A br1ef h1st0ry of P@ssw0rds

Hello!

Rob N ★

Email: robn@fastmail.com
Twitter: @robn
Github: @robn

https://robn.io/passwords-compcon-2016/

What I did

What I did

- 1998 - Started a Computer Science degree

What I did

- 1998 - Started a Computer Science degree
- 1999-2012 - Monash Uni, doing mail and web stuff
  - Netscape Mail → Lotus Notes → Google Apps

What I did

- 1998 - Started a Computer Science degree
- 1999-2012 - Monash Uni, doing mail and web stuff
  - Netscape Mail → Lotus Notes → Google Apps
- 2012-today - FastMail, doing mail and web stuff

What I did

- 1998 - Started a Computer Science degree
- 1999-2012 - Monash Uni, doing mail and web stuff
  - Netscape Mail → Lotus Notes → Google Apps
- 2012-today - FastMail, doing mail and web stuff
- I do operations - keeping the lights on

I am not a security expert

Passwords

Passwords are terrible

Passwords have always been terrible

1961

First use of passwords

1961

First use of passwords

- MIT's "Compatible Time Sharing System" (CTSS)

1961

First use of passwords

- MIT's "Compatible Time Sharing System" (CTSS)
- Allowed a running task to be interrupted so a higher priority task could be run
    - and then, once finished, the original task continues

1961

First use of passwords

- MIT's "Compatible Time Sharing System" (CTSS)
- Allowed a running task to be interrupted so a higher priority task could be run
  - and then, once finished, the original task continues
- Usernames & passwords used to protect files and allocate run time

1962

First password hack

1962

First password hack

- Allan Scherr, Ph.D student

1962

First password hack

- Allan Scherr, Ph.D student
- Allocated four hours per week, needed more for his simulations

1962

First password hack

- Allan Scherr, Ph.D student
- Allocated four hours per week, needed more for his simulations
- Print service ran as a privileged service

1962

First password hack

- Allan Scherr, Ph.D student
- Allocated four hours per week, needed more for his simulations
- Print service ran as a privileged service
- Wrote a program to request a printout of the password file

1962

First password hack

- Allan Scherr, Ph.D student
- Allocated four hours per week, needed more for his simulations
- Print service ran as a privileged service
- Wrote a program to request a printout of the password file
- Gave everyone a copy to cover his tracks

1966

First password leak

1966

First password leak

- One user editing the password file

1966

First password leak

- One user editing the password file
- Another user editing the MOTD file

1966

First password leak

- One user editing the password file
- Another user editing the MOTD file
- Editor used a hardcoded file for temp storage

1966

First password leak

- One user editing the password file
- Another user editing the MOTD file
- Editor used a hardcoded file for temp storage
- Password file was written to MOTD file

1966

First password leak

- One user editing the password file
- Another user editing the MOTD file
- Editor used a hardcoded file for temp storage
- Password file was written to MOTD file
- Displayed to users on login


THIS IS FINE.

1966-1974

Hashed passwords

```
mem = 1042
RESTRICTED RIGHTS

Use, duplication or disclosure is subject to
restrictions stated in Contract with Western
Electric Company, Inc.
# CAT /ETC/PASSWD
ROOT::0:3::/:
DAEMON::1:1::/:
BIN::3:3::/BIN:
KEN::6:1::/USR/KEN:
# PASSWD KEN BIGSECRET
# CAT /ETC/PASSWD
ROOT::0:3::/:
DAEMON::1:1::/:
BIN::3:3::/BIN:
KEN:A042VD2G:6:1::/USR/KEN:
#
```

1966-1974

Hashed passwords

- Experiments with "encoded" passwords in CTSS, MULTICS and UNIX

```
mem = 1042
RESTRICTED RIGHTS

Use, duplication or disclosure is subject to
restrictions stated in Contract with Western
Electric Company, Inc.
# CAT /ETC/PASSWD
ROOT::0:3::/:
DAEMON::1:1::/:
BIN::3:3::/BIN:
KEN::6:1::/USR/KEN:
# PASSWD KEN BIGSECRET
# CAT /ETC/PASSWD
ROOT::0:3::/:
DAEMON::1:1::/:
BIN::3:3::/BIN:
KEN:A042VD2G:6:1::/USR/KEN:
#
```

1966-1974

Hashed passwords

- Experiments with "encoded" passwords in CTSS, MULTICS and UNIX
- Renewed interest in one-way hash functions
  - Don't store the password, store a value derived from the password
  - Do the same thing with the login password, compare

```
mem = 1042
RESTRICTED RIGHTS

Use, duplication or disclosure is subject to
restrictions stated in Contract with Western
Electric Company, Inc.
# CAT /ETC/PASSWD
ROOT::0:3::/:
DAEMON::1:1::/:
BIN::3:3::/BIN:
KEN::6:1::/USR/KEN:
# PASSWD KEN BIGSECRET
# CAT /ETC/PASSWD
ROOT::0:3::/:
DAEMON::1:1::/:
BIN::3:3::/BIN:
KEN:A042VD2G:6:1::/USR/KEN:
#
```

1966-1974

Hashed passwords

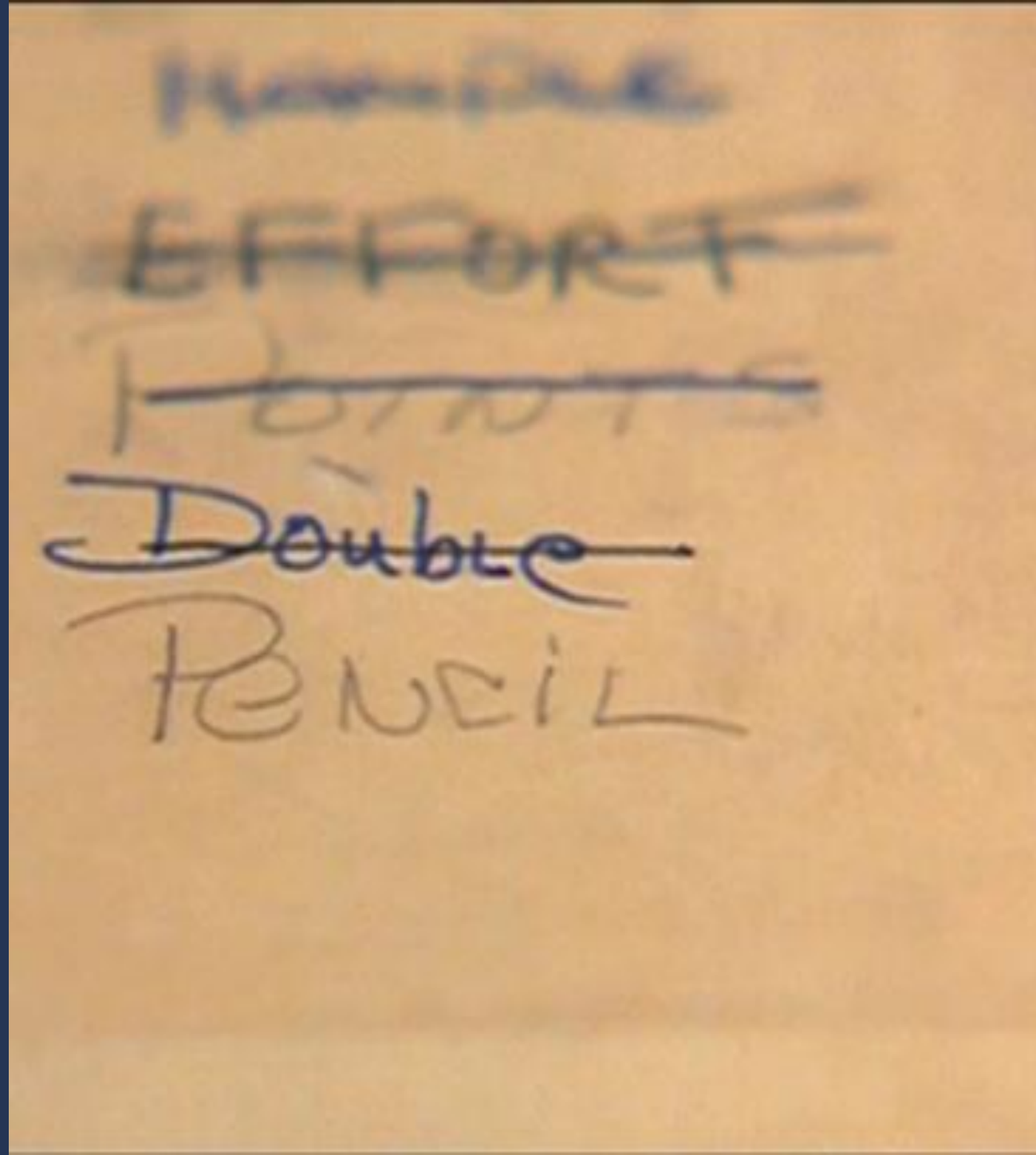
- Experiments with "encoded" passwords in CTSS, MULTICS and UNIX
- Renewed interest in one-way hash functions
  - Don't store the password, store a value derived from the password
  - Do the same thing with the login password, compare
- Robert Morris implements `crypt()` in 6th Edition UNIX

```
mem = 1042
RESTRICTED RIGHTS

Use, duplication or disclosure is subject to
restrictions stated in Contract with Western
Electric Company, Inc.
# CAT /ETC/PASSWD
ROOT::0:3::/:
DAEMON::1:1::/:
BIN::3:3::/BIN:
KEN::6:1::/USR/KEN:
# PASSWD KEN BIGSECRET
# CAT /ETC/PASSWD
ROOT::0:3::/:
DAEMON::1:1::/:
BIN::3:3::/BIN:
KEN:A042VD2G:6:1::/USR/KEN:
#
```

1979

Password Security: A Case History



Password Security: A Case History

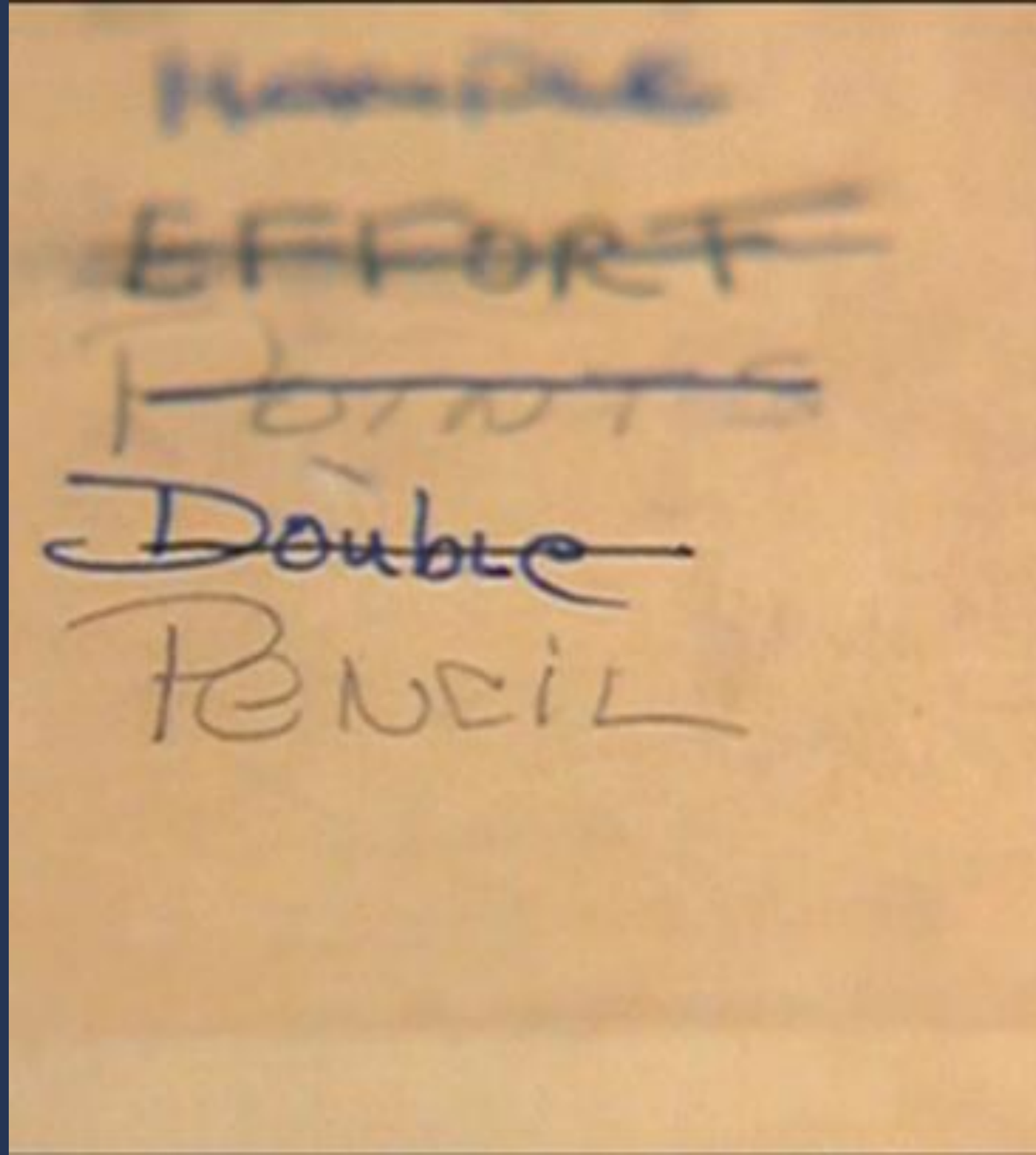
The authors have conducted experiments to try to determine typical users' habits in the choice of passwords when no constraint is put on their choice. The results were disappointing, except to the bad guy. In a collection of 3,289 passwords gathered from many users over a long period of time,

15 were a single ASCII character;
72 were strings of two ASCII characters;
464 were strings of three ASCII characters;
477 were strings of four alphamerics;
706 were five letters, all upper-case or all lower-case;
605 were six letters, all lower-case.

An additional 492 passwords appeared in various available dictionaries, name lists, and the like. A total of 2,831 or 86 percent of this sample of passwords fell into one of these classes.

