PASSWORDS – YOU'RE DOING IT ALL WRONG!

We're following Best Practices for password construction, storage, etc. But what if the Best Practices are WRONG?

AARON CURE
STEVE KOSTEN
March 5, 2020

Introduction: Aaron Cure

Principal Security Consultant

SANS Instructor

- DEV544: Secure Coding in .NET
- SEC542: Web App Penetration Testing and Ethical Hacking

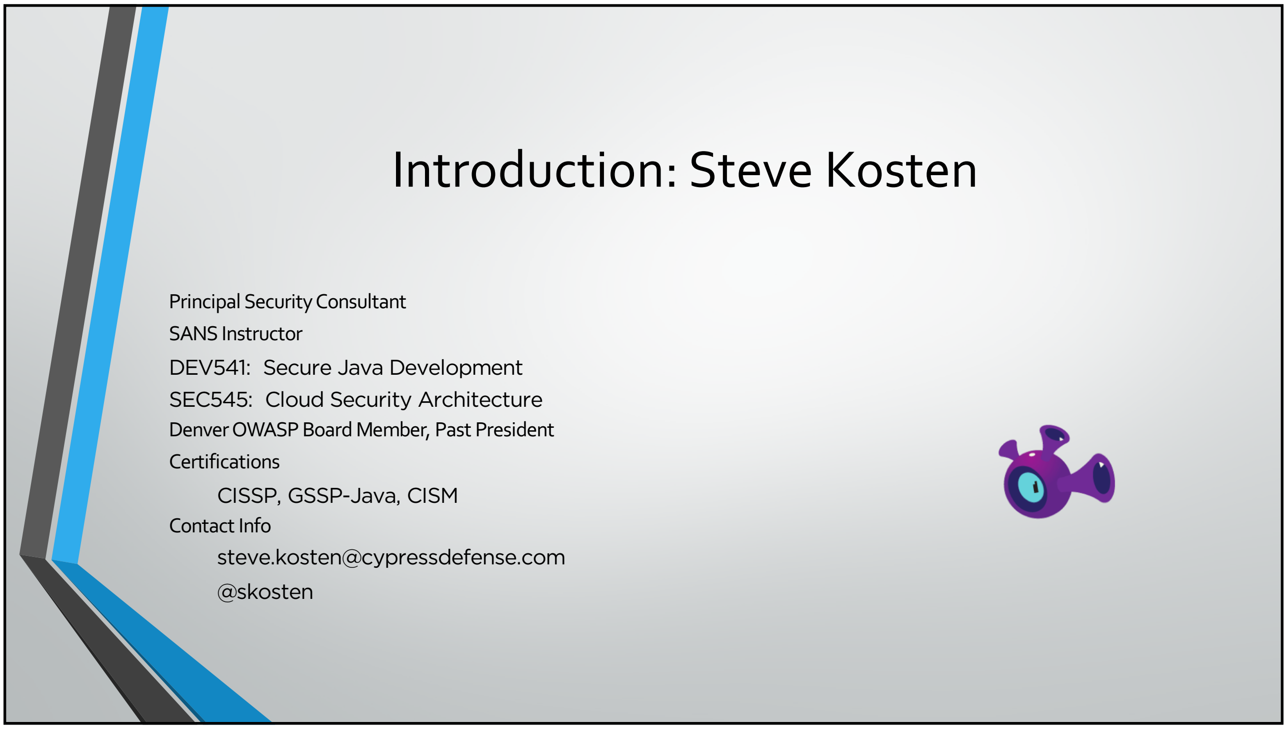
Denver OWASP Board Member

Certifications

- CISSP, GSSP.NET, GWAPT, GPEN, GMOB

Contact Info

- aaron.cure@cypressdefense.com
- @curea



Introduction: Steve Kosten

Principal Security Consultant

SANS Instructor

DEV541: Secure Java Development

SEC545: Cloud Security Architecture

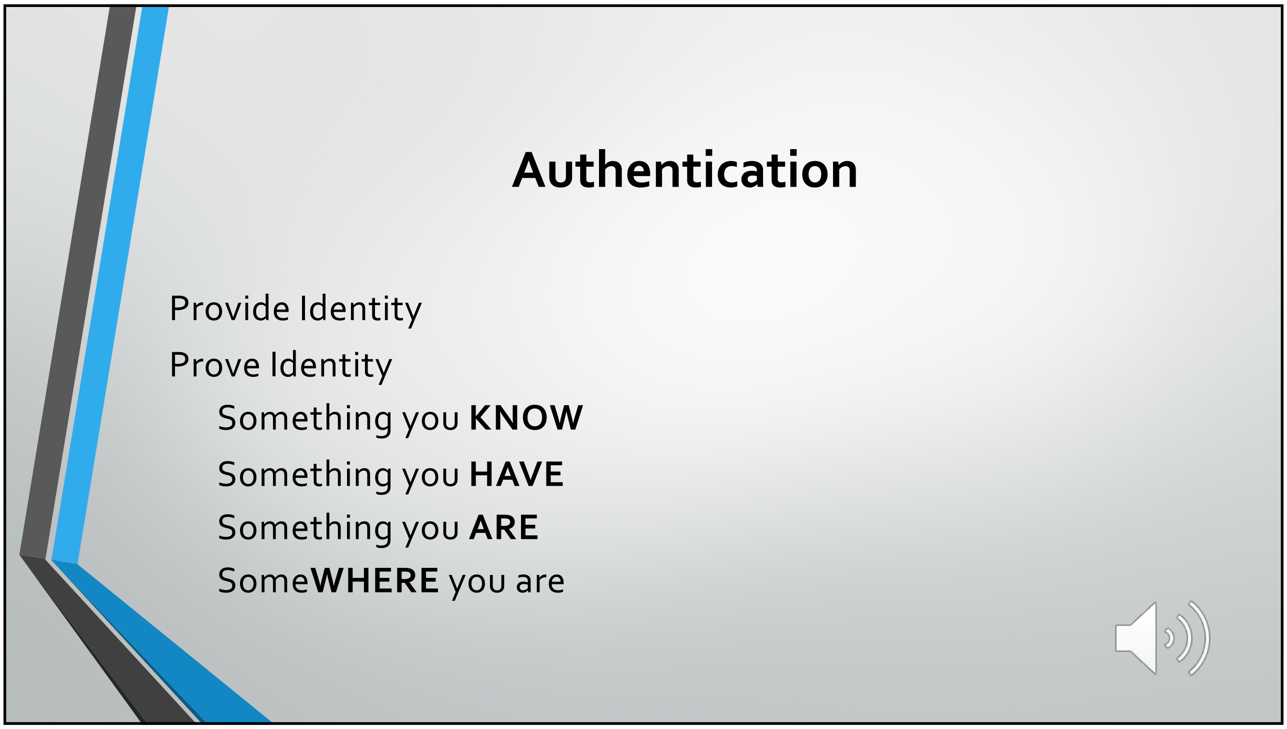
Denver OWASP Board Member, Past President

Certifications

- CISSP, GSSP-Java, CISM

Contact Info

- steve.kosten@cypressdefense.com
- @skosten



Authentication

Provide Identity

Prove Identity

- Something you **KNOW**
- Something you **HAVE**
- Something you **ARE**
- Some**WHERE** you are

Password History

Goes back ages …

Well before WWII …. But we'll start there:

IFF (Identify Friend or Foe)
Challenge / Response

"flash" / "thunder"

