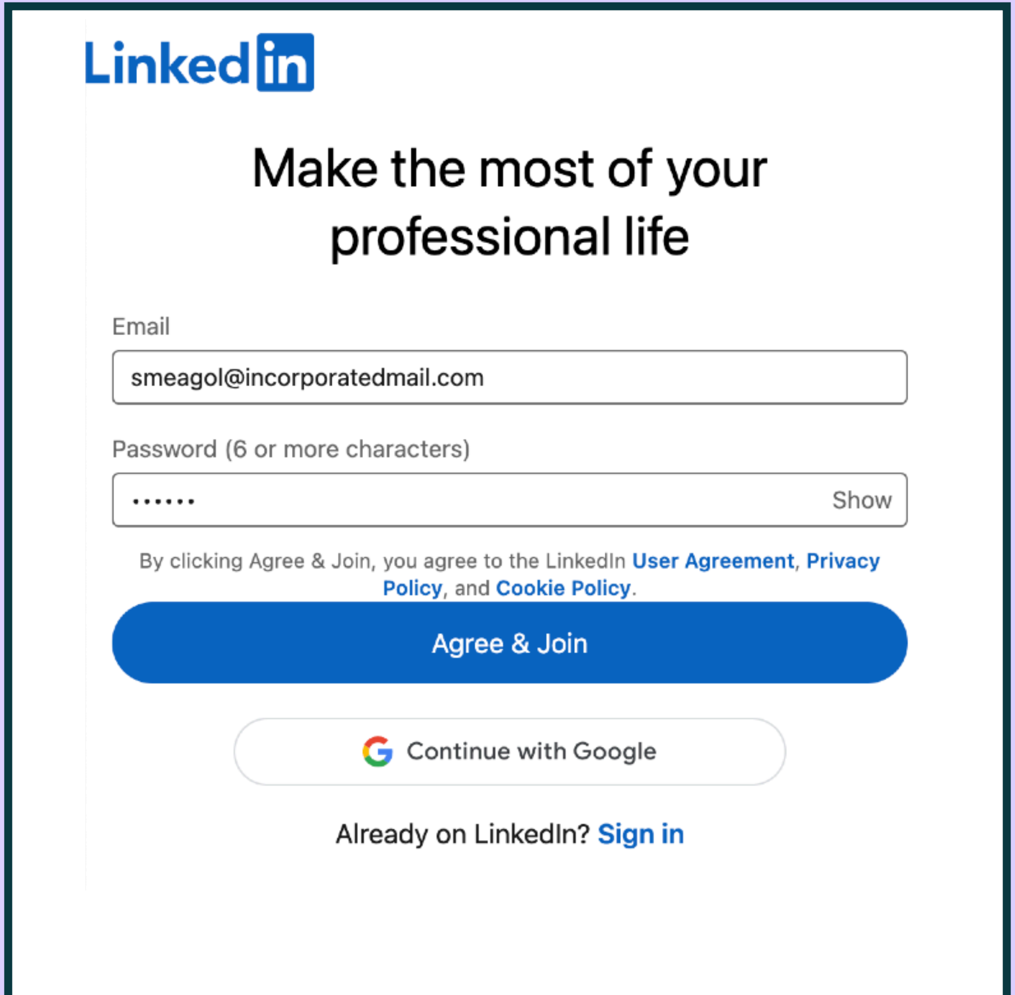
You agree to the LinkedIn User Agreement, Privacy Policy, and Cookie Policy.

Already on LinkedIn? Sign in

LinkedIn Corporation © 2019

@christine@ruby.social

Strong passwords/passphrase 💪



Make the most of your professional life

Email

smeagol@incorporatedmail.com

Password (6 or more characters)

•••••• Show

By clicking Agree & Join, you agree to the LinkedIn User Agreement, Privacy Policy, and Cookie Policy.

Already on LinkedIn? Sign in

@christine@ruby.social

Let's talk about password hash encryption

- Just an algorithm that takes data and produces fixed-size output
- Some hashes are stronger then others
- MD5/SHA-1 = 👎
- SHA-256/512-bit SHA-2= 👍

Adaptive one-way functions, hashes with more spice

- Compute a one-way (irreversible) transform
- Allows configuration of ‘work factor’
  - Ex. Argon2, PBKDF2, Scrypta, Bcrypt

Head on over to OWASP.org for more details

> …we made the decision to rotate customer accounts on May 5, 2022, out of an abundance of caution due to not all of the customers having multi-factor authentication (MFA) enabled at the time and potential for password reuse.

