Password Security & Best Practices

Neil Lubke
Network Engineer
School District of Milton
lubken@milton.k12.wi.us

http://bit.ly/32Ha07u

Spoilers!

- **USE** a good password manager
- **USE** 2-factor authentication EVERYWHERE it is possible
- **MAKE** an emergency plan to keep access to your passwords

http://bit.ly/32Ha07u

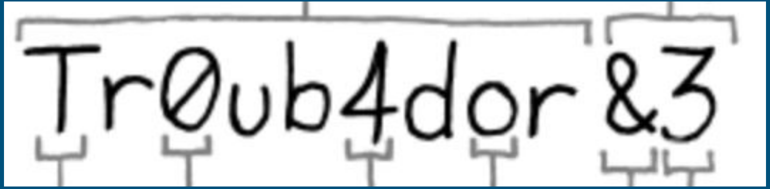
Current Security Challenges

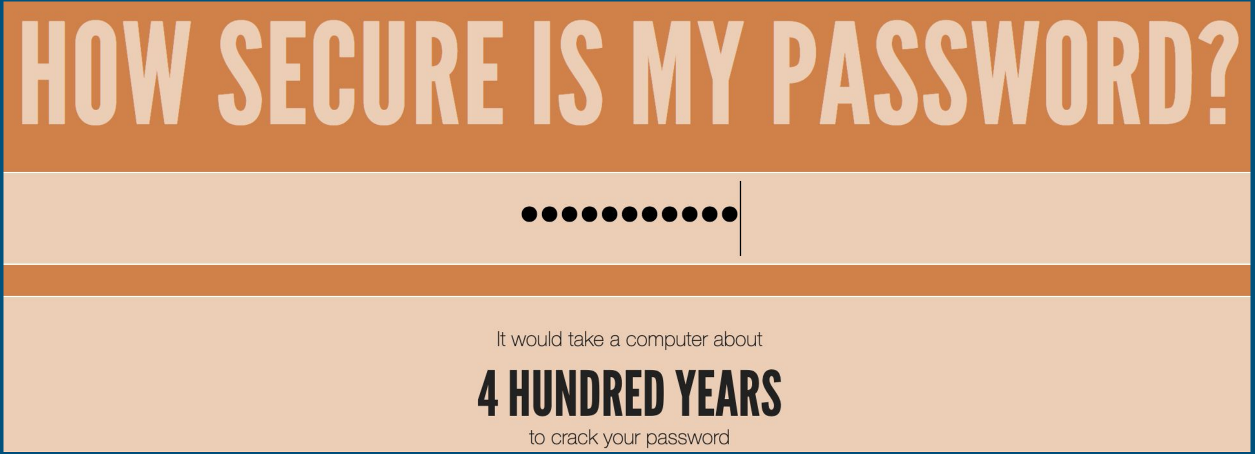
- Good passwords hard to remember
- Forced password changes
- Predictable iteration
- Data Breaches
- Social Engineering/Phishing
- Password re-use

http://bit.ly/32Ha07u

What makes a strong password?

https://howsecureismypassword.net/




HOW SECURE IS MY PASSWORD?

