# 2 FACTOR: GENERAL DISCUSSION

# TOM WEBSTER

## "SAMURAILINK3"

SAMURAILINK3.COM

SAMURAILINK3@GMAIL.COM

PLUS.GOOGLE.COM/+TOMWEBSTER

@SAMURAILINK3

# WHAT IS 2 FACTOR?

Password

+

Either a code or positive verification from another device or application.

Enter this verification code if prompted during account sign-in:

alice@gmail.com
942015

alice.work@company.com
277600

Press Menu for more options.

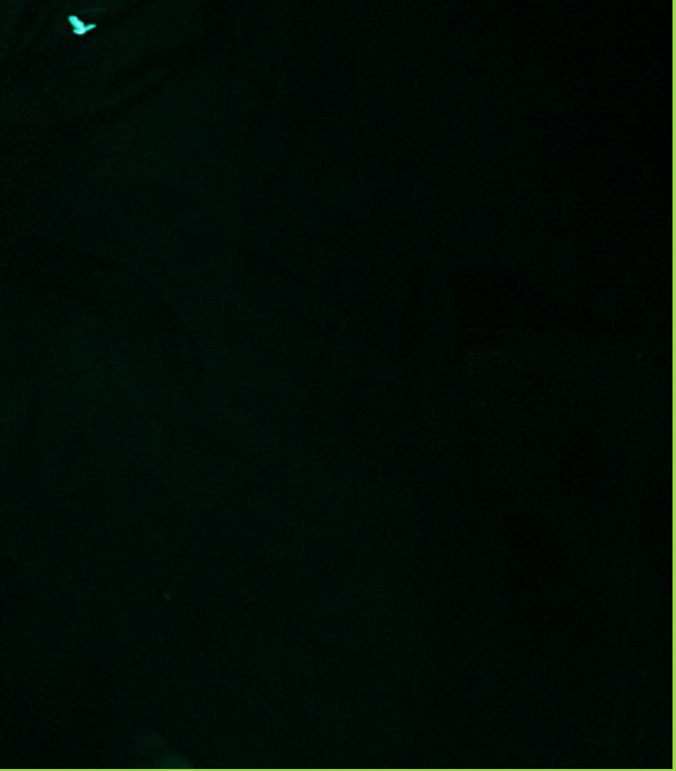
# BENEFITS

When **this guy** gets your password:

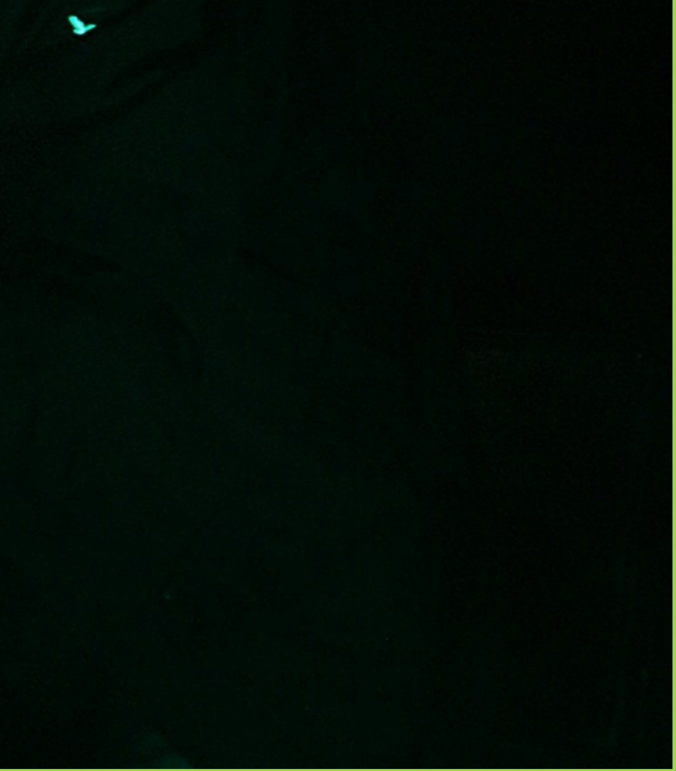
You aren't completely compromised*

letely compromised*

mpromised*



mised*



mised*

# 2 FACTOR AUTH IS NOT PERFECT

# LET'S GET REAL:

How effective is 2FA really?

