# How Secure Are Multi-Word Random Passphrases?

By Bruce K. Marshall
@PwdRsch

PasswordResearch.com

# What Are Passphrases?

- Longer than passwords
- Often words separated by spaces
- Have some overlap with passwords
- Goal is to offer better security than normal passwords while also being more usable

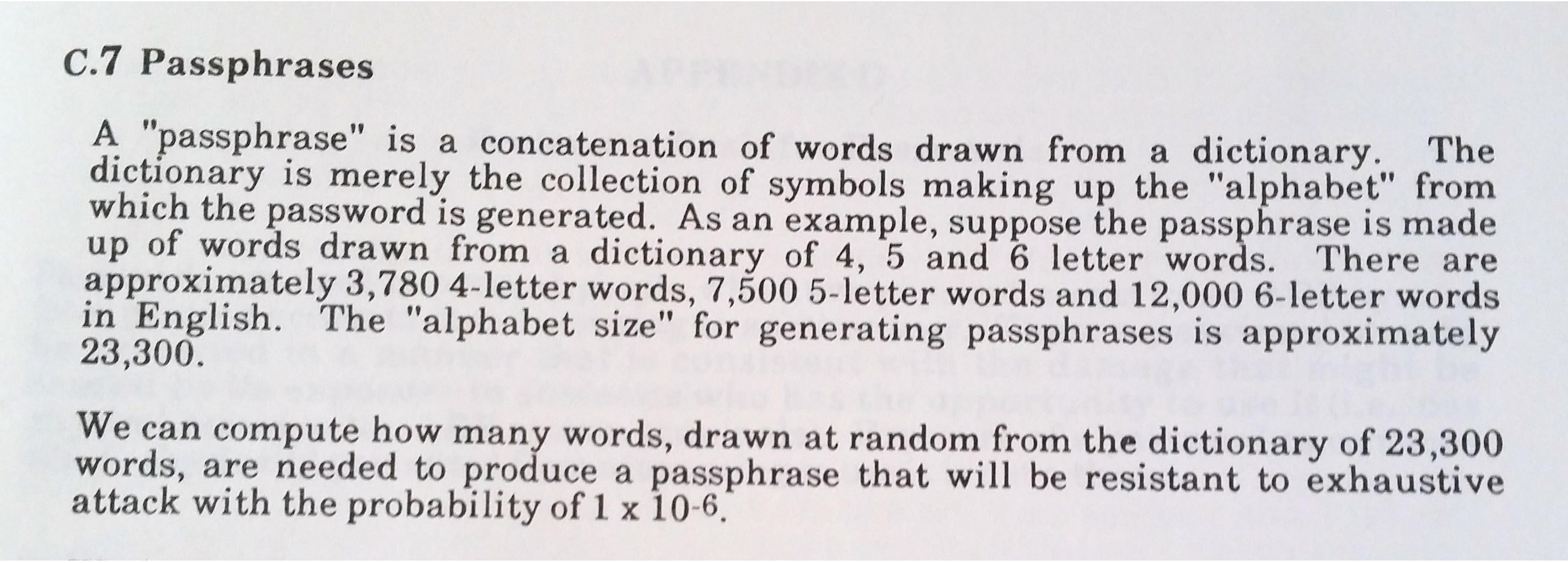
# Types of Passphrases

- Natural language phrases
  - “you can do it”
- Natural language structured phrases
  - “fast doorway took taco”
- Mentally chosen 'random' words
  - “dell chair boring calendar”
- Securely chosen random words
  - “land dear each spend”

CUPCAKES RAINBOWS KITTENS
LOL I'M SO RANDOM
quickmeme.com

[1]

