Passwords: You Are the Weakest Link

Or, Back to the Future

1985 Called they they
want their policy back.

WAY WEST
WILD WEST
HACKIN' FEST
2020
SAN DIEGO, CA | MARCH 11 – 13

In the beginning

- DoD determined a password length that will resist exhaustive enumeration attempt
- In 1985 Passwords should be 8 characters long because people are trying to guess them over a 1200 baud modem
  - Appendix C the Green Book
- It did give us this little hint: All else being equal, the longer the password, the greater the security it provides.

What the Experts Say: PCI

- Minimum length **SEVEN (7)** characters.
- Contain both numeric and alphabetic characters
  - Oh boy C=62
- Change passwords at least every 90 days
- Require that new passwords cannot be the same as the four previously used passwords

It's only money.

What the Experts Say: Microsoft

- – 8

- The primary goal of a more secure password system is password **diversity**. lots of different and hard to guess passwords.
- Maintain an 8-character minimum length requirement *longer isn't <u>necessarily</u> better* (WTF?!?)
- Don't require character composition requirements. For example, *&(^%
- Don't require mandatory periodic password resets for user accounts
- Ban common passwords
- Educate users no re-use of passwords
- Enforce registration for [multi-factor authentication]()
- Enable risk-based multi-factor authentication challenges

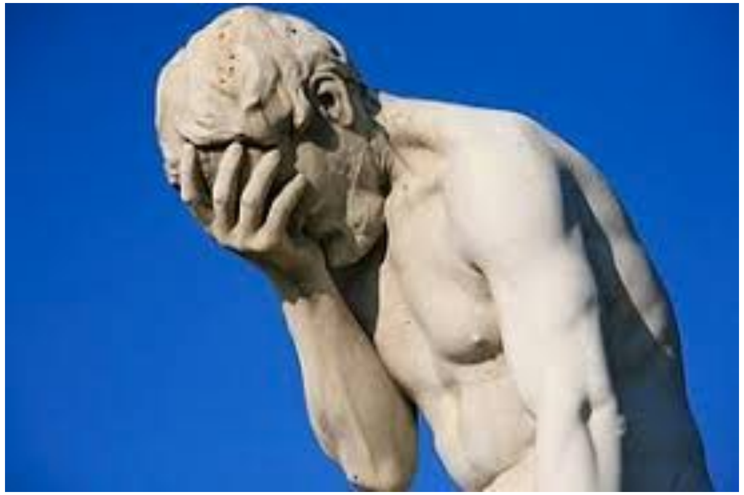
Against stupidity the very gods themselves contend in vain.
[Friedrich Schiller]()

https://docs.microsoft.com/en-us/office365/admin/misc/password-policy-recommendations?view=o365-worldwide

What the Experts Say: Microsoft

Requiring long passwords

- Password length requirements (>10 characters) **can** result in user behavior that is predictable and undesirable.
- users who are required to have a 16-character password **may** choose repeating patterns
  - **fourfourfourfour**
  - **passwordpassword**
  - meet character length not hard to guess.
- Length requirements increase the chances that users will adopt insecure practices, such as writing their passwords down, re-using them, or storing them unencrypted in their documents
- Encourage users to think about a unique password, we (Microsoft) recommends keeping a *reasonable* 8-character minimum length
  - (For the love of God no!)
- Ban Common Passwords
  - Yes and enforce it!
  - How is it different for 8 characters or 24 characters



What the Experts Say: NIST

- Special Publication 800-63-3
- Size matters minimum of 8 characters.
  - Et Tu Brute   But wait….
  - Better yet, NIST says you should allow a maximum length of at least 64, so no more "Sorry, your password can't be longer than 16 characters."
  - advise people to use passphrases, so they should be allowed to use all common punctuation characters and any language to improve usability and increase variety.
- Check new passwords against a dictionary of known-bad choices
- No composition rules.
  - ~~"Your password must contain one lowercase letter, one uppercase letter, one number, four symbols but not…."~~
- USE MULTI FACTOR AUTHENTICATION for all but the least sensitive applications

"William Burr (NIST 2003) says he basically got it wrong when it came to password advice"

What the Experts Say: NIST

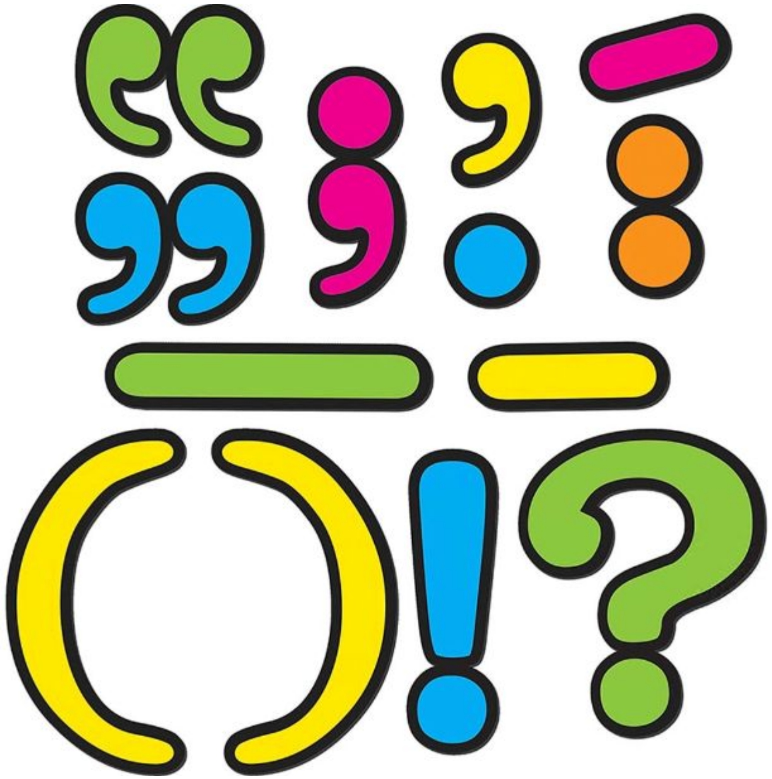
- No password hints
- No more expiration without reason
- All passwords must be hashed, salted and stretched
- SMS should no longer be used in two-factor authentication