stay tuned

# MY 2FA

The Key to the cloud
Try out your YubiKey at
www.yubico.com/start

# GOOGLE AUTHENTICATOR

- Open Source
- Run on your devices
- Run on your servers
- Control your own keys
- Implements open standards
  - RFC 4226
  - RFC 6238
  - Standards-based, you aren't locked in
- Runs on an insane number of platforms in varying implementations

# YUBIKEY NEO

- Partially Open
- Open Auth Modules for Servers
- Shows up as standard USB keyboard
- Uses common keys between international keyboards
- NFC used for smartphone authentication (not very common)
- Control your own keys
- Programmable second function
- Grandma-level easy to use (one button)

# OTHER COMMON 2FA

RSA SecurID

Phone Factor

Other Tokens

# RSA SECURID

Should really be RSA “Secur”ID

- Proprietary technology
- RSA controls keys
- Could be vulnerable to RSA compromise

# RSA SECURID

Should really be RSA “Secur”ID

- Proprietary technology
- RSA controls keys
- Could be vulnerable to RSA compromise

Oops, our bad!

# PHONE FACTOR

## DO YOU WANT TO ALLOW ACCESS?

[YES!! I don't want to break anything!!]

[No! I would like to have all of my apps break forever!]

Asking users to click a link to allow access is stupid.
They will always click “Allow”. Always.

# GETTING REAL

## How effective is 2FA really?

**Google Authenticator**

- Keys can be pulled from phone with ADB IF the phone allows debug access (check your settings!) [1]
- Key QR code and/or link can be pulled from cache if site isn't properly configured [1]

**RSA and Other Tokens**

- Keys are stored at the company and may be vulnerable to extraction
- May not use sufficiently secure implementation

**Yubikey**

- Generated keys may be stolen from the issuing computer
- Older firmware susceptible to physical key recovery, no way to upgrade firmware on older models [2]

**Call / SMS systems**

- Is only as secure as your wireless carrier (not at all)
- If the system just asks for a YES/NO answer instead of providing a code, it's vulnerable to humans being humans

[1]: http://zerocool.is-a-geek.net/google-two-factor-authentication-possible-attacks-and-prevention/
[2]: http://events.ccc.de/congress/2013/Fahrplan/events/5417.html

# GETTING REAL

## How effective is 2FA really?

**Generic Problems:**

- In many cases Customer Service can bypass 2FA.
- Badly coded sites can bypass 2FA prompts entirely.
  - PayPal/Ebay recently had a run-in with this problem.
- Phishing happens. And it works brilliantly.
- It's only one component in a very large system where a lot of things could go wrong.

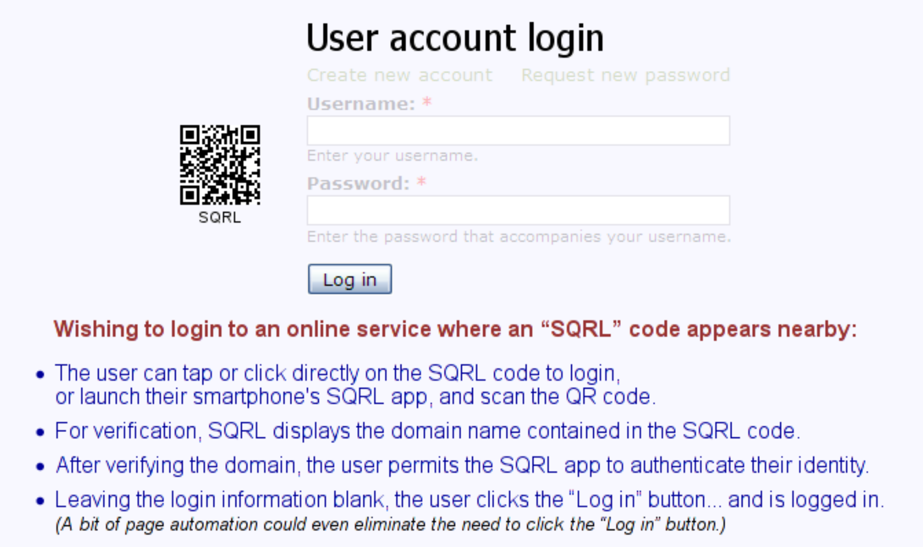
# THE FUTURE ISN'T HERE

2 Factor Authentication only helps our current situation. It's a stop-gap to the much larger problem of secure authentication in an inherently insecure environment.