2015

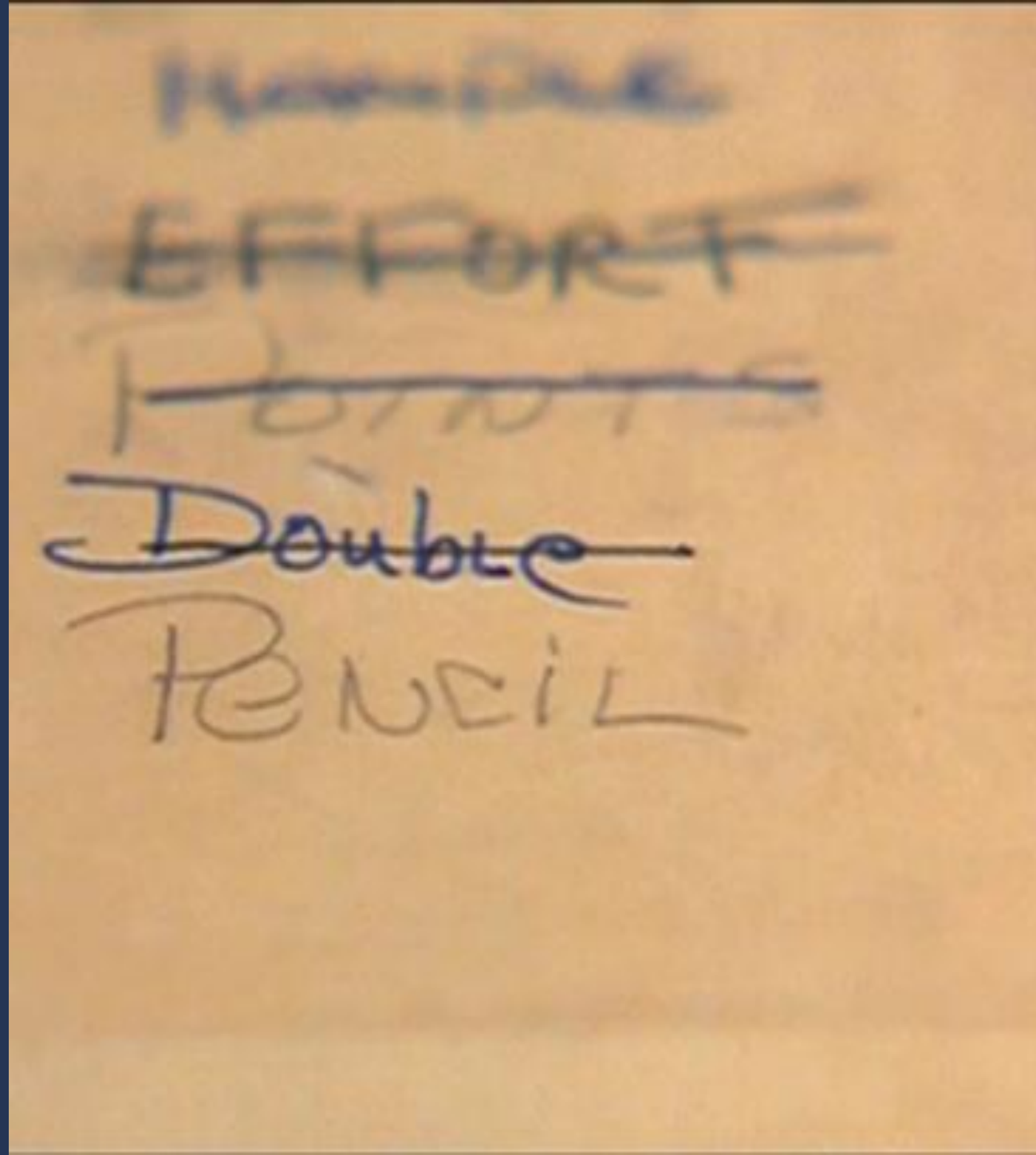
You won't believe what happened next



2015

You won't believe what happened next

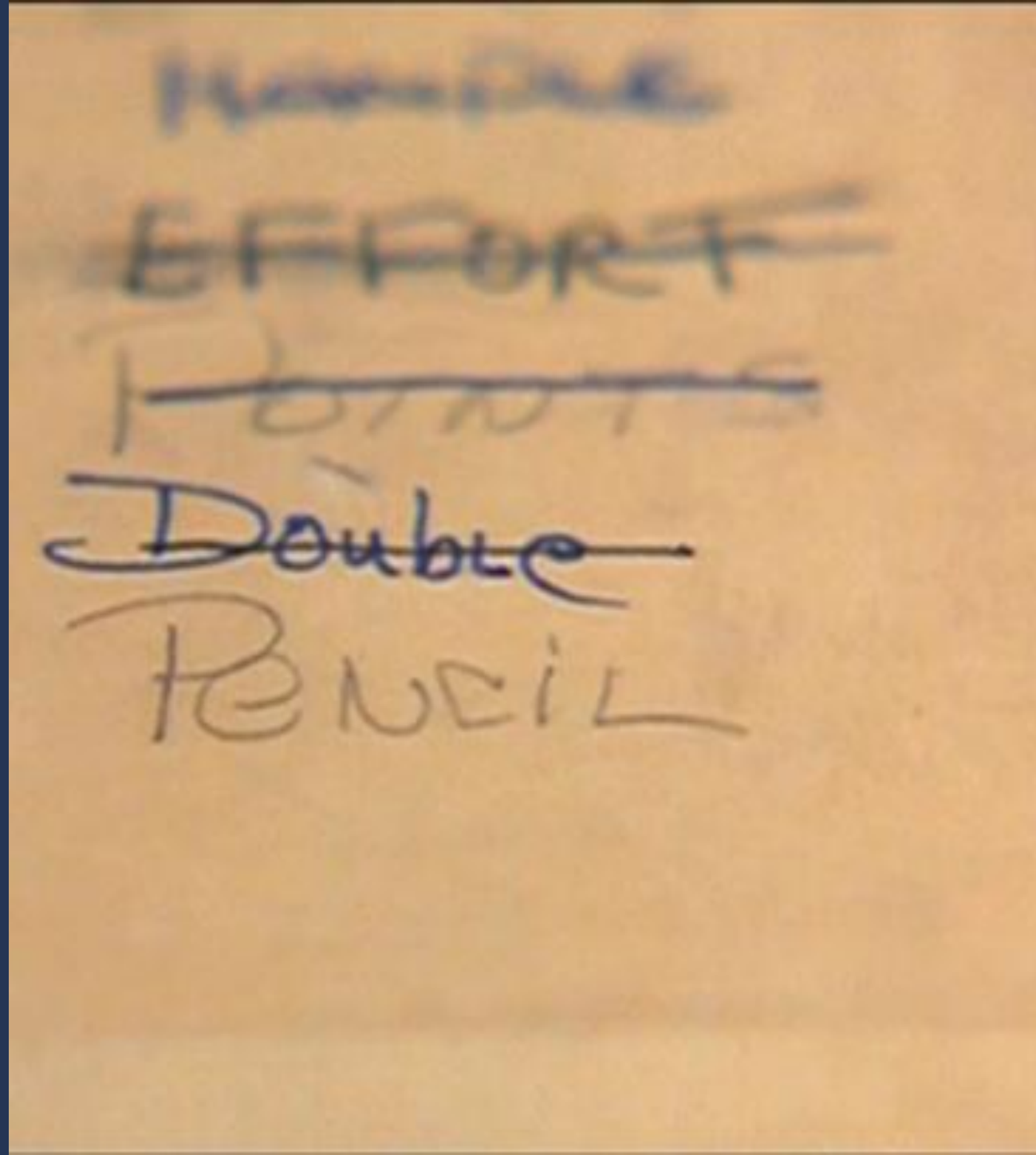
- SplashData's 5th annual "Worst Password List"



2015

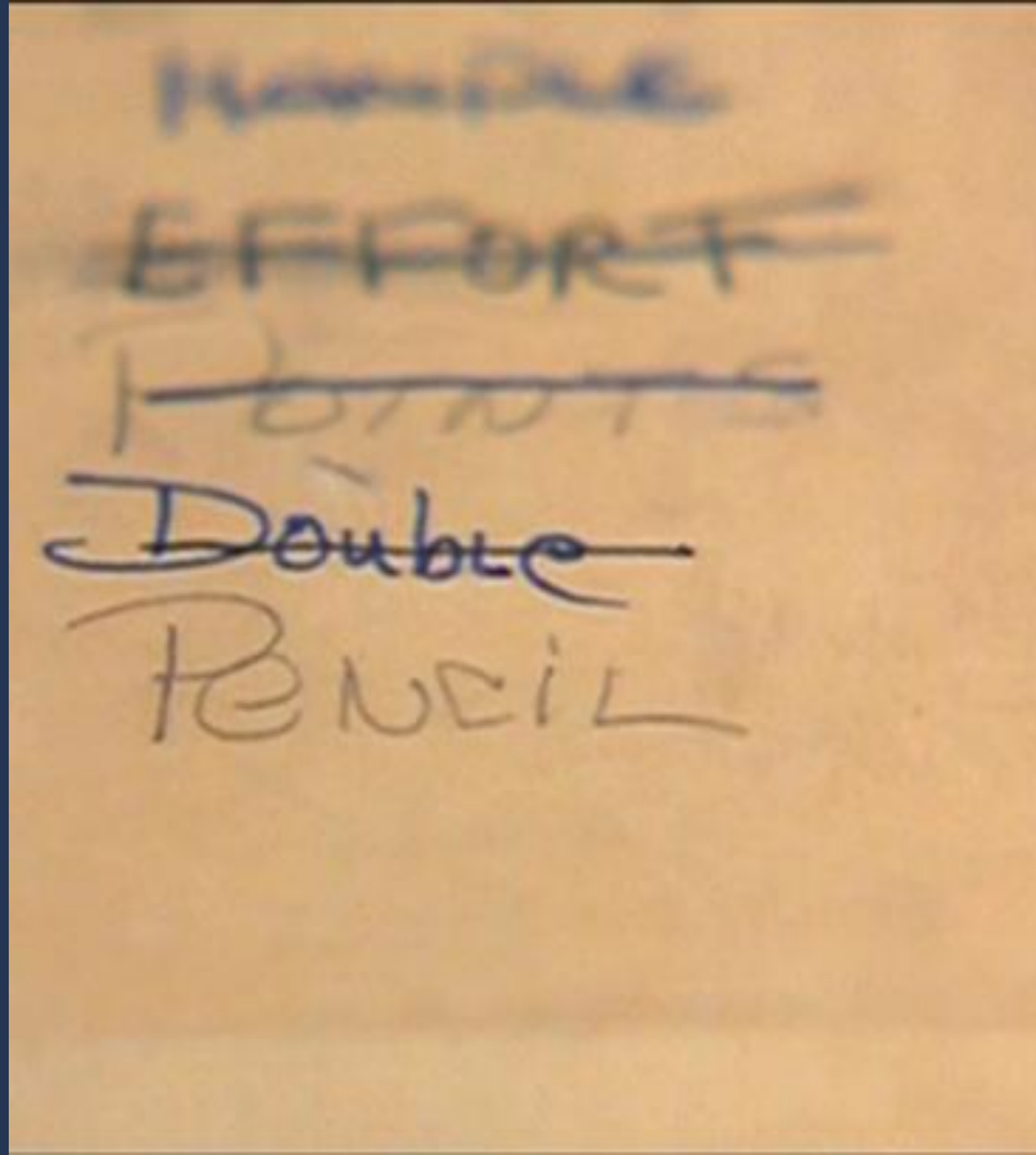
You won't believe what happened next

- SplashData's 5th annual "Worst Password List"
- 2m+ leaked passwords analysed



2015

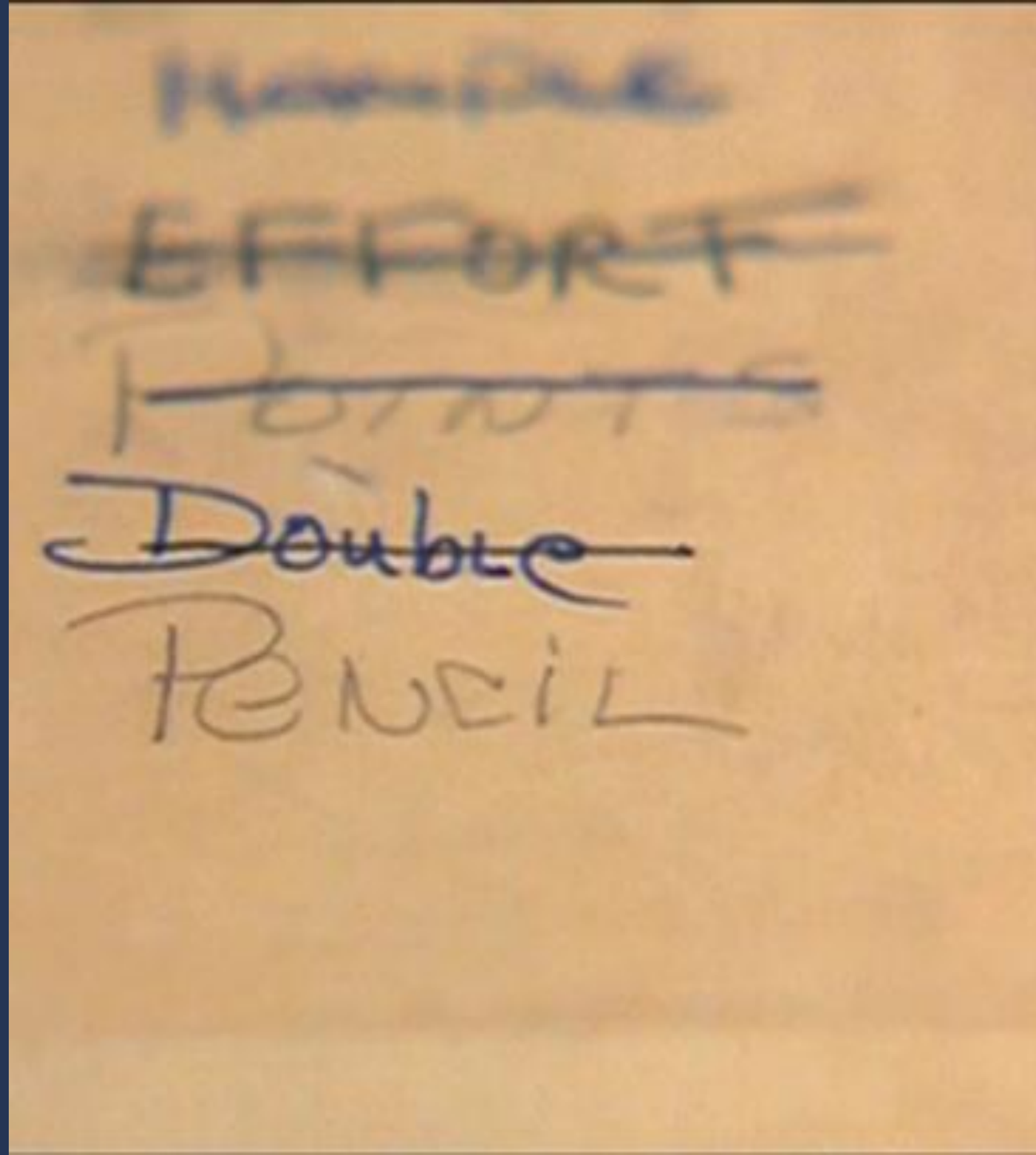
Ten popular passwords you need to know right now



