Modern Times:

Passwords

Tom Webster

"SamuraiLink3"

SamuraiLink3.com

SamuraiLink3@gmail.com

google.com/+TomWebster

@SamuraiLink3

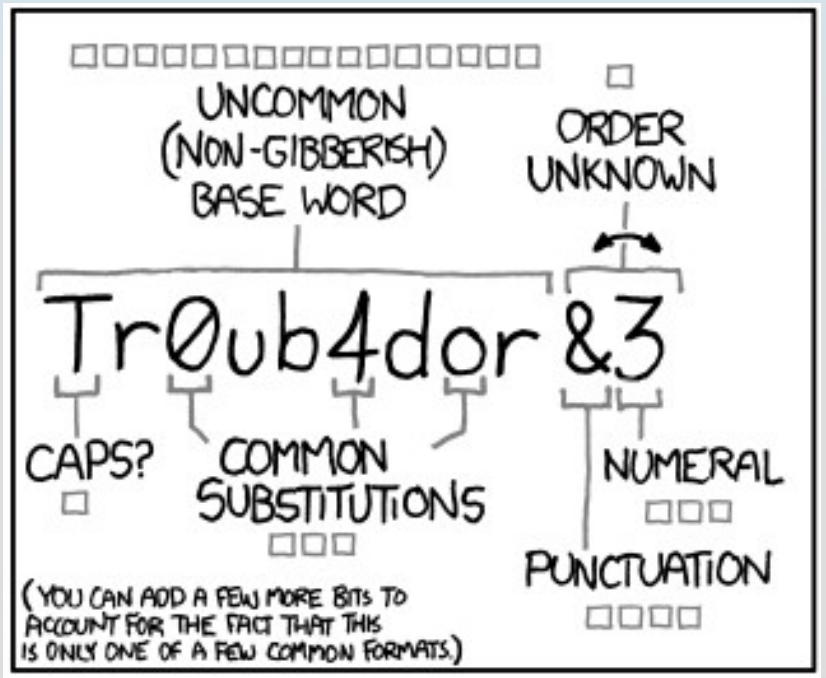
The password is old...

And we've gotten much better at breaking it over the course of human history.

The Bad Guys

- Word List Attacks
  - Take the most commonly-used passwords, try those first.
- Brute Force Attacks
  - Umm.. aaaaa, nope... aaaab, nope... aaaac...
- Common Account Attacks (password-reuse)
  - Is your fantasy football password the same as your company password? If the fantasy football site leaks your password, you could be in big trouble.
- Forgetting Passwords
  - Neither you, nor your help desk really have the time to reset passwords all day.

- **Inconvenience:**



The Good Guys

- Entropy (randomness)
  - Cg*Mb$bKExB&Sx06 is better than AaBbCcDdEe12345
- Length
  - It is much harder for an attacker to guess A9CKSPSA9 compared to A9CK. Longer is better.
- Memorability
  - A password does you no good unless you can use it.
- Uniqueness
  - Don't re-use your passwords. If a service is compromised or your password is leaked somehow (think about key loggers), you don't want everything getting compromised, only one thing. Unique passwords for everything!

The Facts

Brute Force Times (1000 guesses per second):

1234	11.11 seconds
l@Rr	22.87 hours
pass	7.92 minutes
password	6.91 years
Password	17.33 centuries
Password1	4.37 thousand centuries
PASSWORD1	33.22 centuries
P@ssword1	2.03 hundred thousand centuries
P@ssword12	19.24 million centuries

Source: https://www.grc.com/haystack.htm

Which is more secure?

Brute Force Times (1000 guesses per second):

D0g.....................	
PrXyc.N(n4k77#L!eVdAfp9	

Source: https://www.grc.com/haystack.htm

Which is more secure?