# Growing Passphrase Popularity



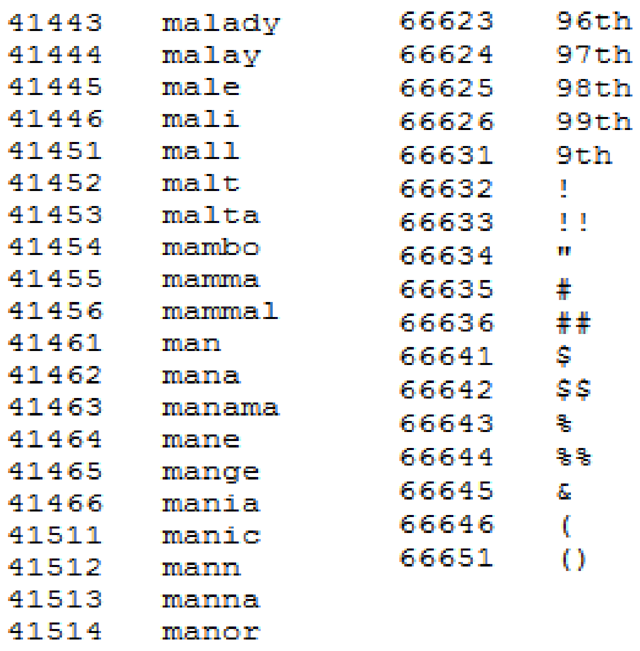
## C.7 Passphrases

A "passphrase" is a concatenation of words drawn from a dictionary. The dictionary is merely the collection of symbols making up the "alphabet" from which the password is generated. As an example, suppose the passphrase is made up of words drawn from a dictionary of 4, 5 and 6 letter words. There are approximately 3,780 4-letter words, 7,500 5-letter words and 12,000 6-letter words in English. The "alphabet size" for generating passphrases is approximately 23,300.

We can compute how many words, drawn at random from the dictionary of 23,300 words, are needed to produce a passphrase that will be resistant to exhaustive attack with the probability of 1 x $10^{-6}$.

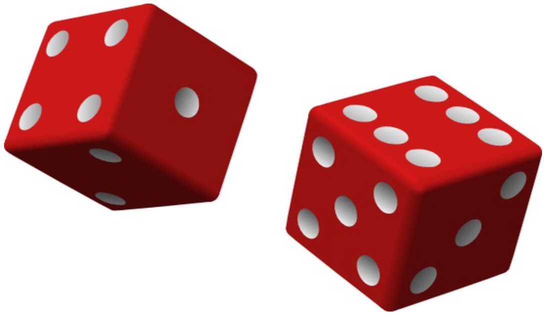
# What is Diceware?

- Formal system for generating random word passphrases published in 1985 by Arnold Reinhold.
- Roll one die five times or five dice one time. Look up index of dice values and use corresponding word