2015

Ten popular passwords you need to know right now

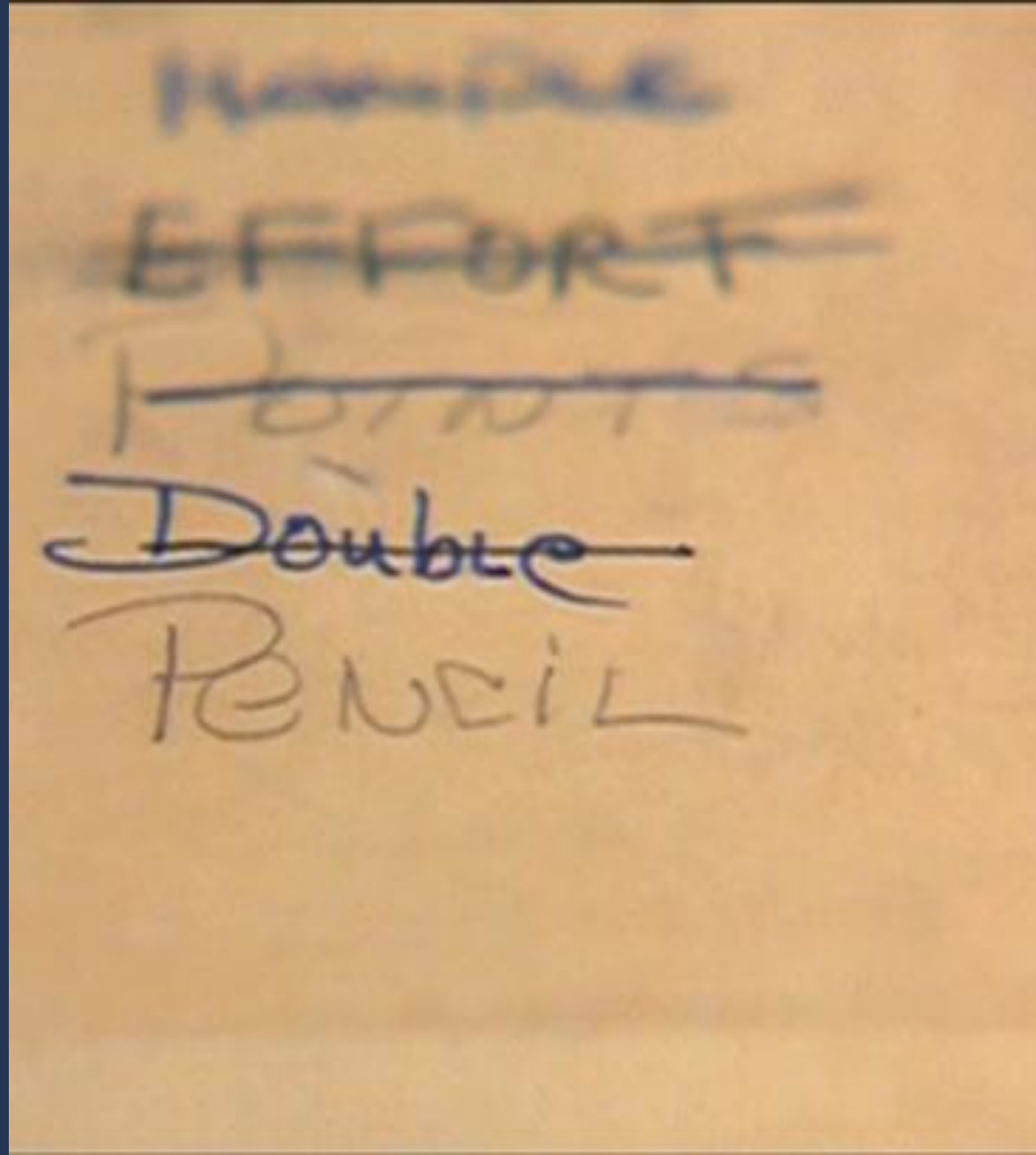
123456



2015

Ten popular passwords you need to know right now

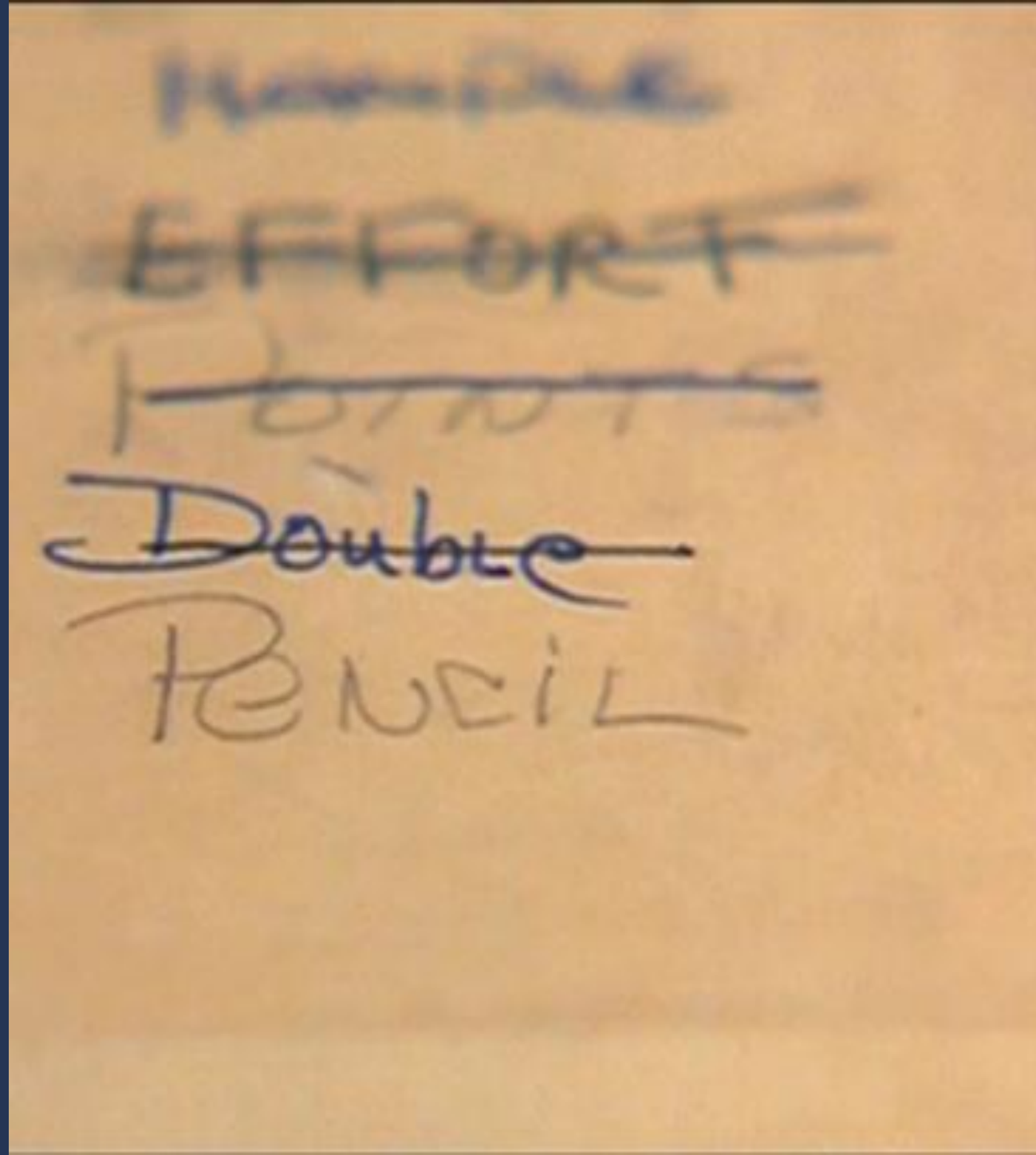
123456
password



2015

Ten popular passwords you need to know right now

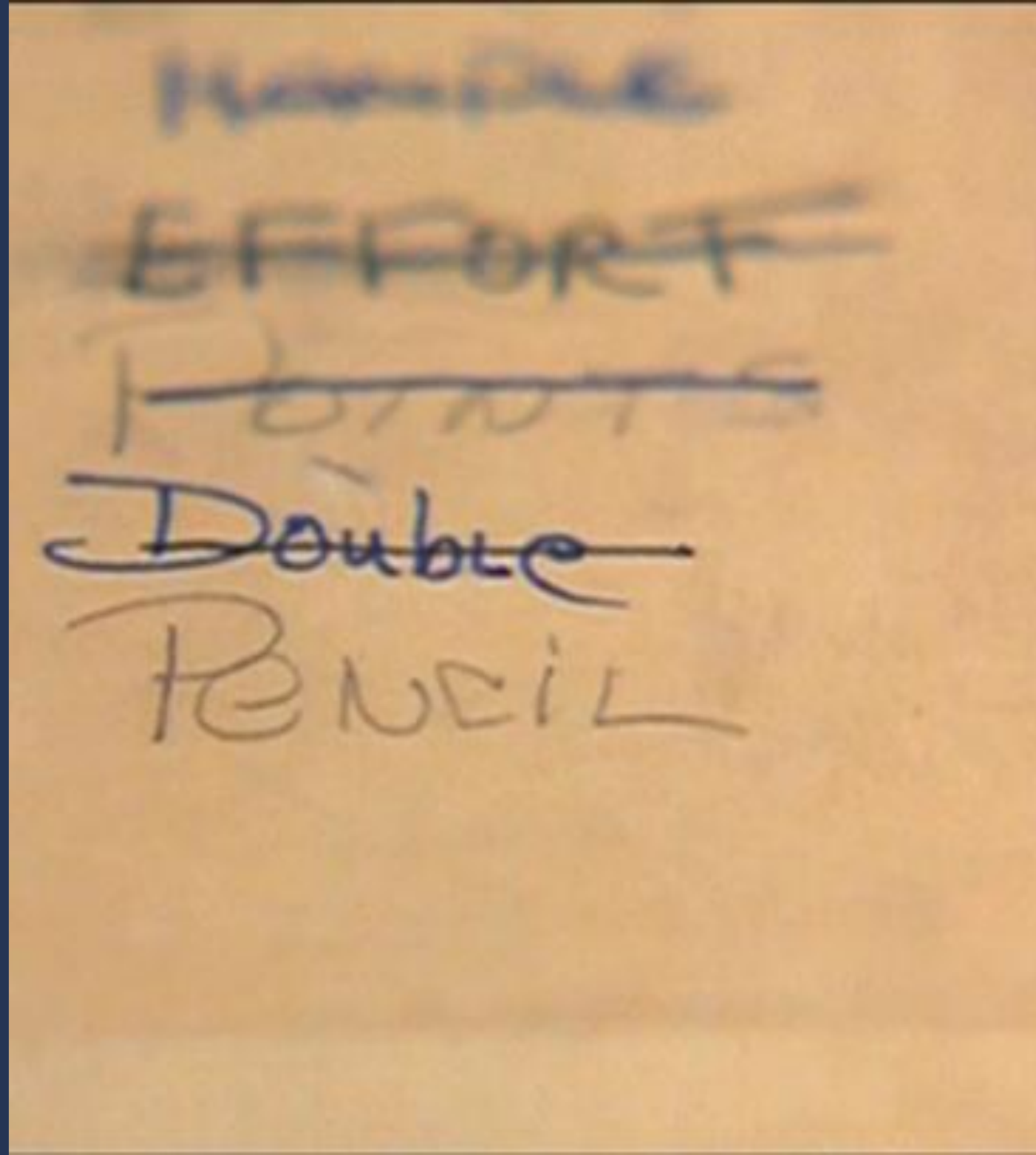
123456
password
12345678



2015

Ten popular passwords you need to know right now

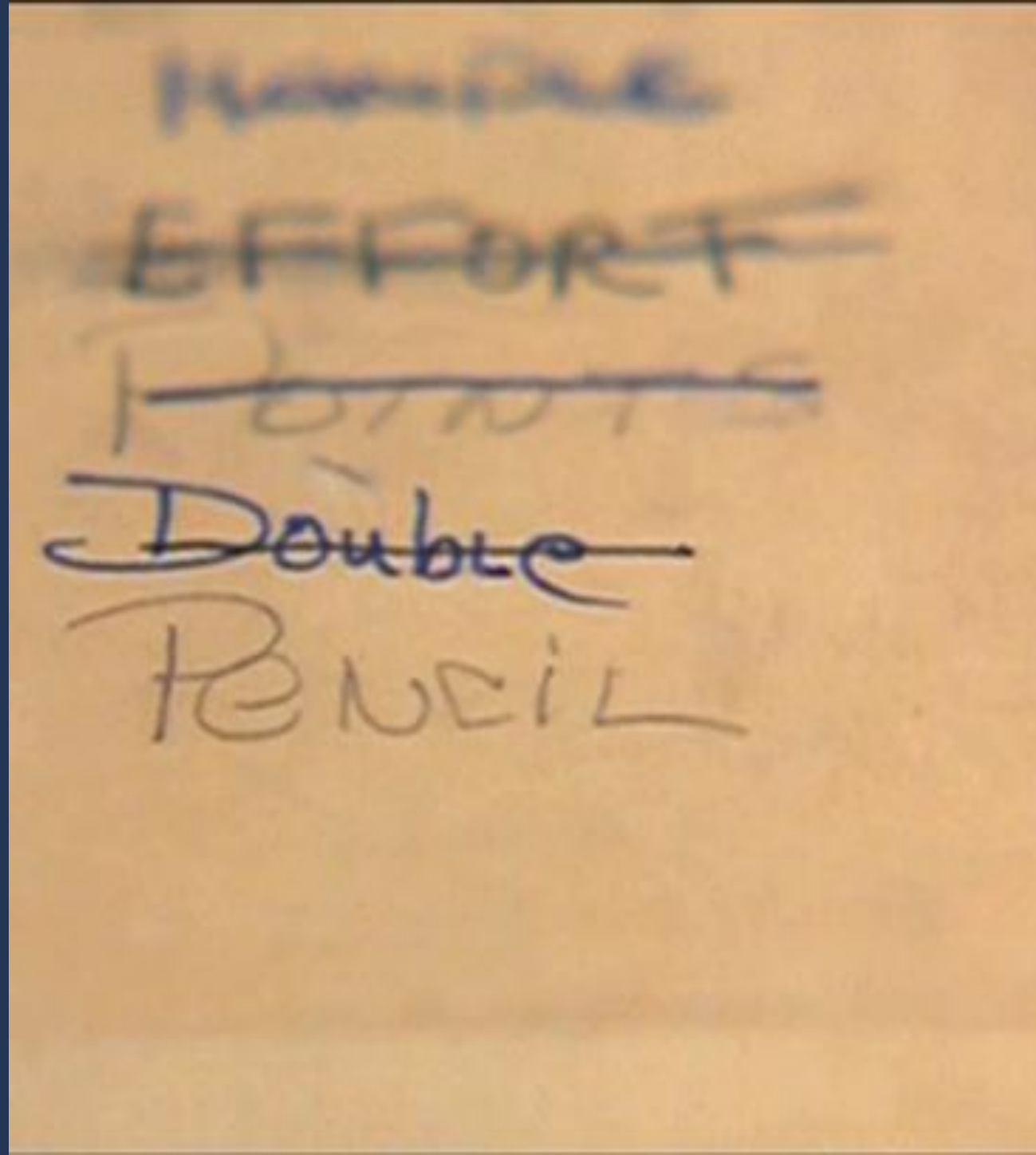
123456
password
12345678
qwerty



2015

Ten popular passwords you need to know right now