●●●●●●●●●●●

It would take a computer about

4 HUNDRED YEARS

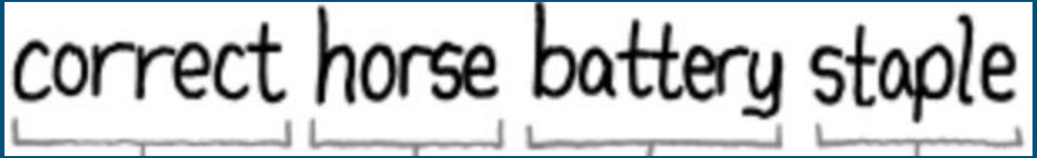
to crack your password

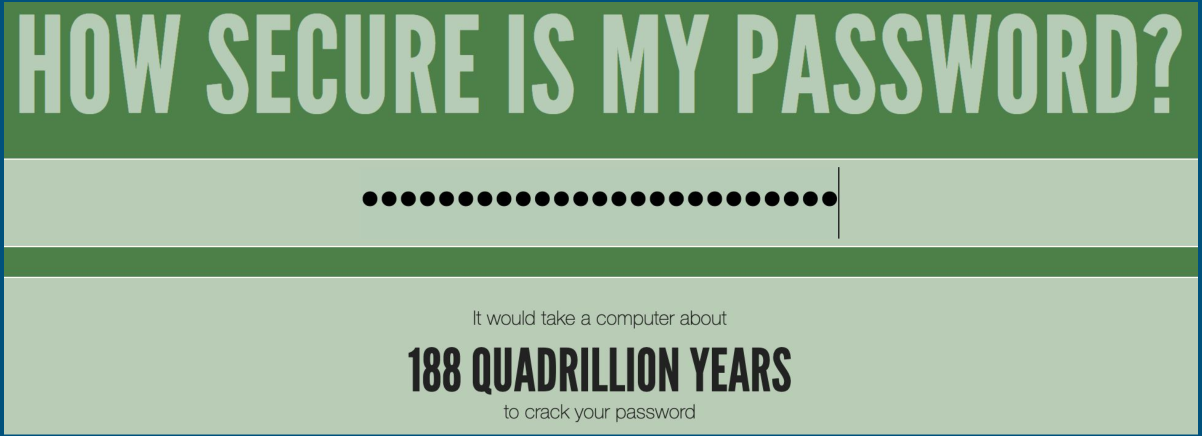
https://xkcd.com/936/

http://bit.ly/32Ha07u

What makes a strong password?

https://howsecureismypassword.net/




HOW SECURE IS MY PASSWORD?

●●●●●●●●●●●●●●●●●●●●●●●●●

It would take a computer about

188 QUADRILLION YEARS

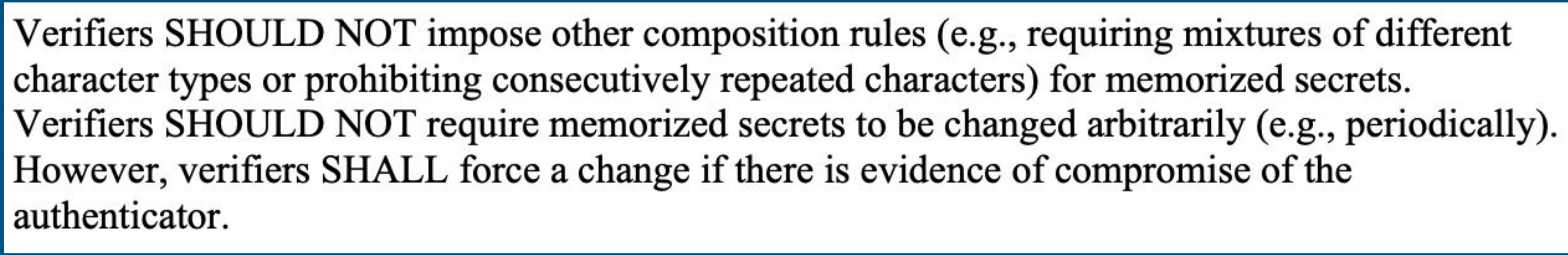
to crack your password

https://xkcd.com/936/

http://bit.ly/32Ha07u

Forced Password Changes

- If you like your password, you can keep it!
- https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf



Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets. Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.