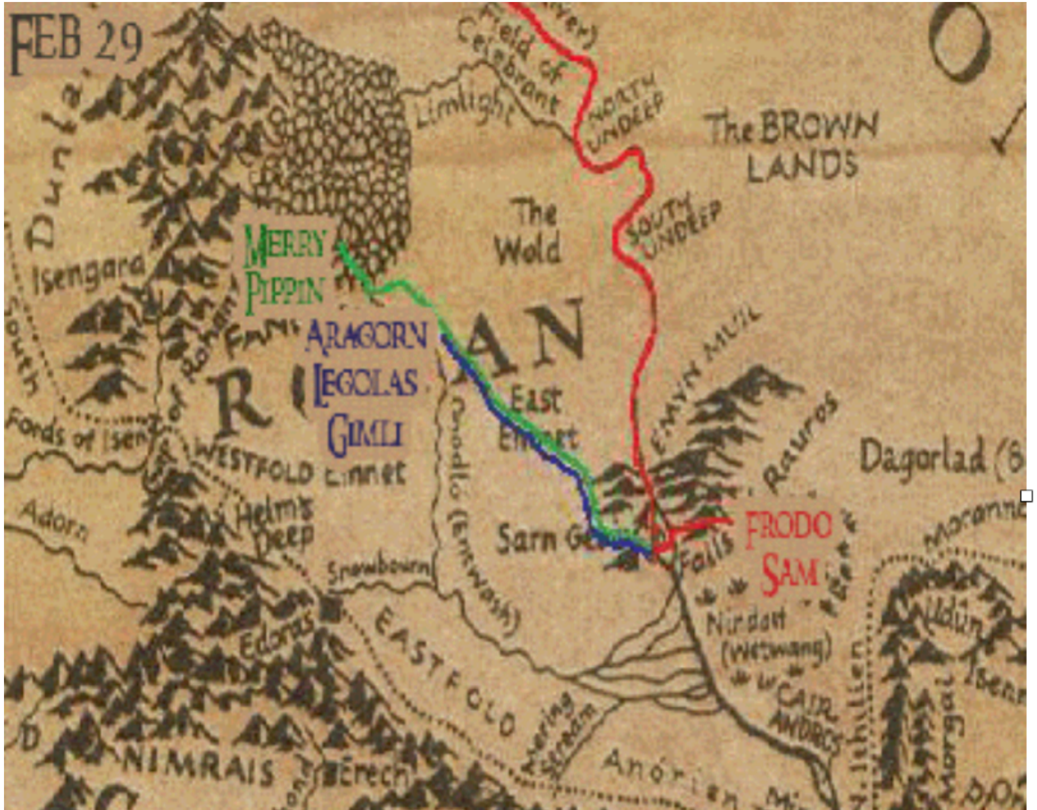
Bob Wise
Heroku General Manager and Salesforce