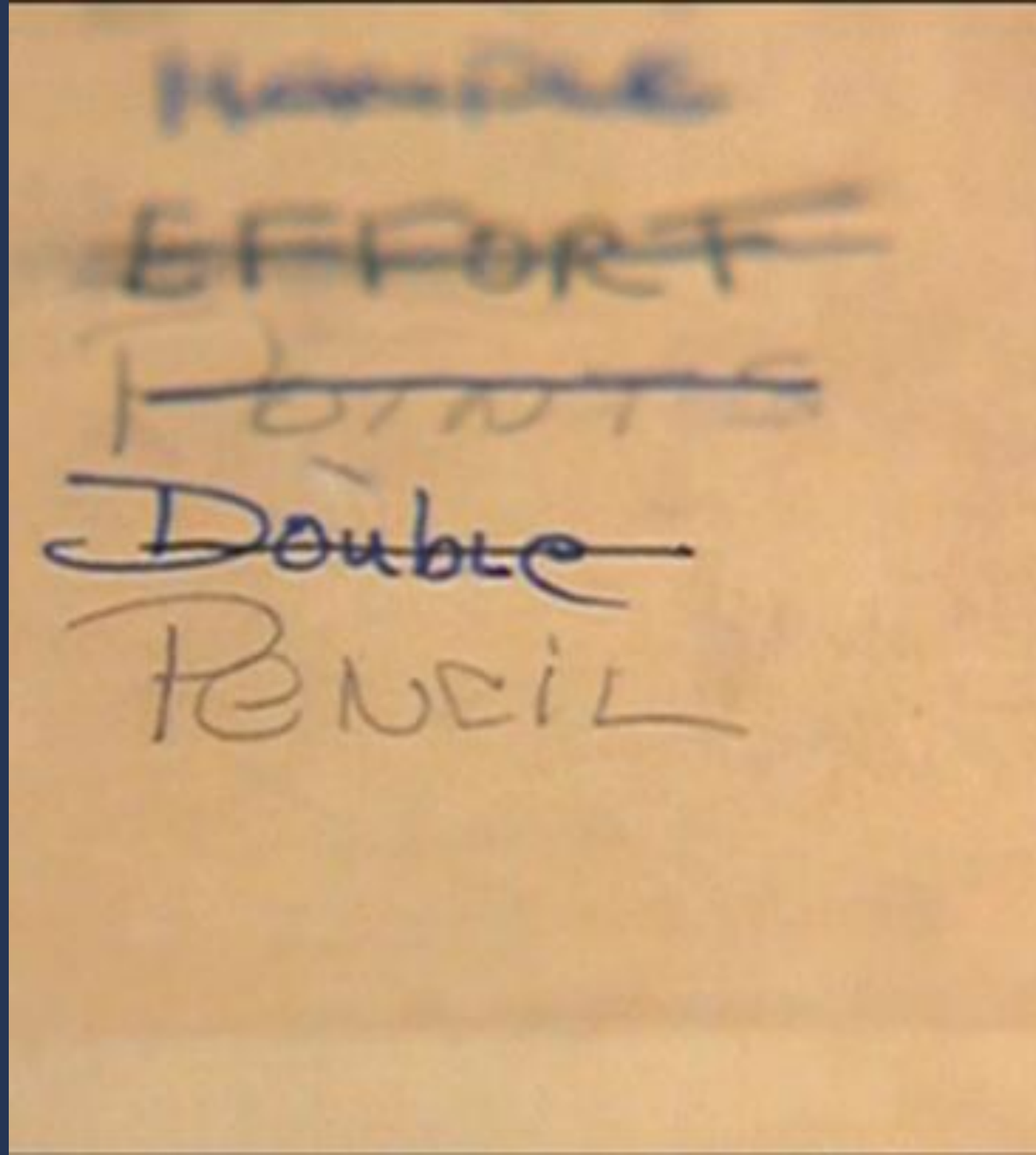
123456
password
12345678
qwerty
12345



2015

Ten popular passwords you need to know right now

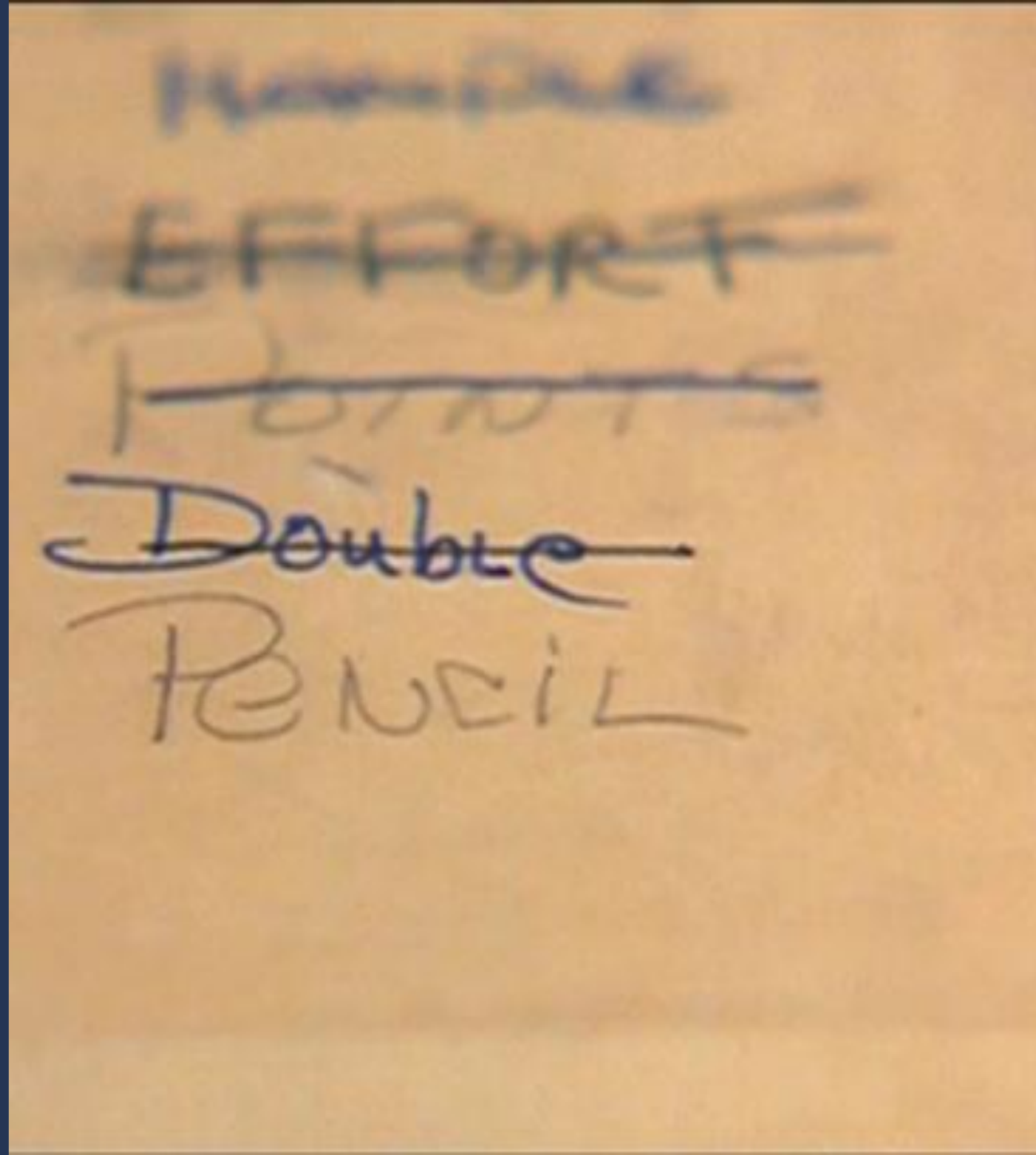
123456
password
12345678
qwerty
12345
123456789



2015

Ten popular passwords you need to know right now

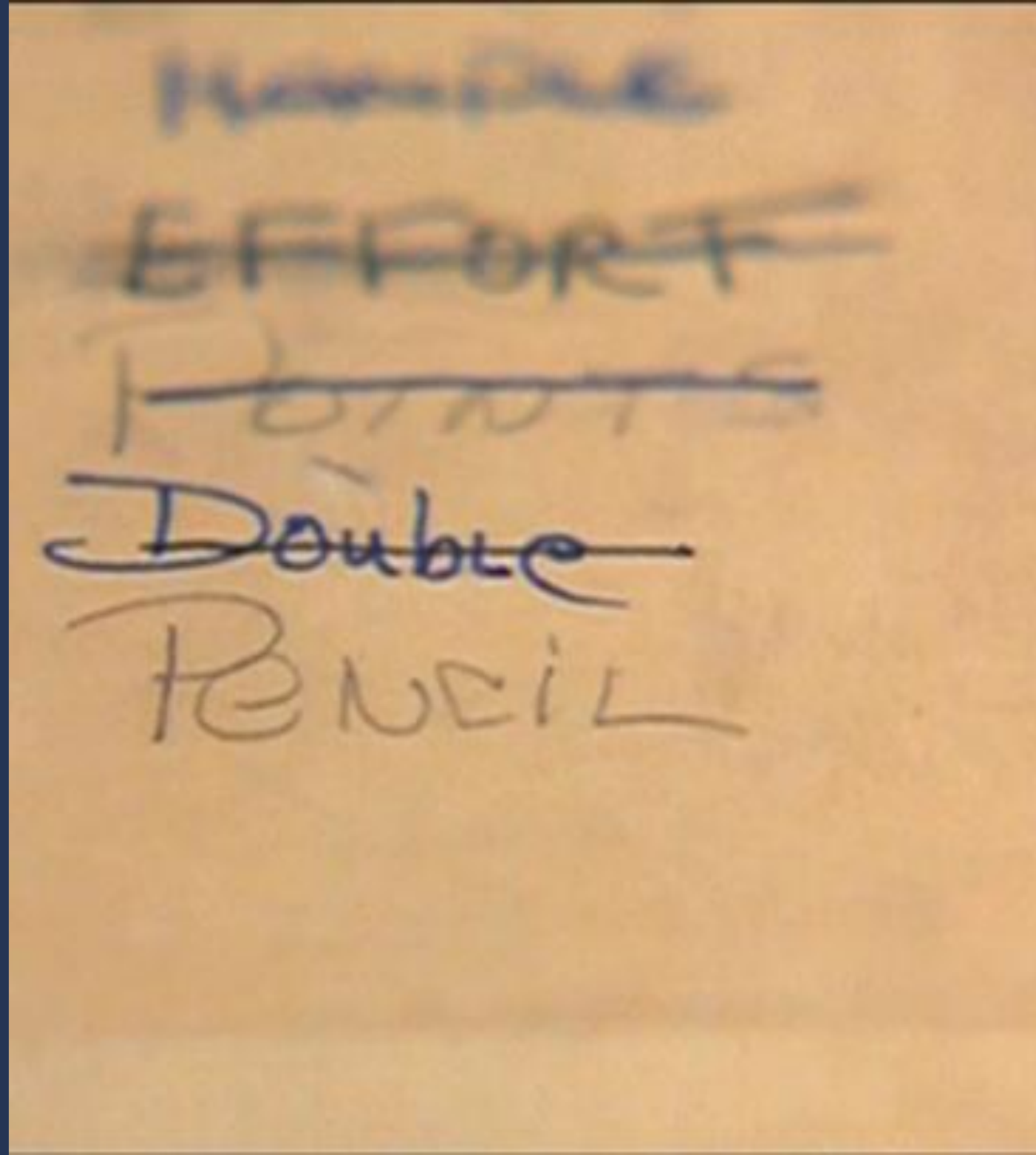
123456
password
12345678
qwerty
12345
123456789
football



2015

Ten popular passwords you need to know right now

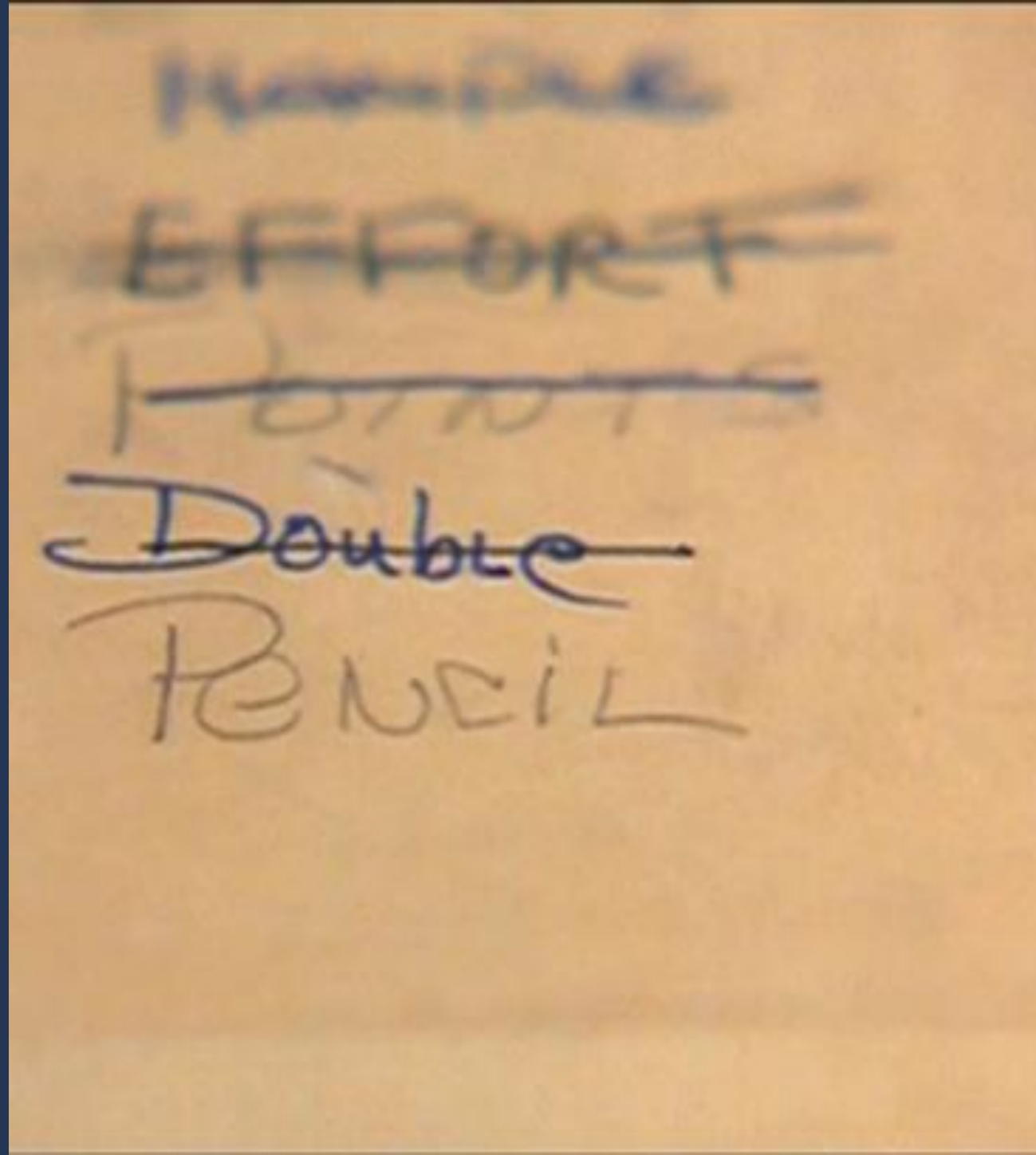
123456
password
12345678
qwerty
12345
123456789
football
1234



