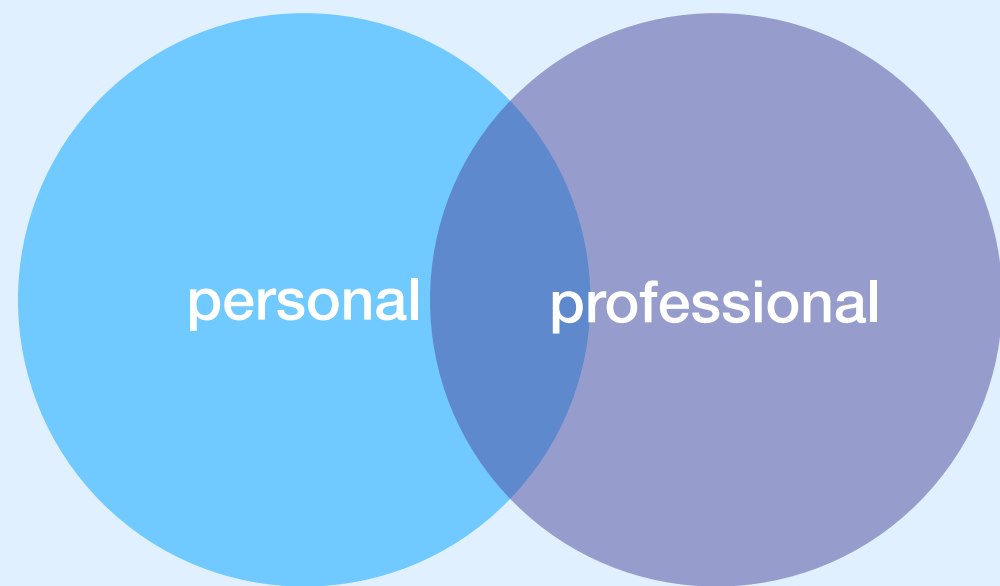


cyber security

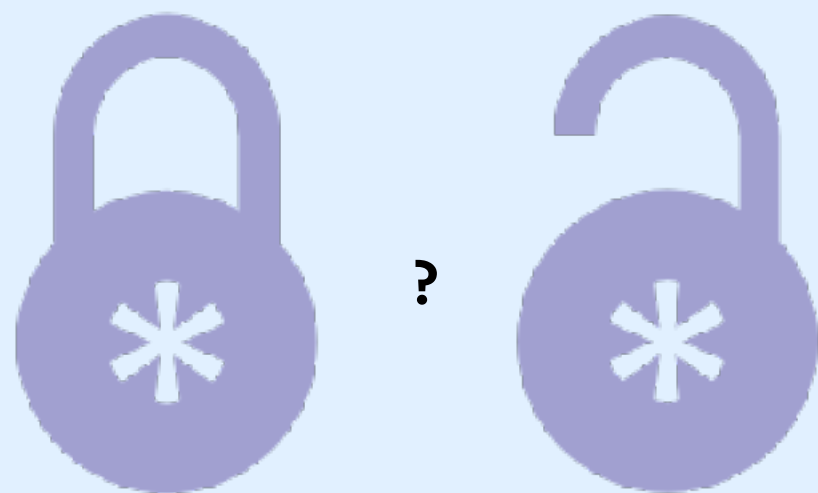
taking care of your digital assets in 5 minutes

Why this matters for our workplace?



professional overlaps with personal

Why this matters for our workplace?



professional overlaps with personal

consistency of habits

Why this matters for our workplace?

