HI!

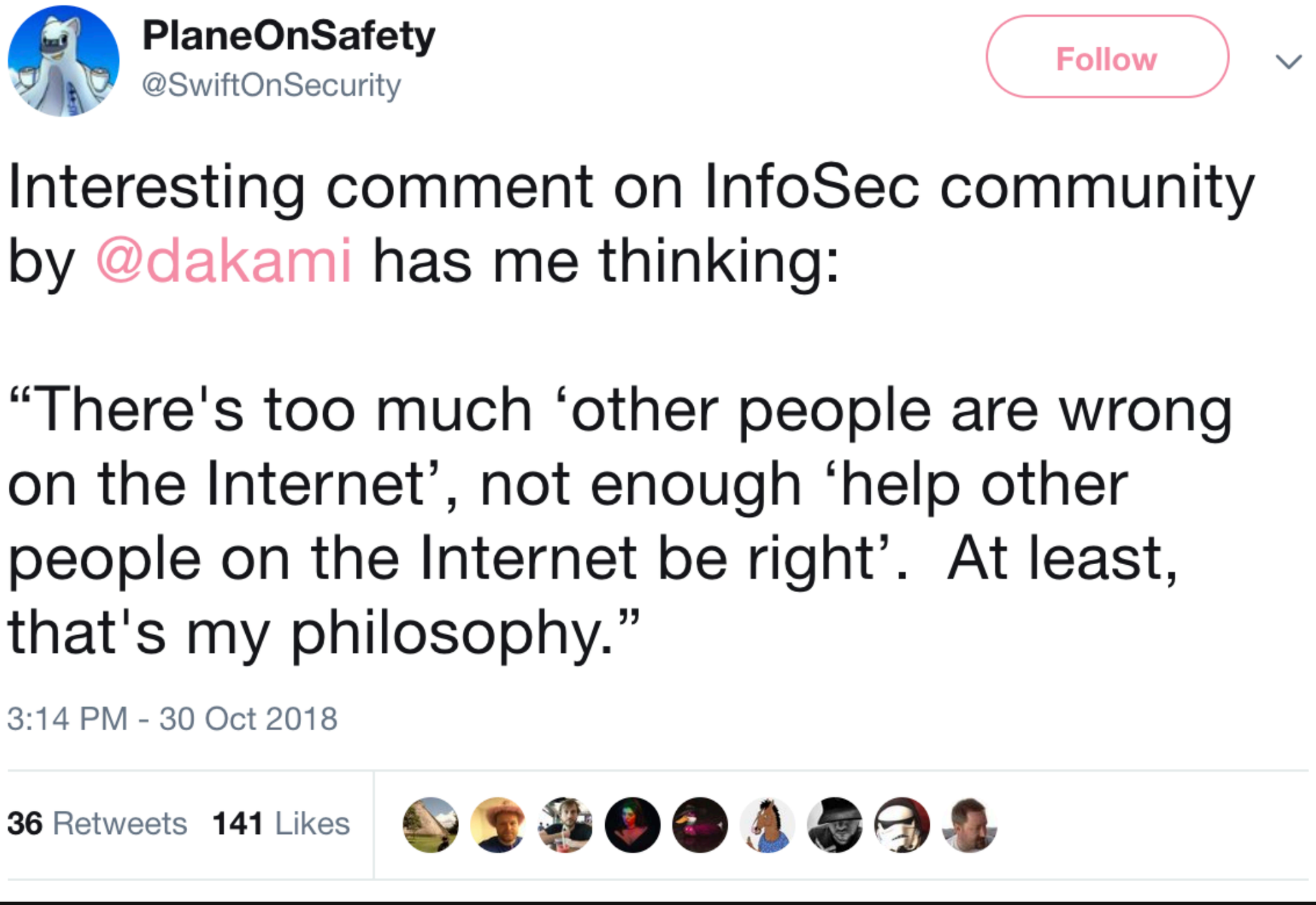
MY NAME IS:

James Bennett · @ubernostrum

(and this talk was presented November 4th 2018 at North Bay Python)

FALSEHOODS PROGRAMMERS BELIEVE ABOUT USERNAMES

FALSEHOODS PROGRAMMERS BELIEVE ABOUT USERNAMES



https://twitter.com/swiftonsecurity/status/1057395418760429568

(((Rachel Blum)))
@groby

Follow

Hey, here's another one for the "basic algorithms are harmless, my work has no political meaning" crowd.

