RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **IDP-F08V**

# Breaking Bad … Passwords


**Hamed Merati**

Senior Security Consultant
Sense of Security

**Willem Mouton**

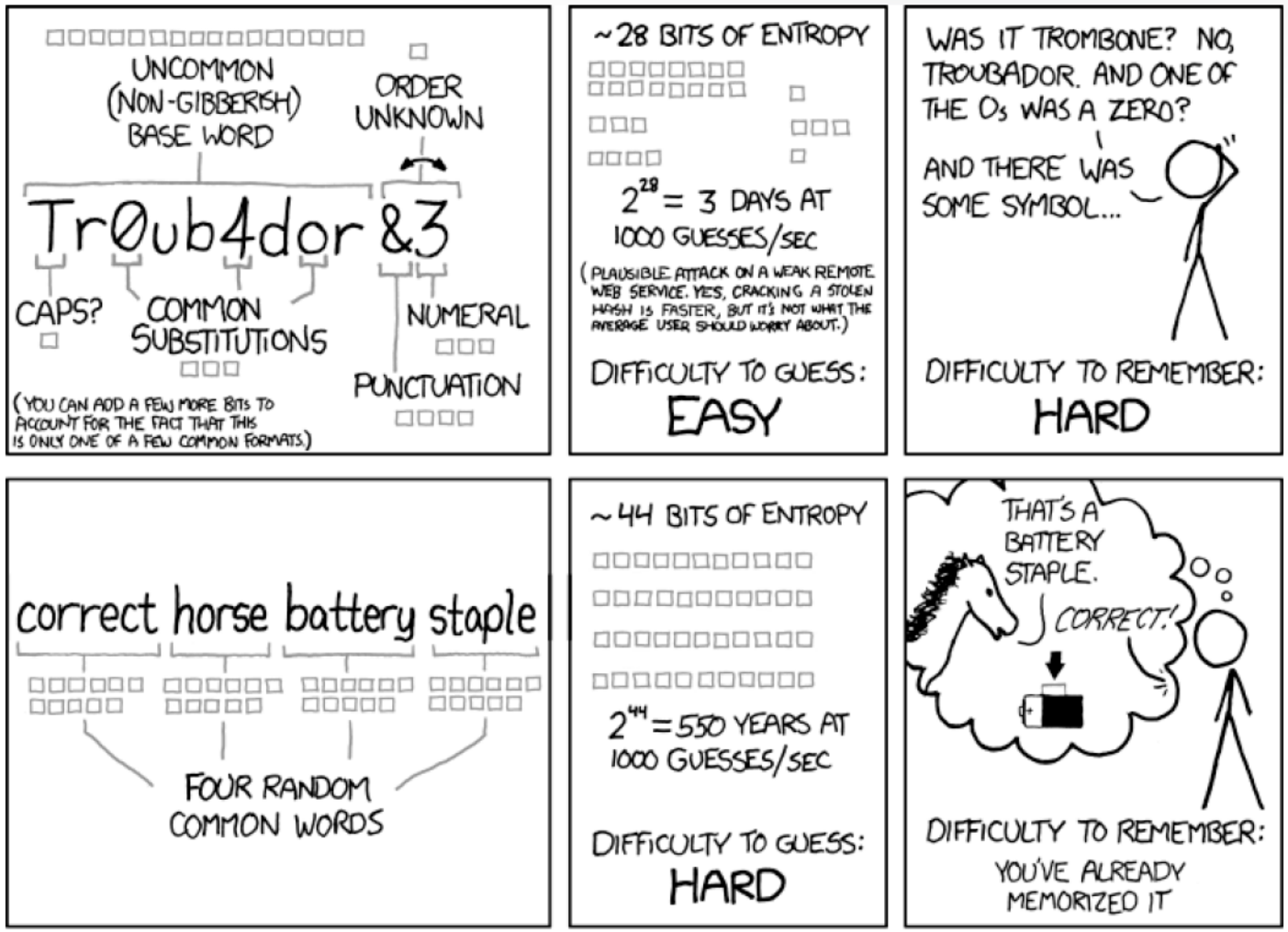
Head of Research
Sense of Security
@__w_m_