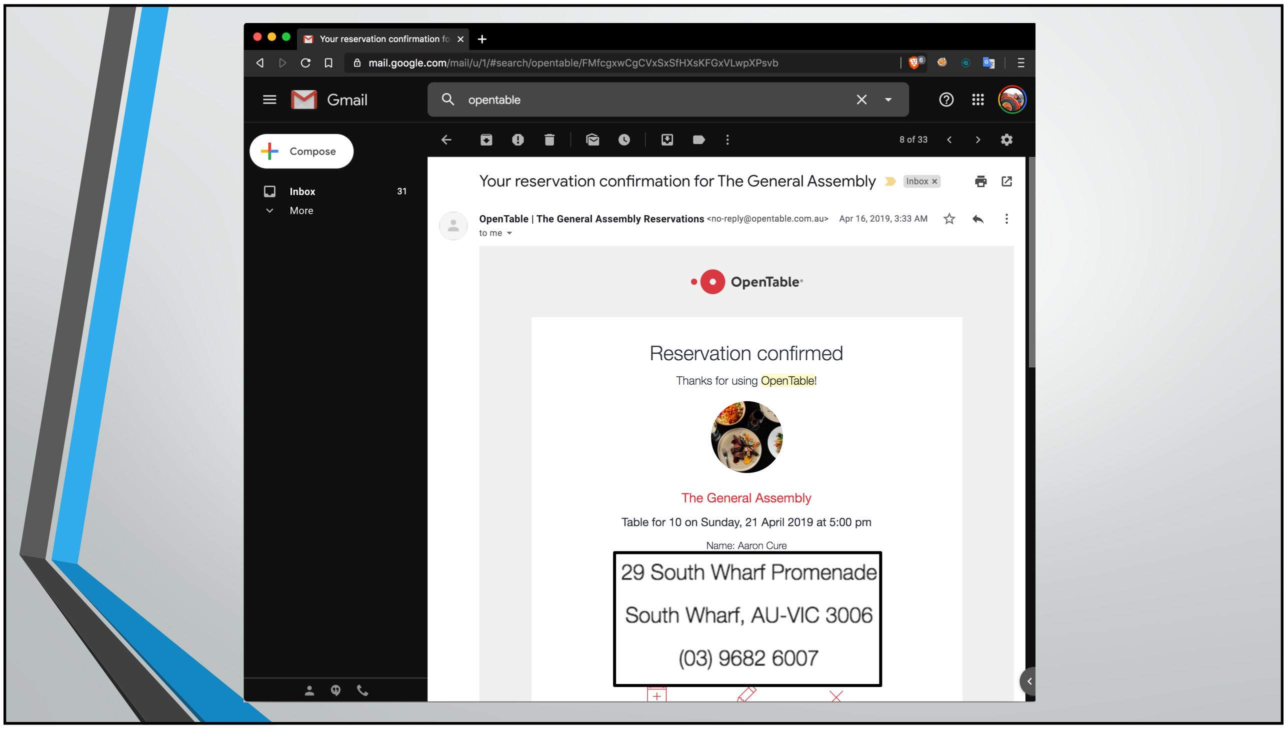
Cricket Clicker

only as good as its ability to remain a secret

MY

favorite password

TigGer99


Your reservation confirmation fo
mail.google.com/mail/u/1/#search/opentable/FMfcgxwCgCVxSxSfHXsKFGxVLwpXPsvb
Gmail
opentable
Compose
Inbox 31
More
8 of 33
Inbox ×
OpenTable

Your reservation confirmation for The General Assembly

OpenTable | The General Assembly Reservations <no-reply@opentable.com.au> Apr 16, 2019, 3:33 AM
to me

Reservation confirmed

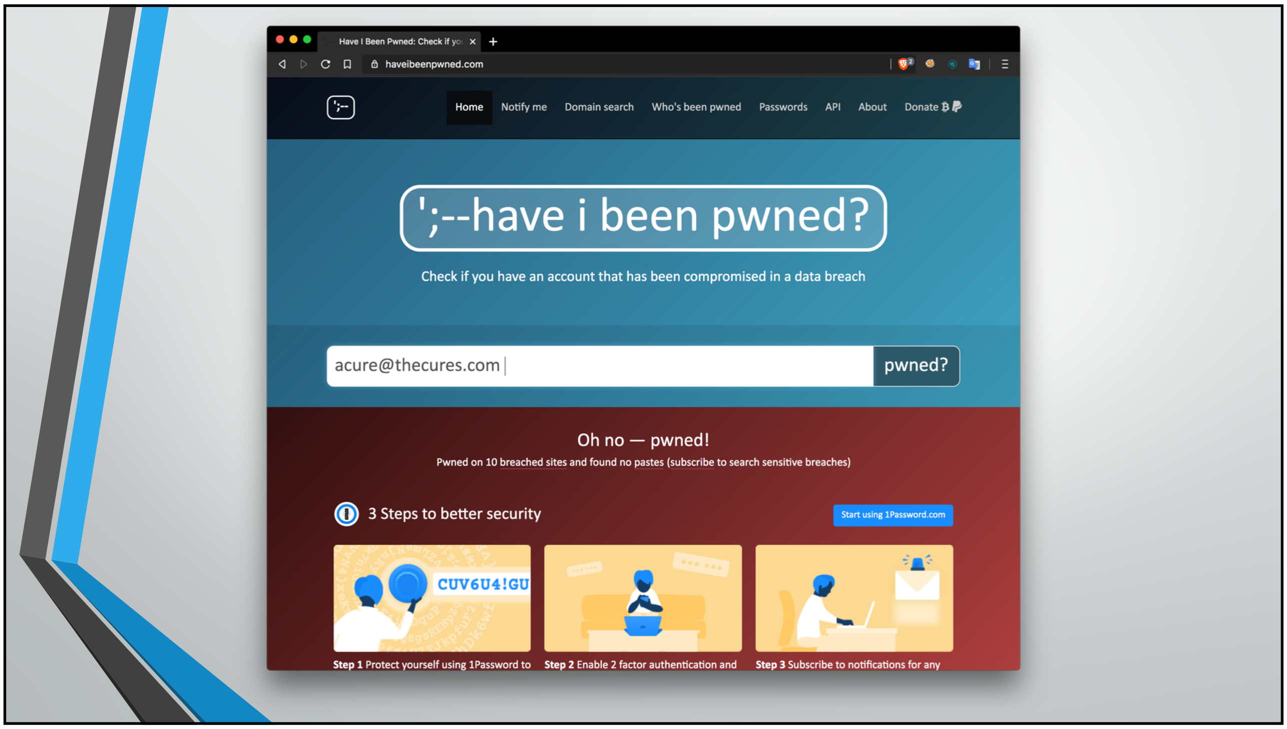
Thanks for using OpenTable!

The General Assembly

Table for 10 on Sunday, 21 April 2019 at 5:00 pm

Name: Aaron Cure

29 South Wharf Promenade
South Wharf, AU-VIC 3006
(03) 9682 6007



';--have i been pwned?

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

acure@thecures.com

Oh no — pwned!

