

Password security

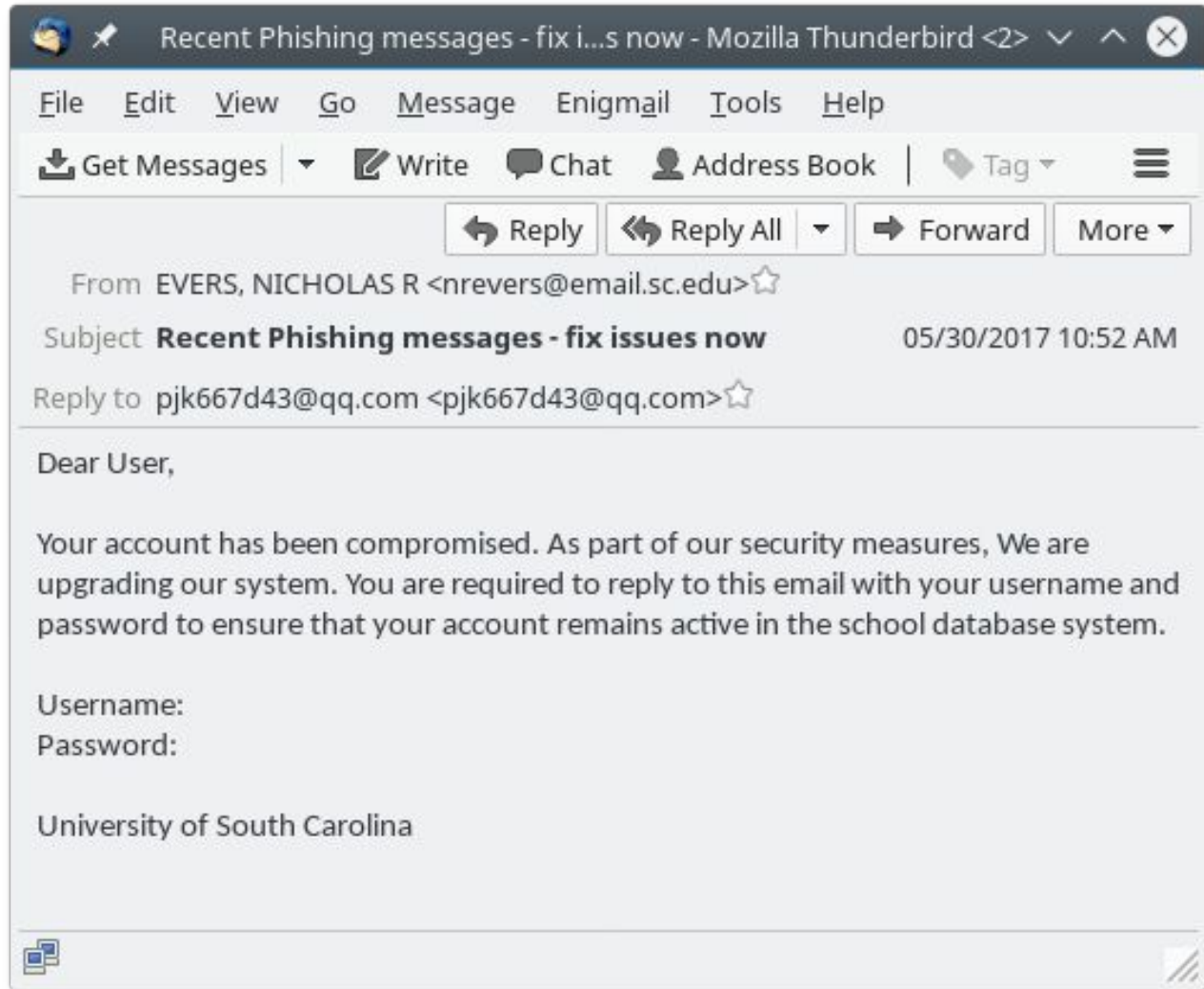
How to be smart with your passwords

How are passwords lost?

1. Phishing
2. Hacking
3. Cracking

Phishing

1. Check question
 - Is it reasonable?
 - Would an office ask for this?
2. Check source address
3. Check reply-to address
4. Check signature
 - Does it look real?
 - Was it sent with the University logo?



Hacking

- A [quarter](#) of Google users have had passwords stolen
- [140 million](#) SSNs were lost in Equifax breach
- DNC [breached](#) during 2016 election

For users:

- Don't reuse passwords
- Use sites that store [salted hashes](#)
- Change passwords if they're leaked

For websites:

- Salt and hash!!
- Keep passwords server-side
- Validate posts to avoid XSS
- Randomise cookies (and make them long)
- Randomise open urls (if applicable)

Cracking

[Automated tools](#) freely available

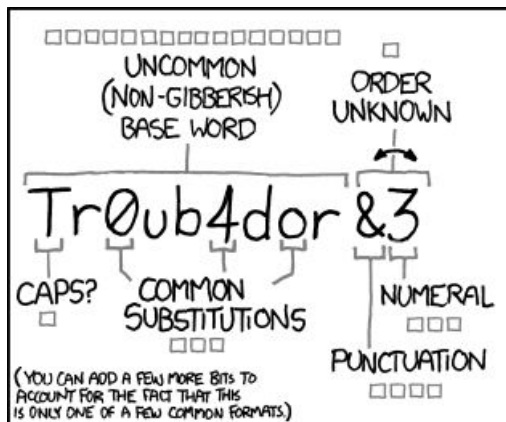
Works like this:

1. Try common passwords
2. Try variations to common passwords
3. Try words in the dictionary
4. Try random numbers and symbols

Only way to prevent is strong passwords, aka '[password entropy](#)', and 'lockouts' if service is online

Entropy

Source:
<https://www.xkcd.com/936/>



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

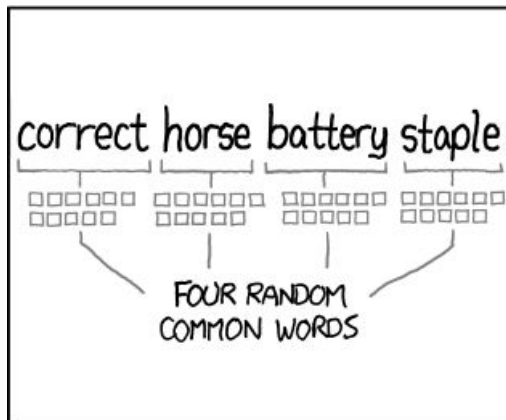
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS:
EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O's WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER:
HARD



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS:
HARD

THAT'S A BATTERY STAPLE.

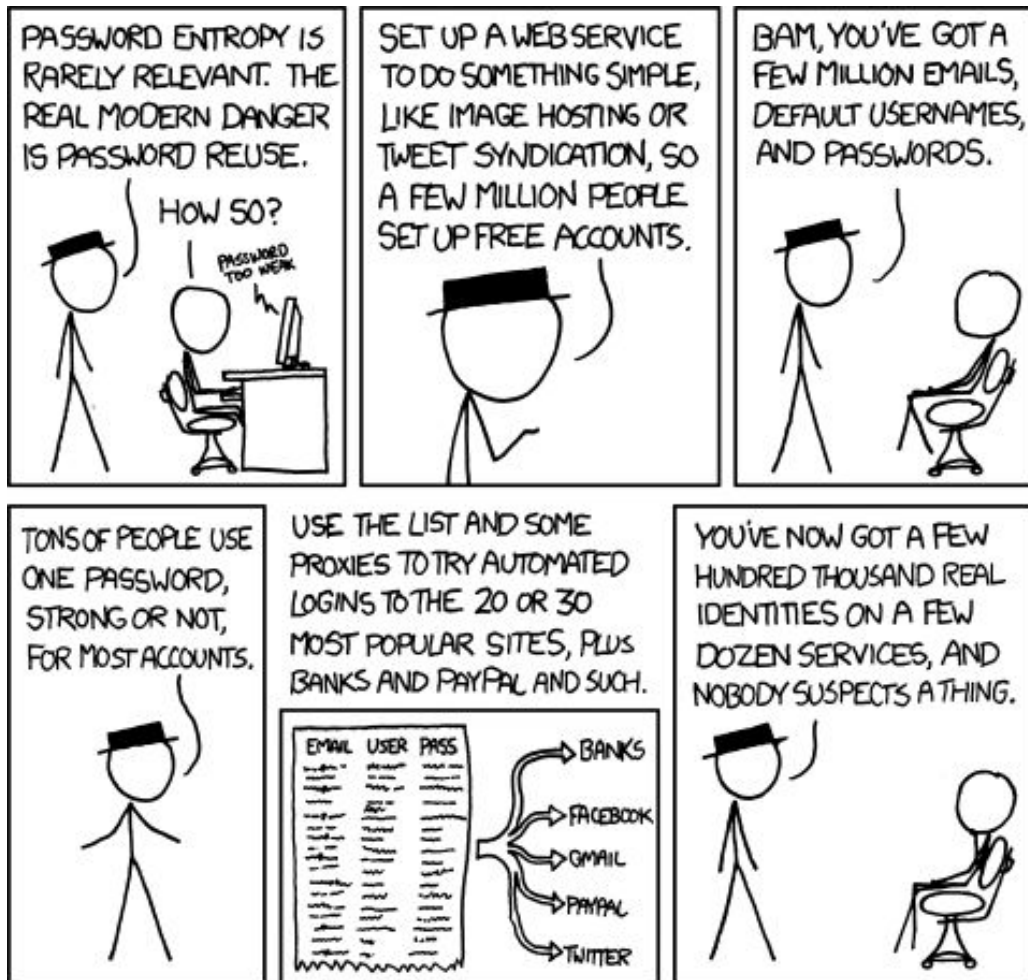
CORRECT!

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.

Reuse

Source: <https://www.xkcd.com/792/>



Password managers

Pros

- Stronger passwords
- Less reuse
- Convenient for users
- Encrypted at rest

Cons

- Master password can't be reset

Choices

- Keepass ([Windows](#), [Linux/Mac](#))
- [LastPass](#)
- A word document saved to your network drive (bad)