2015

Ten popular passwords you need to know right now

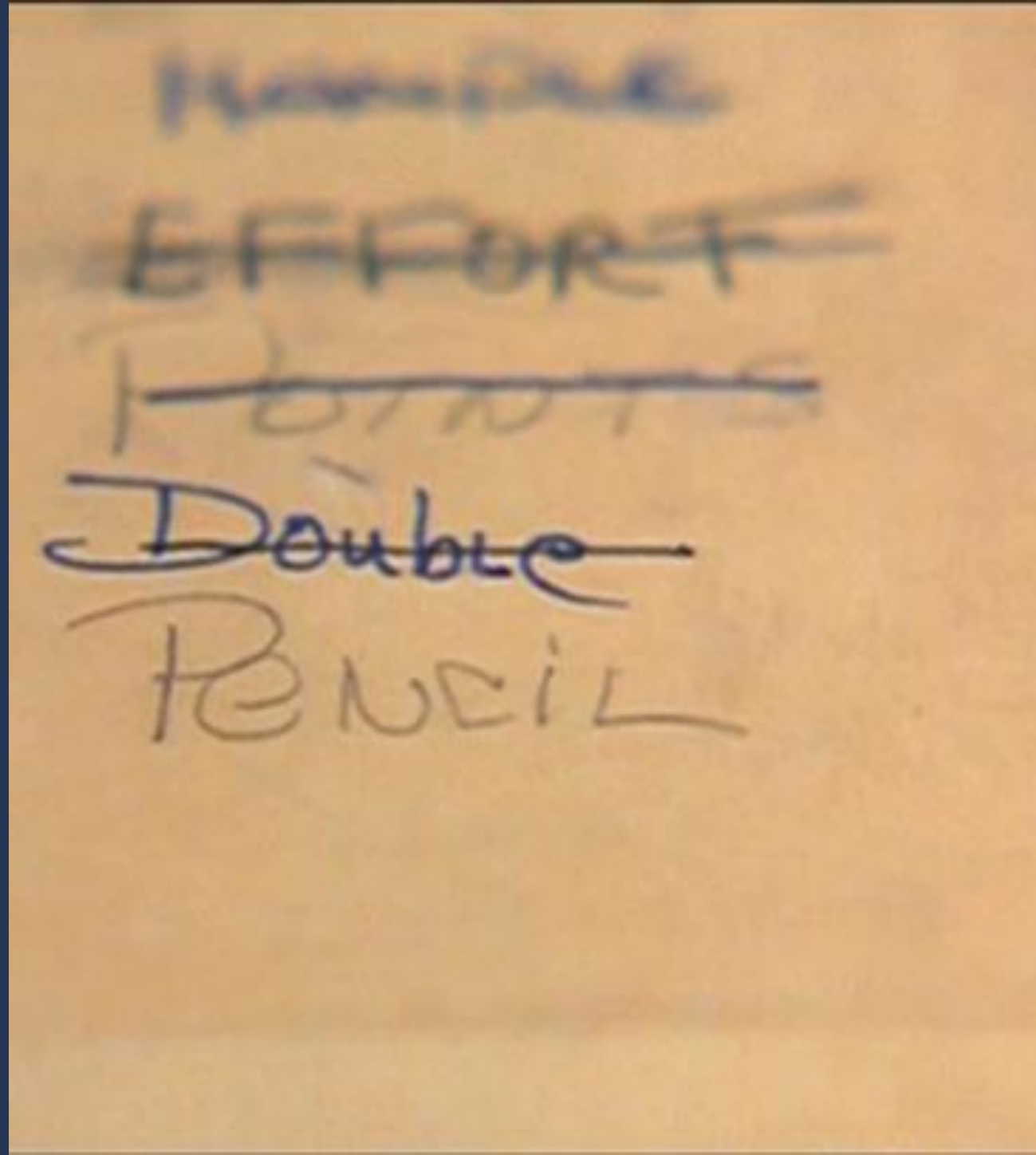
123456
password
12345678
qwerty
12345
123456789
football
1234
1234567

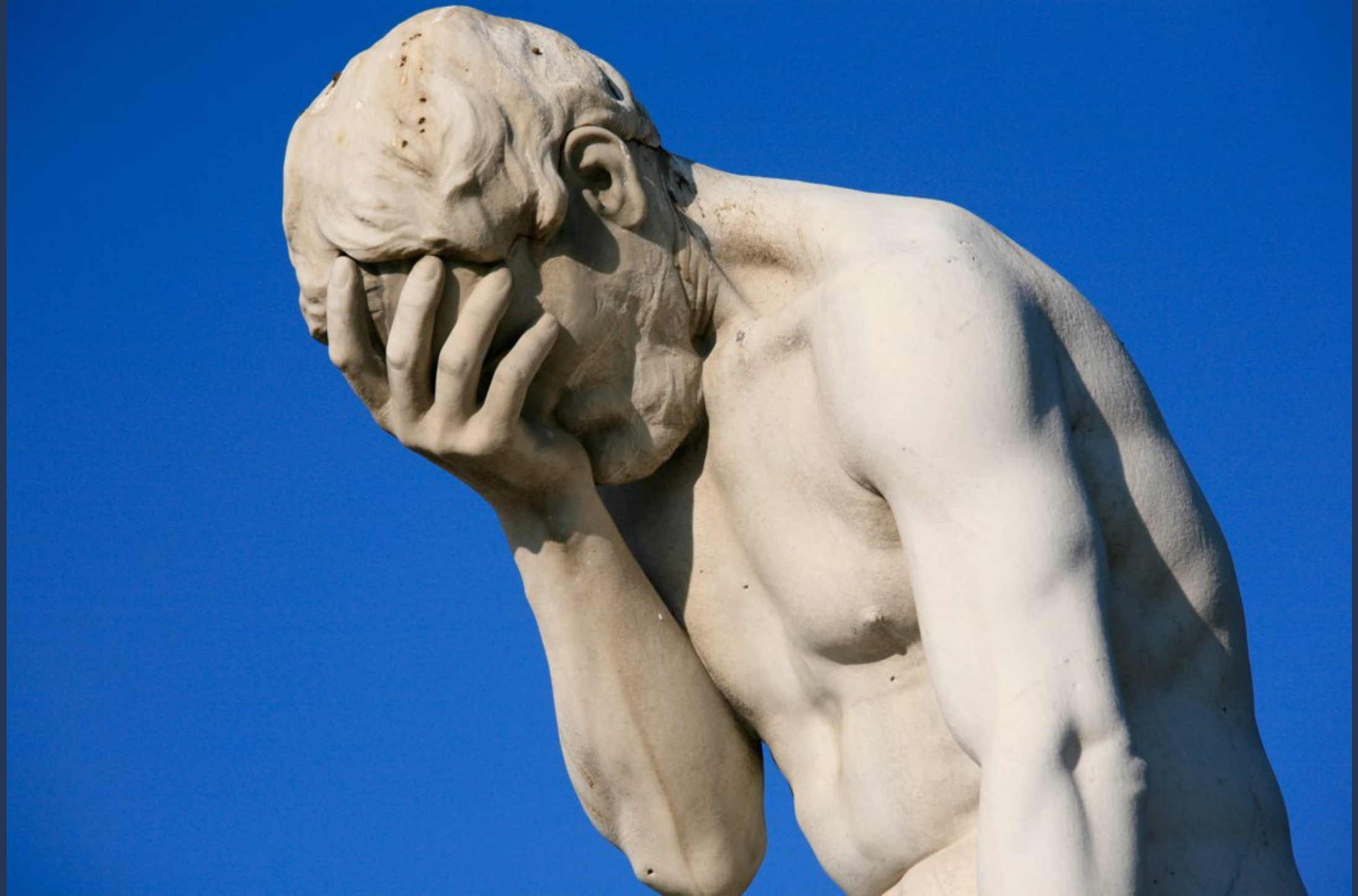


2015

Ten popular passwords you need to know right now

123456	123456789
password	football
12345678	1234
qwerty	1234567
12345	baseball





¯_(ツ)_/¯

You (human)

Your password is:

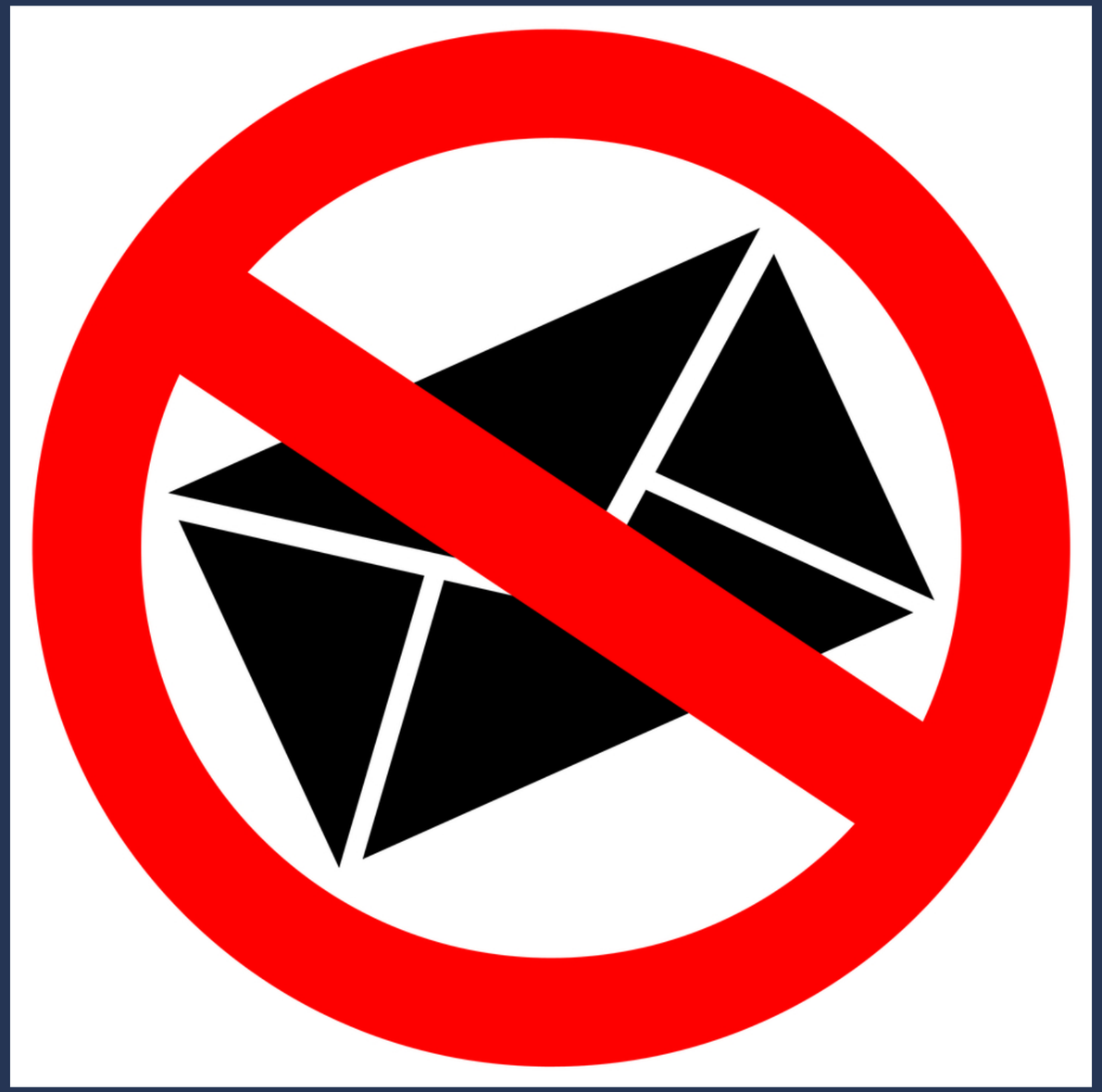
Easy to guess

Your password is:

Easy to brute-force

Your password is:

Likely to be reused



You (service)

Your service is:

Responsible

Your service is:

Trustworthy

My good opinion once lost is lost forever.