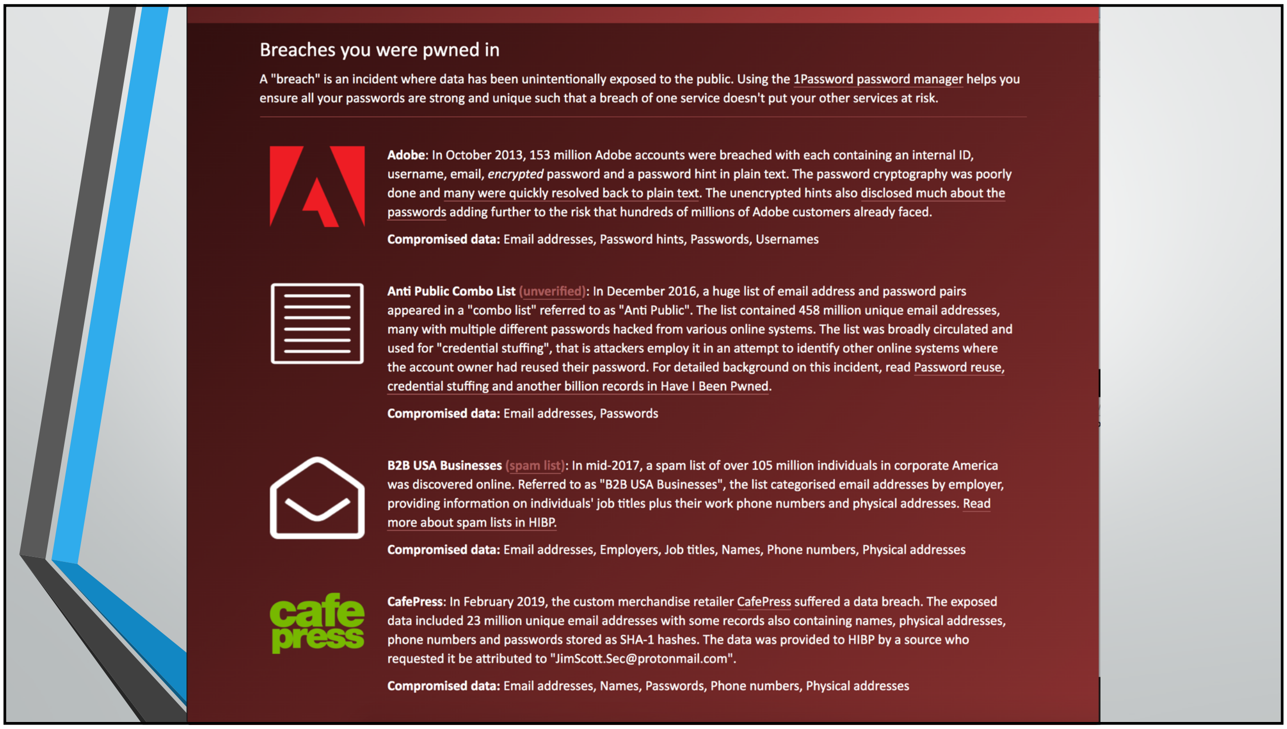
Pwned on 10 breached sites and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Step 1 Protect yourself using 1Password to

Step 2 Enable 2 factor authentication and

Step 3 Subscribe to notifications for any



Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Anti Public Combo List (unverified): In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.

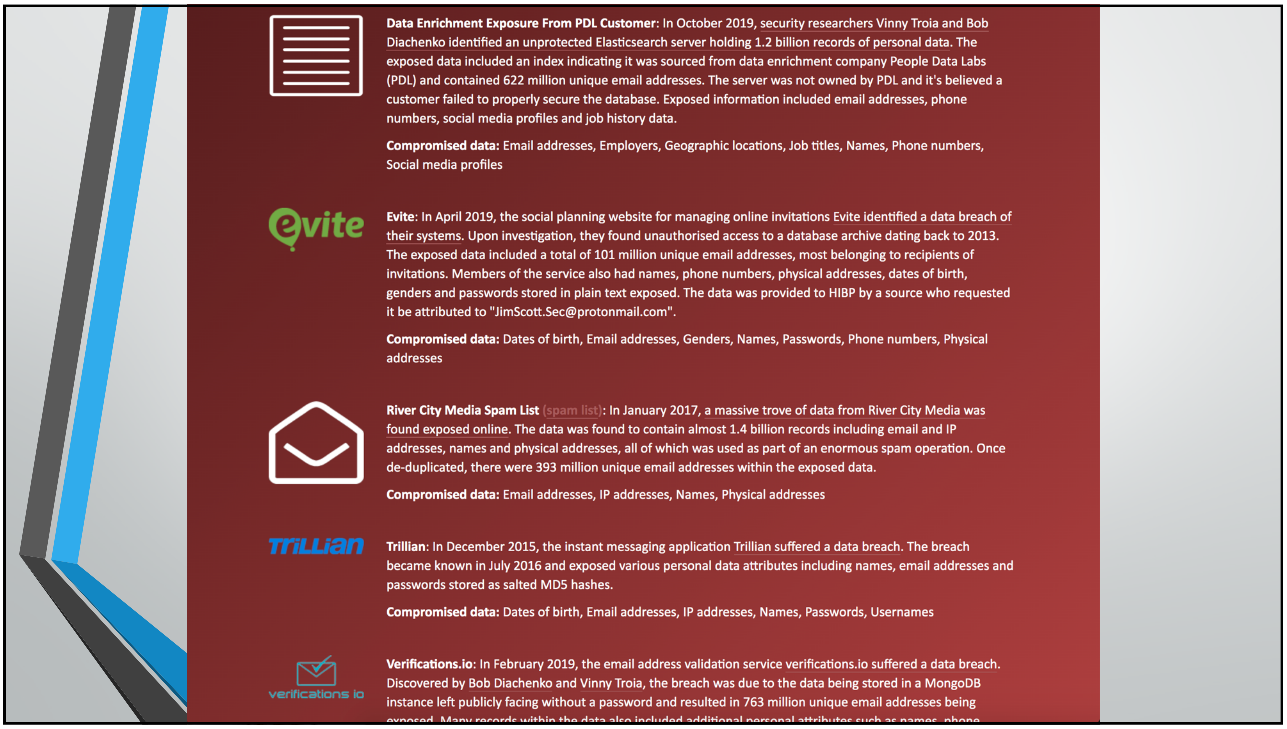
Compromised data: Email addresses, Passwords

B2B USA Businesses (spam list): In mid-2017, a spam list of over 105 million individuals in corporate America was discovered online. Referred to as "B2B USA Businesses", the list categorised email addresses by employer, providing information on individuals' job titles plus their work phone numbers and physical addresses. Read more about spam lists in HIBP.

Compromised data: Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses

CafePress: In February 2019, the custom merchandise retailer CafePress suffered a data breach. The exposed data included 23 million unique email addresses with some records also containing names, physical addresses, phone numbers and passwords stored as SHA-1 hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Names, Passwords, Phone numbers, Physical addresses



Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

Evite: In April 2019, the social planning website for managing online invitations Evite identified a data breach of their systems. Upon investigation, they found unauthorised access to a database archive dating back to 2013. The exposed data included a total of 101 million unique email addresses, most belonging to recipients of invitations. Members of the service also had names, phone numbers, physical addresses, dates of birth, genders and passwords stored in plain text exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Dates of birth, Email addresses, Genders, Names, Passwords, Phone numbers, Physical addresses