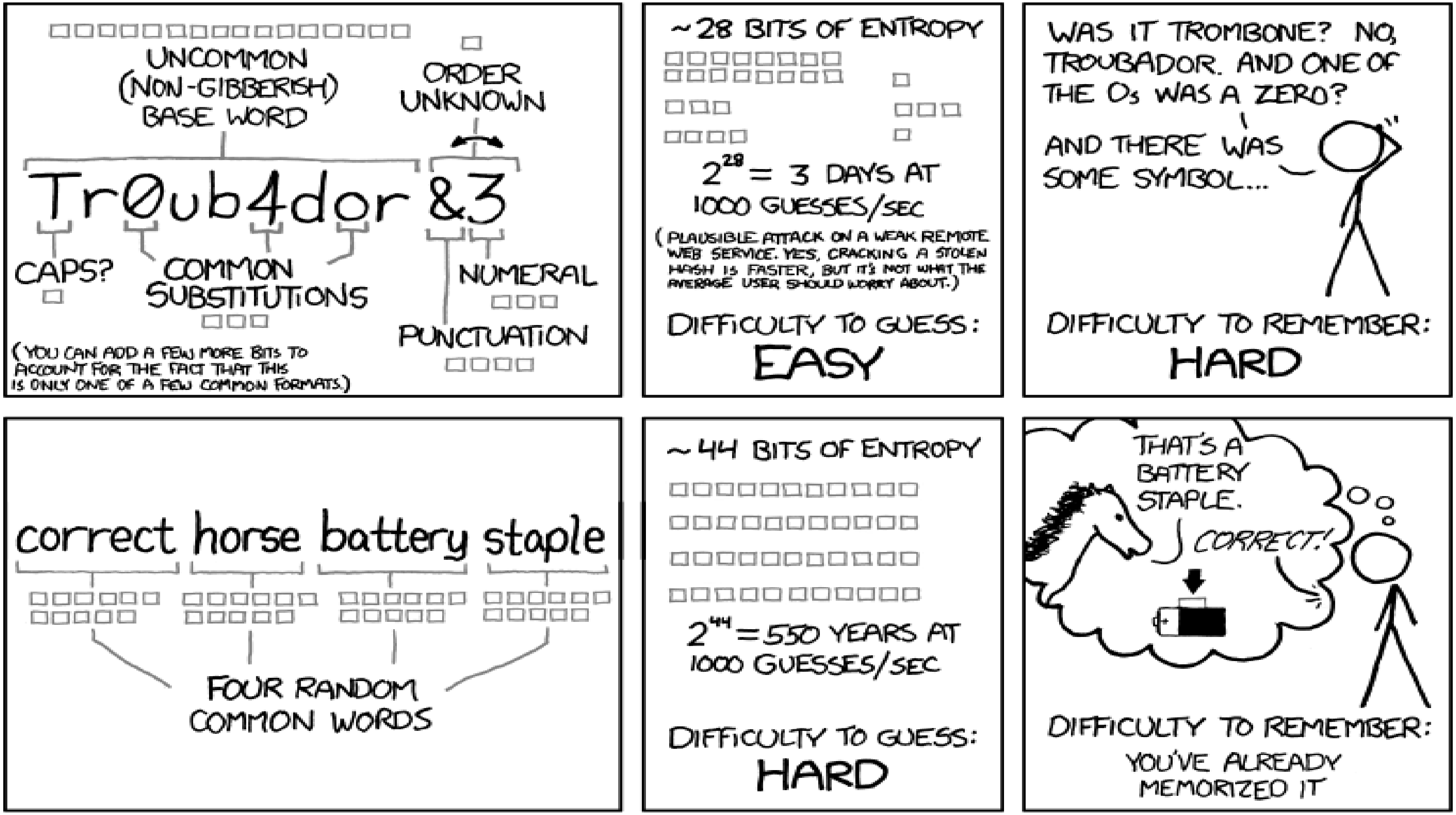


| | |
|---|---|
| 41443 | malady |
| 41444 | malay |
| 41445 | male |
| 41446 | mali |
| 41451 | mall |
| 41452 | malt |
| 41453 | malta |
| 41454 | mambo |
| 41455 | mamma |
| 41456 | mammal |
| 41461 | man |
| 41462 | mana |
| 41463 | manama |
| 41464 | mane |
| 41465 | mange |
| 41466 | mania |
| 41511 | manic |
| 41512 | mann |
| 41513 | manna |
| 41514 | manor |

| | |
|---|---|
| 66623 | 96th |
| 66624 | 97th |
| 66625 | 98th |
| 66626 | 99th |
| 66631 | 9th |
| 66632 | ! |
| 66633 | !! |
| 66634 | " |
| 66635 | # |
| 66636 | ## |
| 66641 | $ |
| 66642 | $$ |
| 66643 | % |
| 66644 | %% |
| 66645 | & |
| 66646 | ( |
| 66651 | () |



# What is XKCD 936?


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
$2^{28}$ = 3 DAYS AT 1000 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 Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
$2^{44}$=550 YEARS AT 1000 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.

By Randall Monroe, Aug 2011

# Attacks Against Passphrases

- Offline Passphrase Cracking
- Online Passphrase Guessing
- Shoulder Surfing
- Keystroke logging /
  Man-in-the-Middle /
  Phishing /
  Social Engineering /
  Rubber Hose

# How to Estimate Random Passphrase Strength

Possible word choices ^ words long

Convert to bits by taking log(2) of total

- XKCD suggests using 2,048 words

  2048 ^ 4 = 17,592,186,044,416 = 44 bits

- Diceware has 7776 words in base wordlist

  7776 ^ 5 = 28,430,288,029,929,700,000 = 64.6 bits

# How Random Passphrases Compare to Random Passwords

| Wordlist | Len Words | Num | Bits |
|---|---|---|---|
| 2,048 | 4 | 1.7 x 10^13 | 44 |
| | | | |
| 7,776 | 5 | 2.8 x 10^19 | 64.6 |
| 7,776 | 6 | 2.2 x 10^23 | 77.5 |
| 7,776 | 7 | 1.7 x 10^27 | 90.5 |

| Charlist | Len Chars | Num | Bits |
|---|---|---|---|
| 95 | 7 | 6.9 x 10^13 | 46 |
| 95 | 8 | 6.6 x 10^15 | 52.6 |
| 95 | 9 | 6.3 x 10^17 | 59 |
| 95 | 10 | 5.9 x 10^19 | 65.7 |
| 95 | 11 | 5.7 x 10^21 | 72.3 |