http://bit.ly/32Ha07u

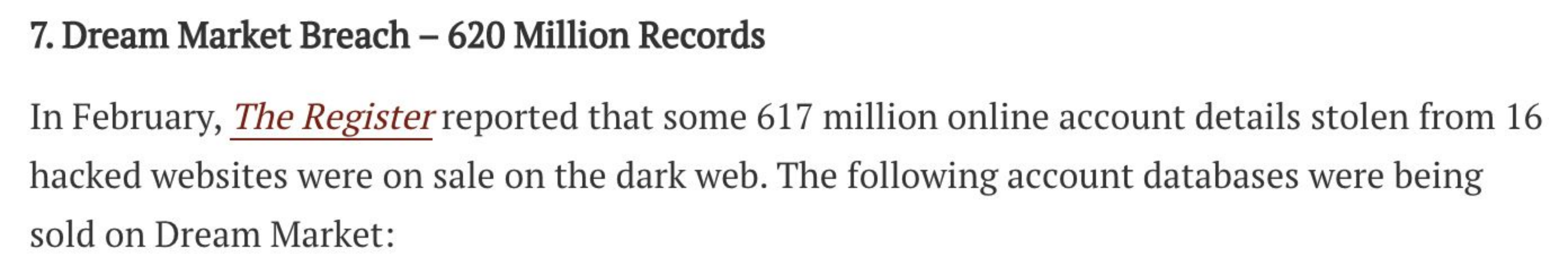
Predictable Iteration

- Complexity requirements: 3 out of 4 upper, lower, number, symbol
- Password1
- Spring2019

When these passwords expire in 90 days - what’s next?

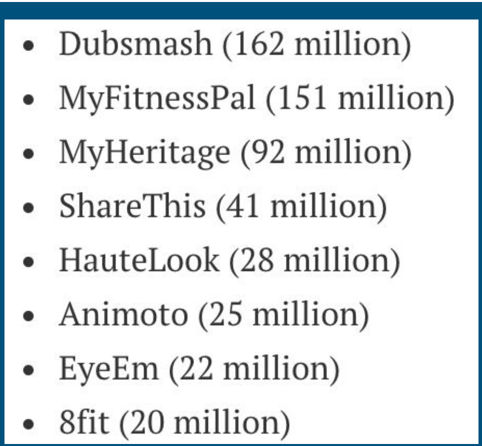
Data Breaches

https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019

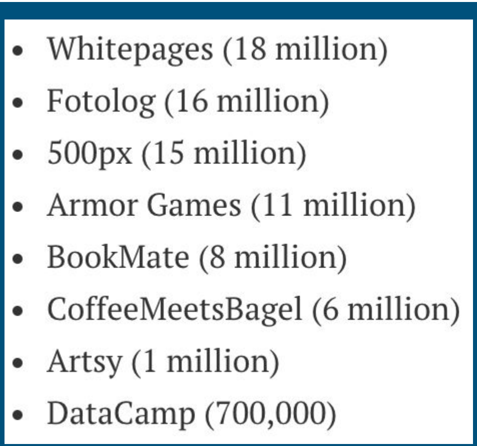


7. Dream Market Breach – 620 Million Records

In February, *The Register* reported that some 617 million online account details stolen from 16 hacked websites were on sale on the dark web. The following account databases were being sold on Dream Market:



- Dubsmash (162 million)
- MyFitnessPal (151 million)
- MyHeritage (92 million)
- ShareThis (41 million)
- HauteLook (28 million)
- Animoto (25 million)
- EyeEm (22 million)
- 8fit (20 million)