– Mr. Darcy, *Pride and Prejudice*

Your service is:

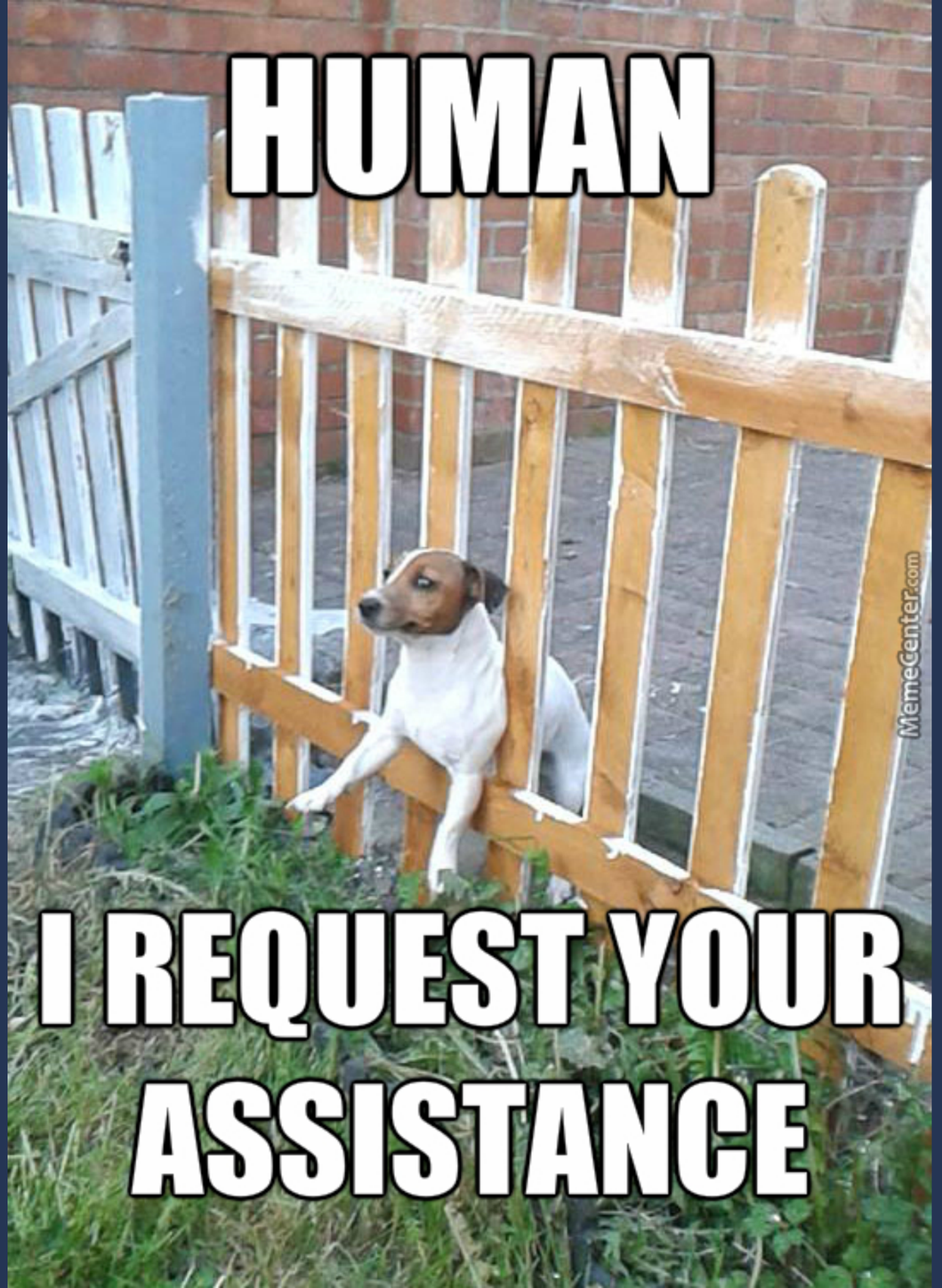
At the mercy of other services

You (pet)

SOMEONE FIGURED OUT MY PASSWORD

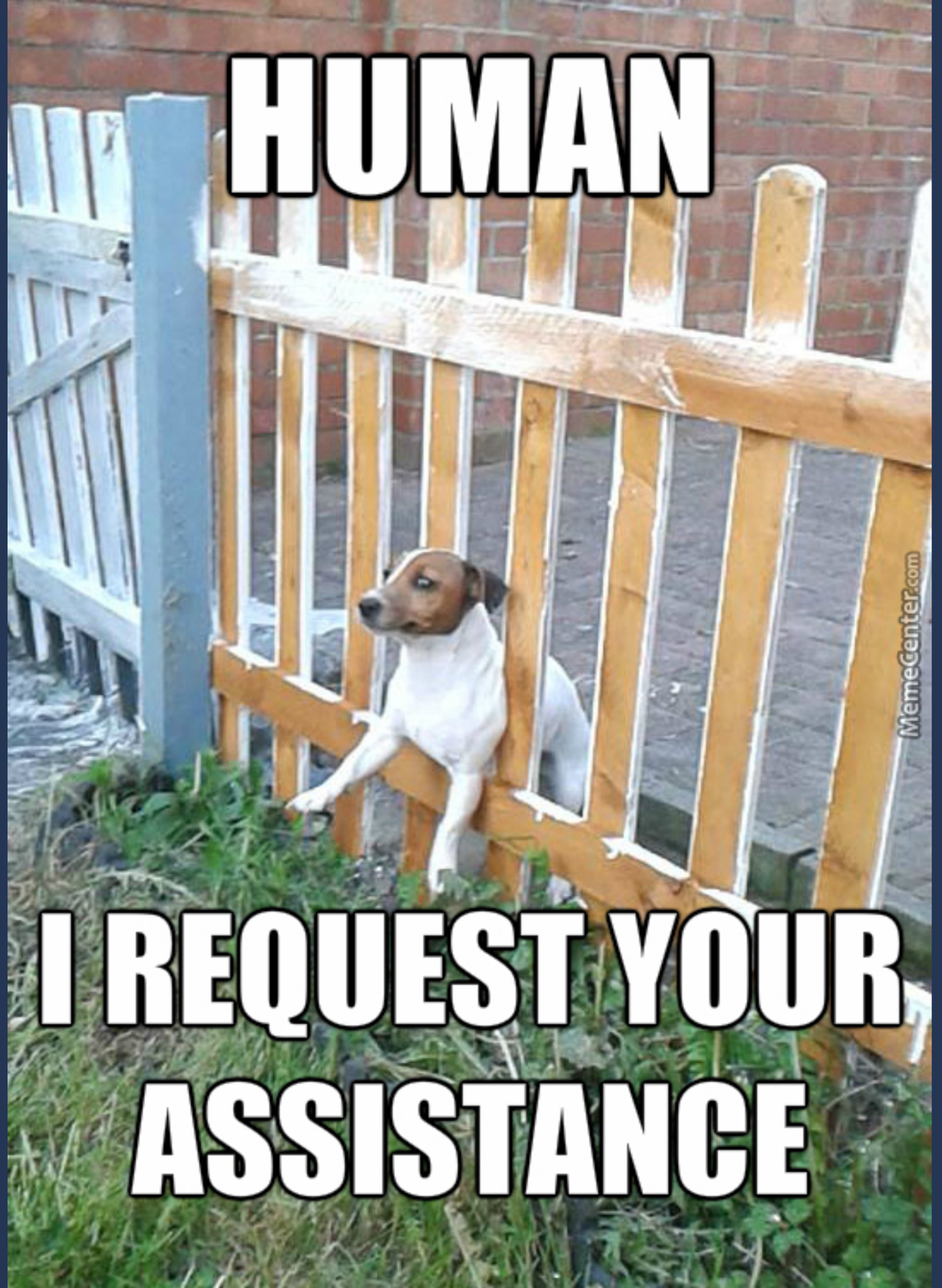
NOW I HAVE TO RENAME MY DOG

We can help



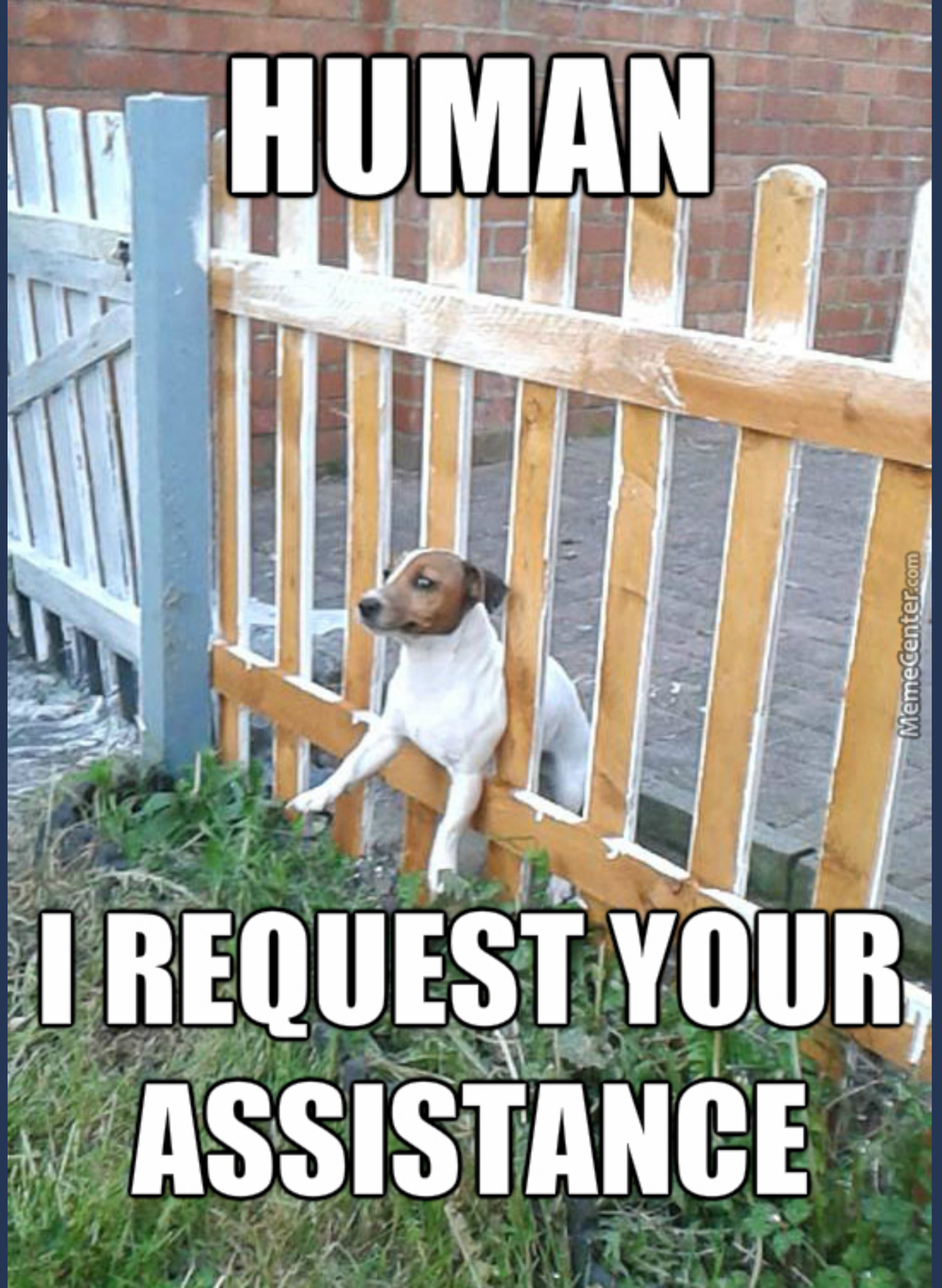
We can help

- Encourage high-quality passwords



We can help

- Encourage high-quality passwords
- Keep passwords secret



We can help

- Encourage high-quality passwords
- Keep passwords secret
- Make passwords useless

Encourage high-quality passwords

Password policies

A traditional password policy

A traditional password policy

- Must be at least 8 characters

A traditional password policy

- Must be at least 8 characters
- Must contain at least one upper-case character

A traditional password policy

- Must be at least 8 characters
- Must contain at least one upper-case character
- Must contain at least one lower-case character

A traditional password policy

- Must be at least 8 characters
- Must contain at least one upper-case character
- Must contain at least one lower-case character
- Must contain at least one number

A traditional password policy

- Must be at least 8 characters
- Must contain at least one upper-case character
- Must contain at least one lower-case character
- Must contain at least one number
- Must contain at least one symbol

No

A traditional password policy

A traditional password policy

- Good password: `P@ssword1`

A traditional password policy

- Good password: `P@ssword1`
- Bad password: `4u8zvbvabxmdx56s`

Password strength

Password strength

- Isn't about the length of a password

Password strength

- Isn't about the length of a password
- Isn't about the number of weird characters

Password strength

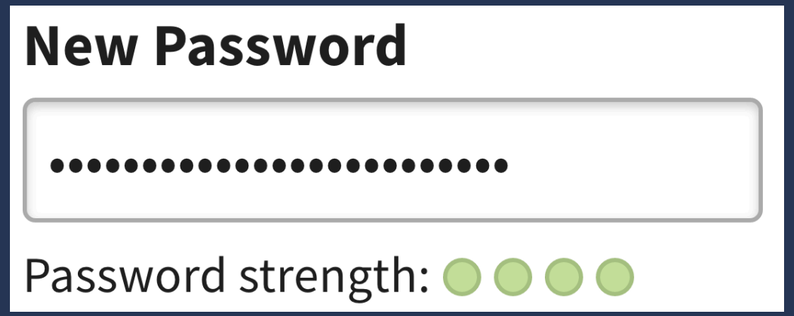
- Isn't about the length of a password
- Isn't about the number of weird characters

- Well, not exactly

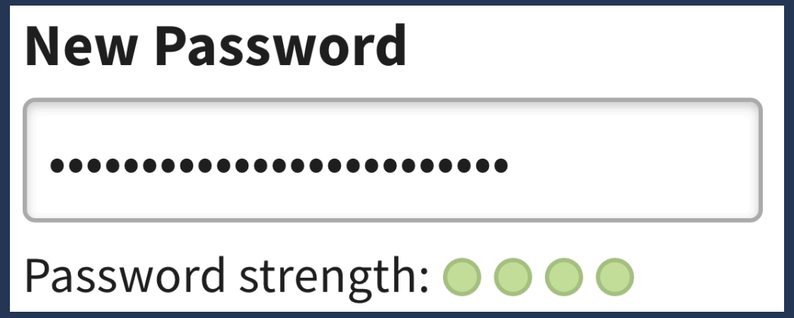
Randomness

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

Strength test

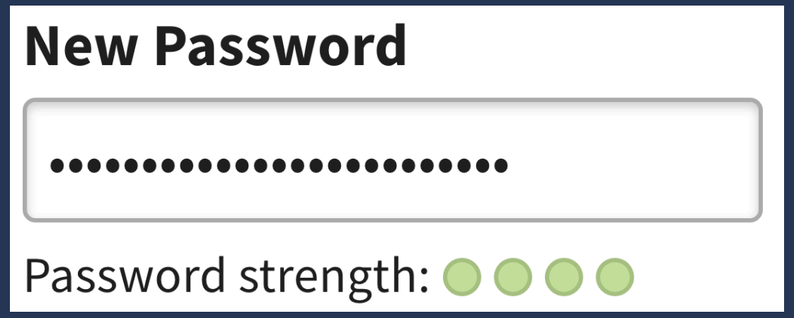


Strength test



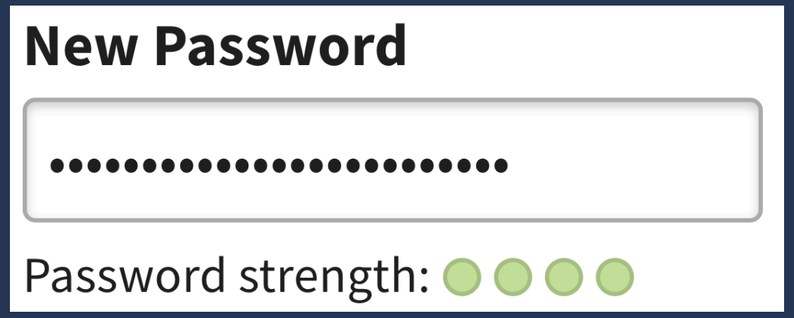
- Test the password and tell the user how strong it is

Strength test



- Test the password and tell the user how strong it is
- Considering common templates, words, sequences, etc

Strength test



- Test the password and tell the user how strong it is
- Considering common templates, words, sequences, etc
- zxcvbn by Dropbox

Keep passwords secret


ONCE MORE UNTO THE BREACH, DEAR FRIENDS
ONCE MORE
quickmeme.com

Have i been pwned?

haveibeenpwned.com

Have i been pwned?