What the Experts Say: Google

- Create your password using 8 characters or more.
- You can’t use a password that:
  - Is particularly weak. Example: “password123”
  - You have used before on your account
  - Starts or ends with a blank space
- Make your password longer and more memorable
  - Long passwords are stronger, so make your password at least 8 characters.

What the Experts Say: Apple

- Apple policy requires you use strong passwords with your Apple ID.
- Your password must have eight or more characters and include upper and lowercase letters, and at least one number.
- You can also add extra characters and punctuation marks to make your password even stronger.
- Apple also uses other password rules to make sure your password isn't easy to guess.



Still More Experts

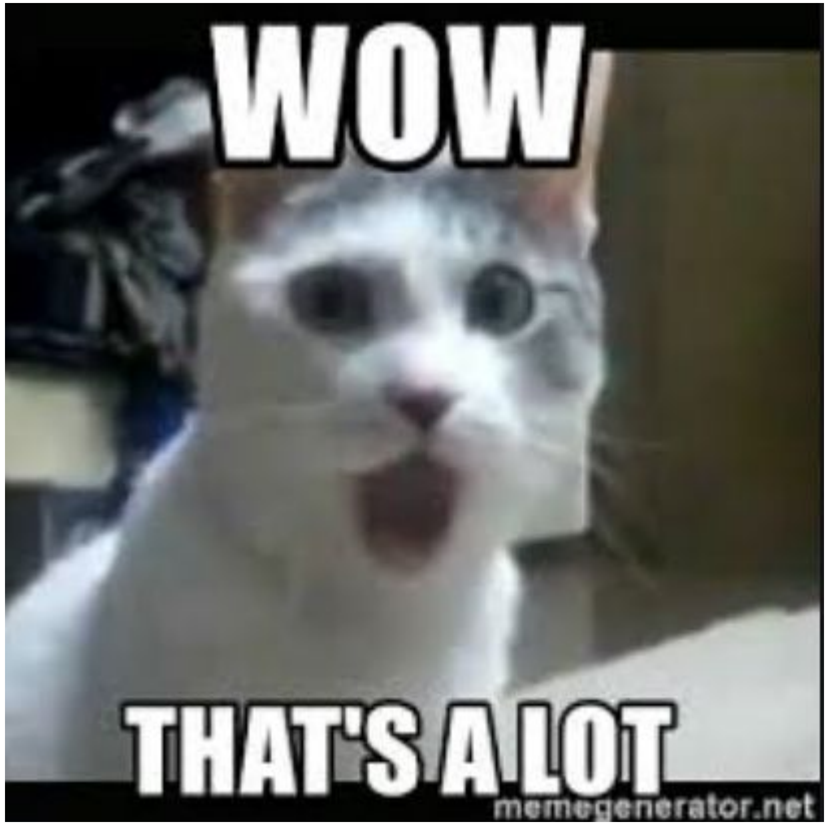
- Leo Laporte
  - 12-16 yeah, the computer guy
  - Love us some Leo
- It's better to allow people to use pass phrases
  - Bruce Schneier
- “A longer password is usually better than a more random password,”
  - Mark Burnett, author of Perfect Passwords, “as long as the password is at least 12-15 characters long.” from wired magazine
- Teen Vogue
  - 15 characters
- At least 15…. just to break lanman
  - BHIS and everyone else who does penetration testing

Who ya gonna call?

Are you gonna believe me or your lyin’ eyes?