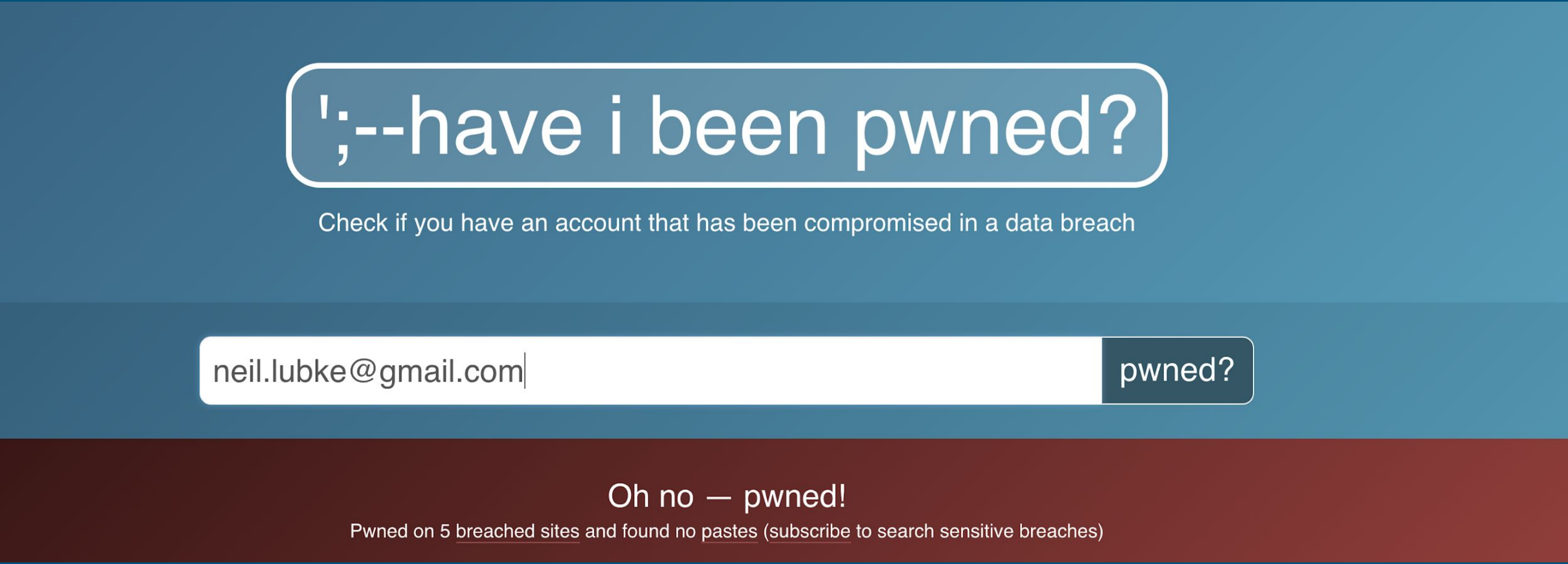


- Whitepages (18 million)
- Fotolog (16 million)
- 500px (15 million)
- Armor Games (11 million)
- BookMate (8 million)
- CoffeeMeetsBagel (6 million)
- Artsy (1 million)
- DataCamp (700,000)