# A Look at Diceware Words

- Short words = possibility of short passphrases
- User stuck with choice of using short passphrase or generating new one
- Refusing any 5 word passphrase under 14 chars eliminates 0.00037% of possible 5 word combinations

| Length | Words | % of Total |
|---|---|---|
| 1 | 52 | 0.7% |
| 2 | 773 | 9.9% |
| 3 | 839 | 10.8% |
| 4 | 2,345 | 30.2% |
| 5 | 3,136 | 40.3% |
| 6 | 631 | 8.1% |

# Ways to Increase Passphrase Strength

- Increase number of words used
  - 6 words from 9,030 word list = 78.8 bits
- Increase number of words in source word list
  - 4 words from 858,000 word list = 78.8 bits
- Modify words from their original form
  - Change word case, change spelling, change separator, or apply other transformation randomly
  - CORRECT:horse:battery:STAPLE

# What the Shortest Passphrase You Can Safely Use?

- Diceware recommendations:
  - ~~5~~ 6 for normal use
  - 6 for wireless security / file encryption
  - 7-8 for 'high value' like Bitcoin wallet
- EFF echos 6 word advice
- SecureDrop uses 7 (from modified 6,800 list)
- Realistically you can use 3 word (especially modified) for lower risk apps

# Passphrase Cracking Speed ESTIMATES

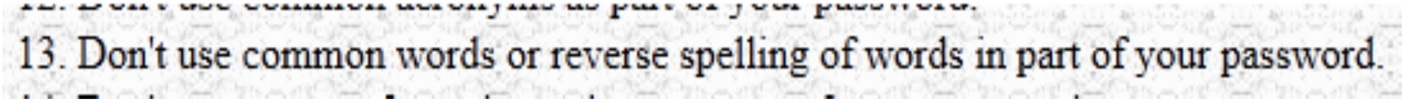
| Wordlist | Words | Bits | TrueCrypt PBKDF2-HMAC-SHA512 + AES x 8 GPU | MD5 x 8 GPU | Snowden Mystery Box |
|---|---|---|---|---|---|
| 2,048 | 4 | 44 | 76 days | <1 hour | <1 hour |
| 7,776 | 5 | 64.6 | 335,535 years | 8.8 years | 329 days |
| 7,776 | 6 | 77.6 | 2.6 billion years | 68,235 years | 7,010 years |
| 88,000 | 4 | 65.7 | 707,765 years | 18.5 years | 1.9 years |
| 9,030 | 6 | 78.8 | 6.4 billion years | 167,560 years | 17,191 years |

[2]

# Possible Cracking Shortcuts

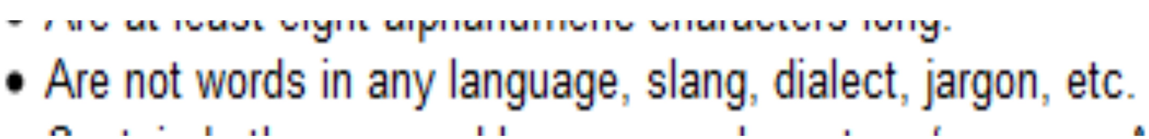
- Discover and exploit word acceptance bias that results in users rejecting passphrases with some specific words.
- Find a combination that happens to also match a captured natural language phrase.
- Find a combination that has been leaked in plaintext from another source.

# Resistance to Passphrases

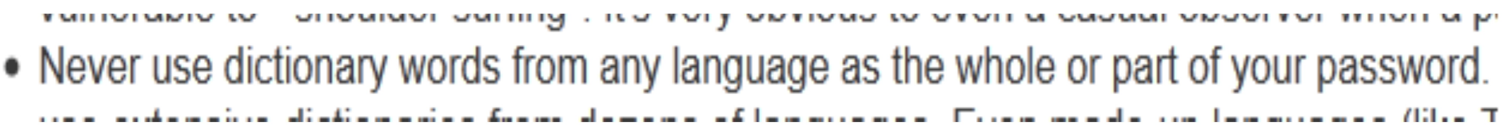


12. Don't use common acronyms as part of your password.

13. Don't use common words or reverse spelling of words in part of your password.

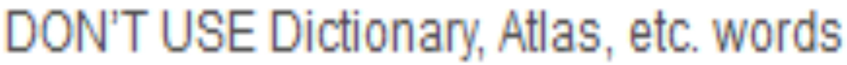


- Are at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.