Why 15 characters

- Brute Force
- Password Spray
- Password Cracking
  - LM Hash

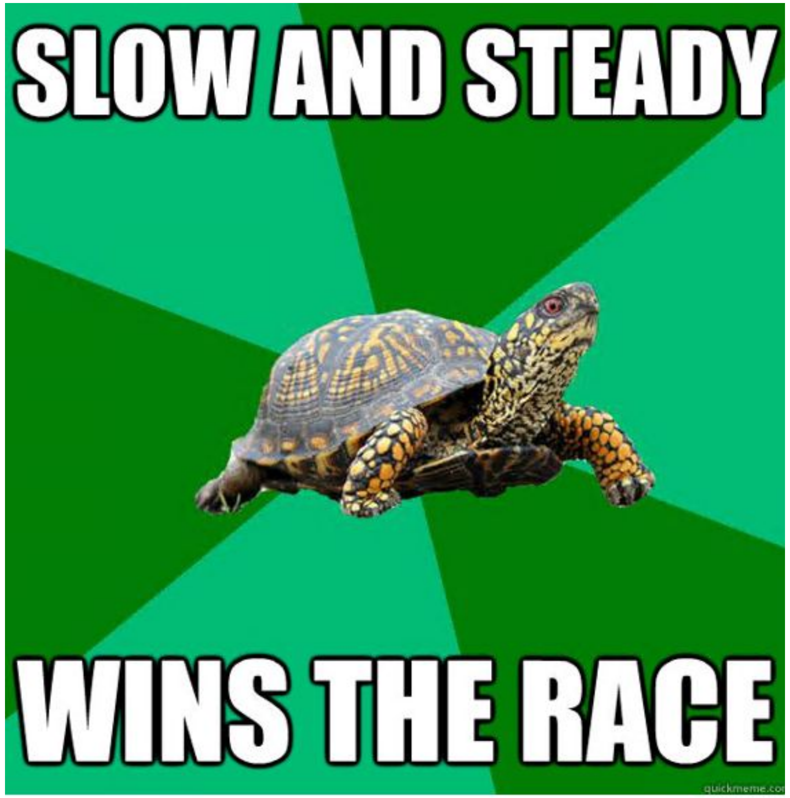


Brute Force

- Find portal with no lockout protections
- Guess passwords as fast as you can for a known user
- Hydra

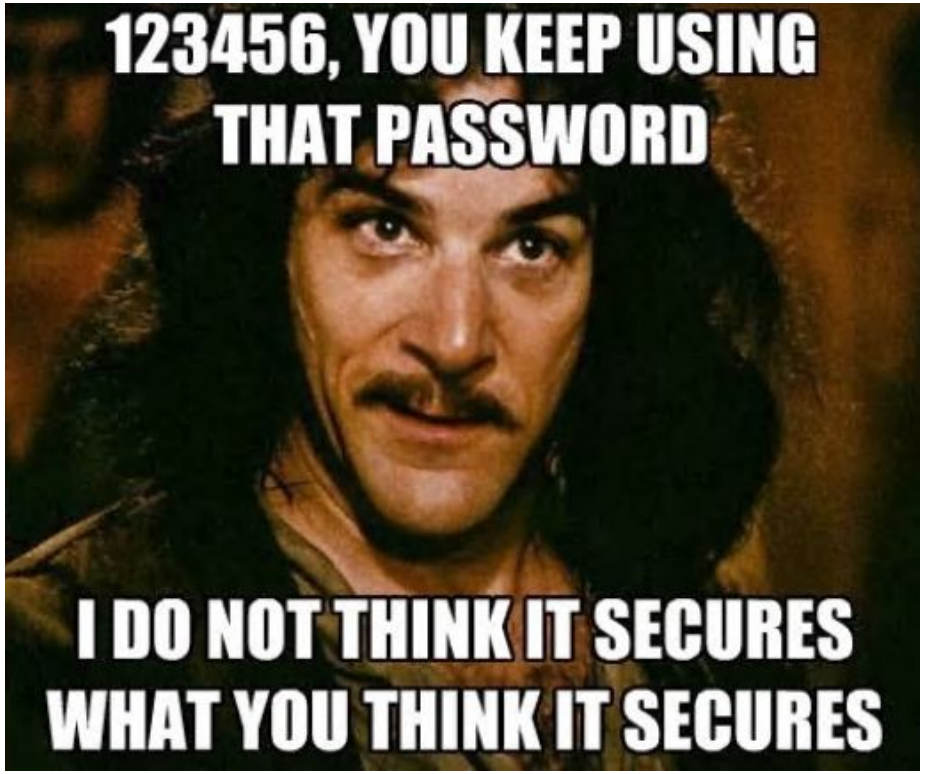
Password Spray

- Find a login portal
- Find as many users as possible
- Guess one password per user
  - BHIS max rate is 1 password per user per hour