DIY or BUY

Choose your User Authentication Journey

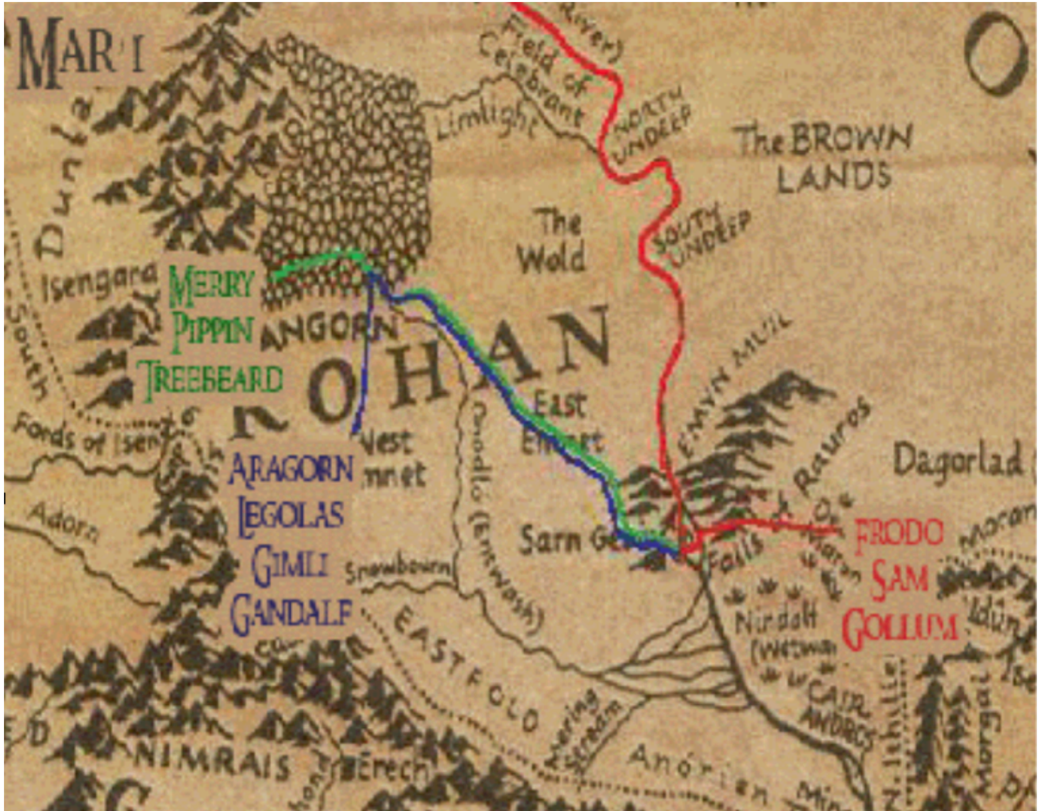
DIY or BUY

Choose your User Authentication Journey

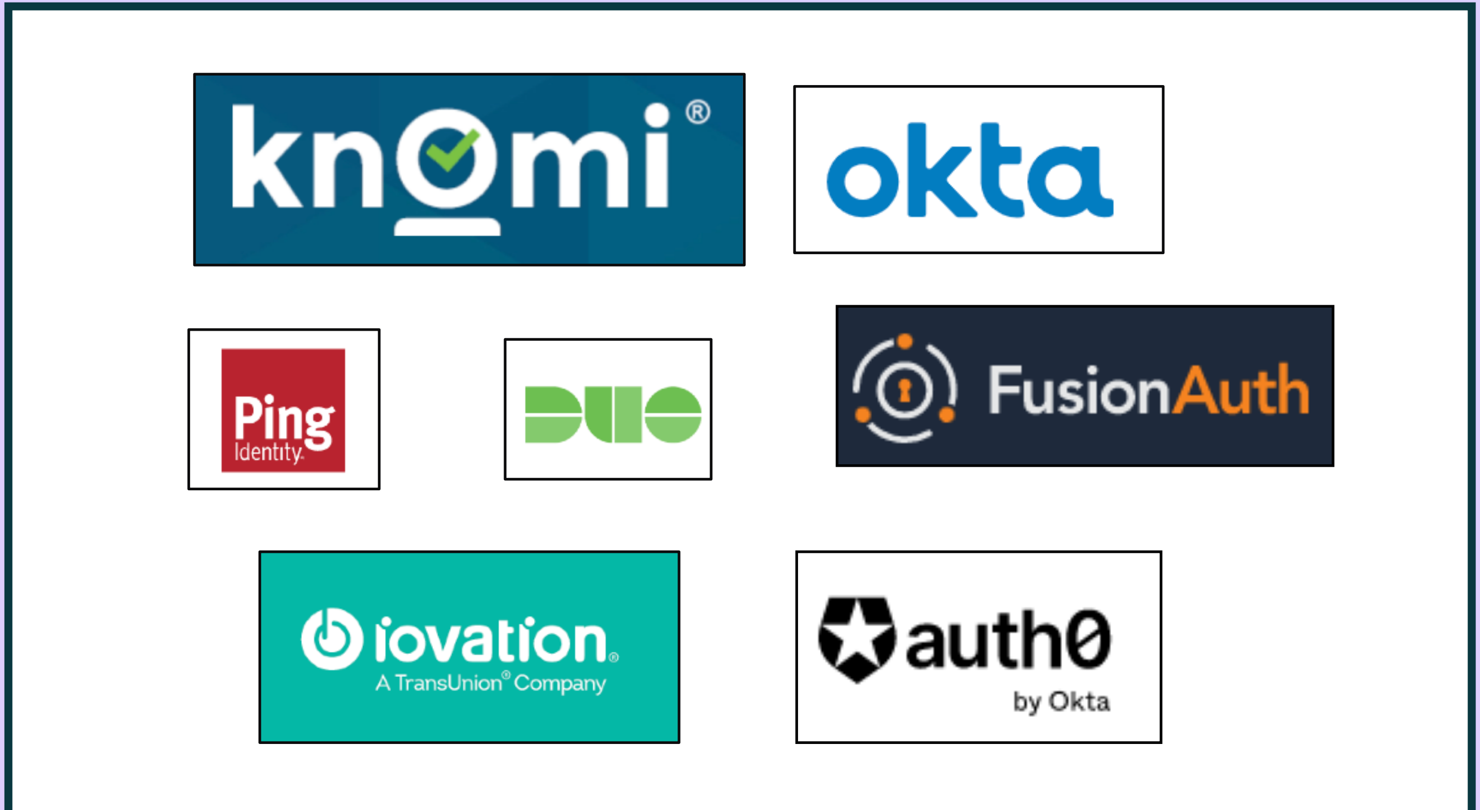


DIY or BUY

Choose your User Authentication Journey