# Another talk on passwords?

- Still the de-facto authentication method in use
- Relies almost always on user generated and chosen values
- The average user today has more credentials than ever before

We are attackers (usually) and we have success with this all the time

# What we (believe) we know



# Our datasets

- The last 3 years of penetration testing – Australian organisations
  - Red teaming
  - Network PenTest
  - Web application PenTest

RSAConference2020 APJ
A Virtual Learning Experience

# Corporate Password Policies

## An analysis of corporate password policies

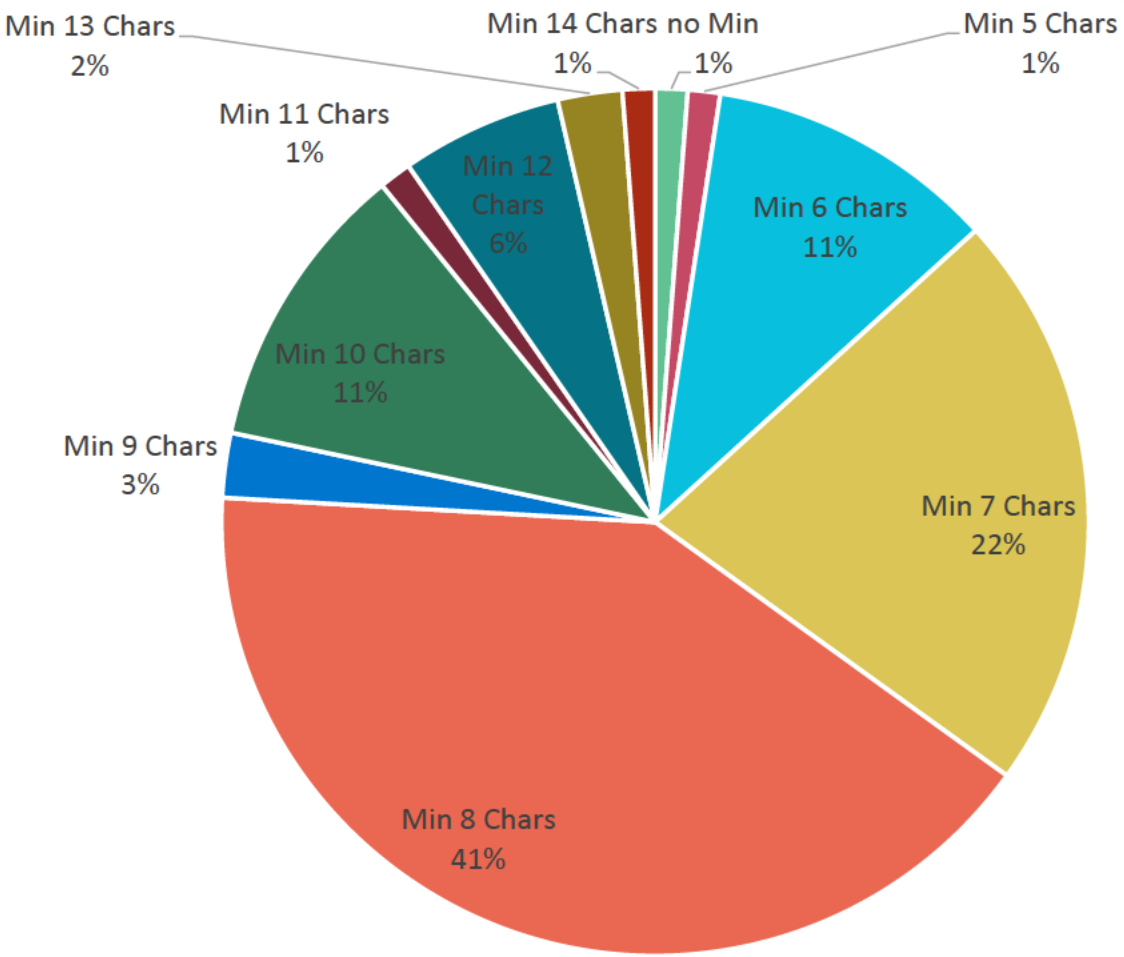
# Industry guidelines and standards

- NIST
- CIS benchmark 2019