Have i been pwned?

Have I been pwned? @haveibeenpwned — Follow

New breach: Paid-to-click site ClixSense had 2.4M user accounts exposed. 51% were already in @haveibeenpwned haveibeenpwned.com

6:09 PM - 11 Sep 2016

32 12

Have I been pwned? @haveibeenpwned — Follow

New breach: Gaming news site DLH had 3.3M user accounts hacked in July. 20% were already in @haveibeenpwned haveibeenpwned.com

9:47 AM - 8 Sep 2016

26 13

Have I been pwned? @haveibeenpwned — Follow

New breach: Flash Flash Revolution had 1.8M user accounts hacked in February. 61% were already in @haveibeenpwned haveibeenpwned.com

7:25 PM - 6 Sep 2016

17 12

Have I been pwned? @haveibeenpwned — Follow

New breach: The InterPals penpal website had 3.4M user accounts hacked in 2015. 40% were already in @haveibeenpwned haveibeenpwned.com

10:08 PM - 30 Aug 2016

10 5

Have I been pwned? @haveibeenpwned — Follow

New breach: Neopets had 27M unique emails leaked May. 44% were already in @haveibeenpwned haveibeenpwned.com

11:31 AM - 8 Jul 2016

61 39

Have I been pwned? @haveibeenpwned — Follow

New breach: The Facebook app "Uiggy" had 2.7M emails exposed this month. 19% were already in @haveibeenpwned haveibeenpwned.com

7:09 PM - 27 Jun 2016

50 26

Have I been pwned? @haveibeenpwned — Follow

New breach: VK had 93M emails exposed in approximately 2012. 9% were already in @haveibeenpwned haveibeenpwned.com

2:33 AM - 10 Jun 2016

47 18

Have I been pwned? @haveibeenpwned — Follow

New breach: In Jan, the Minecraft community "Lifeboat" had 7M accounts exposed. 6% were already in @haveibeenpwned haveibeenpwned.com

8:09 PM - 26 Apr 2016

83 65

Have I been pwned? @haveibeenpwned — Follow

New breach: In Feb, Mate1 had 27M accounts with deeply personal info exposed. 14% were already in @haveibeenpwned haveibeenpwned.com

5:20 PM - 15 Apr 2016

29 10

How can we help people impacted by data breaches without making life worse for them?

– Troy Hunt, Have i been pwned?

Your opponent

Your opponent

has:

Your opponent has:

- Stored password (hashes)

Your opponent has:

- Stored password (hashes)
- Email address / username

Your opponent has:

- Stored password (hashes)
- Email address / username
- Other personal info
  - Physical address
  - Payment details
  - Actual content
  - Control of your account
  - ...

Your opponent

wants:

Your opponent wants:

- Plaintext password

Your opponent

needs:

Your opponent needs:

- Time

Your opponent needs:

- Time
- Money

Hash functions

Choosing a hash function

Choosing a hash function

- Cryptographic hash functions
  - Pre-image resistance
  - Second pre-image resistance
  - Collision resistance

Choosing a hash function

- Cryptographic hash functions
  - Pre-image resistance
  - Second pre-image resistance
  - Collision resistance
- Key-derivation function
  - Produces a high-randomness output from a low-randomness input
  - Slow 👍

Speed test

Speed test

- "Bad" functions
  - sha512 203252/s
  - sha256 456621/s
  - sha1 512821/s
  - md5 2173913/s

Speed test

- "Bad" functions
  - `sha512  203252/s`
  - `sha256  456621/s`
  - `sha1  512821/s`
  - `md5  2173913/s`
- "Good" functions
  - `bcrypt  14.9/s`
  - `scrypt  21.7/s`
  - `pbkdf2  21.8/s`

Further reading


I got pwned!

You've been pwned!

You signed up for notifications when your account was pwned in a data breach and unfortunately, it's happened. Here's what's known about the breach:

Breach:	Last.fm
Date of breach:	22 Mar 2012
Number of accounts:	37,217,682
Compromised data:	Email addresses, Passwords, Usernames, Website activity

n8mlyF75wPjFP0K1

udvrcqt3wk3headj

Your password is not strong enough. New passwords must:

- Be at least six characters long
- Contain one or more numbers
- Include at least one of the following special characters: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~, or a space

Make passwords useless

Two-factor authentication

Something you know

Something you have

Something you have

Something you have

- Some physical thing that only you have access to

Something you have

- Some physical thing that only you have access to
- Previously registered with the account

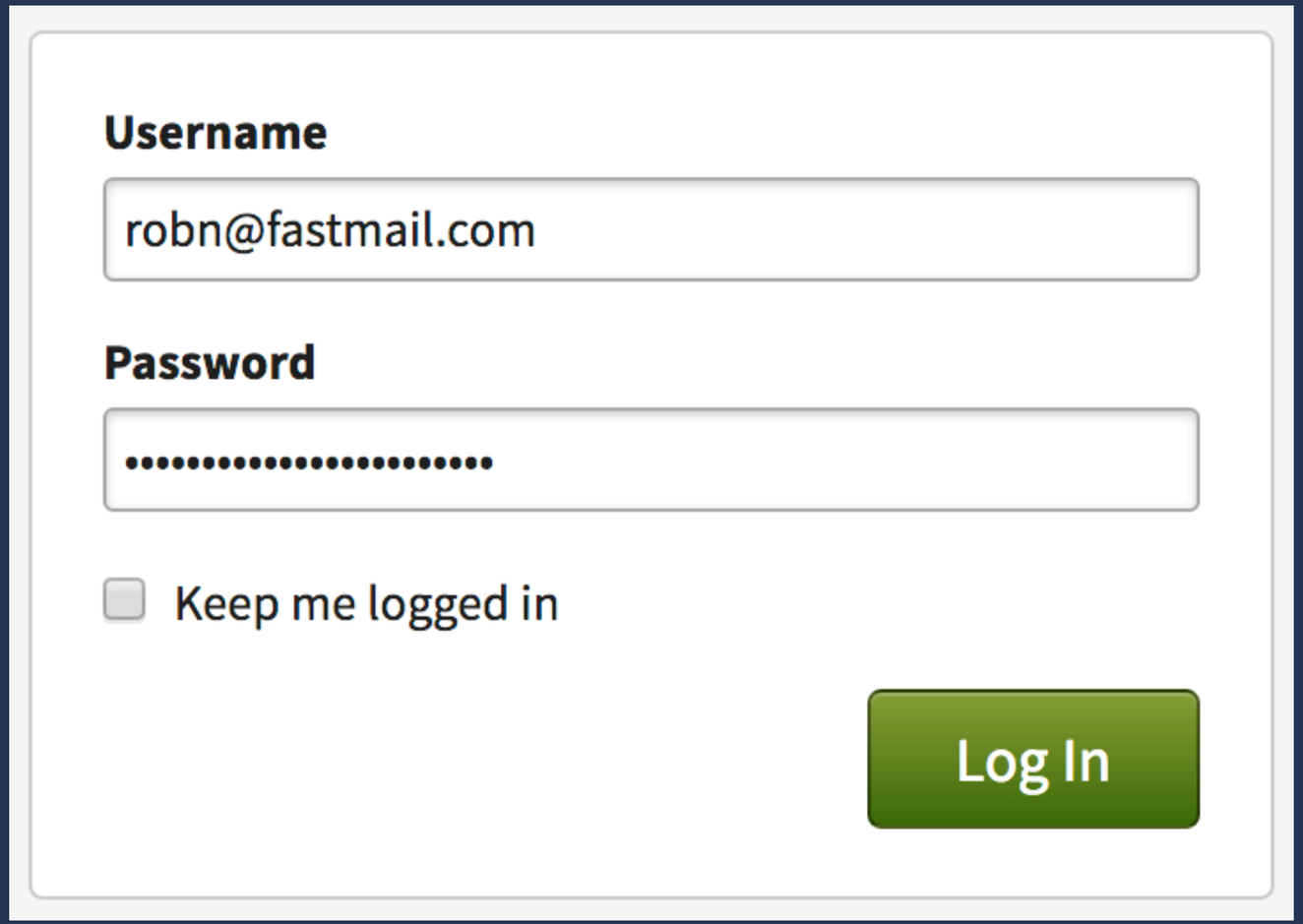
Something you have

- Some physical thing that only you have access to
- Previously registered with the account
- Your phone
  - SMS
  - TOTP

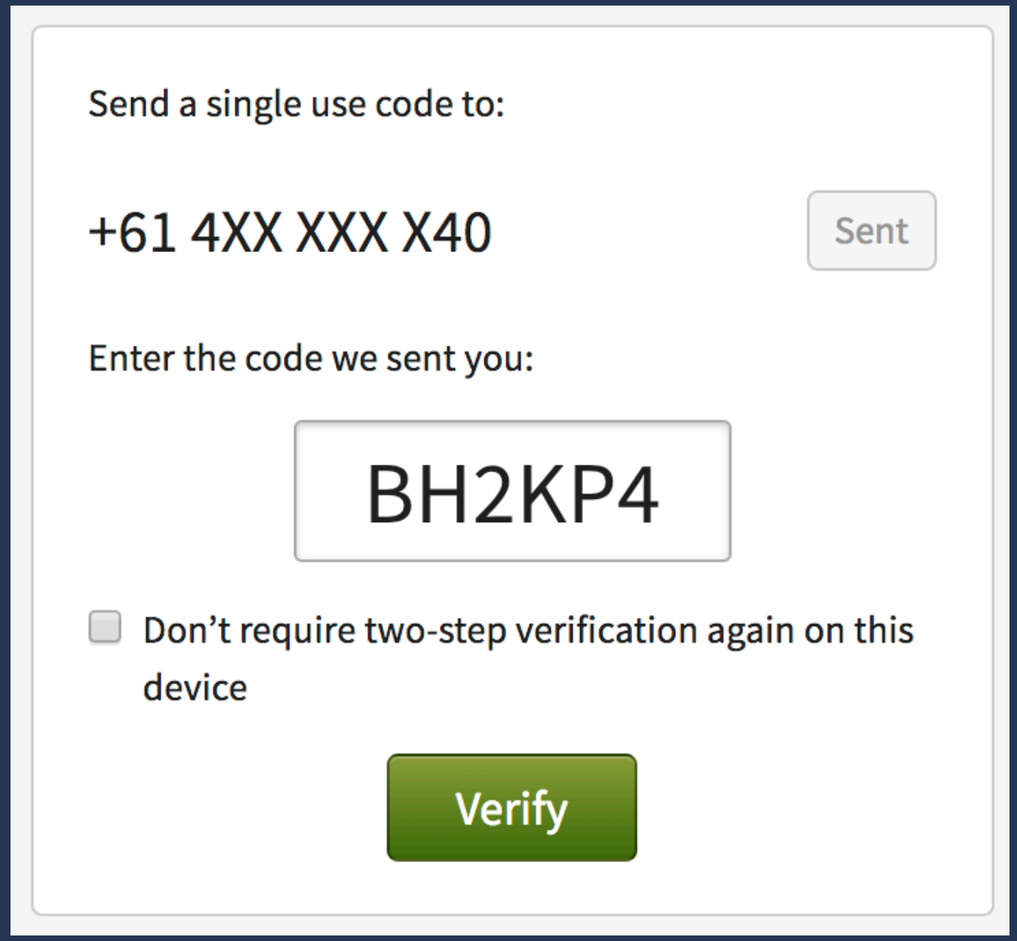
Something you have

- Some physical thing that only you have access to
- Previously registered with the account
- Your phone
  - SMS
  - TOTP
- A standalone security device
  - U2F
  - TOTP