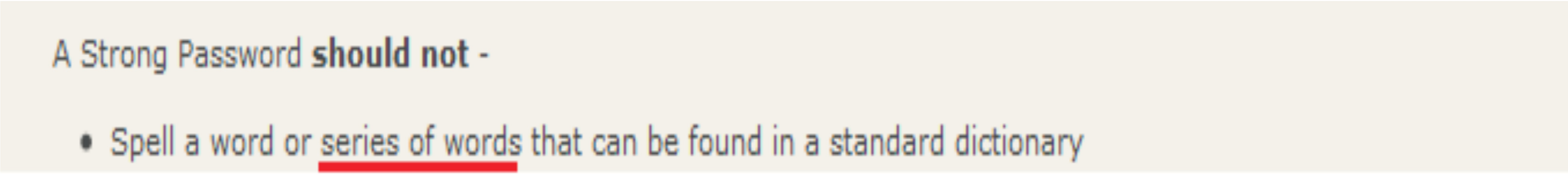


vulnerable to "shoulder surfing". It's very obvious to even a casual observer when a p

- Never use dictionary words from any language as the whole or part of your password.

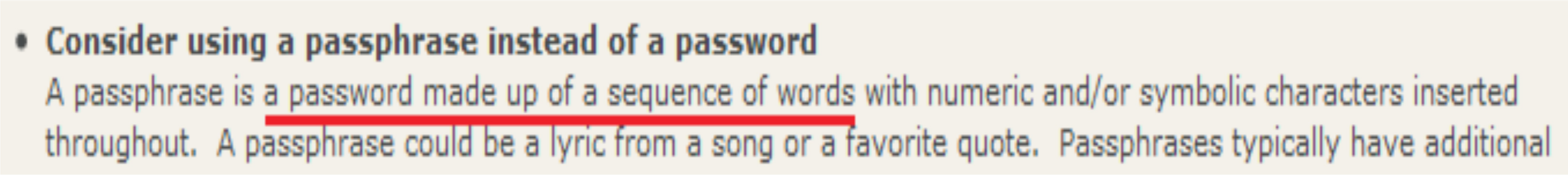


DON'T USE Dictionary, Atlas, etc. words



A Strong Password **should not** -

- Spell a word or series of words that can be found in a standard dictionary



- **Consider using a passphrase instead of a password**
  A passphrase is a password made up of a sequence of words with numeric and/or symbolic characters inserted throughout. A passphrase could be a lyric from a song or a favorite quote. Passphrases typically have additional

# Resistance to Passphrases

- Bruce Schneier Blog Choosing Secure Passwords from March, 2014

Quoted Ars Technica article from May 2013 that reported that these passwords had been cracked: “allineedislove”, “iloveyousomuch”, “sleepingwithsirens”, & “i hate hackers”

“This is why the oft-cited XKCD scheme for generating passwords – string together individual words like "correcthorsebatterystaple" - is no longer good advice. The password crackers are on to this trick.”

# Passphrase Usability Research

- Correct Horse Battery Staple: Exploring the Usability of System-Assisted Passphrases
  - No significant difference in percent of people storing passwords compared to passphrases.
  - Passphrase users took median 7 seconds to enter compared to 3 seconds for passwords.
  - Successful logins by passphrase non-storage participants were 47%.  Compared to 58% for password.  Storage groups both = 85% success.
  - The passphrases (3-4 word range) had a mean length of 18.3 / 25.5 characters.

[3]

# Passphrase Usability Research

- A Behavioral Analysis of Passphrase Design and Effectiveness
  - Passphrase group was asked to create a 3-5 word phrase at least 16 characters in length. Resulted in an 18.2 character and 3.6 word average.
  - The passphrase group experienced the lowest login failure rate at 11% (combining memory and typographical errors).