- ACSC ISM
- PCI DSS

| STANDARD | MIN LEN (chars) | Complexity | History (passwords) | Max Age (days) | Lockout Threshold (attempts) | Lockout Duration (minutes) |
|---|---|---|---|---|---|---|
| Microsoft | 8 (default 7) | Yes | 24 | 42 | 10 | - |
| NIST | 8 | - | - | - | - | - |
| CIS | 14 | Yes | 24 | 60 | 10 | >15 |
| ISM | 10 | Yes | 8 | 90 | 5 | - |
| PCI DSS | 7 | Yes | 4 | 90 | 6 | >30 |

The recommendation values per standard

# “Our” average password policy – Min Chars

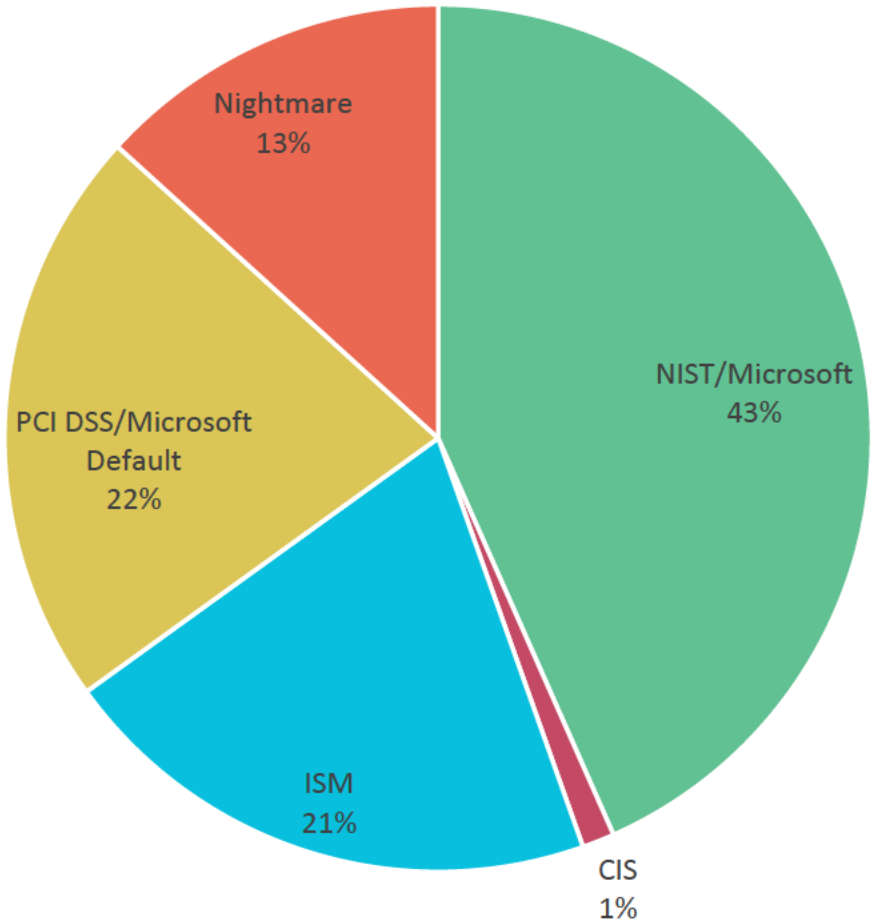



- The average min char for password policies is 8.1

| STANDARD | MIN LEN* |
|---|---|
| Microsoft | 8 (default 7) |
| NIST | 8 |
| CIS | 14 |
| ISM | 10 |
| PCI DSS | 7 |