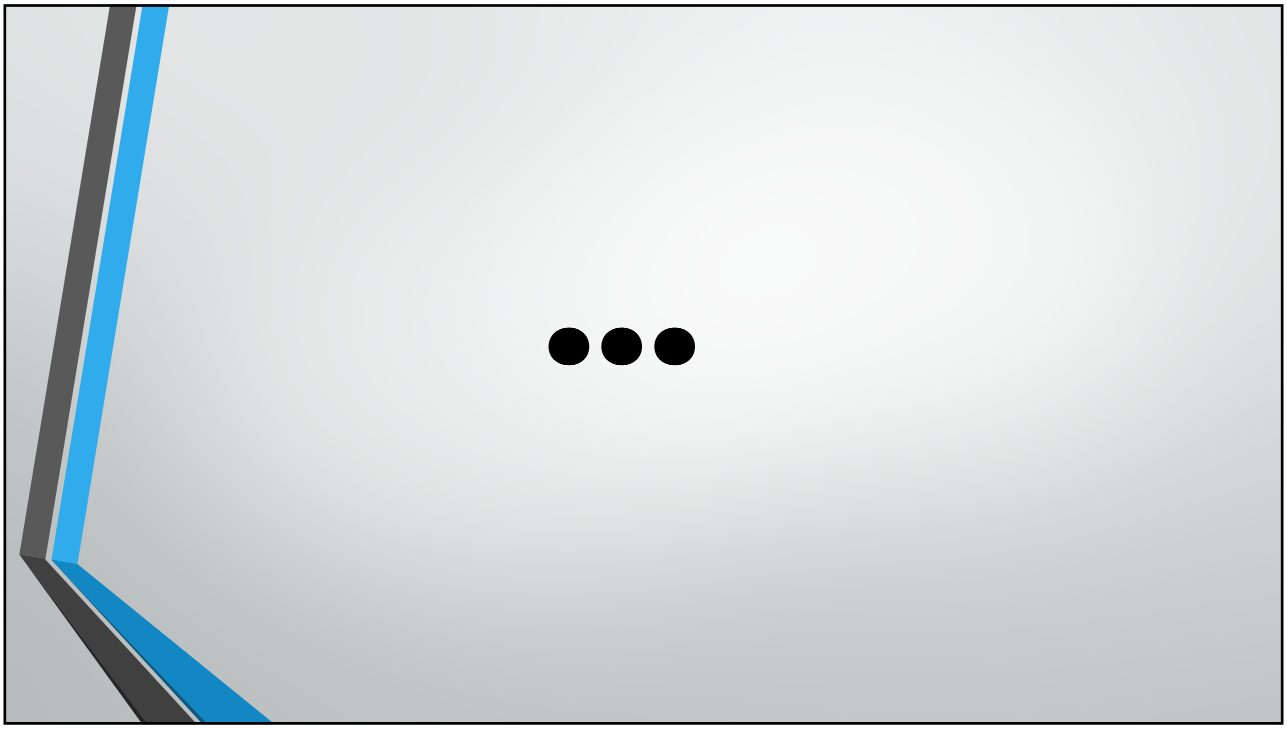
River City Media Spam List (spam list): In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

Compromised data: Email addresses, IP addresses, Names, Physical addresses

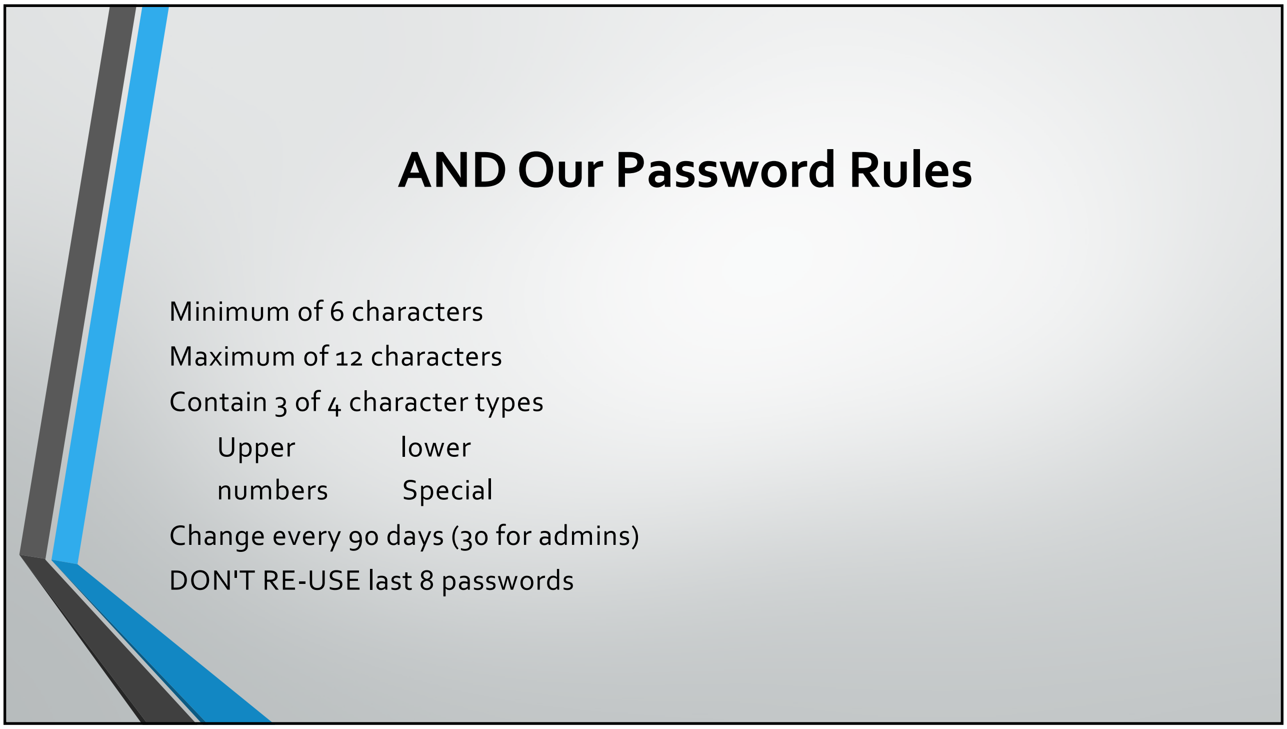
Trillian: In December 2015, the instant messaging application Trillian suffered a data breach. The breach became known in July 2016 and exposed various personal data attributes including names, email addresses and passwords stored as salted MD5 hashes.

Compromised data: Dates of birth, Email addresses, IP addresses, Names, Passwords, Usernames

Verifications.io: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone



●●●



AND Our Password Rules

Minimum of 6 characters

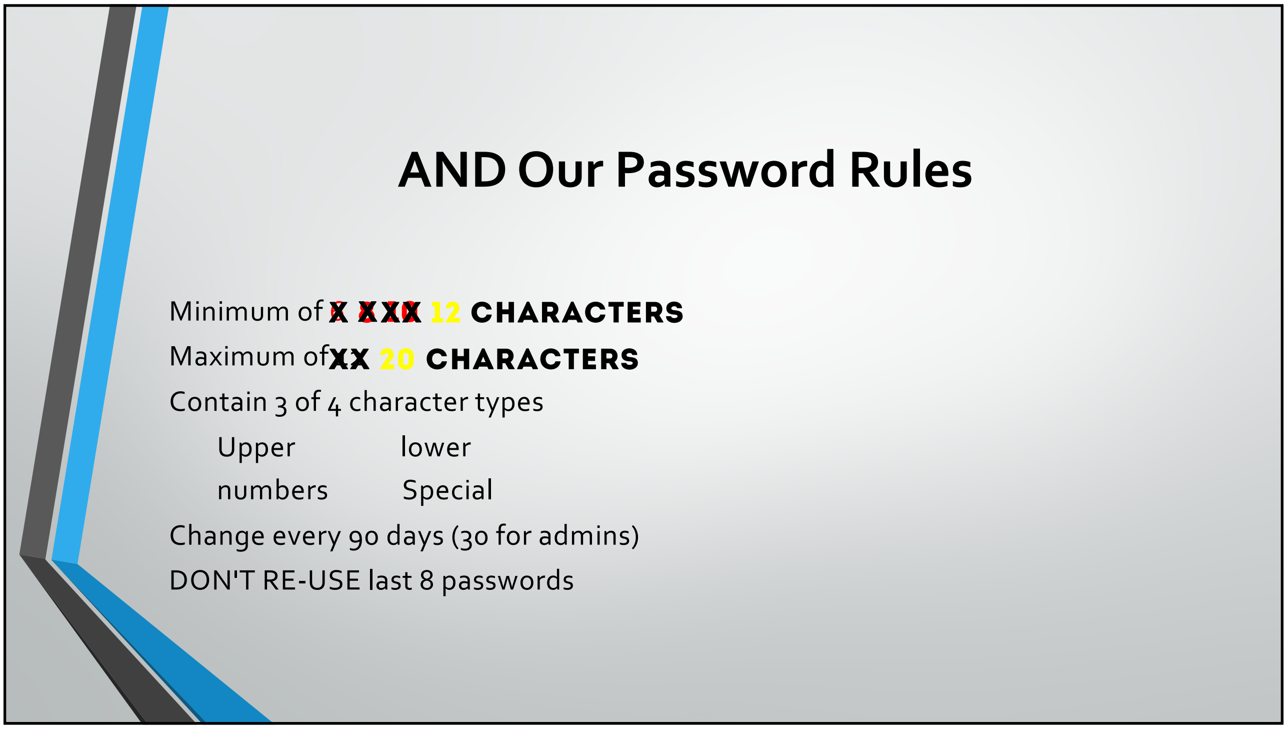
Maximum of 12 characters

Contain 3 of 4 character types

Upper lower
numbers Special

Change every 90 days (30 for admins)