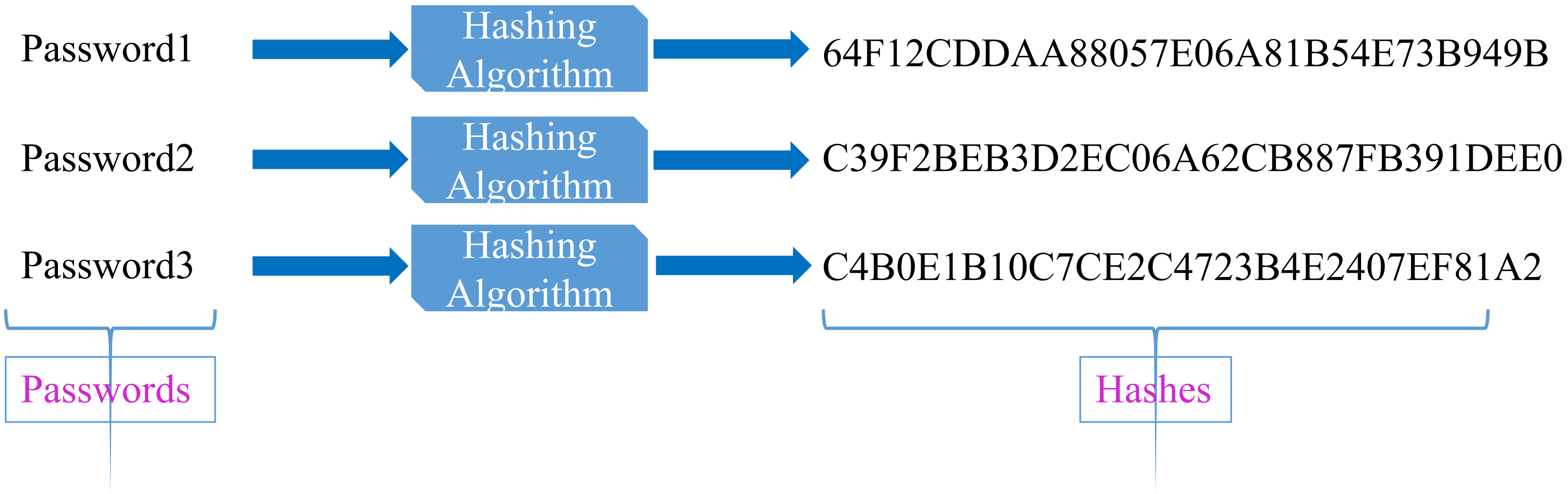
Password Spray

- Use easy to guess passwords
  - Winter2019
  - Winter2019!
  - Company123
- With large number of users (>1000) and 8-character password policy we will get in


123456, YOU KEEP USING THAT PASSWORD
I DO NOT THINK IT SECURES WHAT YOU THINK IT SECURES

Password Cracking

Computers (typically) store the hash of your password, not the password itself.



Password1 → Hashing Algorithm → 64F12CDDAA88057E06A81B54E73B949B

Password2 → Hashing Algorithm → C39F2BEB3D2EC06A62CB887FB391DEE0

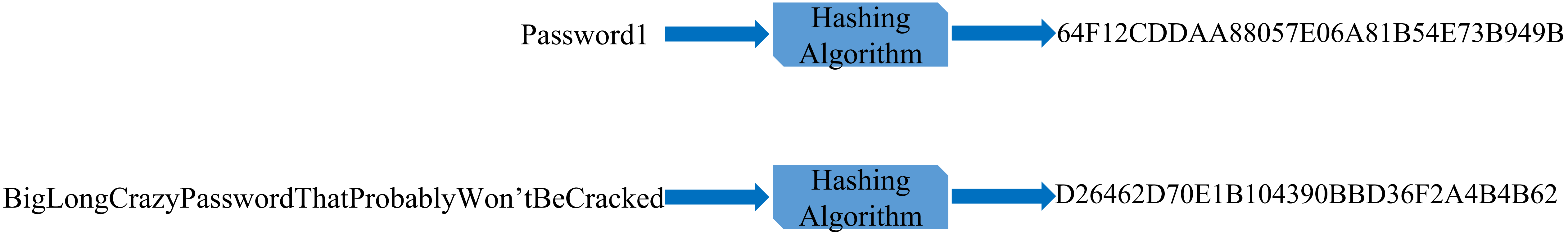
Password3 → Hashing Algorithm → C4B0E1B10C7CE2C4723B4E2407EF81A2

Passwords

Hashes

A Hashing Algorithm:

- Encodes data into a small, fixed size
  Always gives the same output for the same input

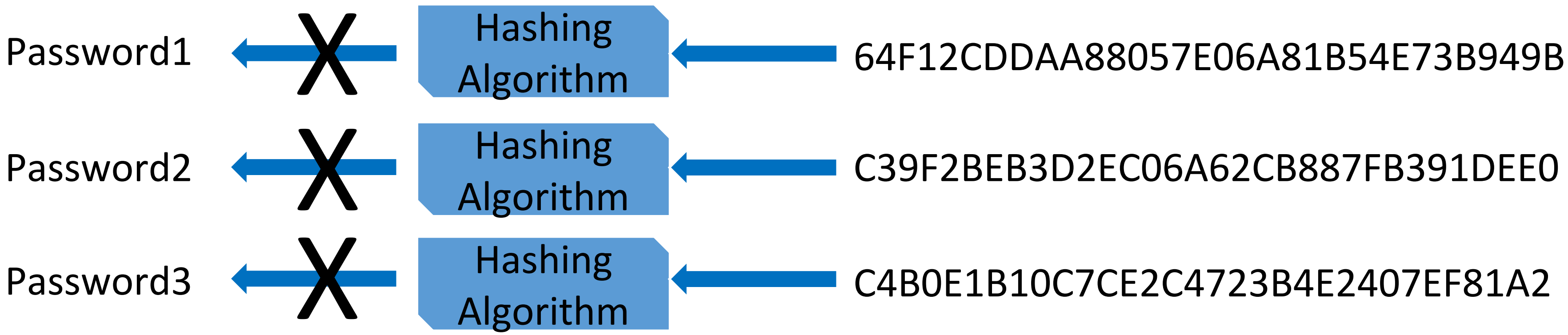


Password1 → Hashing Algorithm → 64F12CDDAA88057E06A81B54E73B949B

BigLongCrazyPasswordThatProbablyWon’tBeCracked → Hashing Algorithm → D26462D70E1B104390BBD36F2A4B4B62