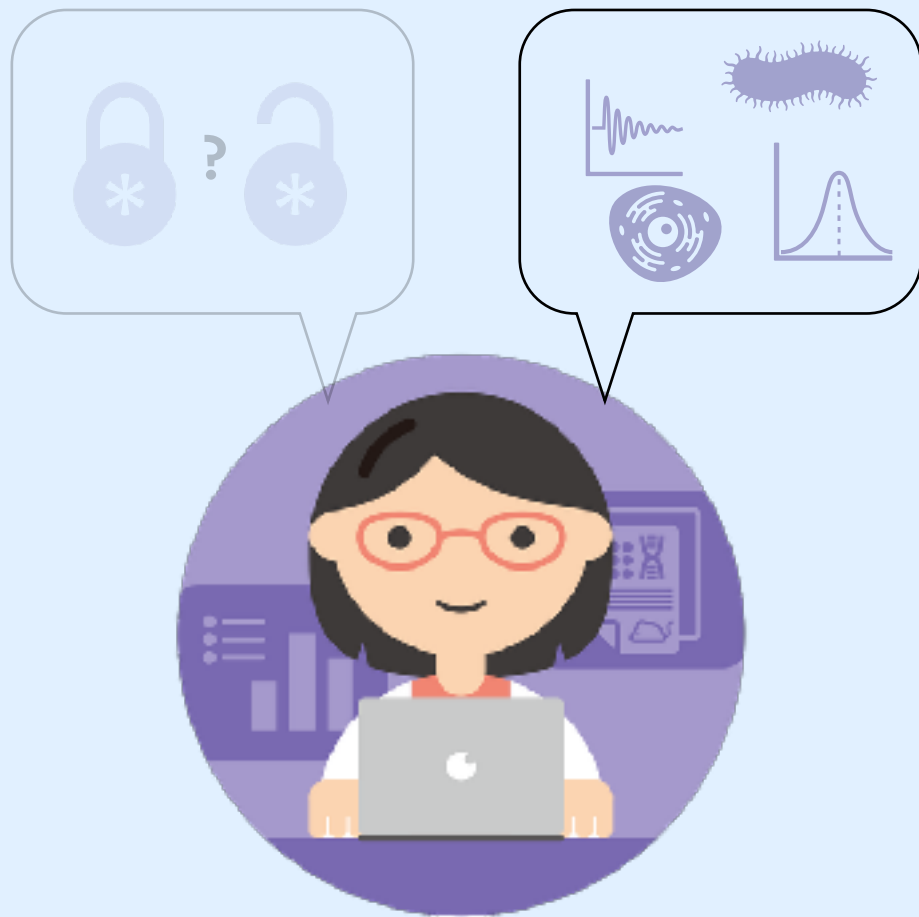


professional overlaps with personal

consistency of habits

peace of mind = efficiency at workplace

Why this matters for our workplace?



professional overlaps with personal

consistency of habits

peace of mind = efficiency at workplace

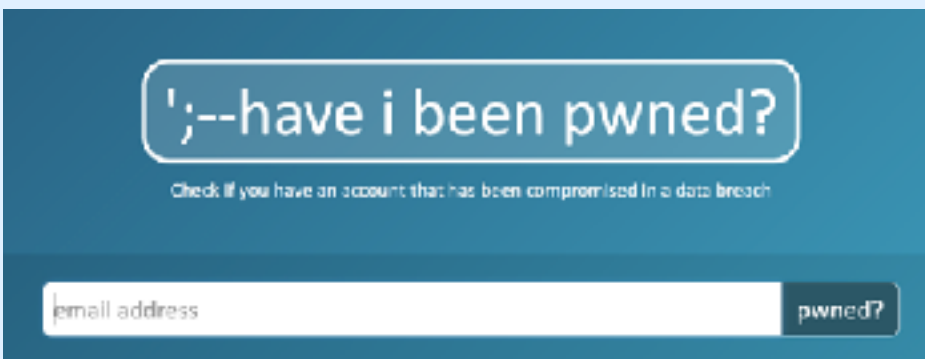
What should I do then?



lock your computer screen when you leave

What should I do then?

lock your computer screen when you leave
check if your digital assets are compromised



<https://haveibeenpwned.com/>

What should I do then?