DON'T RE-USE last 8 passwords



AND Our Password Rules

Minimum of ~~6~~ ~~8~~ ~~10~~ 12 **CHARACTERS**

Maximum of XX 20 **CHARACTERS**

Contain 3 of 4 character types

Upper lower

numbers Special

Change every 90 days (30 for admins)

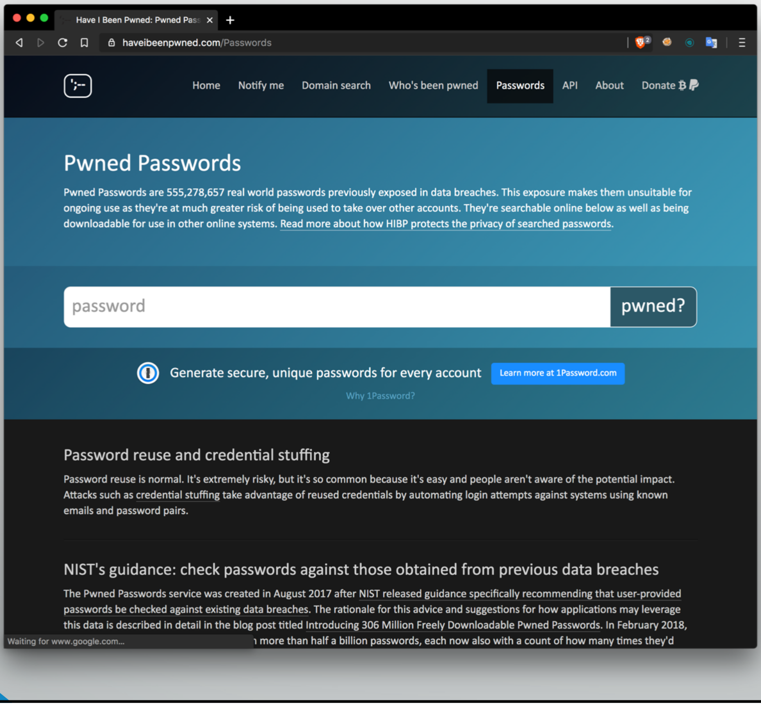
DON'T RE-USE last 8 passwords

My favorite password

TigGer99

“MUCH OF WHAT I DID I NOW REGRET.”

BILL BURR, FORMER NIST MANAGER


Have I Been Pwned: Pwned Pass
haveibeenpwned.com/Passwords
';--
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate ₿
password
pwned?
Learn more at 1Password.com
Why 1Password?
Waiting for www.google.com...

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.

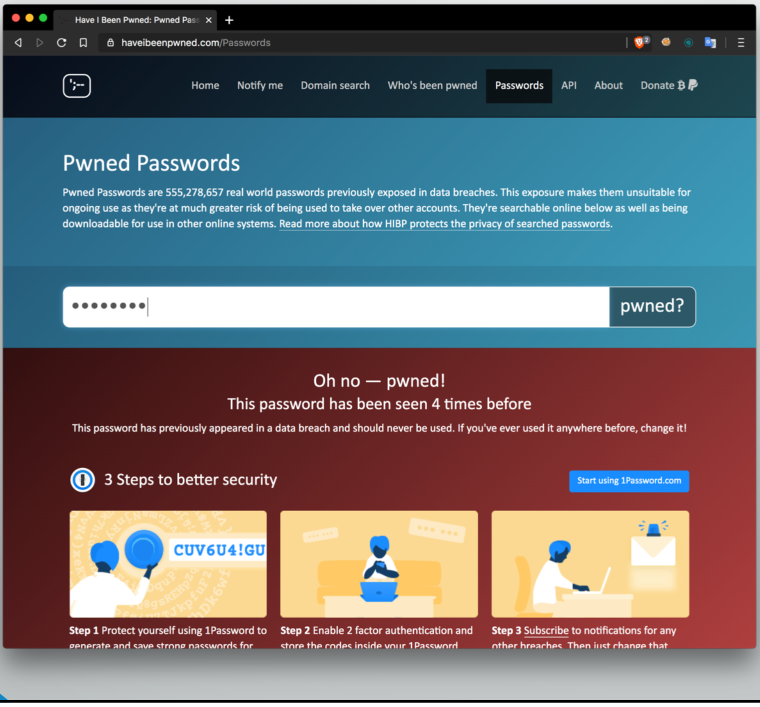
Generate secure, unique passwords for every account

Password reuse and credential stuffing

Password reuse is normal. It's extremely risky, but it's so common because it's easy and people aren't aware of the potential impact. Attacks such as credential stuffing take advantage of reused credentials by automating login attempts against systems using known emails and password pairs.

NIST's guidance: check passwords against those obtained from previous data breaches

The Pwned Passwords service was created in August 2017 after NIST released guidance specifically recommending that user-provided passwords be checked against existing data breaches. The rationale for this advice and suggestions for how applications may leverage this data is described in detail in the blog post titled Introducing 306 Million Freely Downloadable Pwned Passwords. In February 2018,
n more than half a billion passwords, each now also with a count of how many times they'd


Have I Been Pwned: Pwned Pass
haveibeenpwned.com/Passwords
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
CUV6U4!GU
Start using 1Password.com

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.

••••••••

pwned?

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!

3 Steps to better security

Step 1 Protect yourself using 1Password to generate and save strong passwords for

Step 2 Enable 2 factor authentication and store the codes inside your 1Password

Step 3 Subscribe to notifications for any other breaches. Then just change that

Our Password Rules

Minimum of 8 characters

Maximum of 12 characters

Contain 3 of 4 character types

Upper lower

numbers Special

Change every 90 days (30 for admins)

DON'T RE-USE last 8 passwords

Password Cracking

Cleartext

- https://plaintextoffenders.com/

Hashed

- On/Offline dictionary attacks
- Rainbow tables

GPUs

Adaptive algorithms / salts

Our Password Rules

~~Minimum of 8 characters~~

~~Maximum of 12 characters~~

Contain 3 of 4 character types

- Upper lower
- numbers Special

Change every 90 days (30 for admins)

DON'T RE-USE last 8 passwords

xkcd (2011)

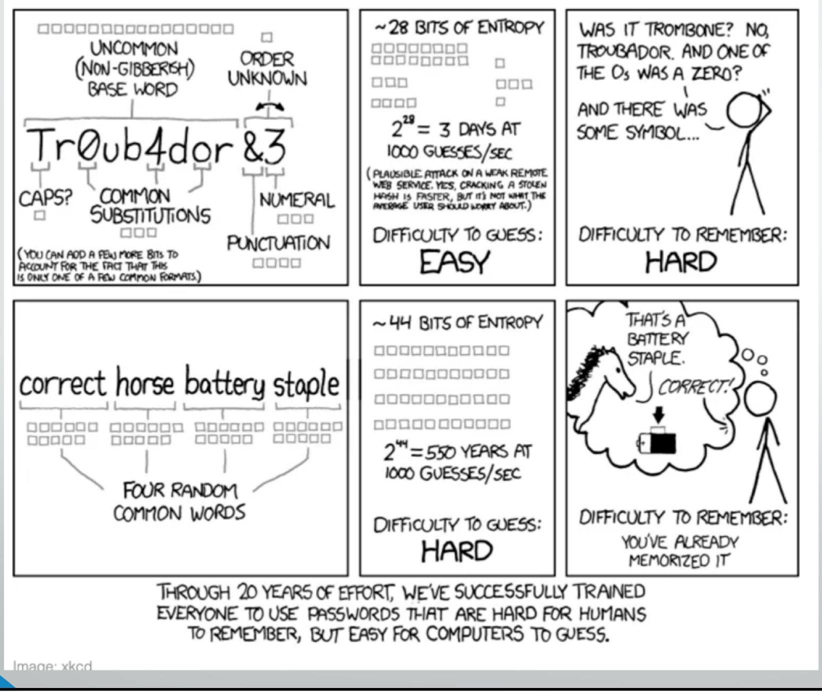

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB 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.