More About Hashes

- Hashing algorithms are one-way algorithms, they are not reversible

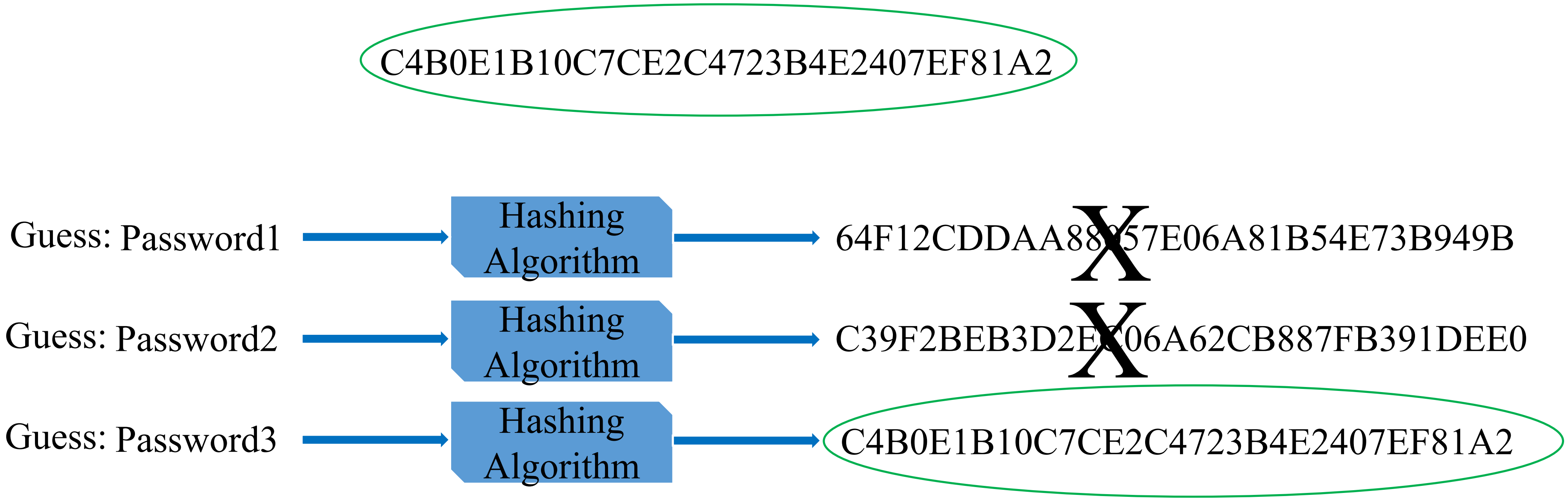


Password1 X Hashing Algorithm 64F12CDDAA88057E06A81B54E73B949B

Password2 X Hashing Algorithm C39F2BEB3D2EC06A62CB887FB391DEE0

Password3 X Hashing Algorithm C4B0E1B10C7CE2C4723B4E2407EF81A2

So What Is Password Cracking?



C4B0E1B10C7CE2C4723B4E2407EF81A2

Guess: Password1 → Hashing Algorithm → 64F12CDDAA88057E06A81B54E73B949B

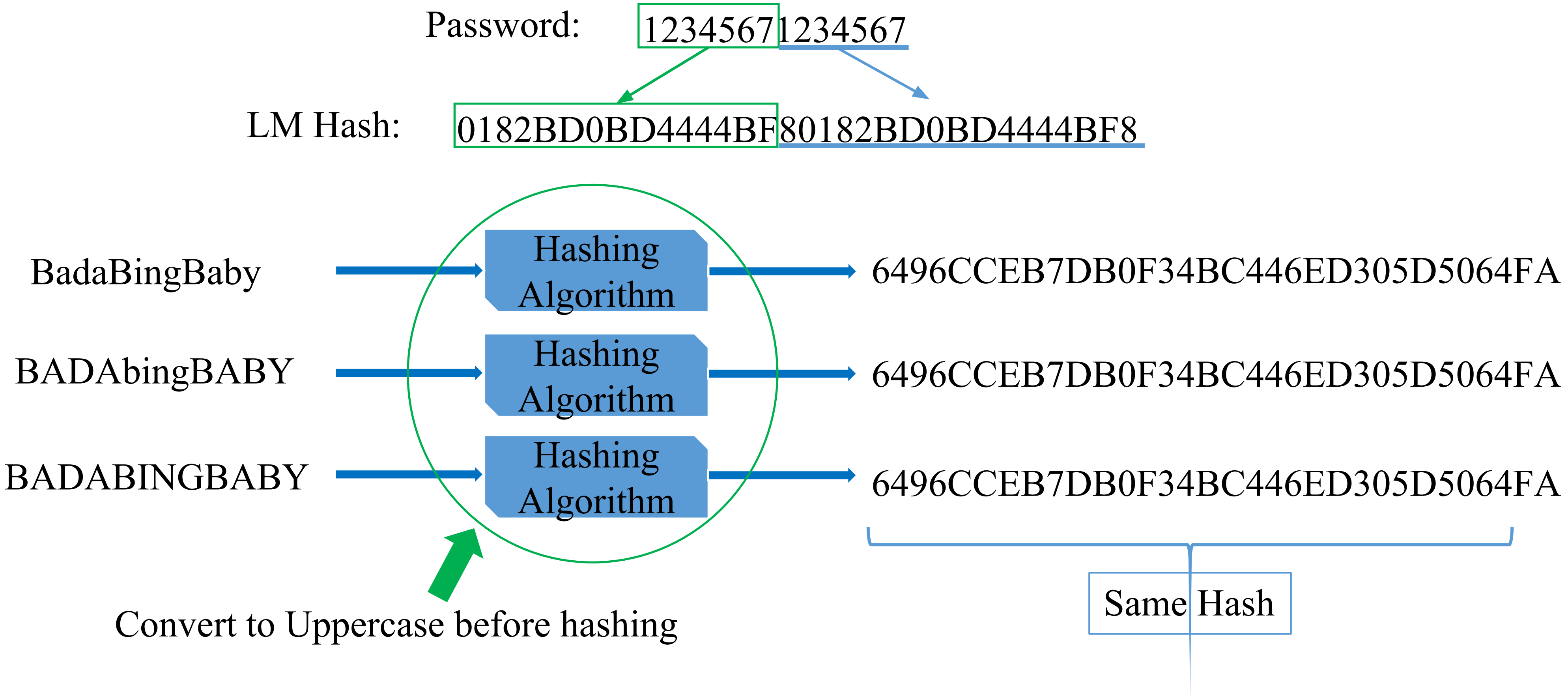
Guess: Password2 → Hashing Algorithm → C39F2BEB3D2EC06A62CB887FB391DEE0

