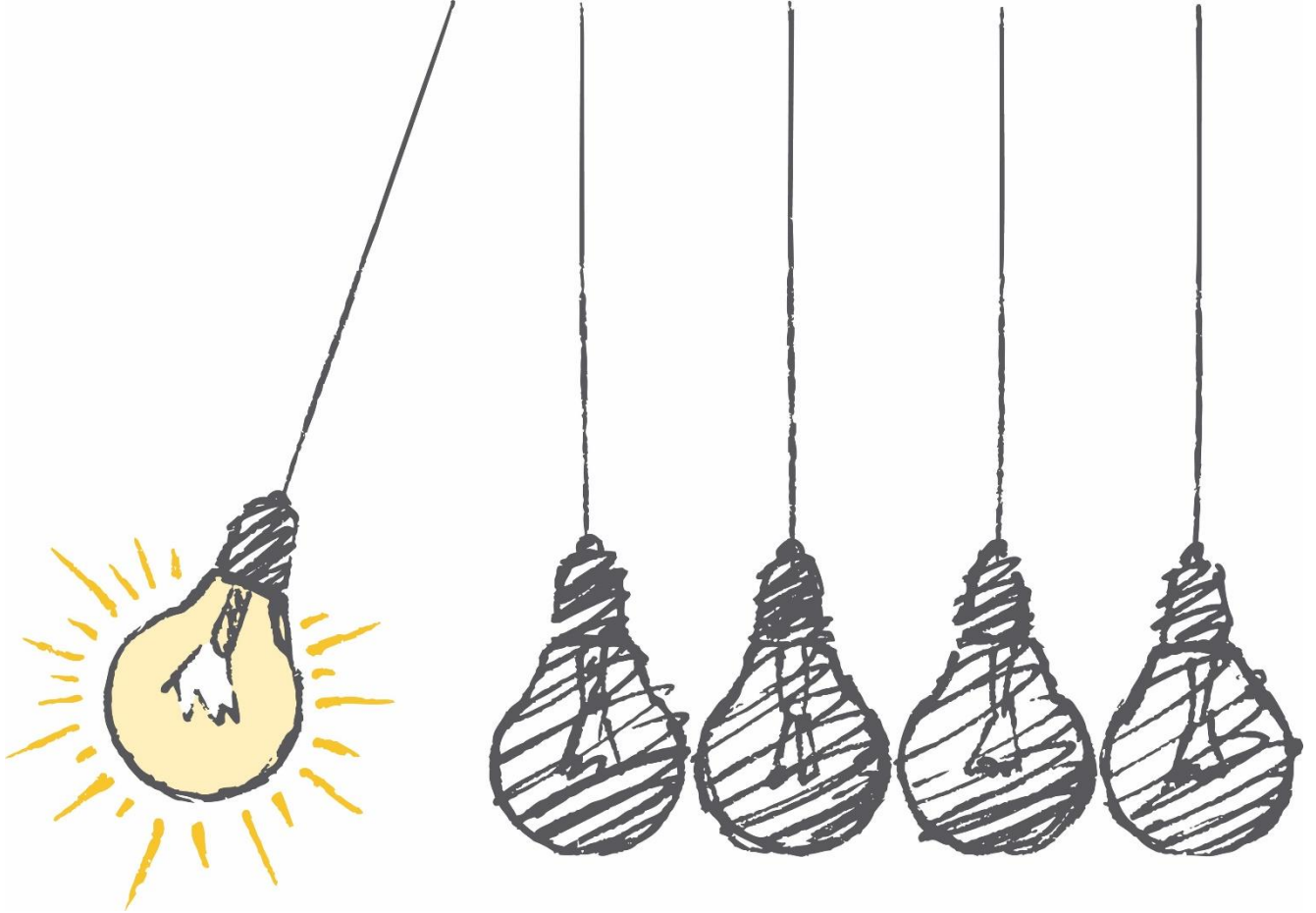
DIME analytics

What is a strong password?

DIME Bootcamp – Data Security



WORLD BANK GROUP

UKaid from the British people

Norad

A website we will use

- While we are waiting to get started, open this website as we will use it later

- haveibeenpwned.com - (Have I been pwned?)

In what ways can a password be weak?

Passwords are the weakest link

- Most successful cyber attacks exploit poor password practices, not poor IT-infrastructure
- Either are plain text passwords leaked/stolen or password hashes are cracked
- Hackers will eventually attempt to crack some of your passwords
- Weak password are cracked in minutes, strong passwords would take thousands of years to crack

How are passwords cracked?

- First approach is brute force (test all possible combinations):

What characters used?	Number of possible characters	Password length	Guesses per second	Time to crack
a-z	26	4	1 Million	*(26^4)/(10^6) =* ?

How are passwords cracked?

- First approach is brute force (test all possible combinations):

What characters used?	Number of possible characters	Password length	Guesses per second	Time to crack
a-z	26	4	1 Million	*(26^4)/(10^6) =* 0.46 seconds

How are passwords cracked?

- First approach is brute force (test all possible combinations):

What characters used?	Number of possible characters	Password length	Guesses per second	Time to crack
a-z	26	4	1 Million	*(26^4)/(10^6) =* 0.46 seconds
a-z,A-Z,0-9,(!,@,&)	82	4	1 Million	*((26+26+10+20)^4)/(10^6) =* ?
a-z	26	5	1 Million	*(26^5)/(10^6) =* ?

How are passwords cracked?