http://bit.ly/32Ha07u

Email Breach Database

https://haveibeenpwned.com/



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

neil.lubke@gmail.com

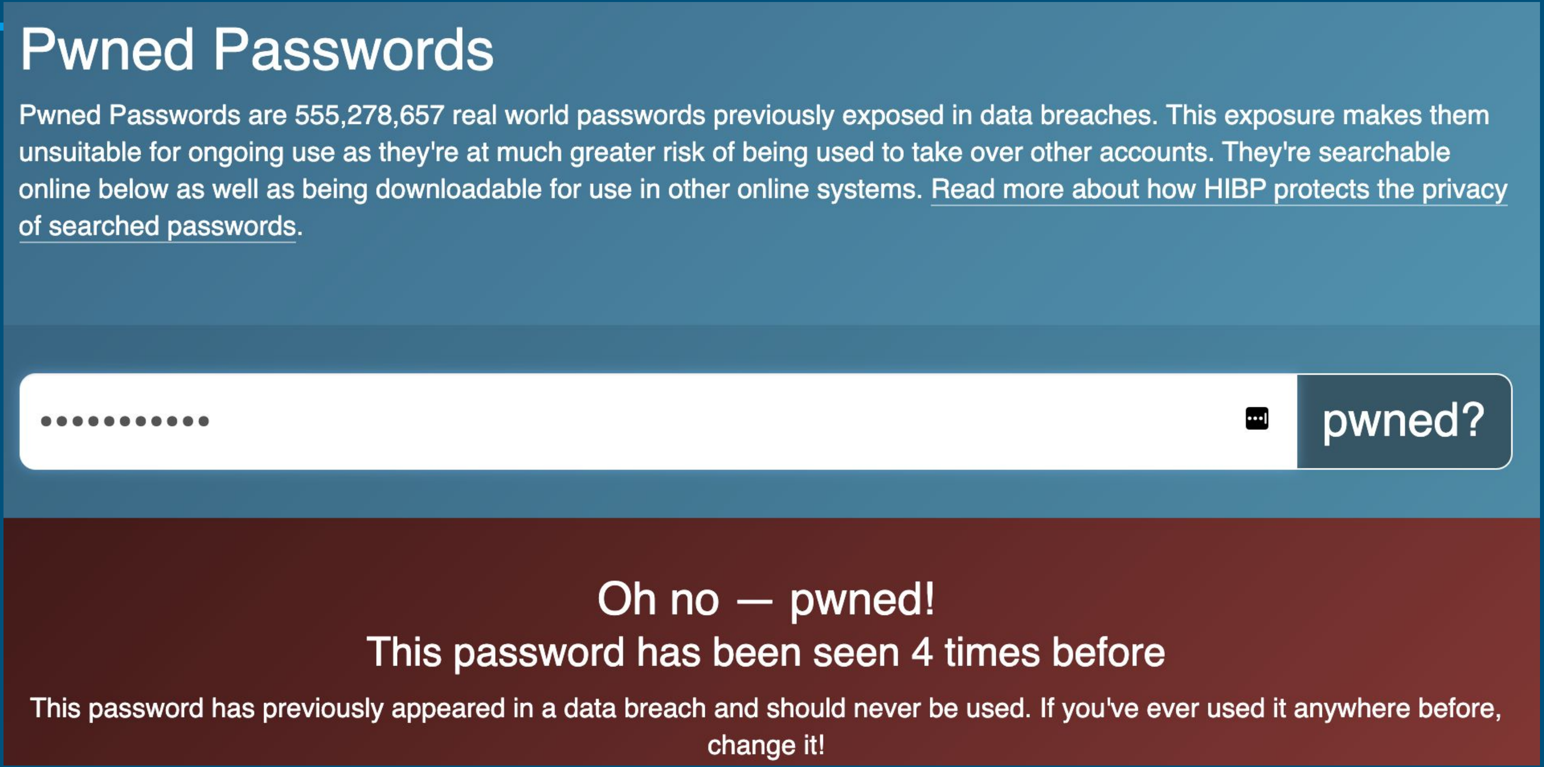
Oh no — pwned!

Pwned on 5 breached sites and found no pastes (subscribe to search sensitive breaches)

http://bit.ly/32Ha07u

Password Breach Database

https://haveibeenpwned.com/Passwords



Pwned Passwords

Pwned Passwords are 555,278,657 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.

Oh no — pwned!

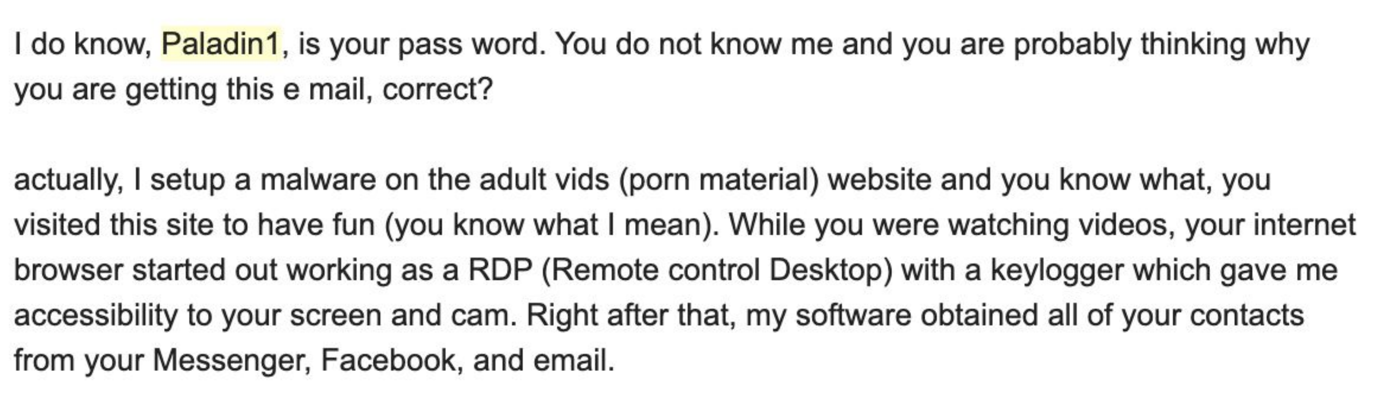
This password has been seen 4 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