Guess: Password3 → Hashing Algorithm → C4B0E1B10C7CE2C4723B4E2407EF81A2

Windows Hashes

- Windows stores two types of Password Hashes
  - Lan Manager (LM) Hashes
  - New Technology LM Hashes (NTLM)

The LM Hashing algorithm is older and only maintained for backward compatibility.



Password: 12345671234567

LM Hash: 0182BD0BD4444BF80182BD0BD4444BF8

BadaBingBaby → Hashing Algorithm → 6496CCEB7DB0F34BC446ED305D5064FA

BADAbingBABY → Hashing Algorithm → 6496CCEB7DB0F34BC446ED305D5064FA

BADABINGBABY → Hashing Algorithm → 6496CCEB7DB0F34BC446ED305D5064FA

Convert to Uppercase before hashing

Same Hash

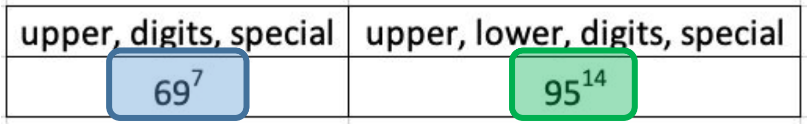
Maximum Password Length of 14 Characters

The LM hash is “Weak”

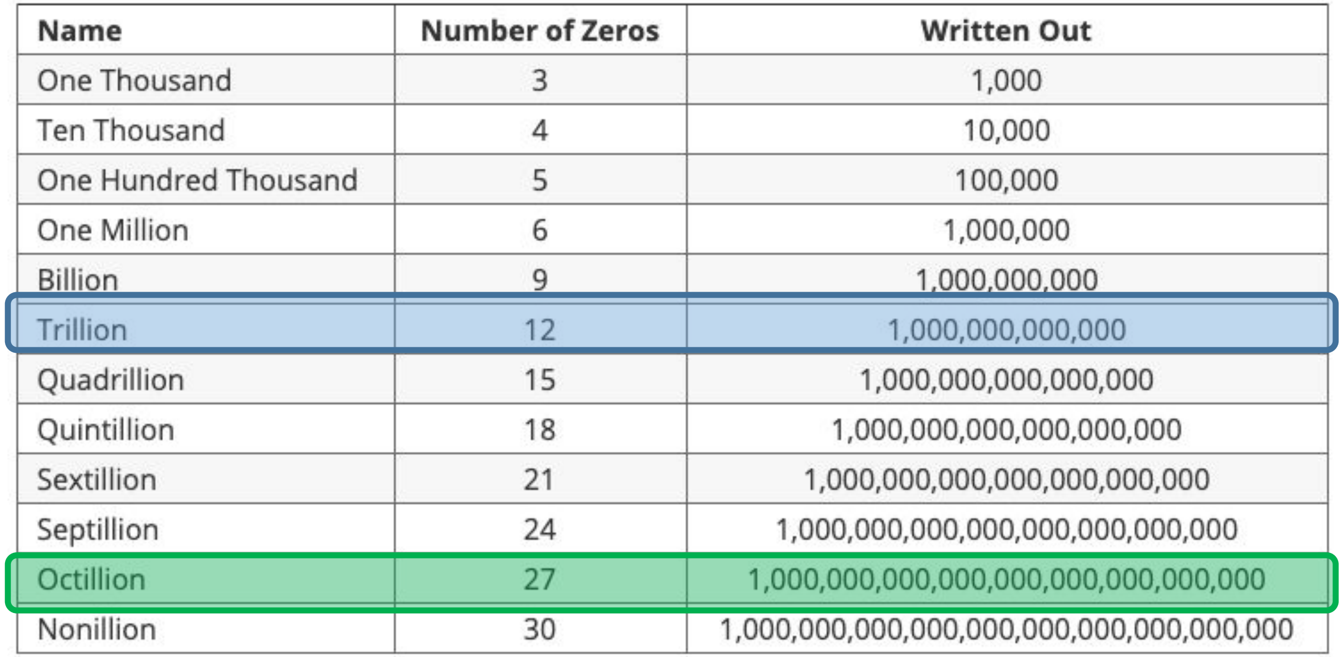
$$\text{Time}_{\text{crack7}} == \text{Time}_{\text{crack8}} == \text{Time}_{\text{crack14}}$$