- First approach is brute force (test all possible combinations):

What characters used?	Number of possible characters	Password length	Guesses per second	Time to crack
a-z	26	4	1 Million	*(26^4)/(10^6) =* 0.46 seconds
a-z,A-Z,0-9,(!,@,&)	82	4	1 Million	*((26+26+10+20)^4)/(10^6) =* 45.21 seconds
a-z	26	5	1 Million	*(26^5)/(10^6) =* 11.88 seconds

How are passwords cracked?

- First approach is brute force (test all possible combinations):

What characters used?	Number of possible characters	Password length	Guesses per second	Time to crack
a-z	26	4	1 Million	*(26^4)/(10^6) =* 0.46 seconds
a-z,A-Z,0-9,(!,@,&)	82	4	1 Million	*((26+26+10+20)^4)/(10^6) =* 45.21 seconds
a-z	26	5	1 Million	*(26^5)/(10^6) =* 11.88 seconds
a-z	26	6	1 Million	*(26^6)/(10^6) =* 308.92 seconds

How are passwords cracked?

- First approach is brute force (test all possible combinations):

What characters used?	Number of possible characters	Password length	Guesses per second	Time to crack
a-z	26	4	1 Million	*(26^4)/(10^6) =* 0.46 seconds
a-z,A-Z,0-9,(!,@,&)	82	4	1 Million	*((26+26+10+20)^4)/(10^6) =* 45.21 seconds
a-z	26	5	1 Million	*(26^5)/(10^6) =* 11.88 seconds
a-z	26	6	1 Million	*(26^6)/(10^6) =* 308.92 seconds
a-z	26	7	1 Million	*(26^7)/(10^6) =* 8,031.79 seconds (2h 13min)
a-z	26	8	1 Million	*(26^8)/(10^6) =* 2 days 10h

How are passwords cracked?

- First approach is brute force (test all possible combinations):

What characters used?	Number of possible characters	Password length	Guesses per second	Time to crack
a-z	26	4	1 Million	*(26^4)/(10^6) =* 0.46 seconds
a-z,A-Z,0-9,(!,@,&)	82	4	1 Million	*((26+26+10+20)^4)/(10^6) =* 45.21 seconds
a-z	26	5	1 Million	*(26^5)/(10^6) =* 11.88 seconds
a-z	26	6	1 Million	*(26^6)/(10^6) =* 308.92 seconds
a-z	26	7	1 Million	*(26^7)/(10^6) =* 8,031.79 seconds (2h 13min)
a-z	26	8	1 Million	*(26^8)/(10^6) =* 2 days 10h
a-z,A-Z,0-9,(!,@,&)	82	8	1 Million	*((26+26+10+20)^8)/(10^6) =* 64 years 298 days 22h

How are passwords cracked?

- First approach is brute force (test all possible combinations):

What characters used?	Number of possible characters	Password length	Guesses per second	Time to crack
a-z	26	4	1 Million	*(26^4)/(10^6) =* 0.46 seconds
a-z,A-Z,0-9,(!,@,&)	82	4	1 Million	*((26+26+10+20)^4)/(10^6) =* 45.21 seconds
a-z	26	5	1 Million	*(26^5)/(10^6) =* 11.88 seconds
a-z	26	6	1 Million	*(26^6)/(10^6) =* 308.92 seconds
a-z	26	7	1 Million	*(26^7)/(10^6) =* 8,031.79 seconds (2h 13min)
a-z	26	8	1 Million	*(26^8)/(10^6) =* 2 days 10h
a-z,A-Z,0-9,(!,@,&)	82	8	1 Million	*((26+26+10+20)^8)/(10^6) =* 64 years 298 days 22h
a-z,A-Z,0-9,(!,@,&)	82	8	1 Billion	*((26+26+10+20)^8)/(10^9) =* 23 days 15h

Experiment

Have I been pawned?

- Enter your email at https://haveibeenpwned.com/
- This website search ***known*** data breaches to see if your email are in these data bases
- If it says that your password hash was leaked, then the hackers have what they need to start cracking your password

Experiment

- I spent 2 hours and no money on this experiment
- Do you recognize the information given to you?

Was this password used at multiple sites?

- If a website you are using gets hacked, you should always change your password for that website immediately
- Assume that your password will eventually be cracked, and associated with your email. So change password on any site where you used the same or a similar password
- If you are using a weak password you will not have time to do this before you are at risk, if you are using a strong password you do have time

How to make passwords long and memorizable?

Use words to create long password

- Example of a great password:
  - **mPFaAse&9x^R9vxg2*8ZA2BFik#KyXuj**
  - Passwords managers makes this easy, but we still need a master password

- What is a trick to create long passwords? Use a phrase like:
  - **somegoodtime**
  - 12 characters. 1 Billion guesses pers second. If **a-z** 3.5 year, if **a-z,A-Z,0-9,(!,@,&)** 2.9 million years.

- However, what if a hacker tests combinations of common words?
  - **some**, **good**, and **time** are all on the top 100 words
  - ((100)^3)/1,000,000 = 1 second for a regular computer

Use uncommon words to create long password

- Password: **forged staple sniper heckle**
  - Fairly easy to remember
  - Network of 1000 super computers (1 trillion guesses per sec):
    - Impossible to brute force 24 lower case character
      - (26^24)/(10^12) = 20,000 times the age of the universe
    - Using words on 20,000 most common words
      - (20000^4)/(10^12) = 1 day and 20 hours

- How to make it impossible even with a network of super computer:
  - **forged staple sjukhus heckled <- use a foreign word**
  - **forGed staple-sniper hec&kled <- use other characters**

Thank you!

Questions?