http://bit.ly/32Ha07u

Social Engineering/Phishing

- A strong password won't save you if someone can convince you to give it to them
- Recently hand-in-hand with data breaches

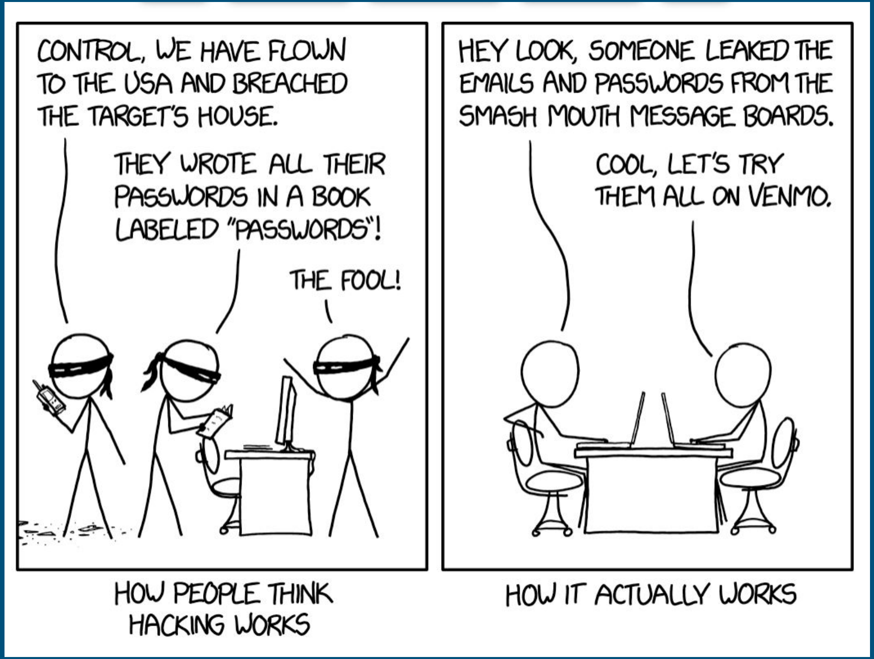


I do know, Paladin1, is your pass word. You do not know me and you are probably thinking why you are getting this e mail, correct?

actually, I setup a malware on the adult vids (porn material) website and you know what, you visited this site to have fun (you know what I mean). While you were watching videos, your internet browser started out working as a RDP (Remote control Desktop) with a keylogger which gave me accessibility to your screen and cam. Right after that, my software obtained all of your contacts from your Messenger, Facebook, and email.

http://bit.ly/32Ha07u

Password re-use


CONTROL, WE HAVE FLOWN TO THE USA AND BREACHED THE TARGET'S HOUSE.
THEY WROTE ALL THEIR PASSWORDS IN A BOOK LABELED "PASSWORDS"!
THE FOOL!
HEY LOOK, SOMEONE LEAKED THE EMAILS AND PASSWORDS FROM THE SMASH MOUTH MESSAGE BOARDS.
COOL, LET'S TRY THEM ALL ON VENMO.
HOW PEOPLE THINK HACKING WORKS
HOW IT ACTUALLY WORKS

https://xkcd.com/2176/

http://bit.ly/32Ha07u

So many problems!

