

2FA, WTF?

HACKERS

ARE

EVERYWHERE







Phil Nash

@philnash

<http://philna.sh>

philnash@twilio.com



2FA, WTF?

TWO FACTOR AUTHENTICATION

Two Factor Authentication

2FA is a security process in which a user provides two different forms of identification in order to authenticate themselves with a system.

The two forms must come from different categories. Normally something you know and something you have.

A person wearing a black balaclava and a black suit is sitting at a desk, typing on a silver laptop. The person's face is mostly covered by the balaclava, with only their eyes and mouth visible. The word "WHY?" is written in large, white, stylized letters across the center of the image, partially obscuring the person's face and the laptop. The background is a plain, light gray.

WHY?

A portrait of a man with dark, curly hair and glasses, looking directly at the camera. He is wearing a light-colored shirt. The background is a solid green color. Overlaid on the lower half of the image is a semi-transparent grid of binary code (0s and 1s).

MIAT HONAN

Mat Honan's Hackers' Timeline

1. Found Gmail address on his personal site
2. Entered address in Gmail and found his @me.com back up email
3. Called Amazon to add a credit card to file
4. Called Amazon again to reset password and got access
5. **4:33pm**: called Apple to reset password
6. **4:50pm**: reset AppleID password and gained access to email

Mat Honan's Hackers' Timeline

7. **4:52pm**: reset Gmail account password
8. **5:01pm**: wiped iPhone
9. **5:02pm**: reset Twitter password
10. **5:05pm**: wiped MacBook and deleted Google account
11. **5:12pm**: posted to Twitter taking credit for the hack

@MAT

A person wearing a black balaclava and a black suit is sitting at a desk, typing on a silver laptop. The person's face is mostly covered by the balaclava, with only their eyes and mouth visible. The word "WHY?" is written in large, white, stylized, jagged letters across the center of the image, partially obscuring the person's face and the laptop. The background is a plain, light gray.

WHY?



LastPass ****

A close-up photograph of a woman's face, focusing on her mouth and nose. She has long, wavy brown hair and is wearing red lipstick. Her right index finger is pressed against her lips in a universal gesture for silence or secrecy. She is also wearing a thin gold ring on her right ring finger. The background is dark and out of focus.