If you choose to BUY



If you choose to BUY

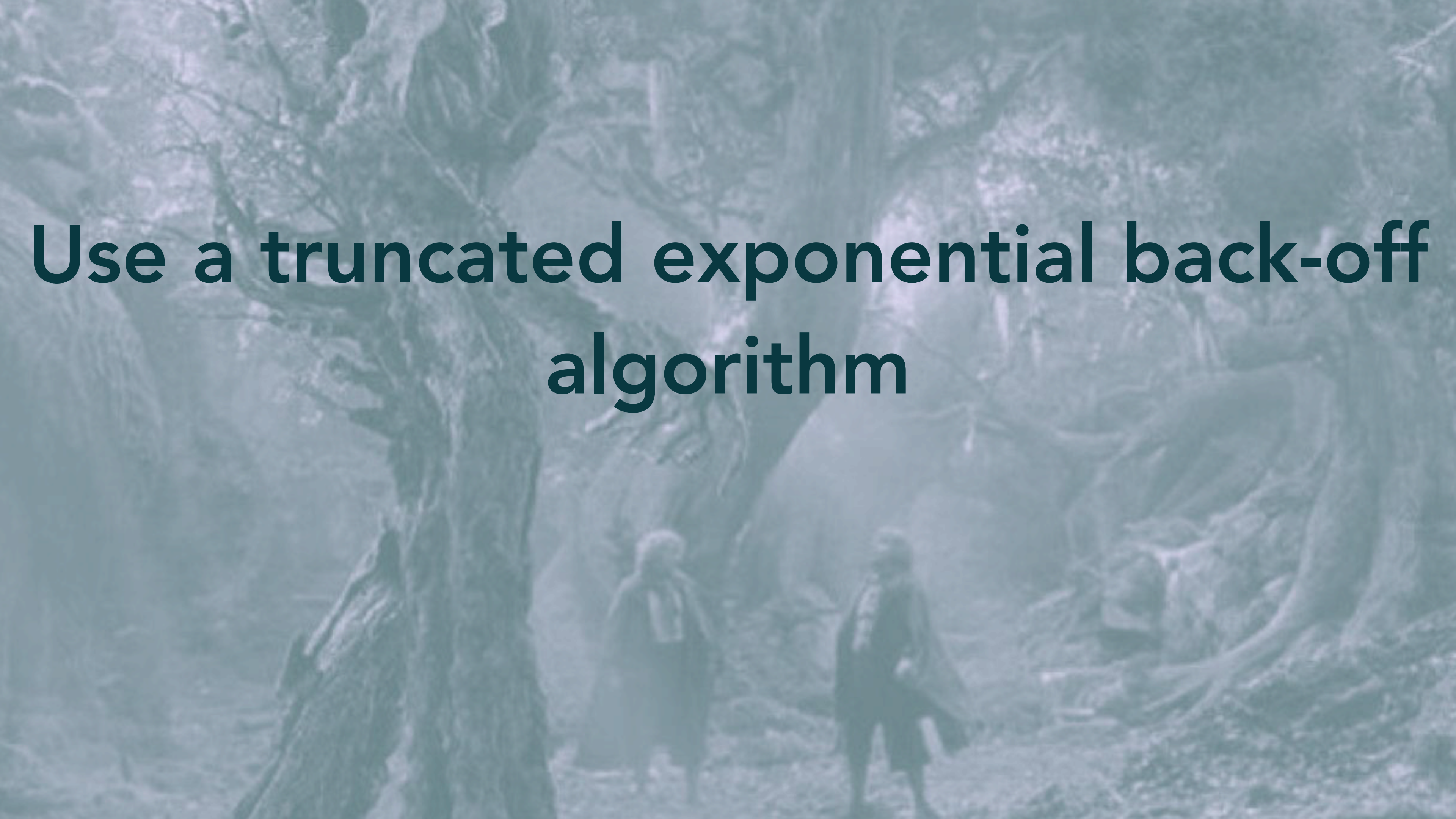
- Choose your vendor wisely
- What factor choices are available?
- What are your authorization and authentication needs?