* Recommended values by the standards

# “Our” average password policy – Min Chars

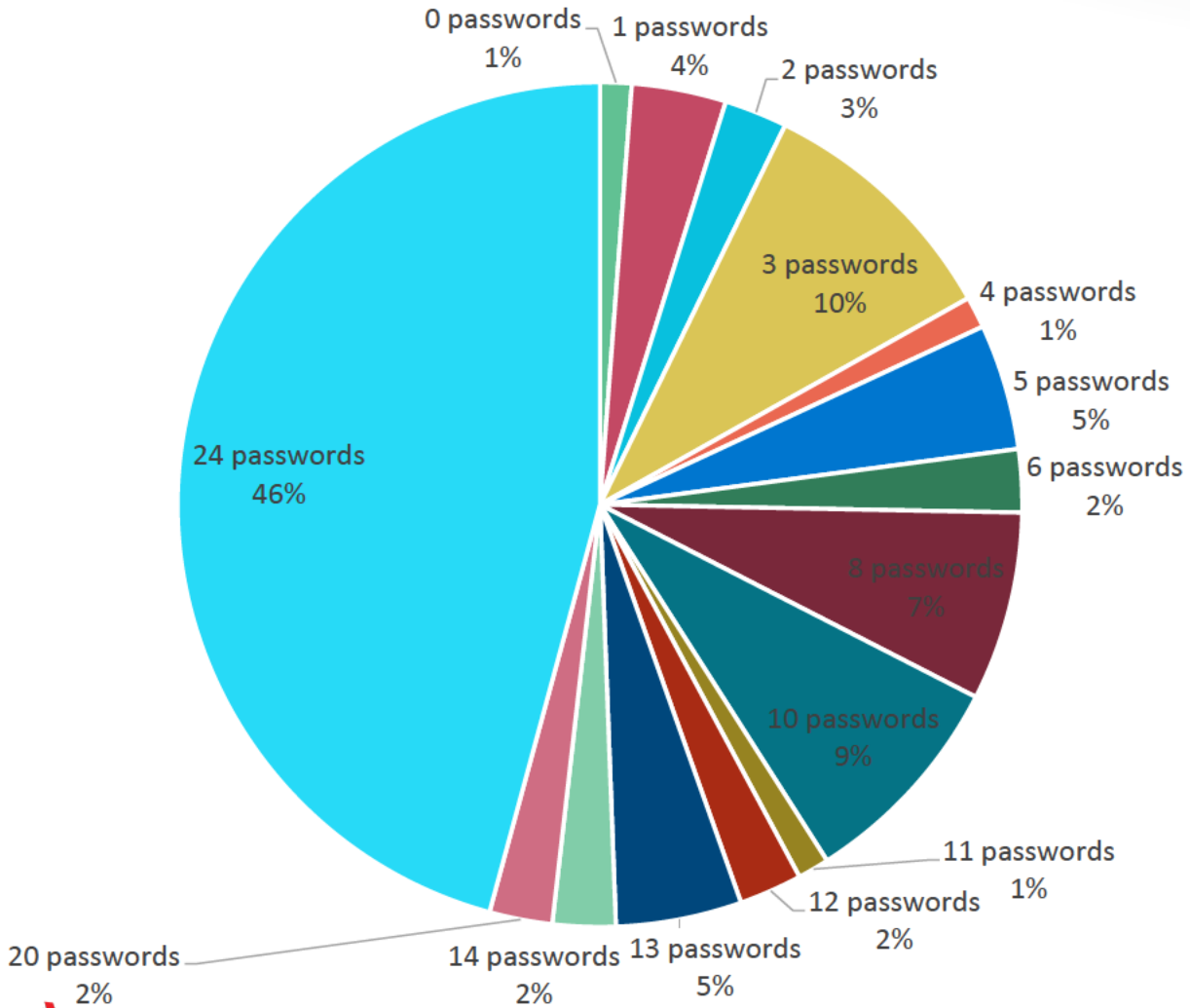



- The average min char for password policies is 8.1

| STANDARD | MIN LEN* |
|---|---|
| Microsoft | 8 (default 7) |
| NIST | 8 |
| CIS | 14 |
| ISM | 10 |
| PCI DSS | 7 |