ASHLEY MADISON

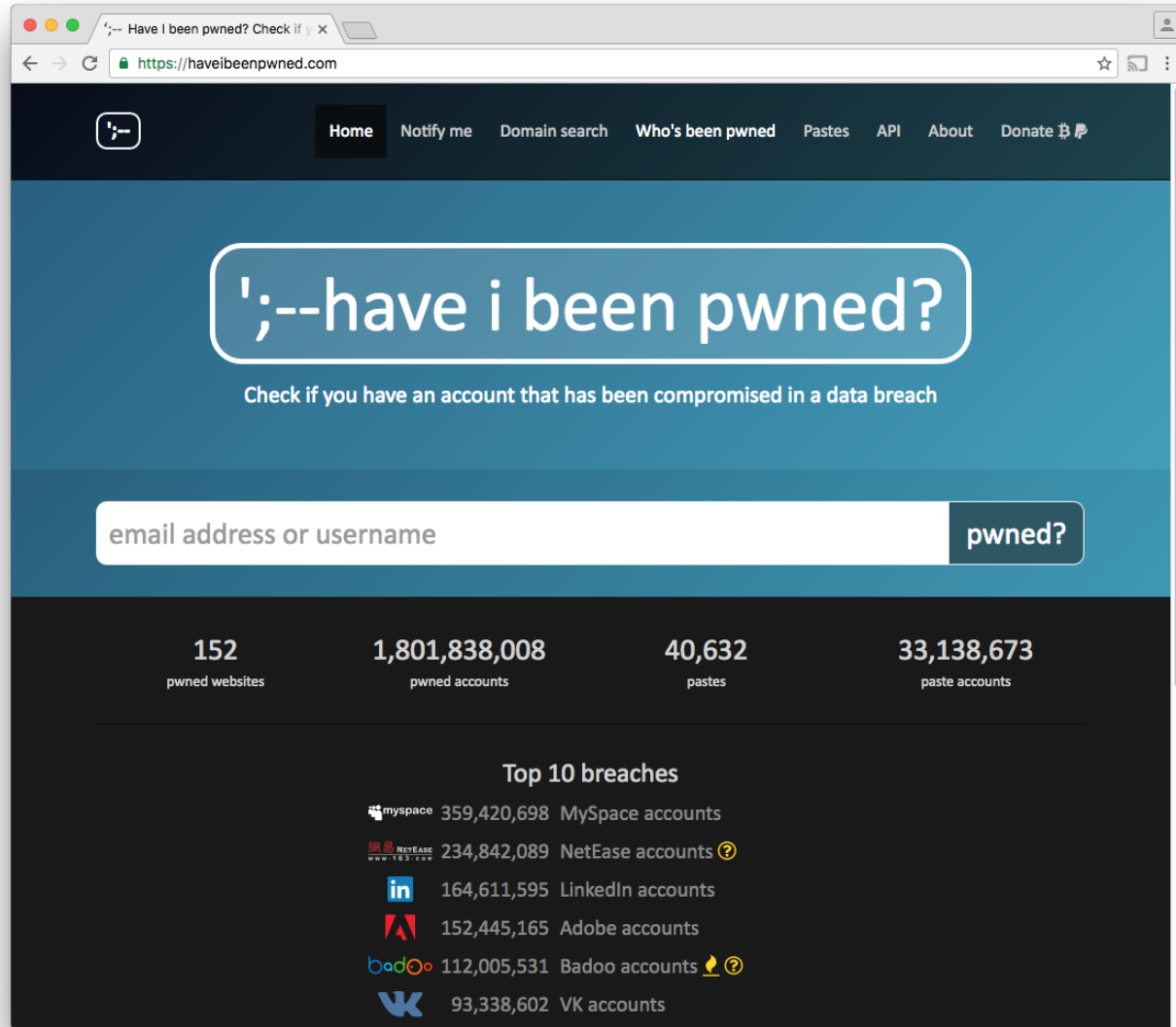
Ashley Madison Top 10 Passwords

1. 123456
2. 12345
3. password
4. DEFAULT
5. 123456789
6. qwerty
7. 12345678
8. abc123
9. NSFW
10. 1234567

Ashley Madison Top 10 Passwords

1. 123456 - 120,511 users
2. 12345 - 48,452 users
3. password - 39,448 users
4. DEFAULT - 34,275 users
5. 123456789 - 26,620 users
6. qwerty - 20,778 users
7. 12345678 - 14,172 users
8. abc123 - 10,869 users
9. NSFW - 10,683 users
10. 1234567 - 9,468 users

Source: <http://qz.com/501073/the-top-100-passwords-on-ashley-madison/>





User Registration Flow

1. Visit registration page
2. Sign up with username and password
3. User is logged in

User Log In Flow

1. Visit login page
2. Enter username and password
3. System verifies details
4. User is logged in

SMS

User Registration Flow

1. Visit registration page
2. Sign up with username, password and phone number
3. User is logged in

User Log In Flow

1. Visit login page
2. Enter username and password
3. System verifies details
4. Verification code sent to user by SMS
5. User enters verification code
6. System verifies code
7. User is logged in

PROS/CONS

SOFT TOKEN

User Registration Flow

1. Visit registration page
2. Sign up with username, password
3. Generate a secret for the user
4. Share the secret somehow
5. User is logged in

User Log In Flow

1. Visit login page
2. Enter username and password
3. System verifies details
4. User opens auth app
5. User finds app verification code and enters on site
6. System verifies code
7. User is logged in