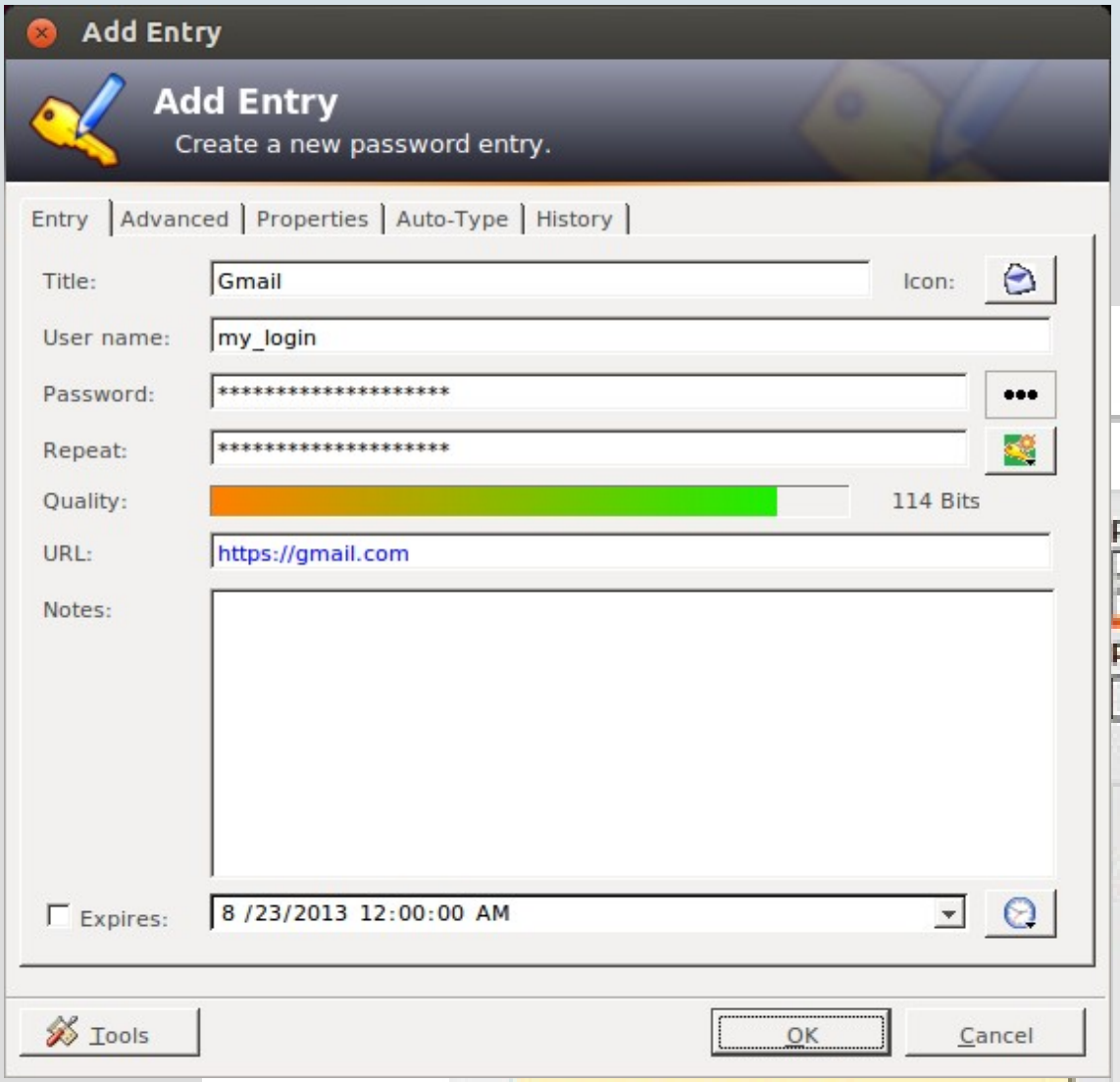
Brute Force Times (1000 guesses per second):

`D0g.....................`	93.83 billion trillion trillion centuries (24 characters)
`PrXyc.N(n4k77#L!eVdAfp9`	9.88 hundred million trillion trillion centuries (23 characters)

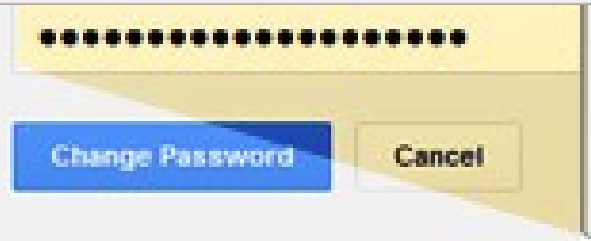
You don't need complexity for security.