If you choose DIY

- More flexibility
- More security surface area to cover
- More control over the user experience
- More choices…
  - When to require re-authentication of MFA
  - Should re-auth occur on new ip/browser/period of time

Some things to keep in mind no matter your path…

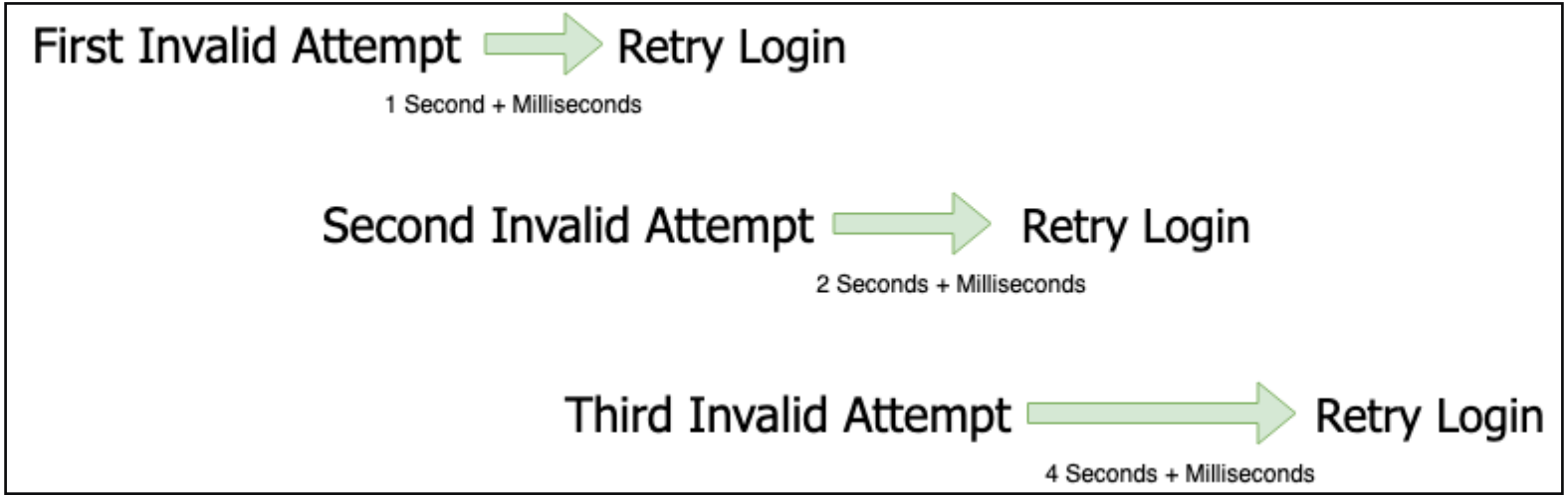
Rate limiting prevents brute force attacks



Use a truncated exponential back-off algorithm

Uh wut now?

What is an exponential back-off algorithm?