# MORE ELEGANT AUTH

## FOR A MORE CIVILIZED AGE

## SQRL



### User account login

**Username: ***

Enter your username.

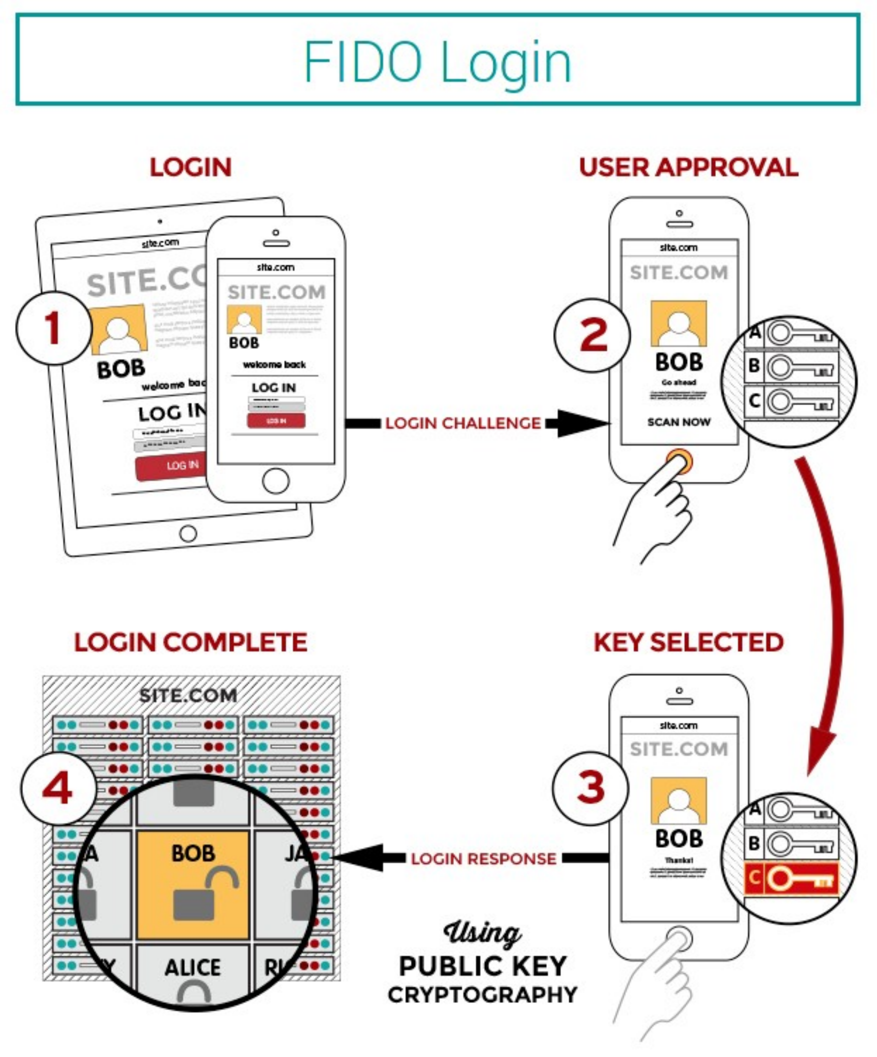
**Password: ***

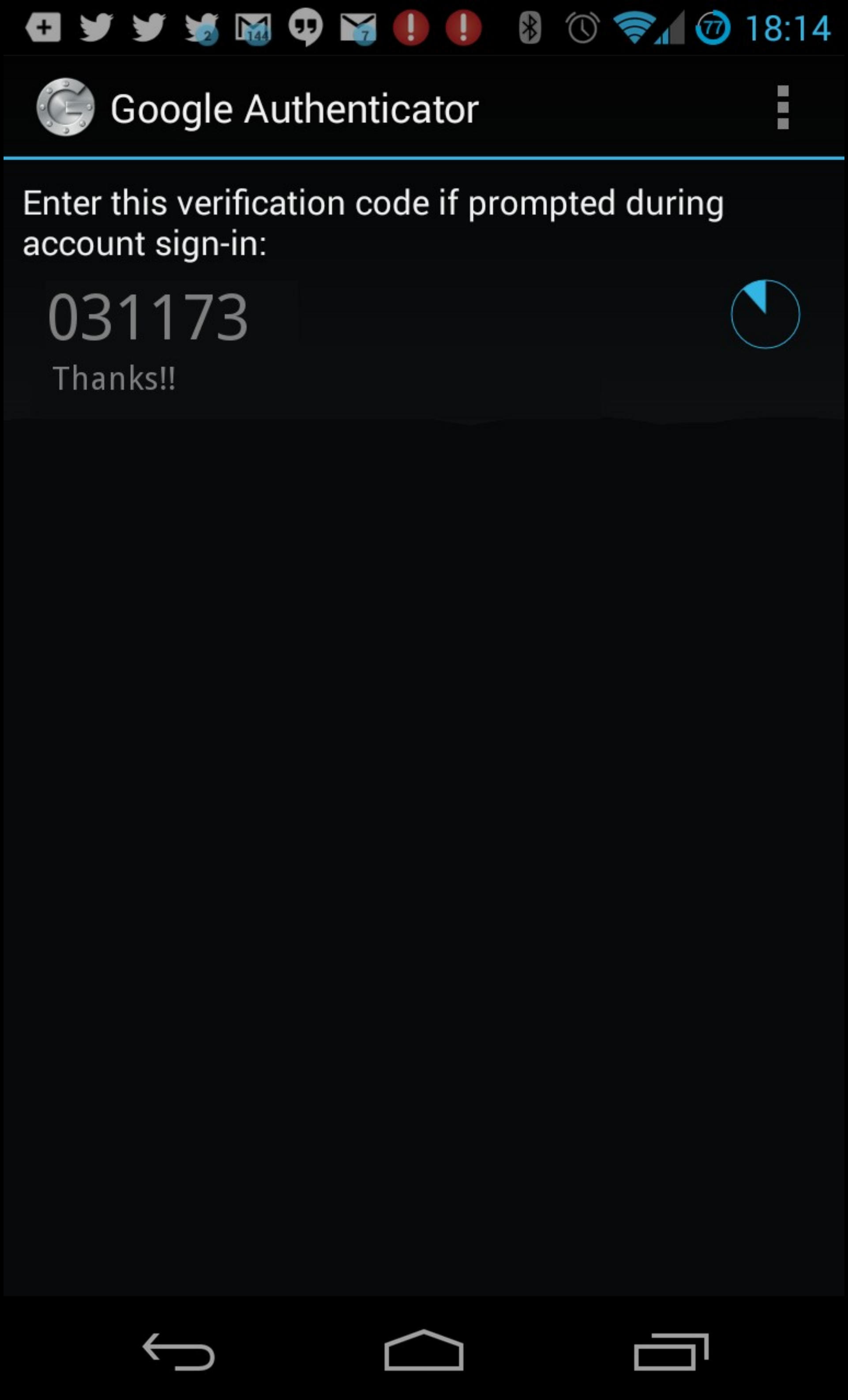
Enter the password that accompanies your username.

**Wishing to login to an online service where an “SQRL” code appears nearby:**

- The user can tap or click directly on the SQRL code to login, or launch their smartphone's SQRL app, and scan the QR code.
- For verification, SQRL displays the domain name contained in the SQRL code.
- After verifying the domain, the user permits the SQRL app to authenticate their identity.
- Leaving the login information blank, the user clicks the “Log in” button... and is logged in.
  *(A bit of page automation could even eliminate the need to click the “Log in” button.)*

## FIDO





Enter this verification code if prompted during account sign-in:

031173

Thanks!!