Username & password

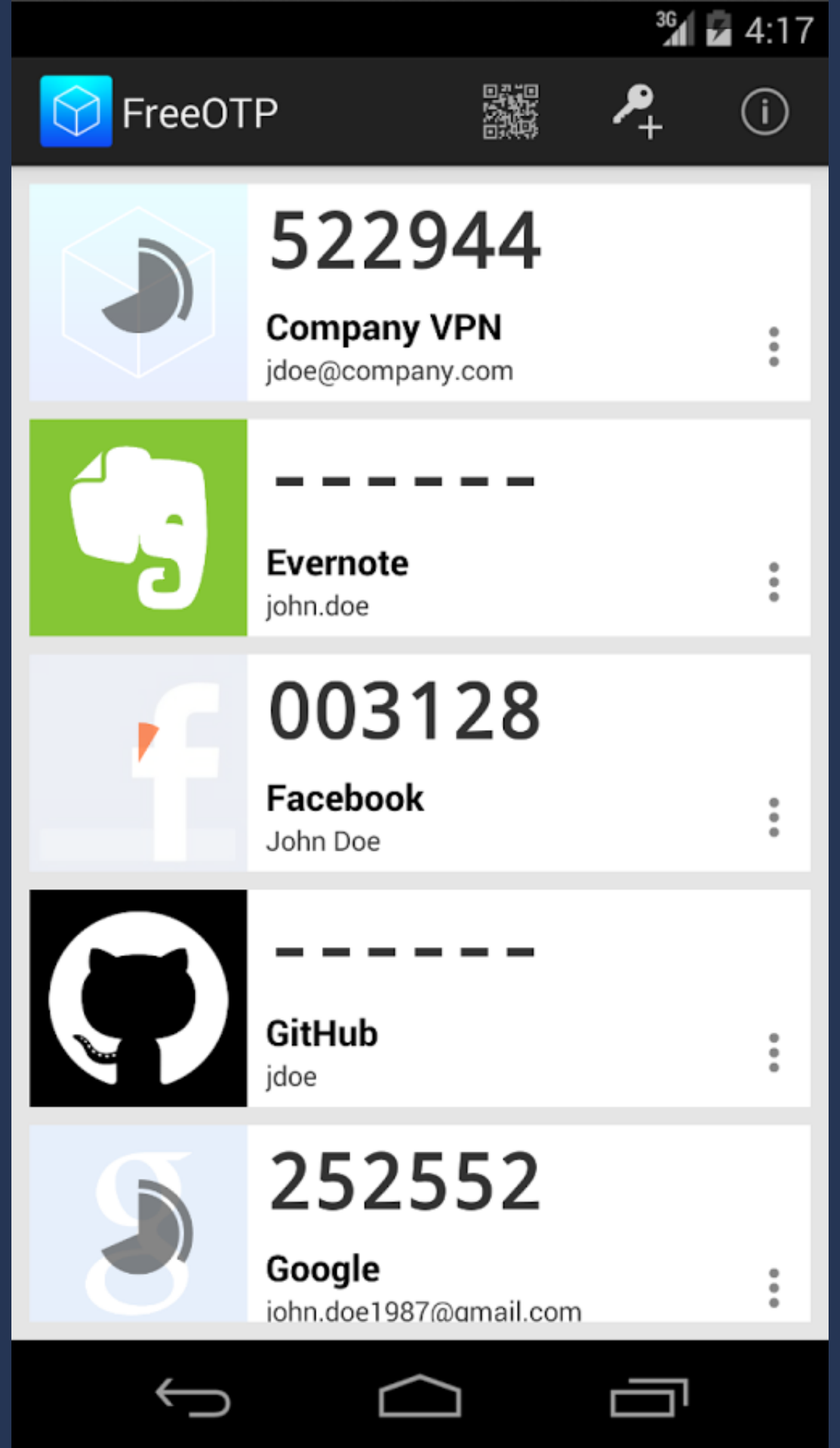


Second factor: SMS

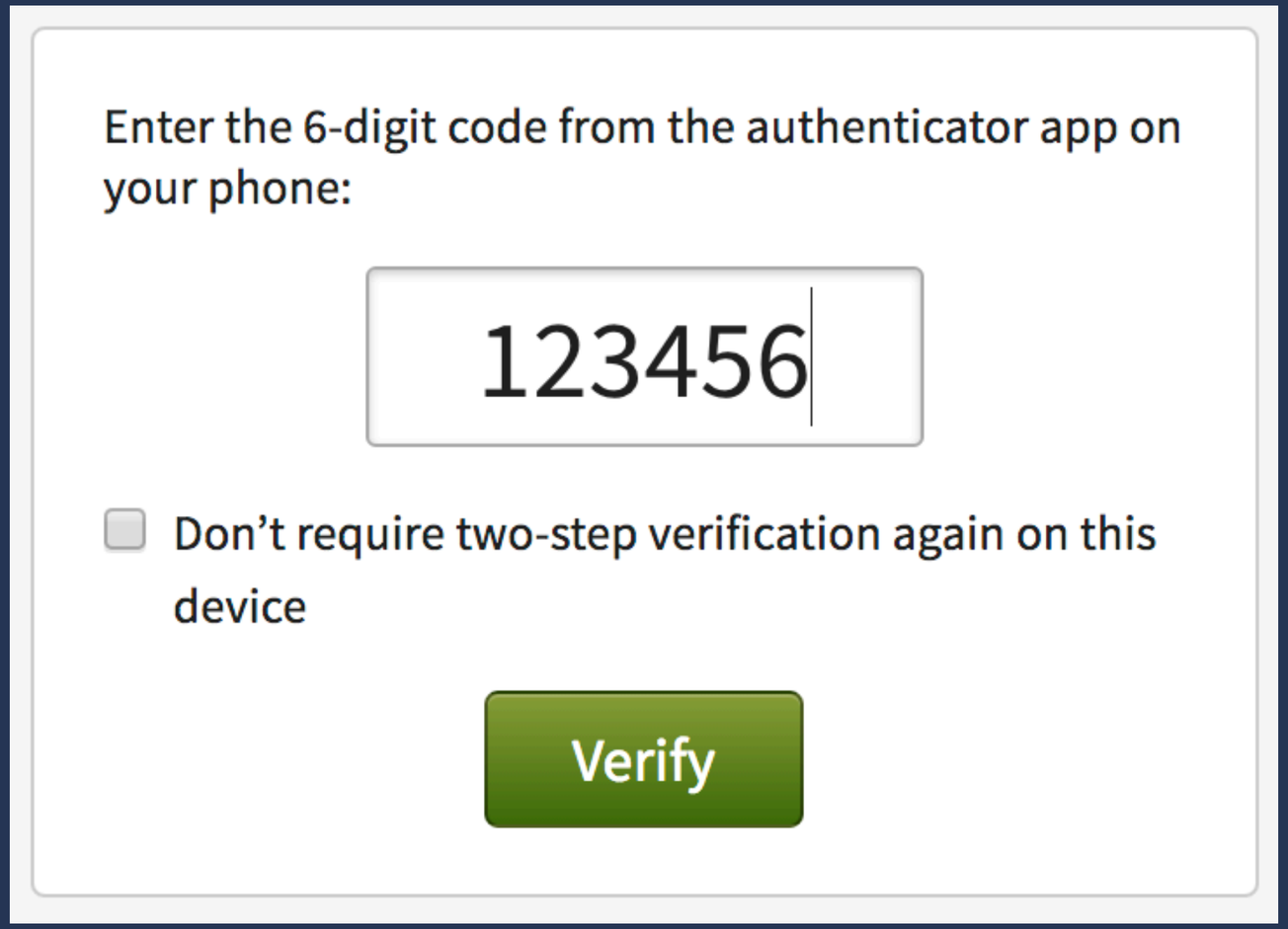


Second factor: TOTP

Second factor: TOTP

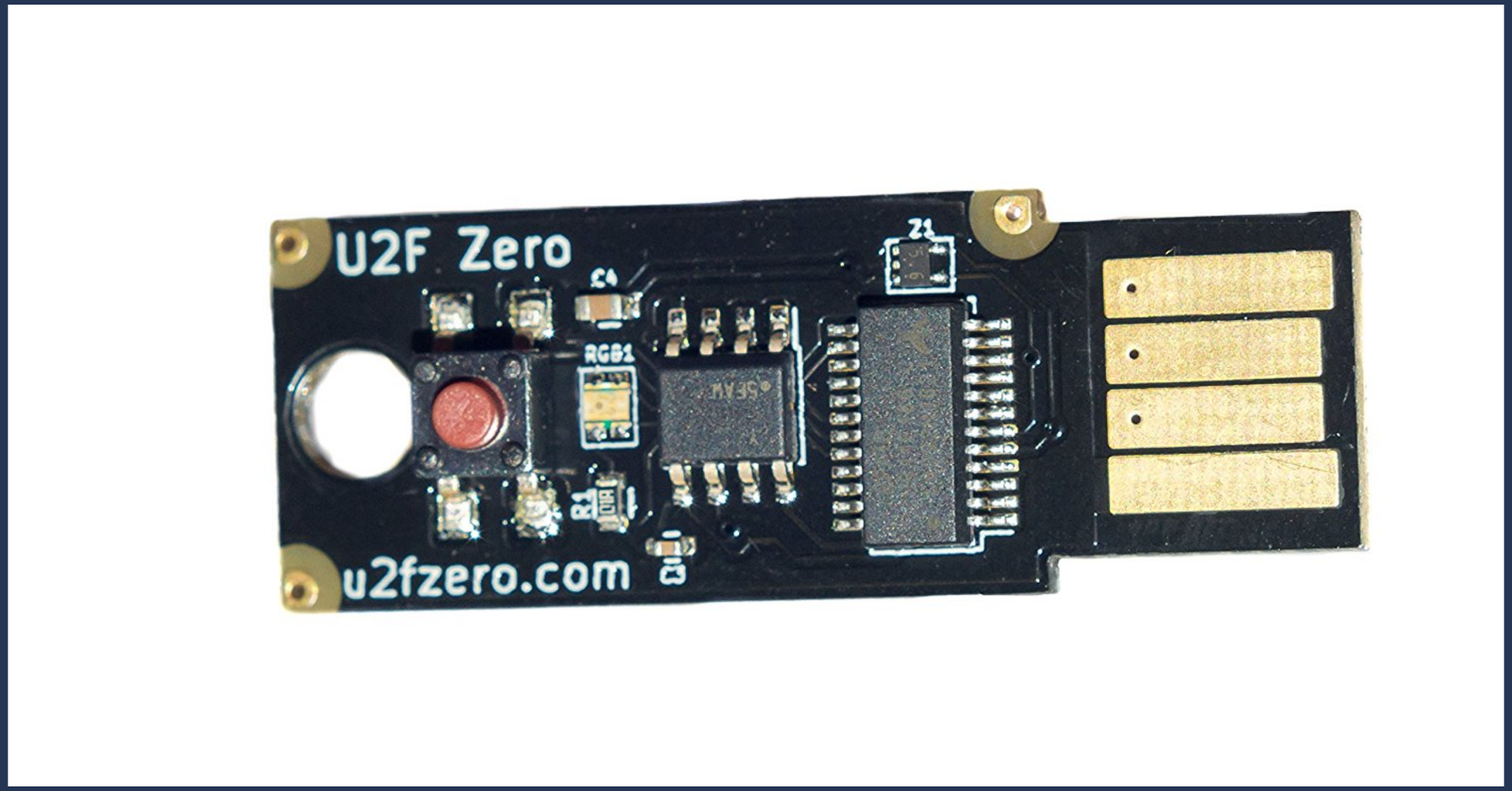


Second factor: TOTP

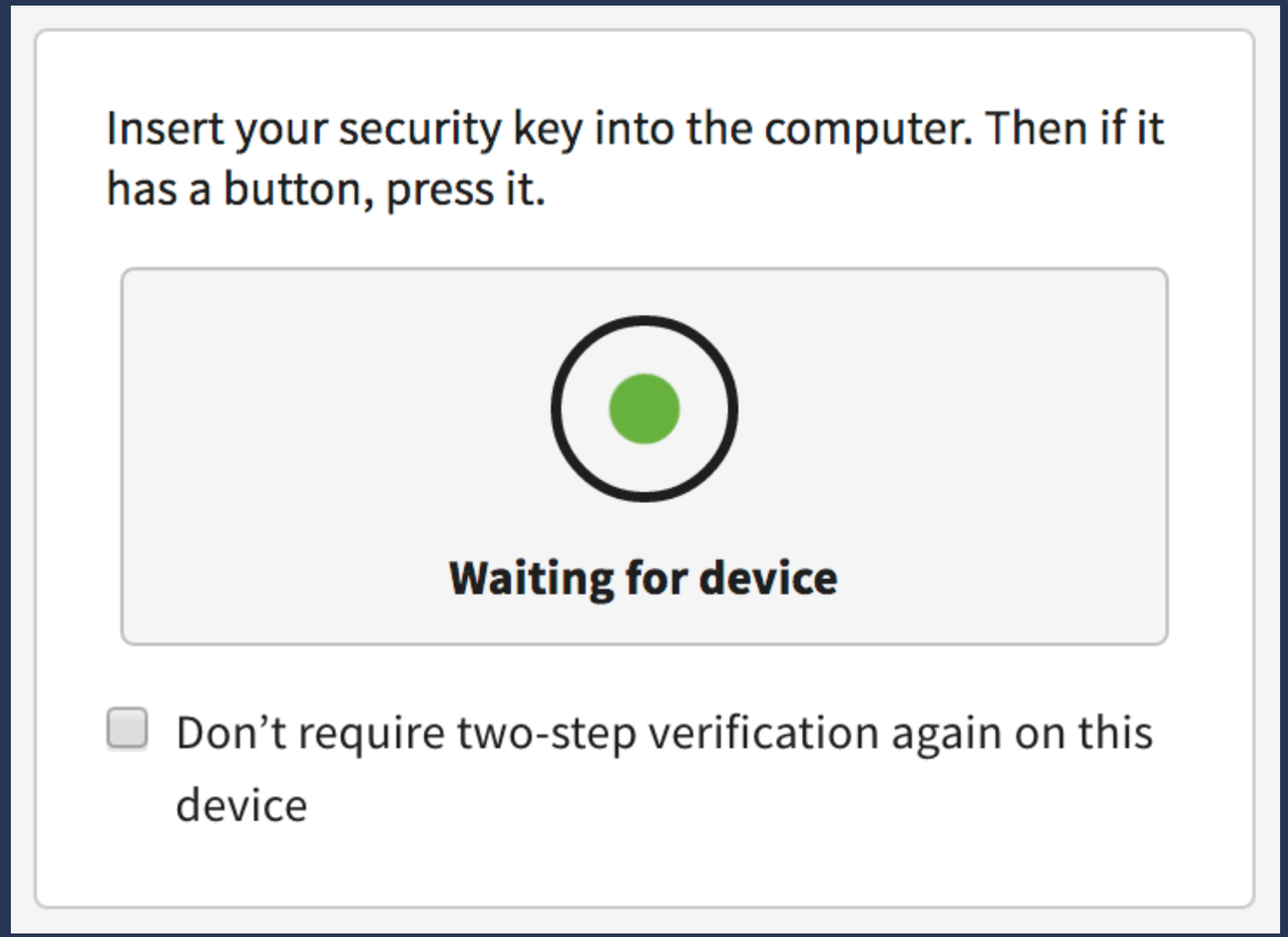


Second factor: U2F

Second factor: U2F



Second factor: U2F



Bonus prize round!

Why two-factor?

Why two-factor?

- Make the password useless by itself

Why two-factor?

- Make the password useless by itself
- Even when leaked or stolen

Why two-factor?

- Make the password useless by itself
- Even when leaked or stolen
- But make the second factor do nothing by itself

Why two-factor?

- Make the password useless by itself
- Even when leaked or stolen
- But make the second factor do nothing by itself
- So you can lose your phone but still keep your account safe

We helped!

We helped!

We helped!

- High-quality passwords
  - Sensible password policy and strength feedback to user

We helped!

- High-quality passwords
  - Sensible password policy and strength feedback to user
- Passwords stored securely
  - Good hash function with salts

We helped!

- High-quality passwords
  - Sensible password policy and strength feedback to user
- Passwords stored securely
  - Good hash function with salts
- Passwords not the whole story
  - Two-factor authentication

Passwords are terrible

Th@nk yOu!

Th@nk y0u!

(don't forget your U2F key)