Cracking 14-character passwords takes the same amount of time, because it is really just two 7-character passwords

Character set size:



upper, digits, special	upper, lower, digits, special
69^7	95^{14}



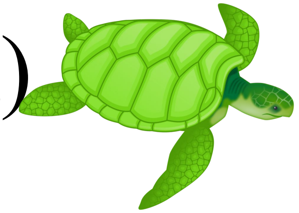
Name	Number of Zeros	Written Out
One Thousand	3	1,000
Ten Thousand	4	10,000
One Hundred Thousand	5	100,000
One Million	6	1,000,000
Billion	9	1,000,000,000
Trillion	12	1,000,000,000,000
Quadrillion	15	1,000,000,000,000,000
Quintillion	18	1,000,000,000,000,000,000
Sextillion	21	1,000,000,000,000,000,000,000
Septillion	24	1,000,000,000,000,000,000,000,000
Octillion	27	1,000,000,000,000,000,000,000,000,000
Nonillion	30	1,000,000,000,000,000,000,000,000,000,000

LM vs. NTLM Cracking

- 14 Character Password Cracking Speeds LM vs NTLM

<u>My Son's Computer</u>

8 minutes (LM Hash)

4.3 <u>billion years</u> (NTLM Hash)


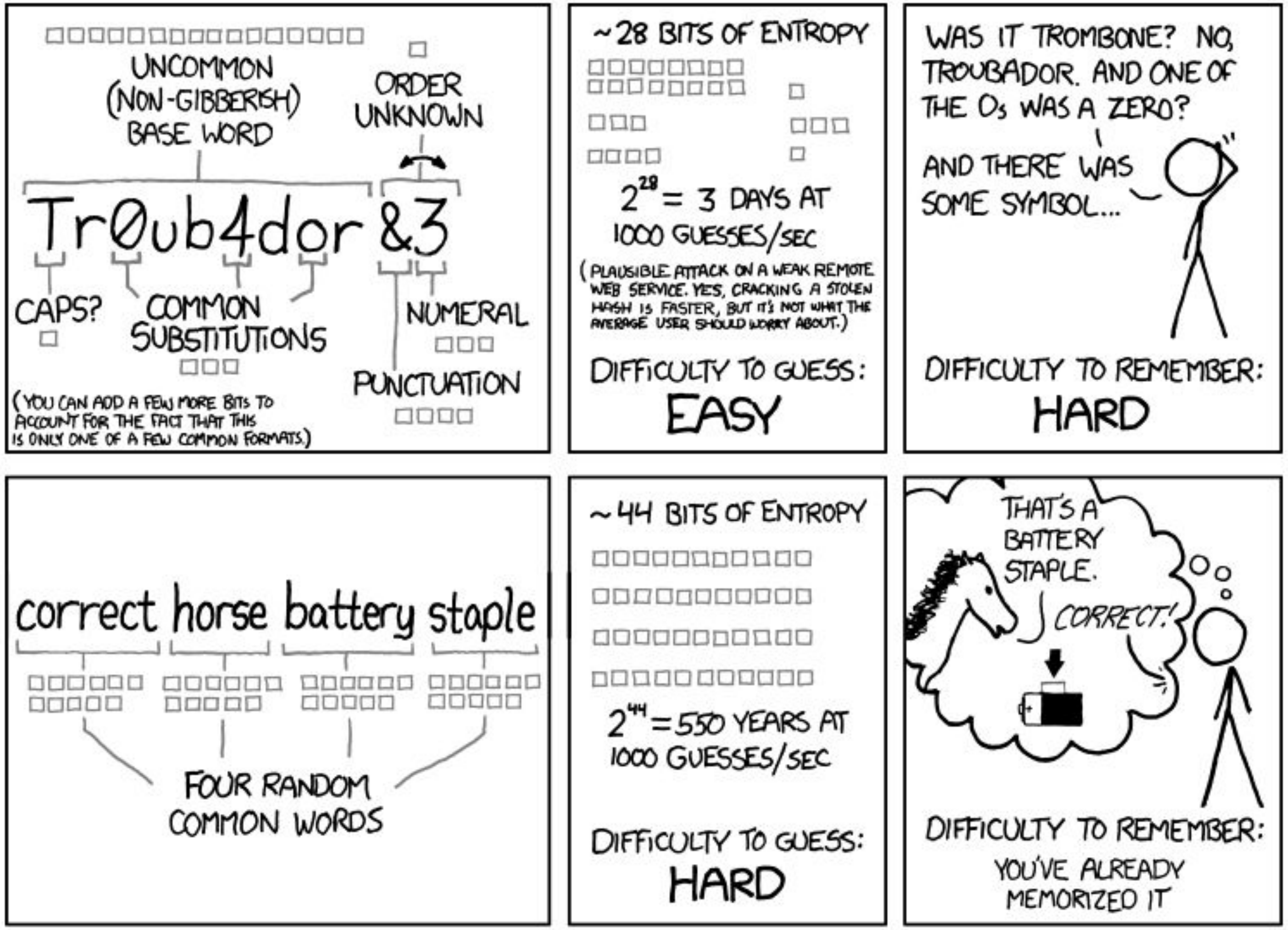
© Black Hills Information Security | @BHinfoSecurity

Why 15-character Passwords?