Source: https://www.grc.com/haystack.htm

What you tell users to do



Password: D8a7@18dGH82$#1!



What they think they do

Password: fluffy1234

What they actually do

Word list attacks are designed to find and exploit commonly-used passwords and commonly used password techniques.

- How many of these do you recognize from your experience?
- How many of these have you seen people use?

Monkey01 Monkey02 Monkey03	[Common Word]+[2 Digit Sequence Number]
Password14May Password14June Password14July	[Common Word]+[2 Digit Year]+[Month]
@pple0514! @pple0614! @pple0714!	[Common Word (with common substitutions)] +[2 Digit Month]+[2 Digit Year]+[Common Punctuation]
taw201401 taw201402 taw201403	[User Initials]+[4 Digit Year]+[2 Digit Sequence Number]

These symptoms may be caused by overbearing security policies. See your security professional for more information.

This is probably the part where you all start yelling at me.

Mandatory Password Changes

1. This is a controversial topic
2. This is a **really** controversial topic

- Forced password changes don't help security in any meaningful way.
  - If someone breaks in, they will run off with all of your data or infect your system with persistent malware.
  - Changing passwords only affects silent stalkers that don't use remote control malware (uncommon).

Mandatory Password Changes

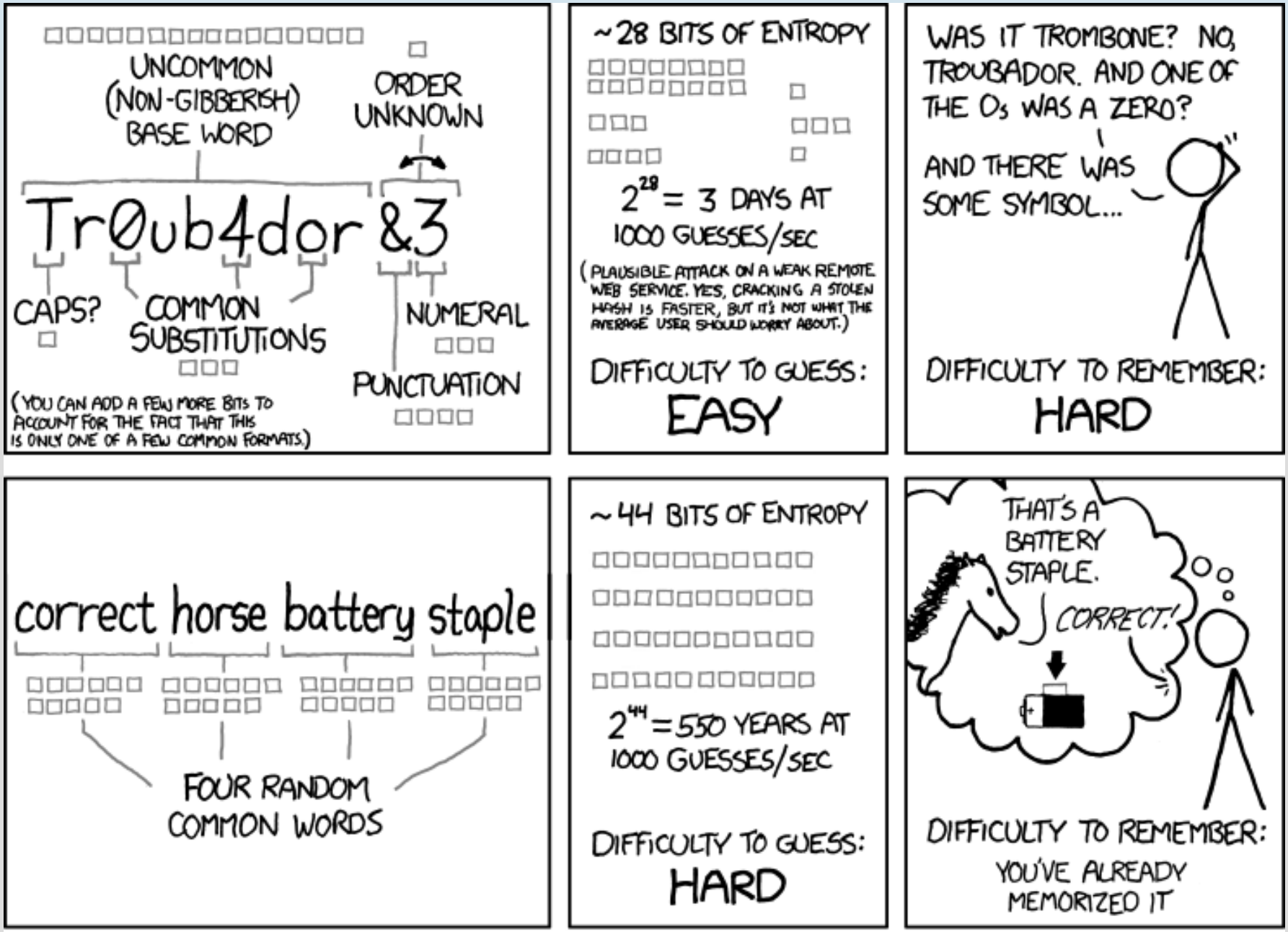
Mandatory password changes can reinforce the dangerous behavior shown in the past slides.