- Good passwords hard to remember
- Forced password changes
- Predictable iteration
- Data Breaches
- Social Engineering/Phishing
- Password re-use

http://bit.ly/32Ha07u

Solution? One Password To Rule Them All

http://bit.ly/32Ha07u

Current best practice?

Use a password manager

LastPass•••|

bitwarden

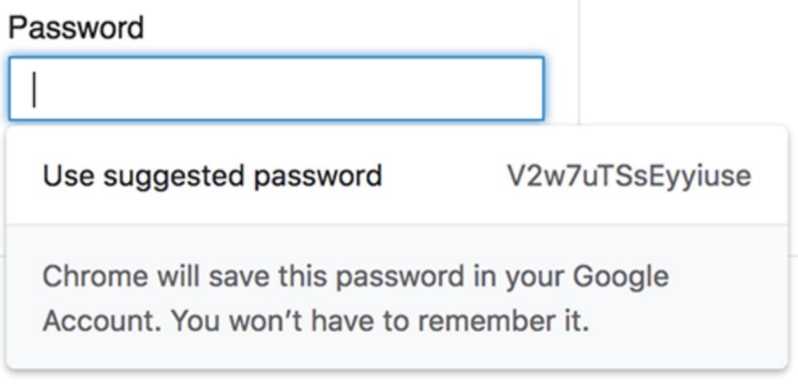
dashlane

1Password

http://bit.ly/32Ha07u

Default Password Managers

Google SmartLock

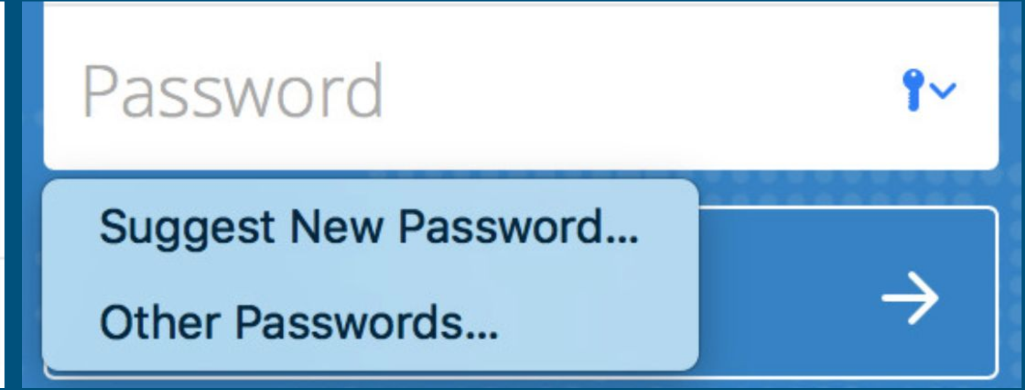


Password

Use suggested password V2w7uTSsEyyiuse

Chrome will save this password in your Google Account. You won't have to remember it.

Apple KeyChain



http://bit.ly/32Ha07u

Password Manager Considerations

- NON default BUT integrates directly in iOS12+
- Cross platform: iOS/Android, Chrome/Firefox/Safari/Edge, Mac app, windows 10 app
- Generates strong, random passwords for each account and saves them
- Can auto-change some passwords
- Can auto-check your email address against database of known compromised accounts
  - Chrome starting to integrate password checking as a feature in 79
- Checks your vault for weak, reused, and compromised passwords
- Family shared folders
- Password manager not silver bullet for security - it SHIFTS risk and MITIGATES the most common attacks when implemented properly

http://bit.ly/32Ha07u

Password Manager Word of Caution

Caution: Having everything in one place means you

NEED

- **STRONG** master password
  - Unique
  - Long
  - Memorable
- 2FA or MFA
- Emergency plan

http://bit.ly/32Ha07u

2FA or MFA

Multifactor authentication

- SMS Text message (most common)
- Generic authenticator app
  - Google Authenticator
  - Authy
  - LastPass Authenticator
- App/platform-specific authenticator
  - Apple
  - Steam
  - Blizzard