- Longer is stronger
- Impossible to save LM hash with 15-character password

LM Hash

CJ’s response to the problem


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.

All I really need to know I learned in kindergarten… or from cartoons

Now let's see the math

Wait, I was told there would be no math!

- log(C) / log(2) * L
  - C is the size of the character set
  - L the length of the password
- it is clear L has a predominant role in the calculation of the entropy bits
- C normally includes symbols, lower and upper case characters and number for a total of 96 possible characters or less

https://crambler.com/password-security-why-secure-passwords-need-length-over-complexity/

Math Examples

I'm not going to show my work!

Type	Password example	Time (HSIMP)	Time (PA)	Security Level
8 character common word	required	52 seconds	<1 day	Useless
8 random characters	qkcrmztd	52 seconds	<1 day	Useless
8 random chars w/numbers	kqwbv832	11 minutes	<1 day	Useless
8 random chars w/mixed case, symbols, & numbers	J5bZ>9p!	20 days	<1 day	Risky

https://crambler.com/password-security-why-secure-passwords-need-length-over-complexity/

Math Examples (cont’d)

There are other experts

Type	Password example	Time (HSIMP)	Time (PA)	Security Level
2 common word password	orange tea	98 days	<1 day	Risky
3 common word password	this is cool	546 years	<1 day	Risky
5 uncommon word password	du-bi-du-bi-doo	12 million years	<1 day	Risky

https://crambler.com/password-security-why-secure-passwords-need-length-over-complexity/

Math Examples (cont'd)

Choose wisely

Type	Password example	Time (HSIMP)	Time (PA)	Security Level
Passphrase 1	i own 2 dogs and 1 cat	1 sextillion years	330130 centuries	Secure forever
Passphrase 2	I own 2 dogs and 1 cat!	30 octillion years	8594846 centuries	Secure forever
Passphrase 3	#I own 2 dogs and 1 cat!?	285 nonillion years	1220882818 centuries	Secure forever

HSIMP = How Secure is My Password which assumes a brute-force attack keeps getting larger and larger

PA = Passfault Analyzer http://passfault.com/

https://crambler.com/password-security-why-secure-passwords-need-length-over-complexity/

From the field

- We password spray and win many times per year
- Details of winning
  - Password=password
  - Password=Winter2019!
  - Password=P@55word
- Our success rate against 15 character password….approaching zero
- Do as we do not as we say
  - BHIS > 20 character passwords and >24 for priv users
  - And it is easy!!
  - Password vaults
  - TWO FACTOR!!!

Molon Labe!

Would you like to play a game?

1. Hand out 3x5 cards to everyone, players put their name on both
2. Show and discuss your existing password policy
3. Players create password they have never used before that meets rules and hand in to the game master
4. Show and discuss a stronger alternative policy using pass phrases (Correct Horse Battery Staple)
5. Players create a password that meets this policy
6. Look through the cards and pull out bad passwords to discuss.
7. Now ask user to remember the passwords they wrote 10 minutes ago

Take Aways

- Perform tests on your company (with permission)
  - Password spray your own portals
  - Crack your own hashes
- Consider lengthening your passwords
- Consider 2FA
- Explicitly accept the risk if you do not choose one of the two above
- Train your users
- Train your leadership

Are you really going to let this guy decide?

- Security is <u>consultant</u> NOT owner of risk
- When you argue
  - Establish Facts
  - Then state opinions
  - Be effective
- Demonstrate risk
  - Spray yourself
  - Crack your own passwords
- Document your recommendations
  - Meeting minutes
  - E-mail
- Document risk decisions in a risk management matrix

DOGBERT'S PASSWORD RECOVERY SERVICE FOR MORONS
I DON'T REMEMBER MY PASSWORD.
IS IT "123"?
THAT'S JUST SPOOKY.
scottadams@aol.com
www.dilbert.com
©2007 Scott Adams, Inc./Dist. by UFS, Inc.

© Scott Adams, Inc./Dist. by UFS, Inc.

Don't give up. Don't give up. Don't give up. -- Peter Gabriel & Kate Bush

Resources

CSC-STD-002-85 "Green Book", DoD Password Management Guideline(April 12, 1985)
https://www.nist.gov/itl/tig/projects/special-publication-800-63
https://www.isacajournal-digital.org/isacajournal/2019_volume_1/MobilePagedArticle.action?articleId=1453151#articleId1453151
https://en.wikipedia.org/wiki/Password_strength#Human-generated_passwords
https://generatepasswords.org/how-to-calculate-entropy/
https://askleo.com/how_long_should_a_password_be/
https://resources.infosecinstitute.com/password-security-complexity-vs-length/#gref
https://www.xtontech.com/blog/longer-password-better/
https://crambler.com/password-security-why-secure-passwords-need-length-over-complexity/
https://nakedsecurity.sophos.com/2016/08/18/nists-new-password-rules-what-you-need-to-know/
https://docs.microsoft.com/en-us/office365/admin/misc/password-policy-recommendations?view=o365-worldwide

Resources

https://nakedsecurity.sophos.com/2016/08/18/nists-new-password-rules-what-you-need-to-know/
https://www.correcthorsebatterystaple.net/