* Recommended values by the standards

# “Our” average password policy – Password History

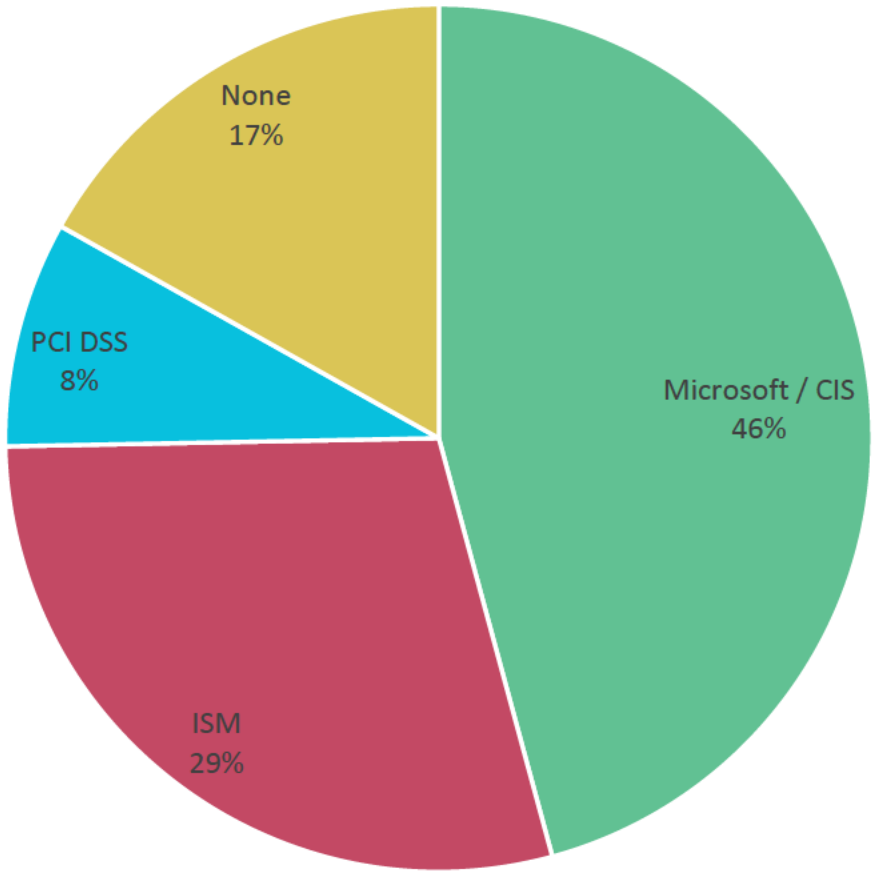



| STANDARD | History* |
|---|---|
| Microsoft | 24 |
| NIST | - |
| CIS | 24 |
| ISM | 8 |
| PCI DSS | 4 |

* Recommended values by the standards

Sense of Security
A CyberCX company

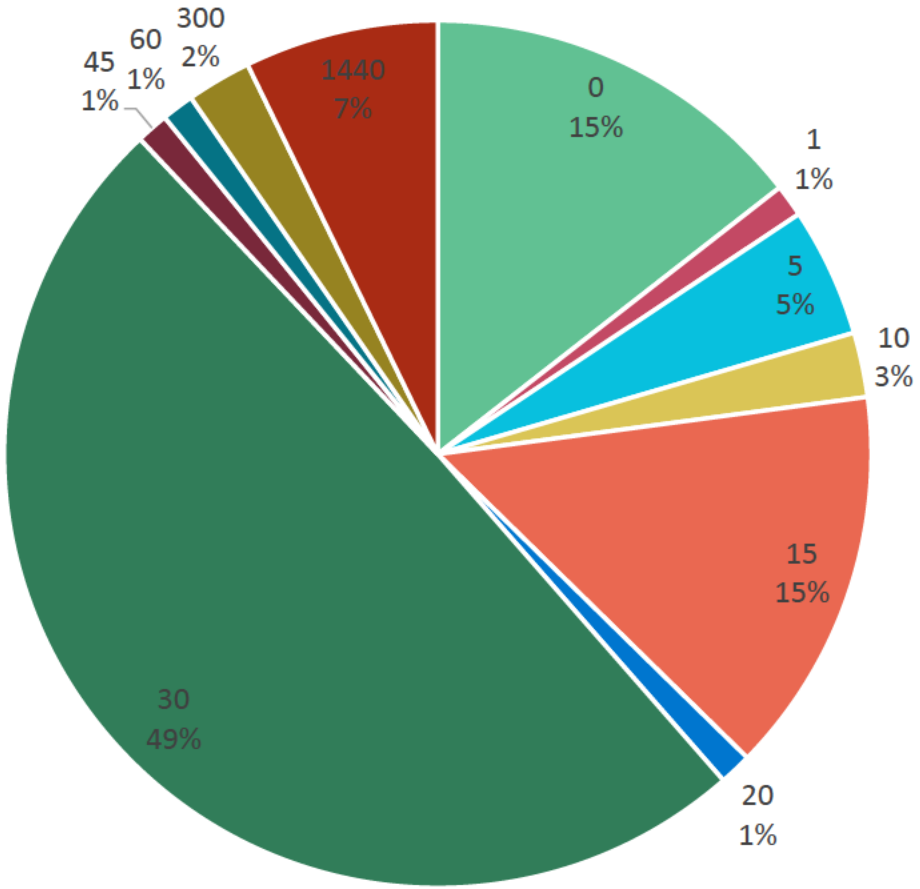
# “Our” average password policy – Password History