- Biometric
  - Fingerprint
  - Face ID
- Physical
  - YubiKey
  - Thetis
  - Google Titan

http://bit.ly/32Ha07u

LastPass & MFA Demo

http://bit.ly/32Ha07u

Emergency Plan

Passwords access plan

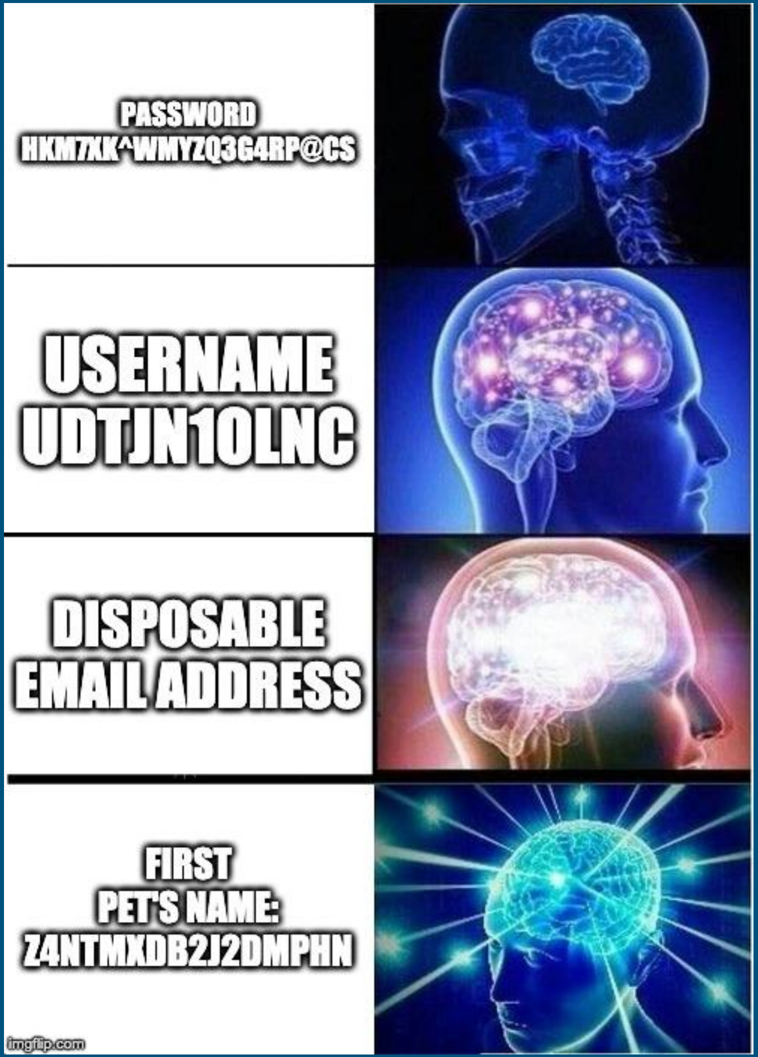
- delegate emergency access
- Printed physical copy of vault kept in a safe

2FA/MFA access plan

- Print/save backup codes
- Additional factors/methods
  - Google Prompt
  - Authenticator app
  - SMS
    - SIM jacking

http://bit.ly/32Ha07u

Paranoia!



http://bit.ly/32Ha07u

Topics NOT covered

Policy for departments

- START with policy and work your way into practice
- Policy should address complexity and expiration

Tools for teams

- Use a shared secure database, whether local or cloud
  - KeePass
  - LastPass Teams
  - Secret Server

Alternate email addresses

- Personal Gmail can use . and + https://www.lifewire.com/easy-gmail-address-hacks-1616186
- Yahoo allows disposable email addresses https://help.yahoo.com/kb/SLN28338.html

Takeaways

- **USE** a good password manager
- **USE** 2-factor authentication EVERYWHERE it is possible
- **MAKE** an emergency plan to keep access to your passwords

http://bit.ly/32Ha07u

Slideshow link

http://bit.ly/32Ha07u