SECRETS

НОТР/ТОТР

HOTP

$\text{HOTP}(K, C) = \text{Truncate}(\text{HMAC}(K, C)) \& 0x7FFFFFFF$

$\text{HOTP-Value} = \text{HOTP}(K, C) \bmod 10^d$

TOTP

DEMO

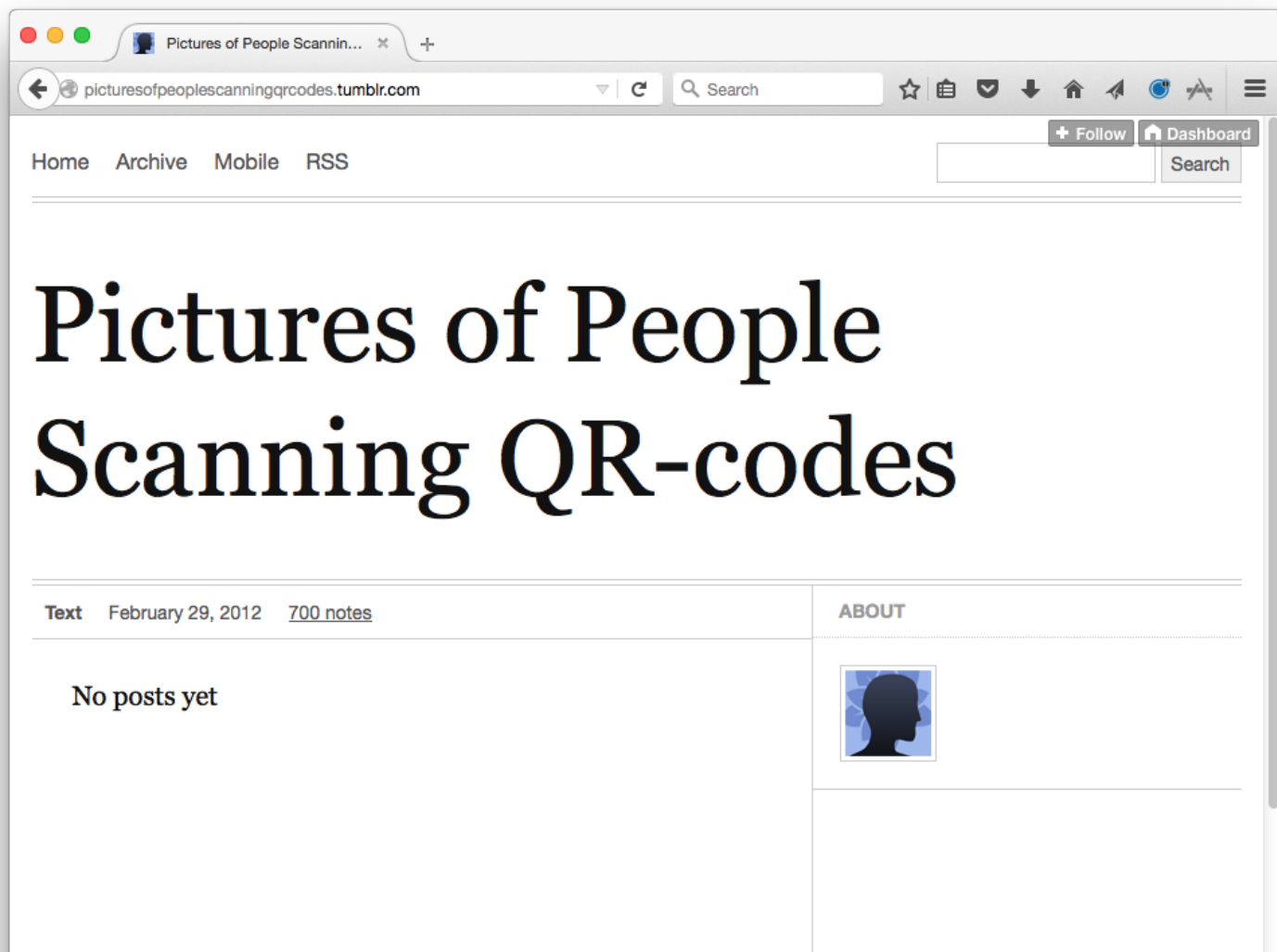
<https://github.com/guyht/notp>

**SHARING
SECRETS**

QR code

otpauth://TYPE/LABEL?PARAMETERS

otpauth://totp/Example:philnash@twilio.com?secret=JBSWY3DPEHPK3PXP&issuer=Example



Pictures of People Scannin... x +

← picturesofpeoplescanningqr.codes.tumblr.com

Search

+ Follow

Dashboard

Home Archive Mobile RSS

Search

Pictures of People Scanning QR-codes

Text February 29, 2012 [700 notes](#)

No posts yet

ABOUT



PROS/CONS

**CAN IT BE
BETTER?**

**FRIENDS DON'T LET
FRIENDS WRITE THEIR**

**OWN AUTHENTICATION
FRAMEWORKS**

**FRIENDS DON'T LET
FRIENDS WRITE THEIR
OWN TWO FACTOR**

**AUTHENTICATION
FRAMEWORKS**



User Registration Flow

1. Visit registration page
2. Sign up with username, password and phone number
3. System registers User with Authy
4. User is logged in

User Log In Flow

1. Visit login page
2. Enter username and password
3. System verifies details
4. Authy prompts user
5. User finds app verification code and enters on site
6. System verifies code with Authy
7. User is logged in