First Invalid Attempt → Retry Login

1 Second + Milliseconds

Second Invalid Attempt → Retry Login

2 Seconds + Milliseconds

Third Invalid Attempt → Retry Login

4 Seconds + Milliseconds

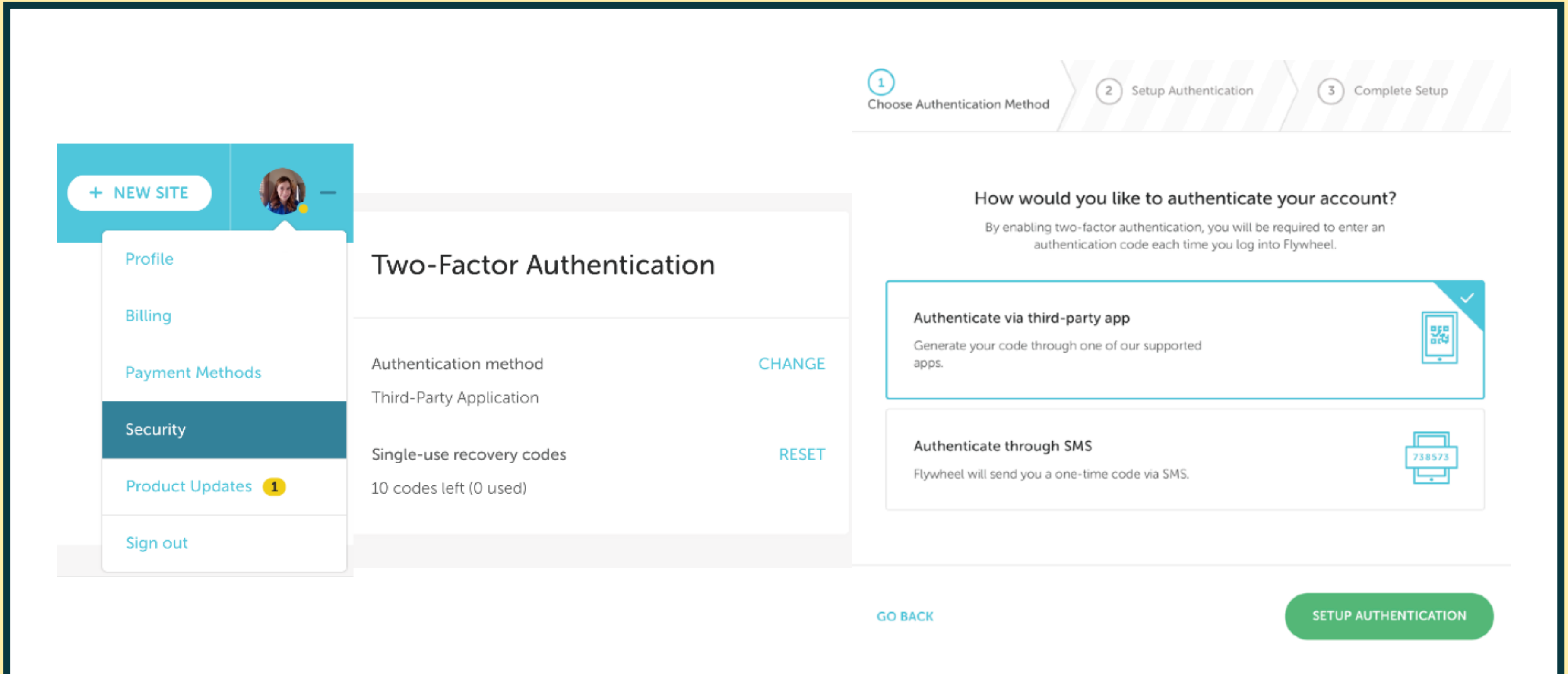
Get user buy-in

Make it easy on your users

Make it easy on your users

- Make it easy opt in
- Make it easy to add
- Make it visible
- Make it flexible

Do this



Two-Factor Authentication

Authentication method

Third-Party Application

Single-use recovery codes

10 codes left (0 used)

How would you like to authenticate your account?

By enabling two-factor authentication, you will be required to enter an authentication code each time you log into Flywheel.

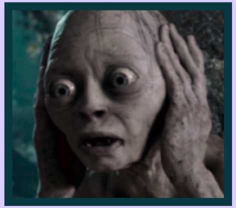
☑ Authenticate via third-party app

Generate your code through one of our supported apps.

Authenticate through SMS

Flywheel will send you a one-time code via SMS.

Not this



intuit
mint
Linkedin
DISCOVER
Spotify
airbnb
AMERICAN EXPRESS
citibank
CHASE

If you choose DIY...

Require more authentication

If you choose DIY…

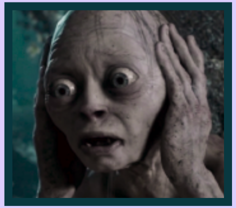
Require more authentication

- For editing/removing of MFA require credentials
- If authentication does fail, be generic in error response

Do this

"Login failed - invalid user ID or password”

Not this



"Login for User awesome: invalid password"