Image: xkcd

Password Space

Password space = x^n

X = possibilities for one "character"

n = number of characters

8 numerical: 10^8 = 100,000,000 or 1×10^8

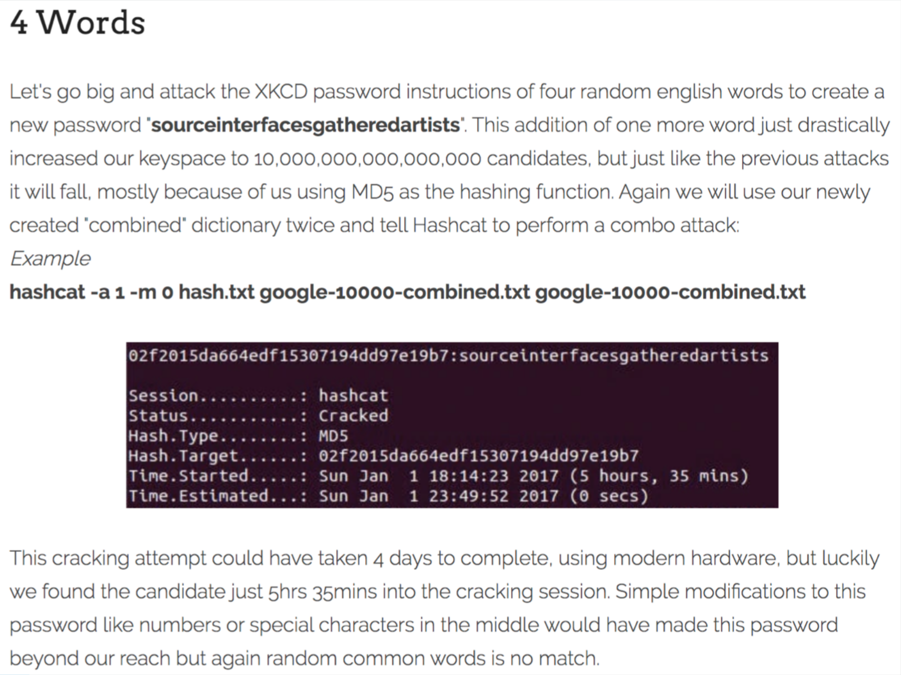
8 alphanumeric: $36^8 = 2.8 \times 10^{12}$

8 mixed alphanumeric: $72^8 = 7.2 \times 10^{14}$

12 mixed alphanumeric: $72^{12} = 1.9 \times 10^{22}$

4 words = $40{,}000^4 = 2.56 \times 10^{18}$

According to lexicographer and dictionary expert Susie Dent, "the **average** active **vocabulary** of an adult **English speaker** is around 20,000 **words**, while his passive **vocabulary** is around 40,000 **words**.



4 Words

Let's go big and attack the XKCD password instructions of four random english words to create a new password "**sourceinterfacesgatheredartists**". This addition of one more word just drastically increased our keyspace to 10,000,000,000,000,000 candidates, but just like the previous attacks it will fall, mostly because of us using MD5 as the hashing function. Again we will use our newly created "combined" dictionary twice and tell Hashcat to perform a combo attack:

Example

hashcat -a 1 -m 0 hash.txt google-10000-combined.txt google-10000-combined.txt

```
02f2015da664edf15307194dd97e19b7:sourceinterfacesgatheredartists

Session..........: hashcat
Status...........: Cracked
Hash.Type........: MD5
Hash.Target......: 02f2015da664edf15307194dd97e19b7
Time.Started.....: Sun Jan  1 18:14:23 2017 (5 hours, 35 mins)
Time.Estimated...: Sun Jan  1 23:49:52 2017 (0 secs)
```

This cracking attempt could have taken 4 days to complete, using modern hardware, but luckily we found the candidate just 5hrs 35mins into the cracking session. Simple modifications to this password like numbers or special characters in the middle would have made this password beyond our reach but again random common words is no match.

Our Password Rules

~~Minimum of 8 characters~~

~~Maximum of 12 characters~~

~~Contain 3 of 4 character types~~

~~Upper lower~~

~~numbers Special~~

Change every 90 days (30 for admins)