All it takes to block 53K voters is to change the rules of string matching. But sure, your work is not having any political impact.

> **Ed Boo-mila** @gin_and_tacos
> Exact Match rules are racist. Full stop. They reject, for example, Quinones / Quiñones, or Smith Williams / Smith-Williams. Also filters out formal surnames (eg Diaz vs Diaz de Delgado)…

7:34 AM - 11 Oct 2018

https://twitter.com/groby/status/1050394295360843777

IDENTIFIERS ARE HARD.

Your number is 078-05-1120.

Maybe write it down and keep it in your wallet.

➤ /users/12345/
➤ /users/23456/
➤ /users/34567/

spoOooOooOo00opy ěr'ə(r) ˈbäfə(ɹ...

@errbufferoverfl

Follow

"bet.(),:;<>[]\".THIS.\"one@\\
\"is\".moreexciting"@emailexamples.err
bufferoverfl.me

7:22 PM - 18 Jul 2018

https://twitter.com/errbufferoverfl/status/1019769424629207041

UNIQUENESS IS HARD.

The invention of writing may have been a bad idea.

```sql
CREATE TABLE accounts (
    id SERIAL PRIMARY KEY,
    username TEXT UNIQUE,
    password TEXT,
    email TEXT
);
```

➤ janedoe

➤ JaneDoe

```
CREATE TABLE accounts (
   id SERIAL PRIMARY KEY,
   username CITEXT UNIQUE,
   password TEXT,
   email TEXT
);
```

ß ➡ ẞ *or* SS

ij ➡ IJ *never* Ij

Σ ➡ σ *or* ς

i ➡ I *or* İ

I ➡ i *or* ı

➤ javier_báez

b\u00e1ez

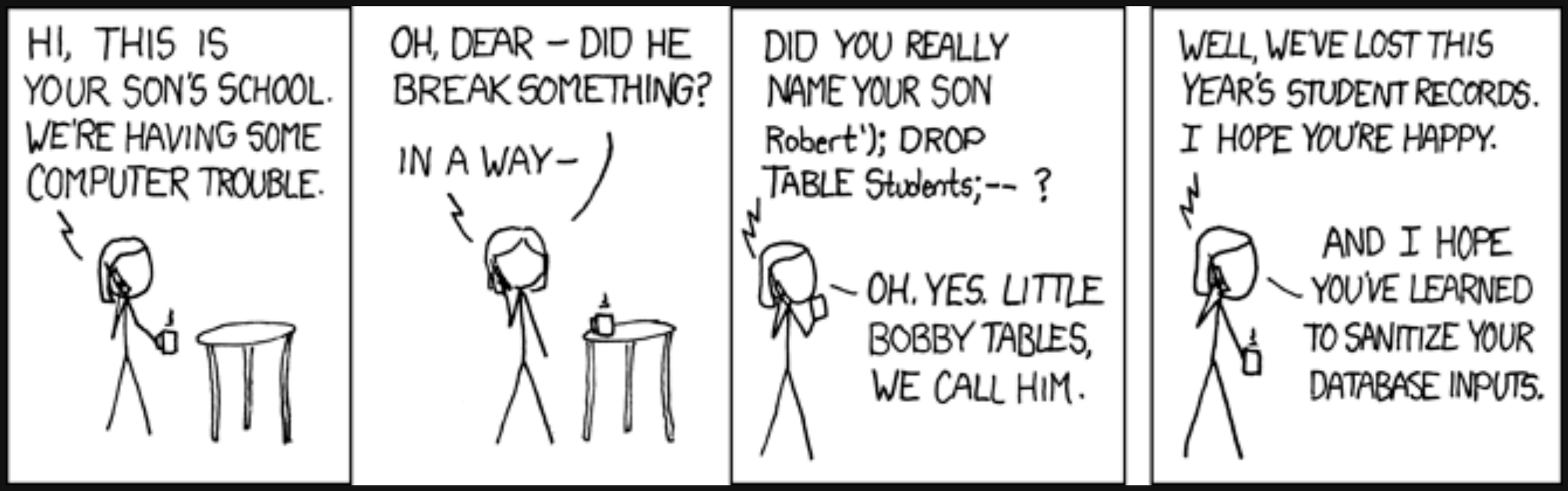
ba\u0301ez

```
from unicodedata import normalize

# The unicodedata module exists in
# Python 2 and 3.
# The casefold() method of strings
# is only in Python 3.

username_for_comparison = normalize(
    'NFKC', username
).casefold()
```

- janedoe@example.com
- JaneDoe@example.com
- jane.doe@example.com

SECURITY IS HARD.