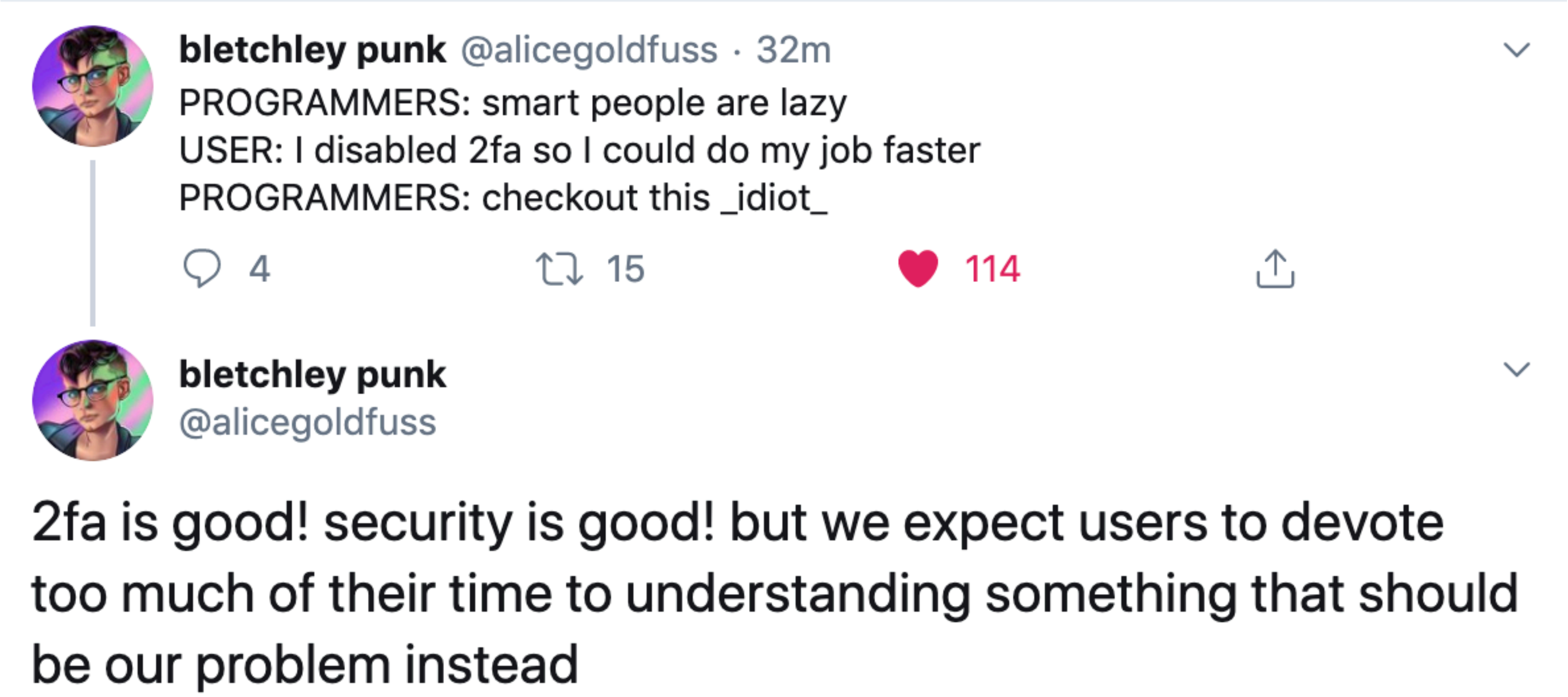
"Login failed, invalid user ID"

"Login failed; account disabled"

"Login failed; this user is not active"

Are we doing all we can to protect our users?

@christine@ruby.social



bletchley punk @alicegoldfuss · 32m

PROGRAMMERS: smart people are lazy
USER: I disabled 2fa so I could do my job faster
PROGRAMMERS: checkout this _idiot_

bletchley punk
@alicegoldfuss

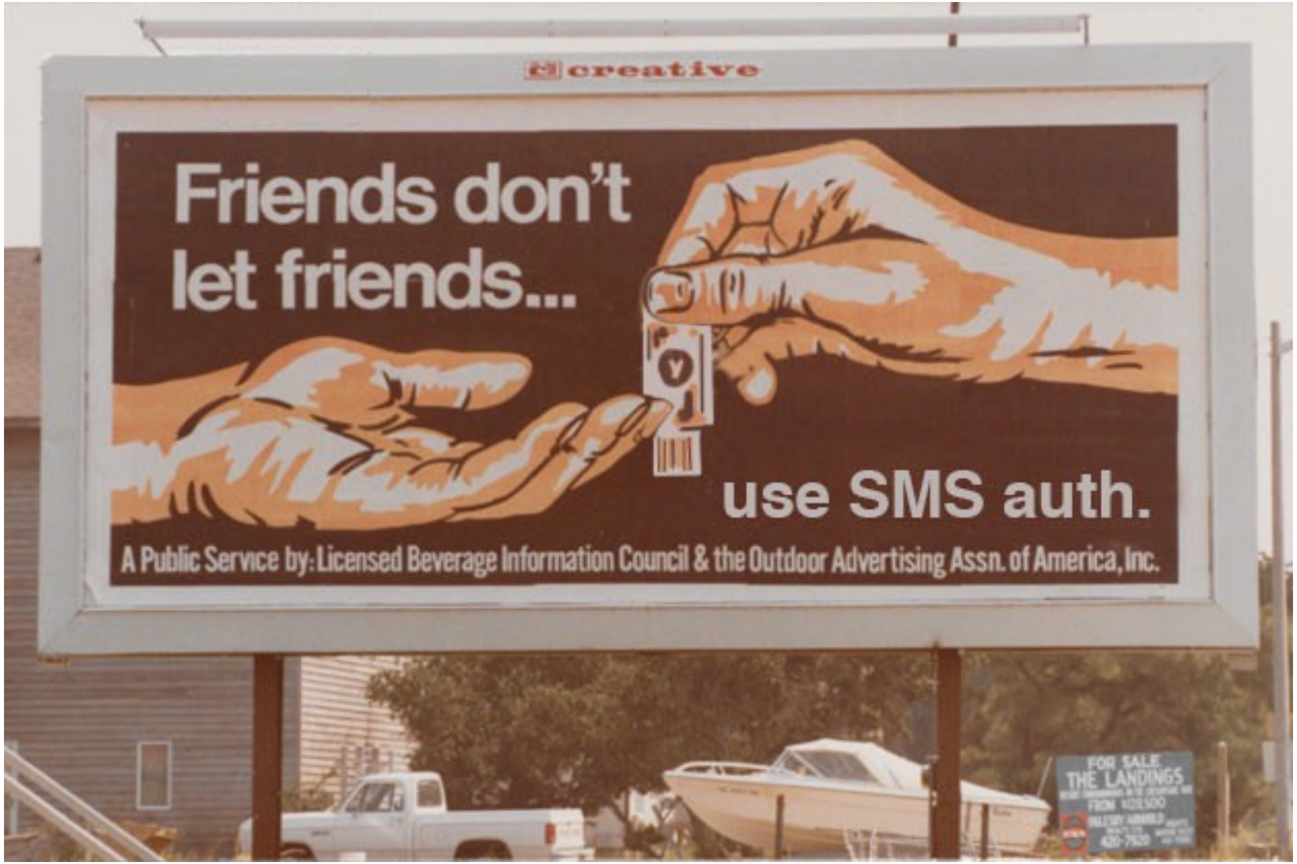
2fa is good! security is good! but we expect users to devote too much of their time to understanding something that should be our problem instead