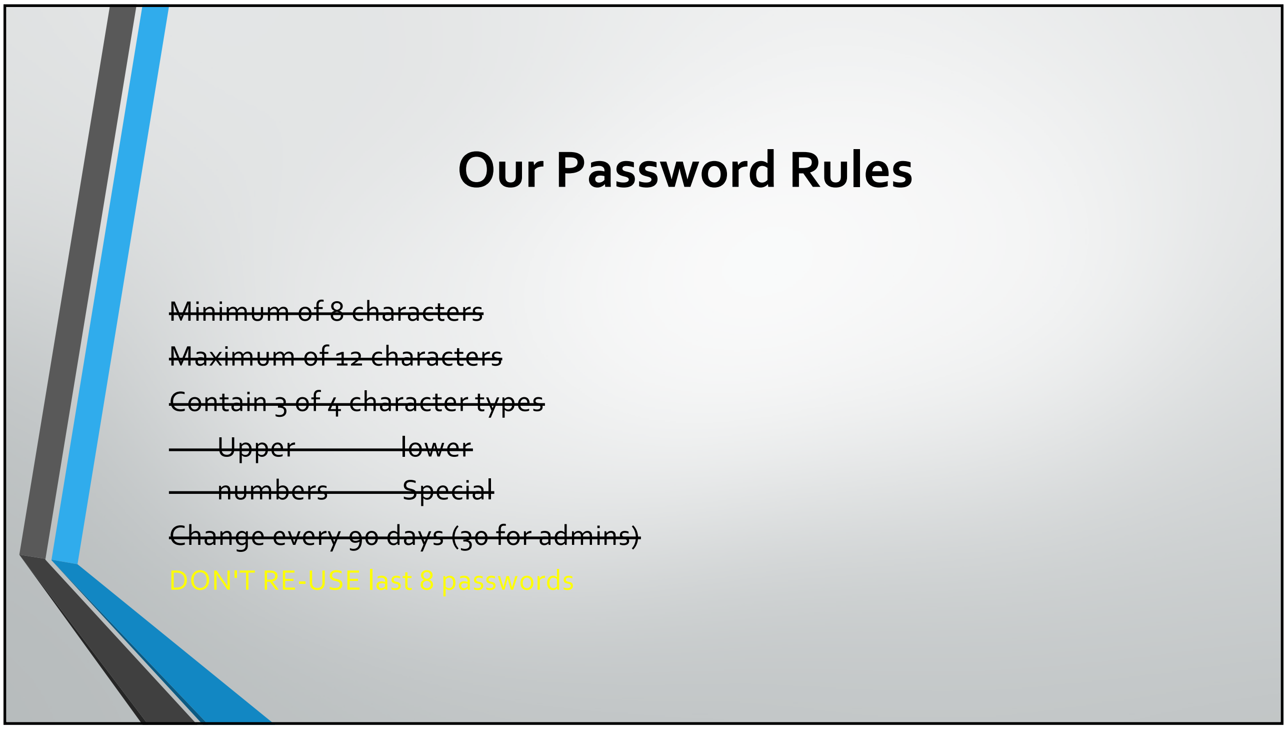
DON'T RE-USE last 8 passwords

My favorite password

~~TigGer99~~

~~TigGer10~~

TigGer11



Our Password Rules

~~Minimum of 8 characters~~

~~Maximum of 12 characters~~

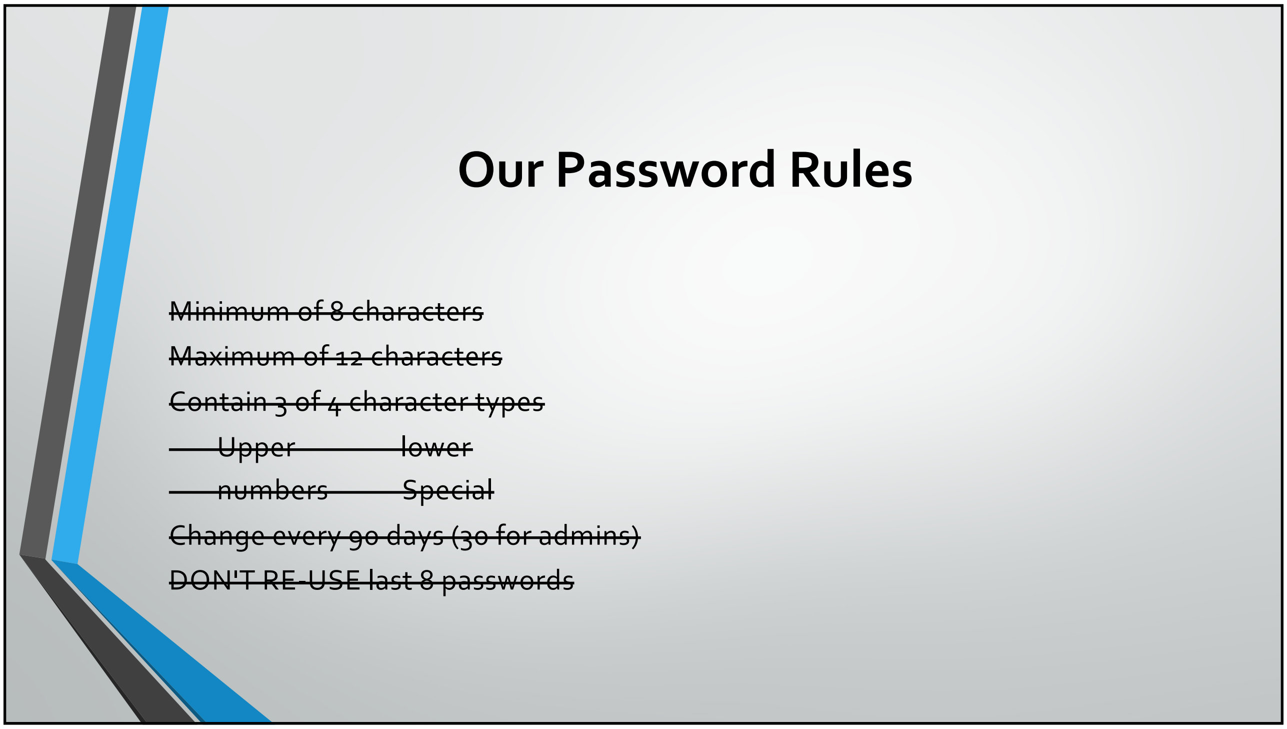
~~Contain 3 of 4 character types~~

~~Upper lower~~

~~numbers Special~~

~~Change every 90 days (30 for admins)~~

DON'T RE-USE last 8 passwords



Our Password Rules

~~Minimum of 8 characters~~

~~Maximum of 12 characters~~

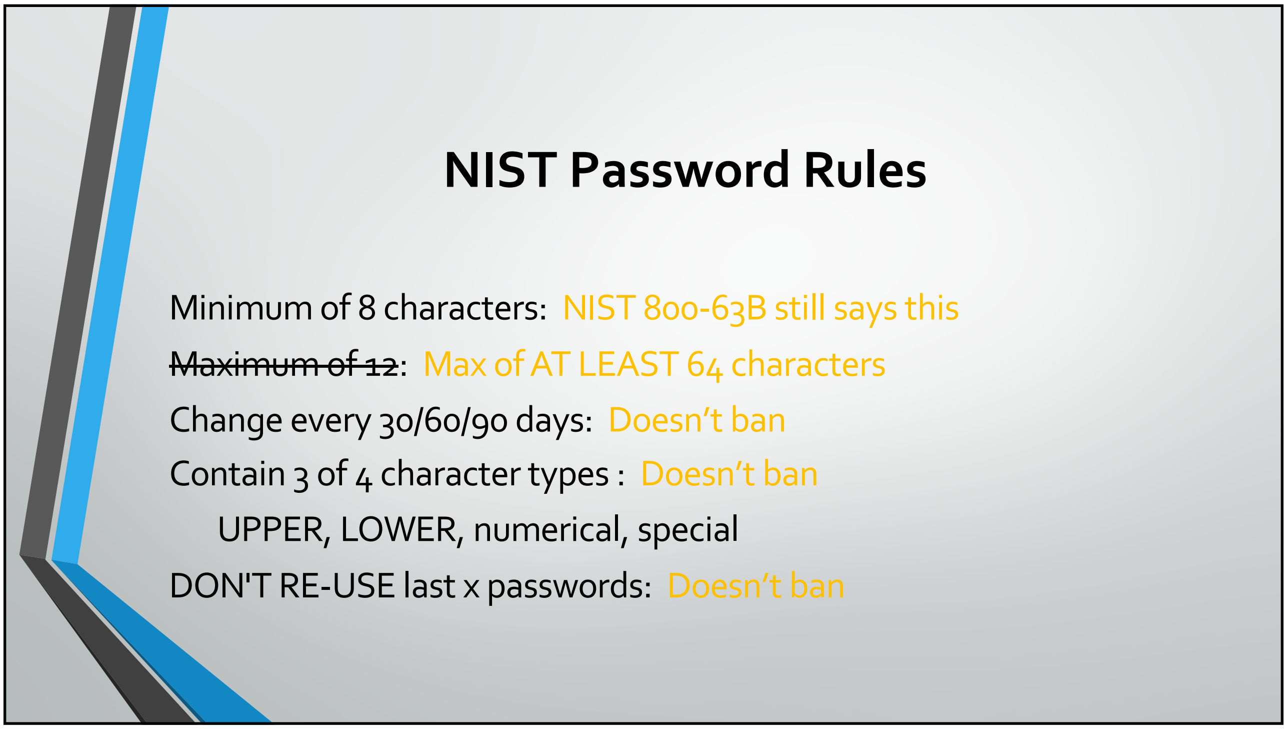
~~Contain 3 of 4 character types~~

~~Upper lower~~

~~numbers Special~~

~~Change every 90 days (30 for admins)~~

~~DON'T RE-USE last 8 passwords~~



NIST Password Rules

Minimum of 8 characters: NIST 800-63B still says this

~~Maximum of 12~~: Max of AT LEAST 64 characters

Change every 30/60/90 days: Doesn’t ban

Contain 3 of 4 character types : Doesn’t ban

UPPER, LOWER, numerical, special

DON'T RE-USE last x passwords: Doesn’t ban

NIST Additions

Restrict sequential/repetitive (1234, aaaa)