Cqtgm1RFcMfidE~5

SgWtitKd8L+T7hrb

J8STts?ntVQU\$3JN

5@2n\$88F536H-8iH

3BvJ*0!=J&0i\$K9m

e7F#8B5xg-u8kP!i

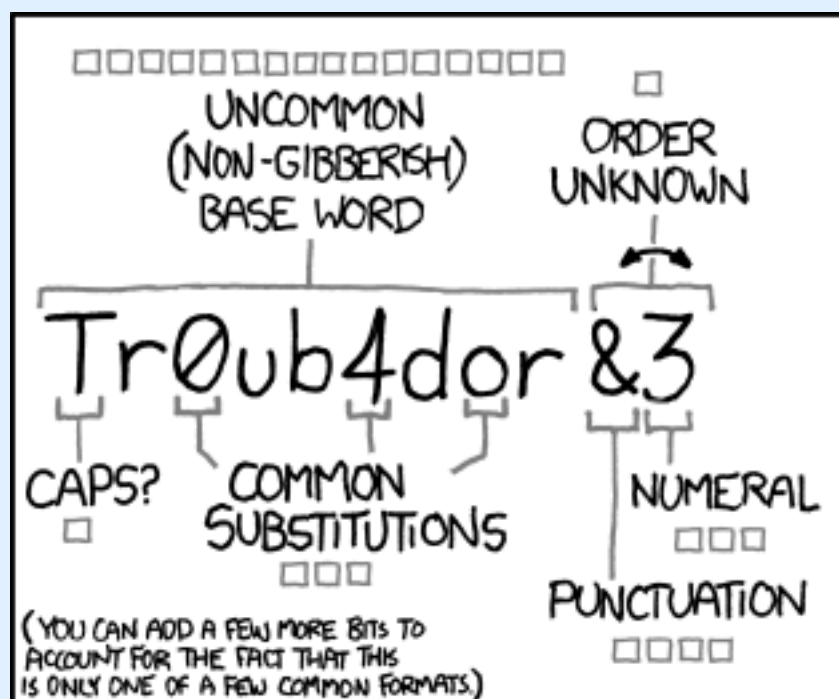
lock your computer screen when you leave

check if your digital assets are compromised

better passwords

Better passwords - again?

correct battery staple horse is a no go



~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.)

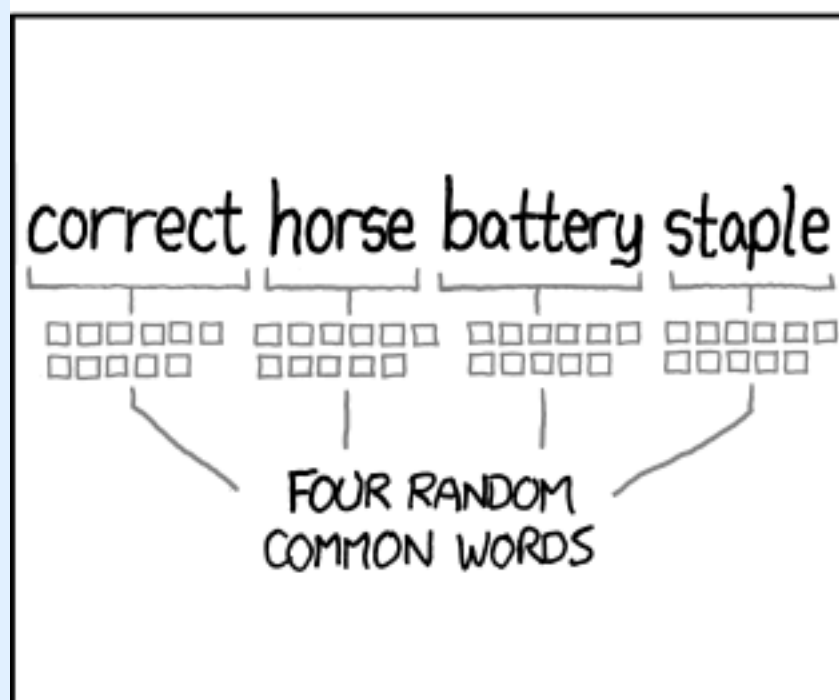
DIFFICULTY TO GUESS:
EASY

WAS IT TROMBONE? NO,
TROUBADOR. AND ONE OF
THE 0s WAS A ZERO?

AND THERE WAS
SOME SYMBOL...