[4]

# Passphrase Usability Research

- Towards Reliable Storage of 56-bit Secrets in Human Memory
  - 96% of passphrase participants and 91% of random letter participants learned well enough to type from memory 3 times in a row.
  - Median typing time for all 3 segments were 8.2 seconds for words and 6.1 seconds for letters.
  - Entry errors for passphrases were median of 5 per user, with random letters a median of 7.

[5]

# Passphrase Field Testing

Tested the following passphrases on large web sites & observed related usability factors:

| | | |
|---|---|---|
| 1. | level drama whoosh funny | (24) |
| 2. | suey 65 swim gain recur | (23) |
| 3. | hovel strafe m's knobs lyric perm | (33) |
| 4. | follow*RUBBER*BENEATH*natural | (29) |
| 5. | BANAL.mayan.skit | (16) |

# Passphrase Field Testing

| Site | Max Length | Passphrases Accepted | Problems |
|---|---|---|---|
| Facebook | 150+ | All | |
| Twitter | 150+ | All | |
| Instagram | 150+ | All | |
| Vine | 100 | All | |
| LinkedIn | 150 | All | |
| Pinterest | 85* | All | Silently truncates |

# Passphrase Field Testing

| Site | Max Length | Passphrases Accepted | Problems |
|---|---|---|---|
| Amazon | 150+ | All | |
| Ebay | 64 | #4 & 5 | Silently truncates, character complexity required |
| AliExpress | 20 | None | No spaces or other symbols allowed, max length too short |
| Walmart | 12 | None | No spaces allowed |
| Target | 20 | #5 | Character complexity required, max length too short |
| Ikea | 20 | None | Character complexity required, max length too short |
| Home Depot | 150+ | All | Some symbols parsed differently |

# Passphrase Field Testing

| Site | Max Length | Passphrases Accepted | Problems |
|---|---|---|---|
| PayPal | 20 | #5 | No spaces allowed, max length too short |
| Chase | 32 | #5 | No spaces allowed, no repeating character > 2, max length too short |
| Discover | 32 | #2 | character complexity required, max length too short |
| Coinbase | 72 | All | Silent truncation |
| Kraken | 128 | #1 3 4 5 | Strange variable character complexity requirements |