If given an opportunity to create one really good password, within a system that enables it, people will do the right thing.

Make intelligent policy decisions: **Great passwords shouldn't expire.**

There are totally two sides to this issue, stop throwing things.

Correct Horse Battery Staple



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.

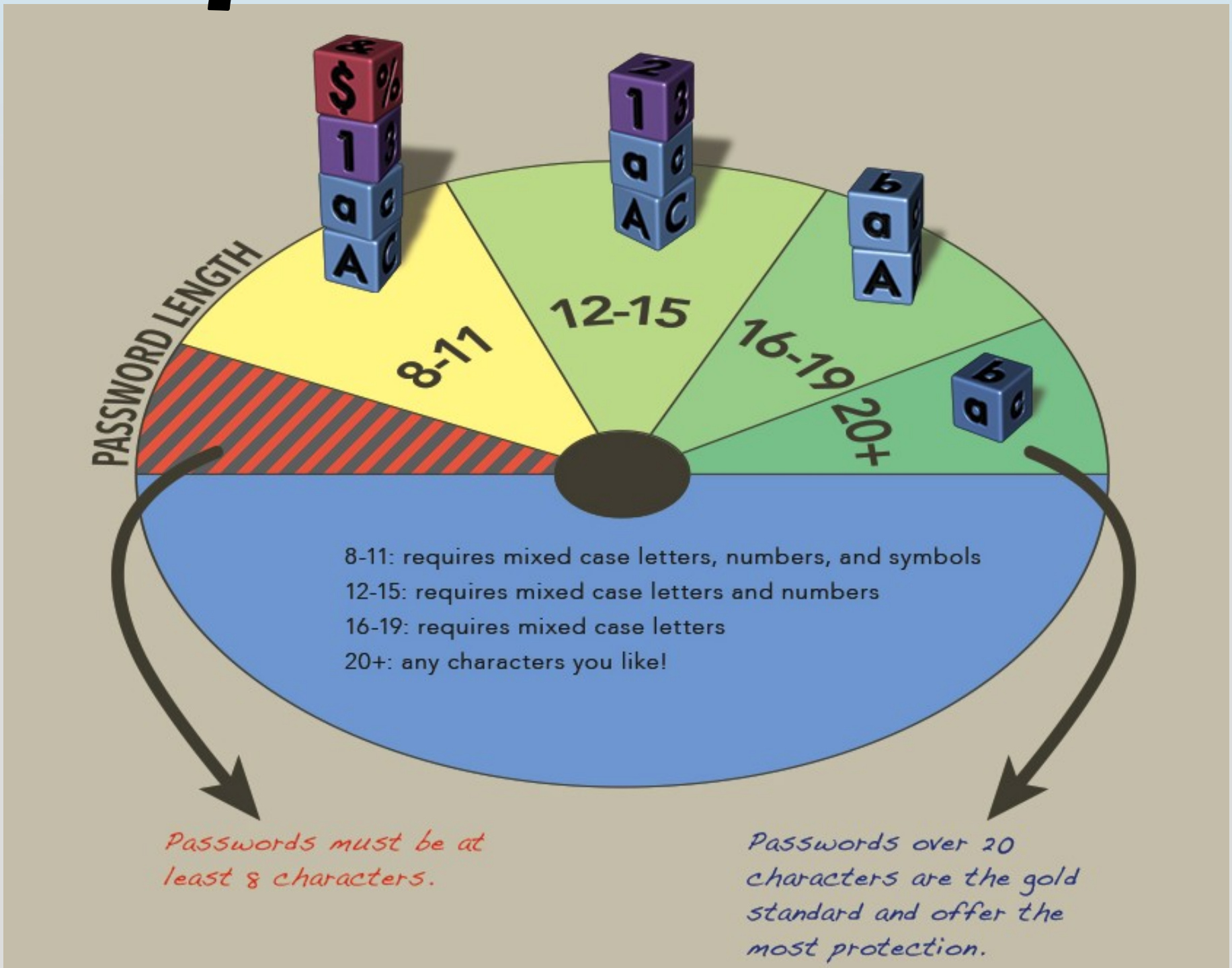
Passphrases

- Passphrases (passwords greater than 16 characters in length) are much more secure than passwords.

- Passphrases don't need the complexity that short passwords require, the length gives them enough entropy to thwart most word list and brute force attacks.

- We should start tailoring password rules based on length (some places already do this [mostly seen in education]).

Stanford's New Rules



Passphrases

Some caveats to consider:

- Wordlist attacks will become phrase list attacks
  - Companies and services should adopt a list of blocked common phrases: Bible Verses, common song lyrics, etc.
- Prevent users from using a single character 20 times as their password.
- Management will probably hate this.

Account Lockout

- Often used to dissuade brute force attacks.
  - If deployed incorrectly this can be unwieldy and lead to user frustration and increased support costs.
  - Too often, the number of incorrect tries is set too low. Brute force and word list attacks will attempt to access an account hundreds or thousands of times, your account lockout should be set to 30-50
  - It would be much better to set a low value for time between bad password attempts (20 tries in a minute? You're locked out!)

  But there's an even better solution:

Let's take things slow...

- Once a threshold is reached, start delaying login requests.
  - If the request persists, start increasing the delay time.
  - After 10 tries, add 10 seconds, after 5 more, add 30 seconds per incorrect login. Time resets after a password change or successful login.
- This technique is employed by many web services today and increases the difficulty of a brute force attack significantly.

- Can have the same downsides as account lockout, so watch those configuration options.

That said...

Watch your logs.
Watch your logs.
Watch your logs.

You could have a slow-burn brute force attack. If you see suspicious activity for an extended period:

- Check for infected machines
- Block and report an external IP address

Recommendations

- Passphrases over Passwords
- Length over Complexity
- Watch your logs
- Forced password lead to bad user behavior
- Fail2Ban is expensive for your help desk and your users, Fail2Delay is much better for the user, while dissuading brute force attacks.


Thanks!