THE FUTURE

**PUSH
NOTIFICATIONS**

OwlBank

www.authydemo.com/login

Search

☆

📁

📧

⬇

🏠

🚀

😊


⌵

🌐

🛠

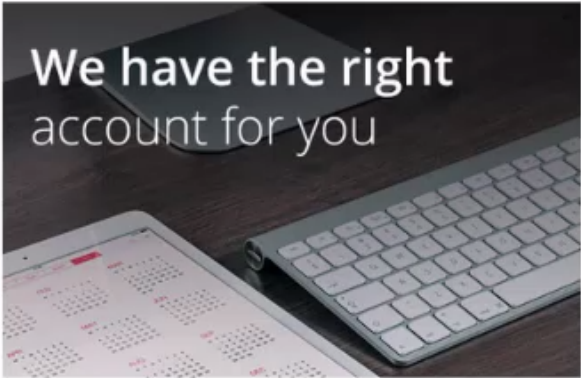
✎

☰

**OWL BANK**

Personal Business Commercial


BANKING CREDIT CARDS INVESTMENTS




We have the right account for you

Save interest with your

Owl Credit Card



Start planning your retirement



Log in Register

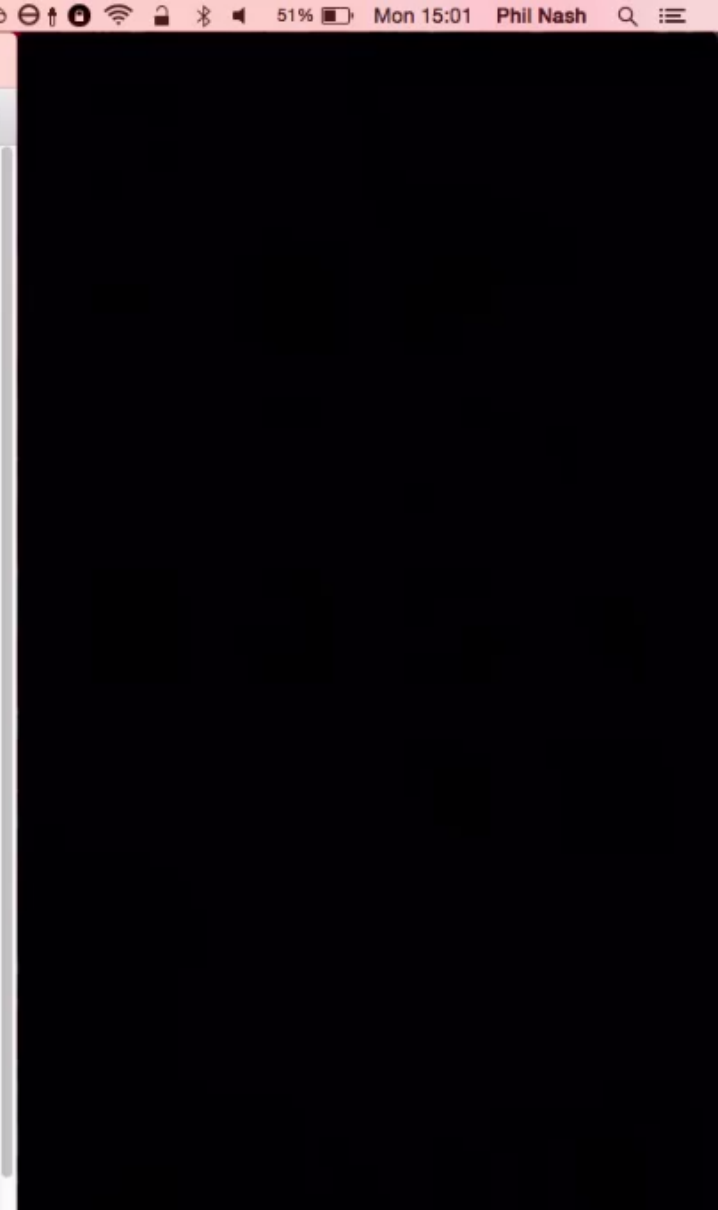
Welcome

User ID

Password

[Click here to reset your password](#)

Log in



PROS/CONS

SUMMARY

**USERS ARE
BAD WITH
PASSWORDS**

**OTHER
WEBSITES ARE
BAD WITH
PASSWORDS**

**2FA CAN BE
PUSH, TOKEN
OR SMS**

**2FA IS FOR
YOUR USERS**



THANKS!

Thanks!

@philnash

<http://philna.sh>

philnash@twilio.com