Restrict context passwords

e.g., username / sitename

Restrict dictionary / common

scott/tiger, sa/sa, admin/password

Restrict previously breached https://haveibeenpwned.com

Our Recommendations

2 factor (**not SMS**)

Time-based one-time Password (TOTP) (Authenticator, RSA, DUO)

Cryptographic challenge/response (yubi-key, DUO)

NO CONSTRUCTION REQUIREMENTS

MIN 12 CHARACTERS/NO MAX

NO EXPIRATION UNLESS LOSS SUSPECTED

NO PREVIOUS BREACH/SIMPLE PASSWORDS

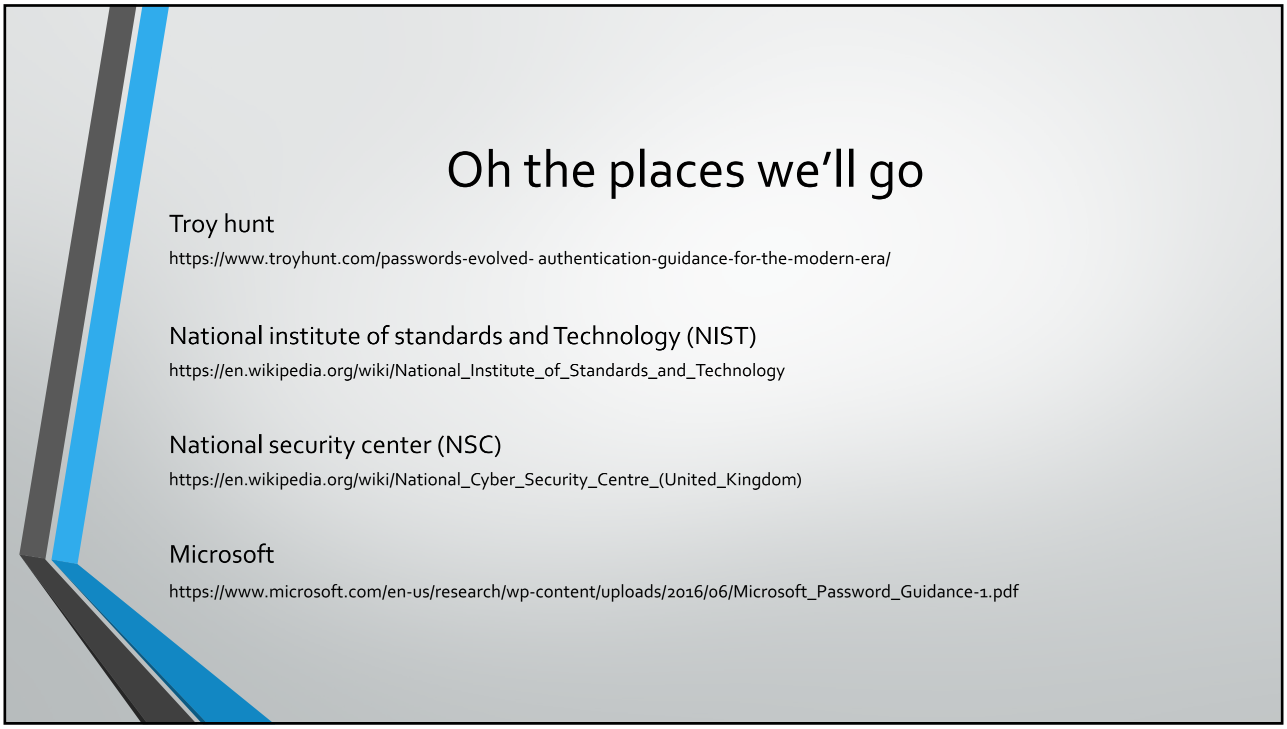
PREFER Passphrase

I only regret that I have but one life to lose for my country.

USE Password Manager (Keepass, LastPass, OnePass)

Lockout + Alerts

last login, failed, change, etc



Oh the places we'll go

Troy hunt

https://www.troyhunt.com/passwords-evolved- authentication-guidance-for-the-modern-era/

National institute of standards and Technology (NIST)

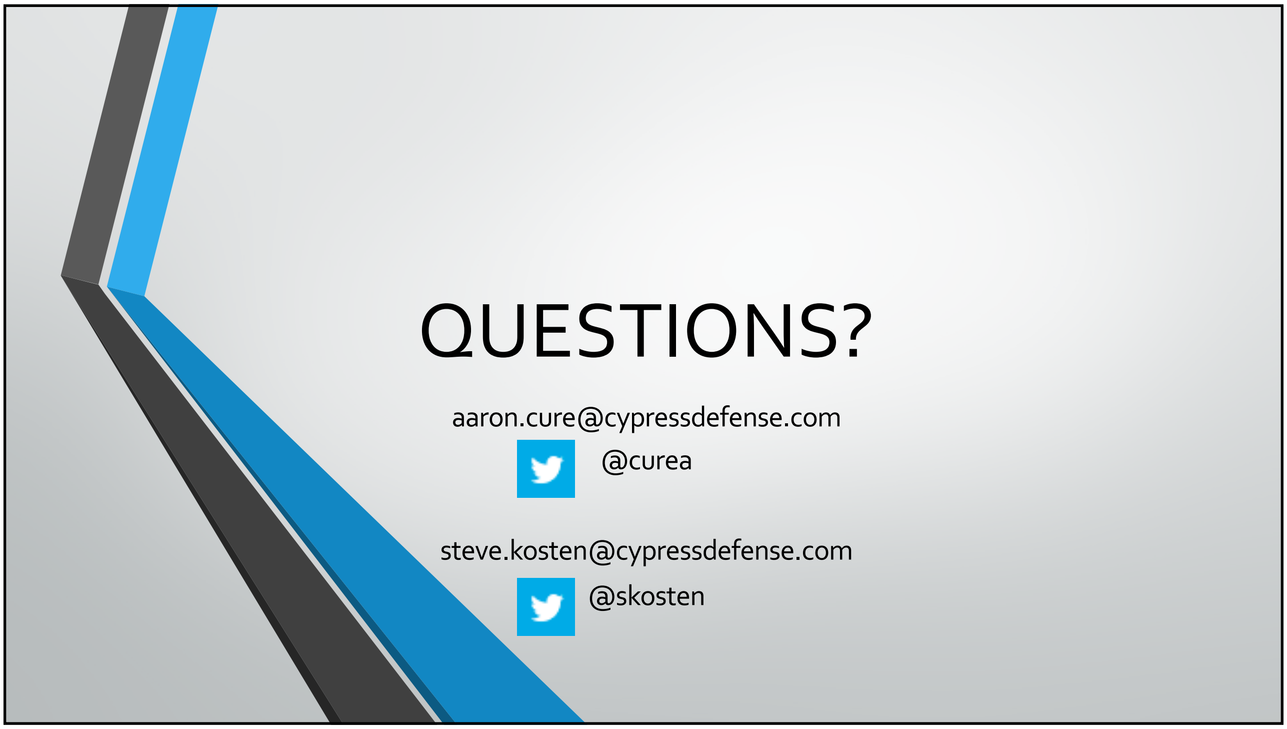
https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology

National security center (NSC)

https://en.wikipedia.org/wiki/National_Cyber_Security_Centre_(United_Kingdom)

Microsoft

https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf



QUESTIONS?

aaron.cure@cypressdefense.com

@curea

steve.kosten@cypressdefense.com

@skosten

Cypress Data Defense, LLC

https://www.cypressdatadefense.com

🐦 @cddsecurity

(720) 588-8133