# When Should You Use Passphrases?

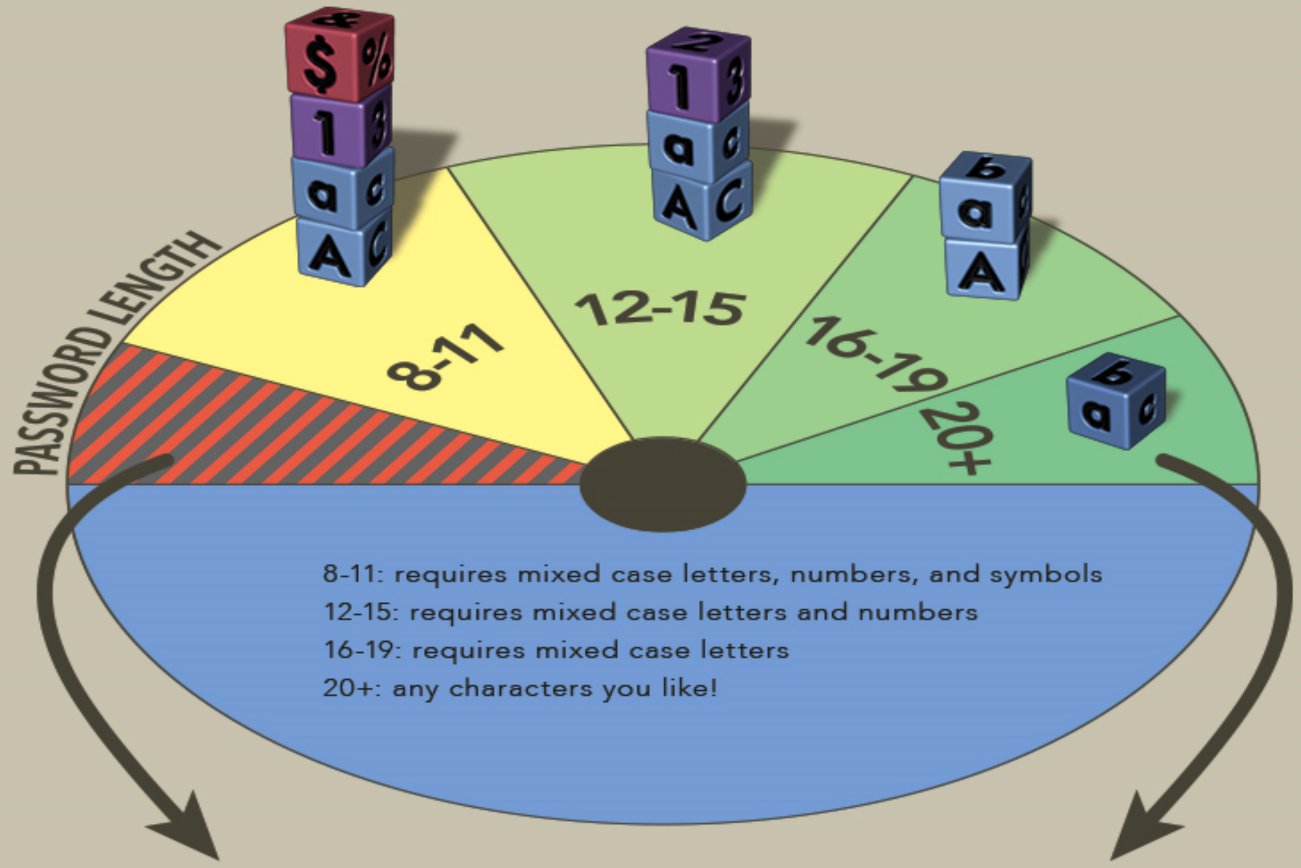
- When you have to type it regularly
- When your password manager isn't usable or easily compatible
- When a particular keyboard makes them preferential to enter versus random passwords
- When you will share it with someone via voice
- For security question answers
- For everything else rely on password managers and random strings

# How to Support Passphrase Use

- Don't impose unnecessary maximum password length restrictions
- Avoid restricting symbol use (and space)
- If scanning for common words evaluate context of that word before rejecting
- Enforce these standards throughout app(s)
- Provide guidance on, and examples of, good passphrase use – ideally complete systems

# WHICH CHARACTERS ARE REQUIRED IN MY **PASSWORD?**

***HINT:*** *it depends on password length!*



8-11: requires mixed case letters, numbers, and symbols

12-15: requires mixed case letters and numbers

16-19: requires mixed case letters

20+: any characters you like!

Passwords must be at least 8 characters.

Passwords over 20 characters are the gold standard and offer the most protection.

I USE A 6 WORD PASSPHRASE
"MA MA MA MA MA MA"
Born to Rule

# References

1. Linguistic Properties of Multi-word Passphrases, J. Bonneau, E. Shutova, 16th International Conference on Financial Cryptography and Data Security, 2012
2. 8x GTX Titan X cudaHashcat Benchmark, Jeremi Gosney, posted Jun 3, 2015, https://gist.github.com/epixoip/63c2ad11baf7bbd57544
3. Correct Horse Battery Staple: Exploring the Usability of System-Assisted Passphrases, Richard Shay, Patrick Gage Kelly, Saranga Komanduri, Michelle L. Mazurek, Blase Ur, Timothy Vidas, Lujo Bauer, Nicholas Christin, Lorrie Faith Cranor, Symposium on Usable Privacy and Security (SOUPS), Jul 2012

# References

4. A Behavioral Analysis of Passphrase Design and Effectiveness, Mark Keith, Benjamin Shao, Paul Steinbart, Journal of the Association for Information Systems, Vol 10, Issue 2, Feb 2009
5. Towards Reliable Storage of 56-bit Secrets in Human Memory, Joseph Bonneau, Stuart Schechter, 23rd USENIX Security Symposium, Aug 2014
6. Can Long Passwords Be Secure and Usable?, Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip (Seyoung) Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Luho Bauer, Nicolas Christin, Lorrie Faith Cranor, CHI '14, Apr 2014

# For More Information

- PasswordResearch.com/Passphrases/
- Bruce K. Marshall   @PwdRsch on Twitter
- bkmarshall@passwordresearch.com