Users with the most privilege, MFA is a requirement not optional

As we come to the end of our journey…

MFA can help but…

- Can only improve security if you are following secure password practices
- Some MFA methods are more secure then others


creative
Friends don't
let friends...
use SMS auth.
A Public Service by: Licensed Beverage Information Council & the Outdoor Advertising Assn. of America, Inc.
FOR SALE
THE LANDINGS
FROM
420-7920

Thanks for having me YOW! Brisbane

Thanks to:
Tyson Reeder slide design and final graphic
@tysondreeder

For references and further reading checkout
christine-seeman.com/talks

What questions can I answer?

Slides QR code

WP engine®

wpengine.careers

@christine@ruby.social

Everyone needs a product designer friend (thanks again Tyson!)

40px - Only text on slide

32px - Large Heading

24px - Body

#093840

#DCCEFE

#FFEEA7

#A3FBBC

#DCCEFE

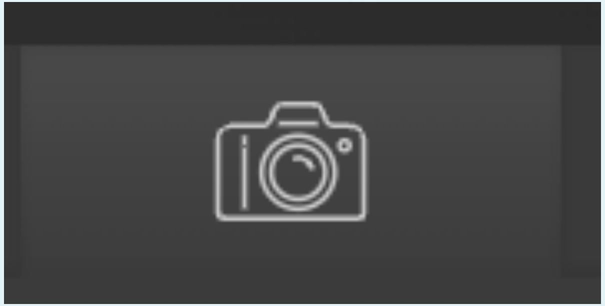
Image frame - teal - 3px wide

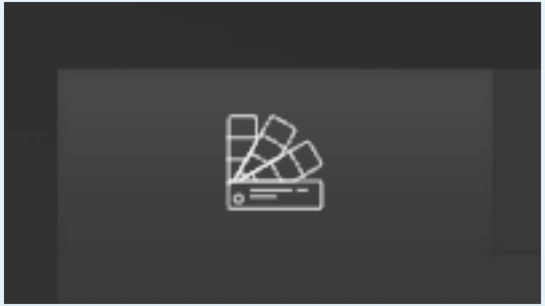
Creating duotone bg images

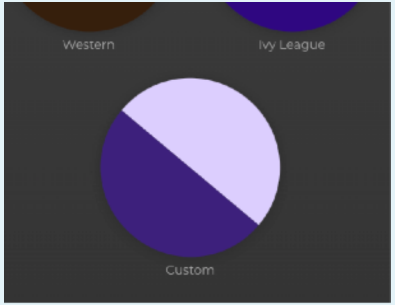
Go here

https://medialoot.com/duotones/

Click the camera and upload an image from your computer. Then go to the color tab and choose custom at the bottom. I try to stick to colors from the deck. Then drop it in and lower the opacity.






Western
Ivy League
Custom