DIFFICULTY TO REMEMBER:
HARD



~44 BITS OF ENTROPY

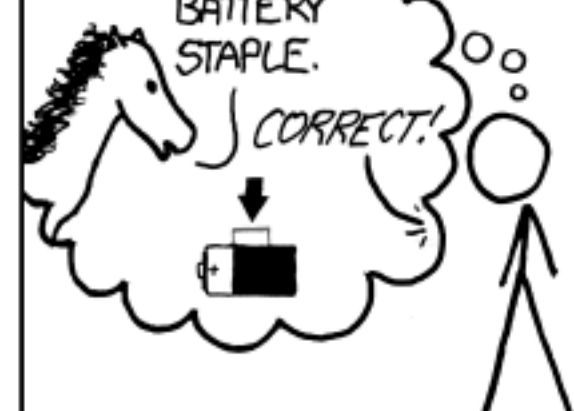
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□

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

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.

Anatomy of a crack

passwords are “hashed” and stored

Anatomy of a crack

passwords are “hashed” and stored

plain text		hash
password	MD5 →	5f4dcc3b5aa765d61d8327deb882cf99
password1	MD5 →	7c6a180b36896a0a8c02787eeafb0e4c

Anatomy of a crack

16,449 hashed passwords

technique

cracked passwords

brute-force all pass with one to six characters

1,316

brute-force all pass with 7 or 8 all lowercase

1,618

brute-force all pass with 7 or 8 all uppercase

708

brute-force all pass with 7 or 8 all digits

312

Anatomy of a crack

16,449 hashed passwords

technique

cracked passwords

brute-force all pass with one to six characters

1,316

brute-force all pass with 7 or 8 all lowercase

1,618

brute-force all pass with 7 or 8 all uppercase

708

brute-force all pass with 7 or 8 all digits

312

word list + best64 rule set

6,228

10,233

Anatomy of a crack

16,449 hashed passwords

technique

cracked passwords

hybrid attack: add 2 digits or symbol at the end of every word	585
hybrid attack: add 3 digits or symbol at the end of every word	527
hybrid attack: add 4 digits at the end of every word	435
hybrid attack: add 3 digits or lowercase at the end of every word	312

12,935

78% of hashes in only 5h

Anatomy of a crack

16,449 hashed passwords

technique

cracked passwords

hybrid attack: add 2 digits or symbol at the end of every word	585
hybrid attack: add 3 digits or symbol at the end of every word	527
hybrid attack: add 4 digits at the end of every word	435
hybrid attack: add 3 digits or lowercase at the end of every word	312

Markov chain

90% of hashes in only 20.5h

Anatomy of a crack

list of passwords cracked

- momof3g8kids
- k1araj0hns0n
- Sh1a-labe0uf
- Apr!1221973
- Qbesancon321
- qeadzcwrsfxv1331
- gonefishing1125
- windermere2313
- BandGeek2014
- i hate hackers
- allinedislove
- ilovemySister31
- iloveyousomuch
- Philippians4:13
- Philippians4:6-7

Anatomy of a crack

list of passwords cracked

- momof3g8kids
- k1araj0hns0n
- Sh1a-labe0uf
- Apr!1221973
- Qbesancon321
- qeadzcwrsfxv1331
- gonefishing1125
- windermere2313
- BandGeek2014
- i hate hackers
- allinedislove
- ilovemySister31
- iloveyousomuch
- Philippians4:13
- Philippians4:6-7

when crackers know the site, they tailor the word list.

Better passwords - again?



correct battery staple horse is a no go

it is only human to be biased

Better passwords - again?

correct battery staple horse is a no go



it is only human to be biased

No password reuse

Better passwords - Use password manager



LastPass



1password



KeePassXC

Better passwords - master password

Generate it randomly

3qA^ju

Better passwords - master password

3qA^ju

Generate it randomly

>8 characters

Better passwords - master password

0ItX91b!ym

Generate it randomly

>8 characters

Better passwords - master password

Generate it randomly

0ItX91b!ym

>8 characters

<u>0I</u>	Portuguese for Hi!
<u>tX</u>	Texas with big X
<u>91b!</u>	who lives in the apt 91-B
<u>ym</u>	why me ?

use mnemonics to remember

Better passwords - what else?

whenever possible - 2 factor authentication (2FA)

<https://lastpass.com/>

<https://keepassxc.org/> <https://haveibeenpwned.com/>

<https://1password.com/>

be safe

Anatomy of a hack: How crackers ransack passwords like "qeadzcvrsfxv1331" by Dan Goodin.