Let's go shopping…
with someone else's credit card!



https://xkcd.com/327/

➤ jane_doe

➤ jane_doe

jane_doe

j\u0430ne_doe

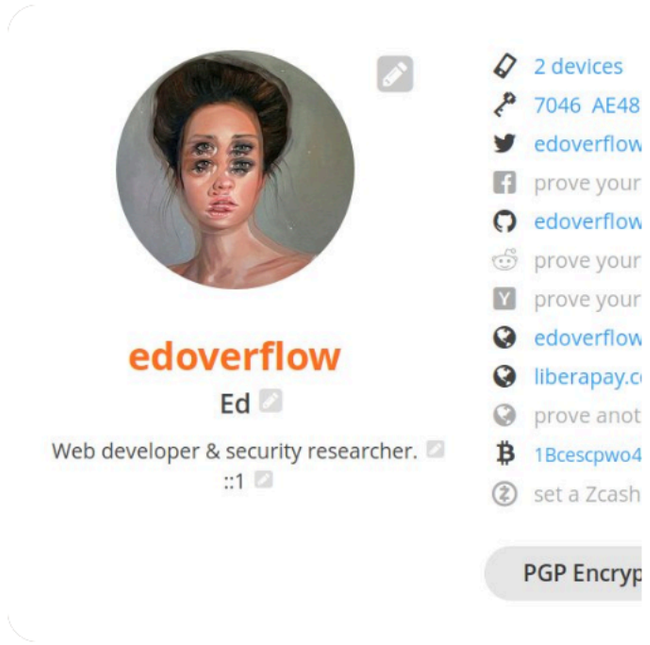
```
$ pip install confusable_homoglyphs

from confusable_homoglyphs import confusables

if confusables.is_dangerous(username):
    # Reject the username here.
    # If you're checking an email address,
    # first split it into local-part and
    # domain, and check those individually.
```

```
➤  jane_doe ➡ /users/jane_doe/
➤  login ➡ /users/login/
```

Ed
@EdOverflow

Follow

I claimed ownership of liberapay.com on Keybase by creating a user called "keybase.txt" and placing the verification snippet in the profile's description. ¯_(ツ)_/¯



12:50 PM - 18 Jan 2018

269 Retweets **634** Likes

https://twitter.com/EdOverflow/status/954093588362809345

```
➤ jane_doe ➡ jane_doe@example.com
➤ postmaster ➡ postmaster@example.com
```

Mike Zusman, a senior consultant at security firm Intrepidus Group, agreed.

“In terms of what the CAs do, it seems like it's a bit of the old west,” he said. “It doesn't seem like anyone is holding them accountable, even when something as severe as the Comodo incident happens.”

Zusman knows about lax CA practices first hand. In 2008, he applied for an SSL certificate that would allow him to pose as the rightful operator of Microsoft's Live.com domain, which is used to logon to Hotmail and other sensitive online services. In about two hours, VeriSign subsidiary Thawte issued the credential with almost no questions asked. Zusman's sole qualification was his control of the email address sslcertificates@live.com, which was enough to convince the automated processes at Thawte that he was authorized to own the certificate.

https://www.theregister.co.uk/2011/04/11/state_of_ssl_analysis/

```
➤ jane_doe ➡ jane_doe.example.com
➤ secure ➡ secure.example.com
```

https://ldpreload.com/blog/names-to-reserve

DOING IT RIGHT IS HARD.

This is the part where I say:
“tripartite identity pattern"

http://habitatchronicles.com/2008/10/the-tripartite-identity-pattern/

DO THE RIGHT THING EVEN THOUGH IT'S HARD.

Come find me if you have questions.

Slides will be online shortly.
@ubernostrum on Twitter for the link.