Password security

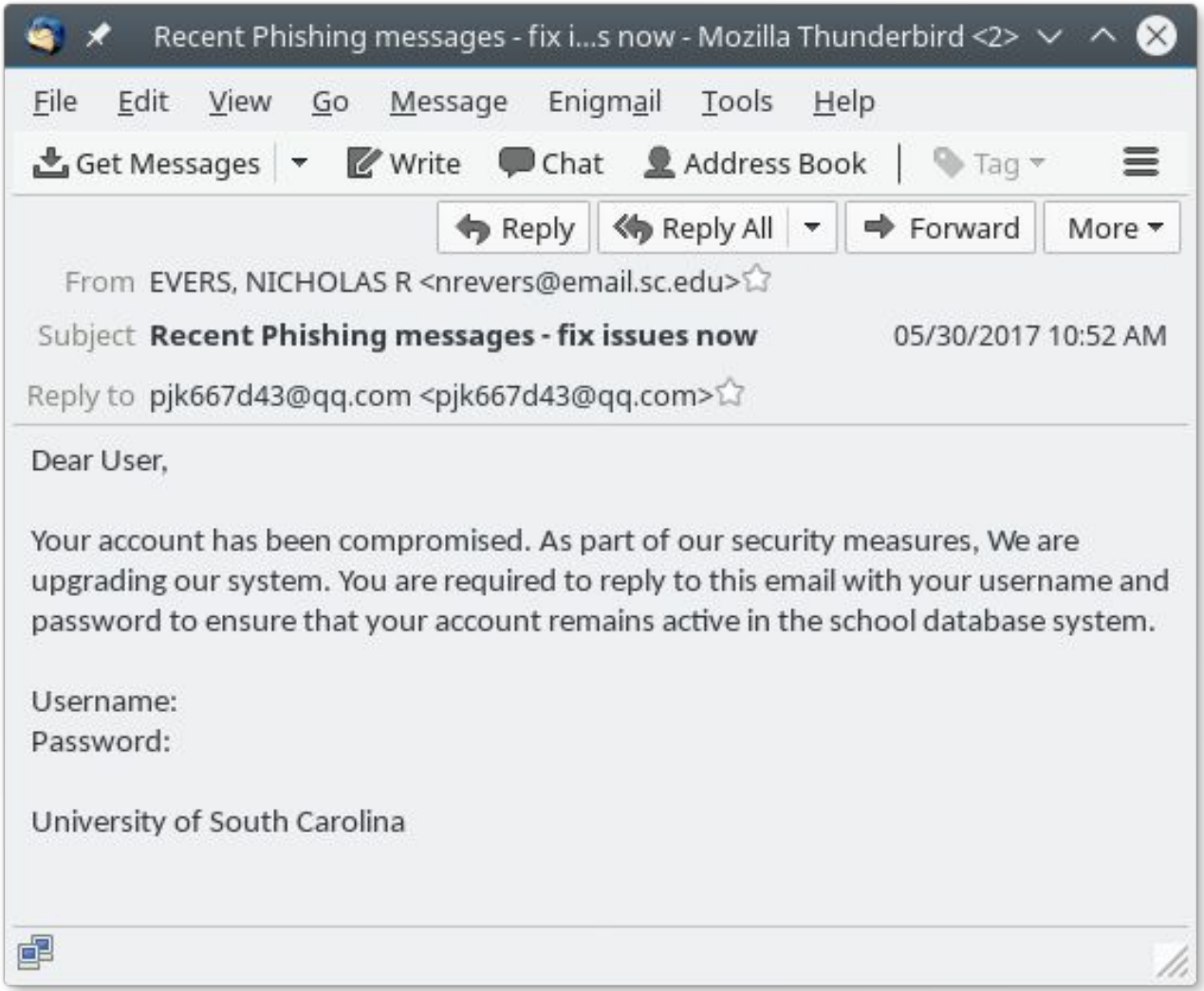
How to be smart with your passwords

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

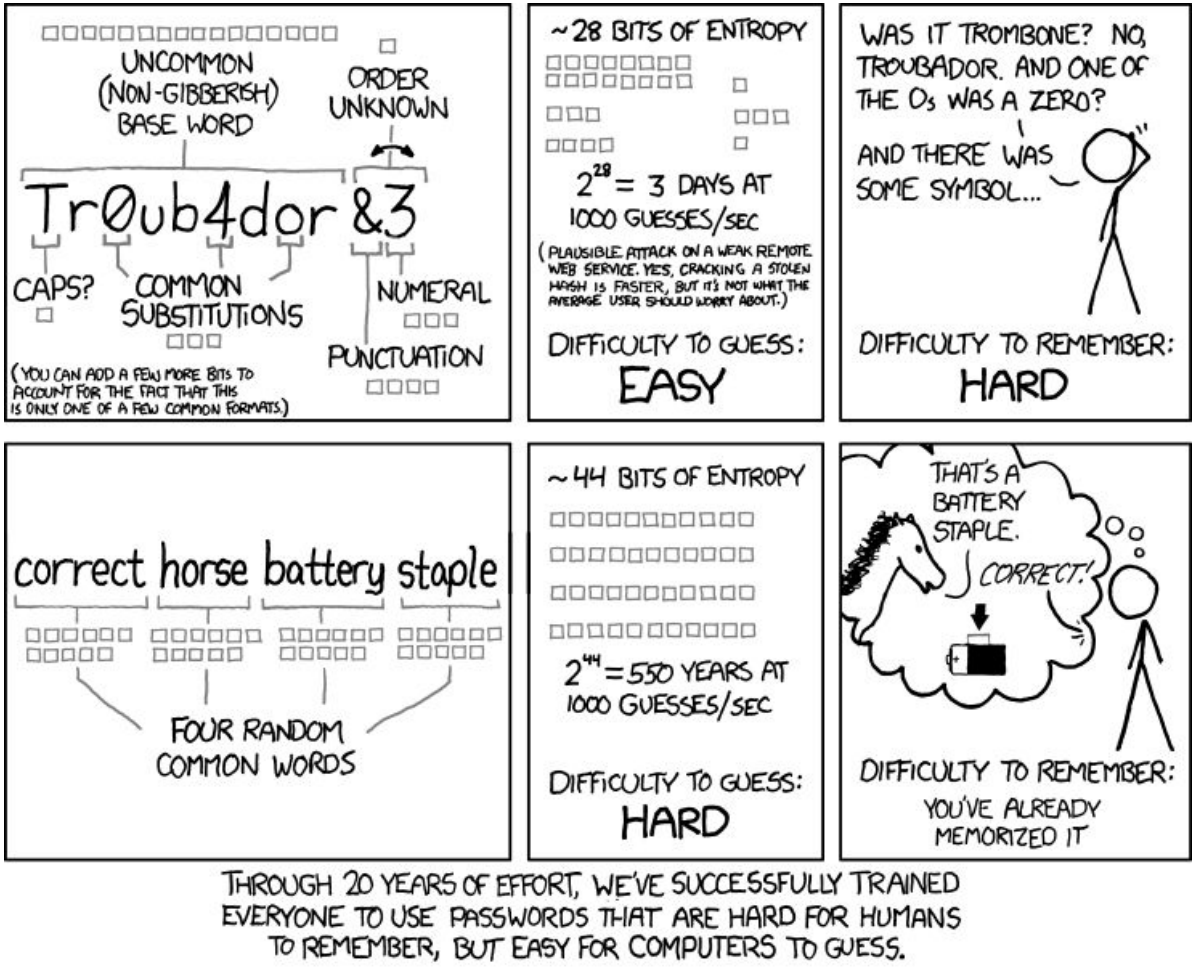
Works like this:

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

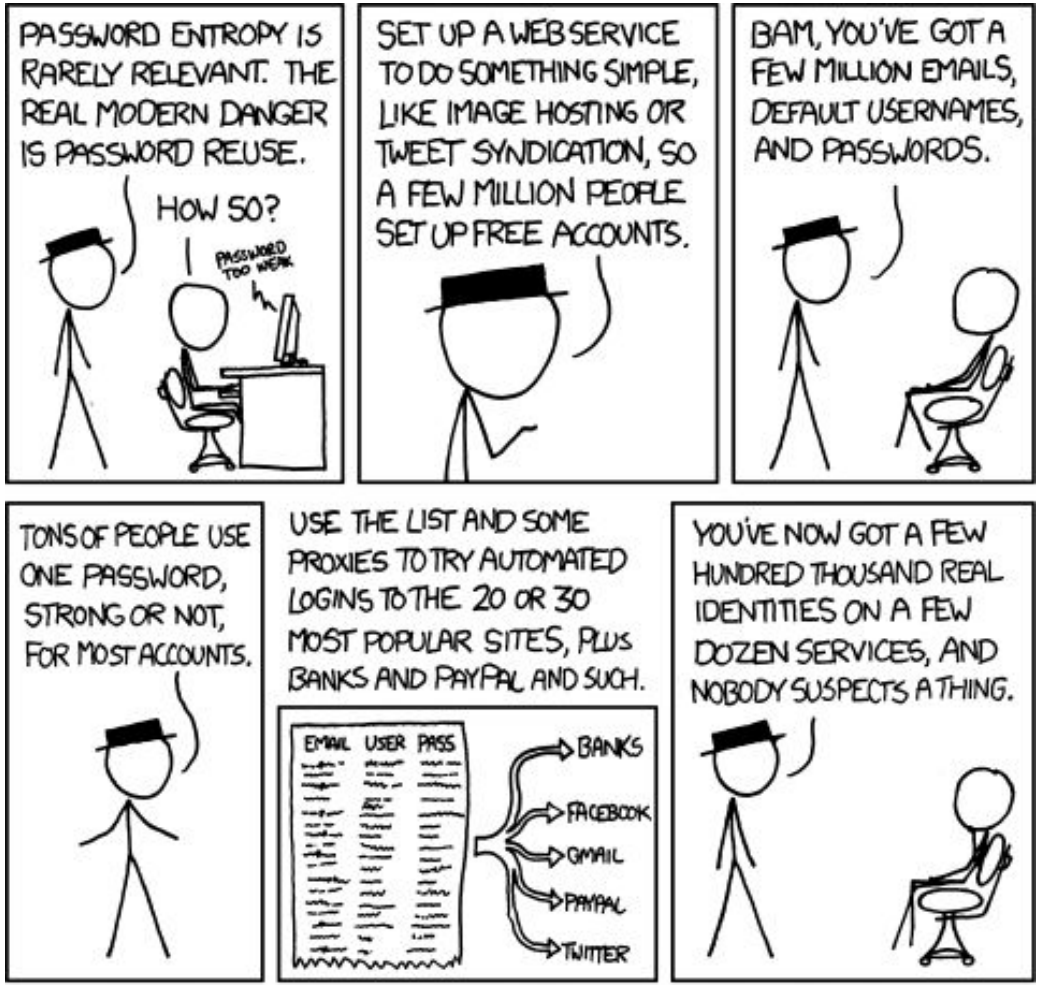
Entropy

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



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)