| STANDARD | History* |
|---|---|
| Microsoft | 24 |
| NIST | - |
| CIS | 24 |
| ISM | 8 |
| PCI DSS | 4 |

* Recommended values by the standards

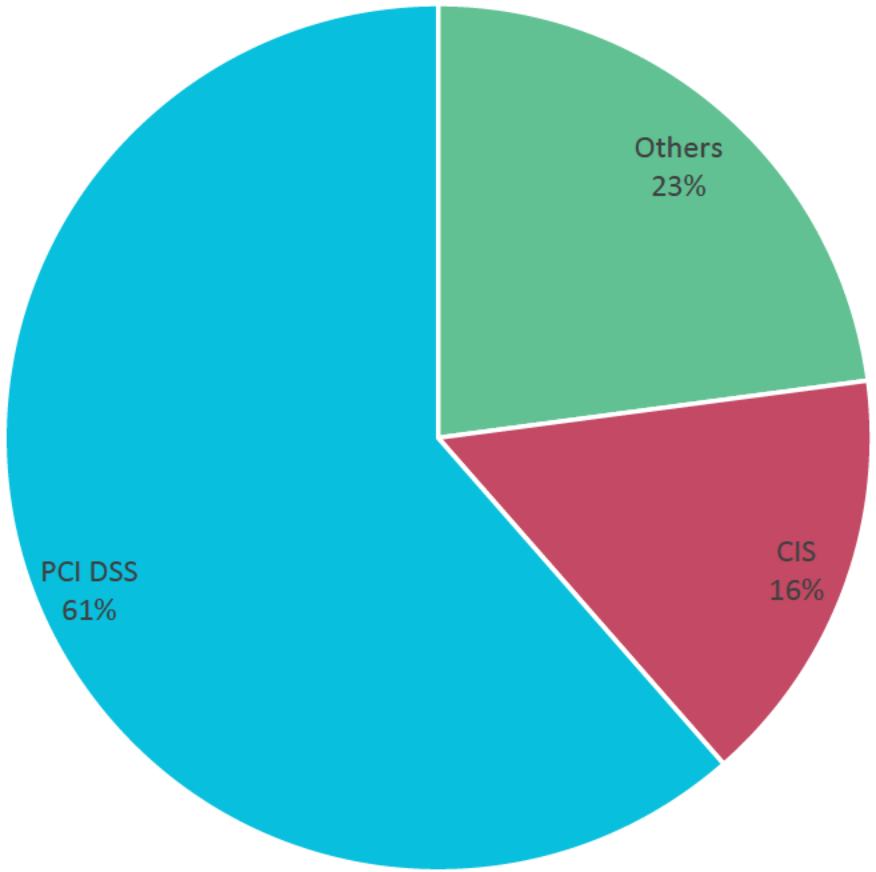
# “Our” average password policy – Lockout Duration




| STANDARD | Lockout Duration* |
|---|---|
| Microsoft | 15 |
| NIST | - |
| CIS | >15 |
| ISM | - |
| PCI DSS | >30 |

* Recommended values by the standards

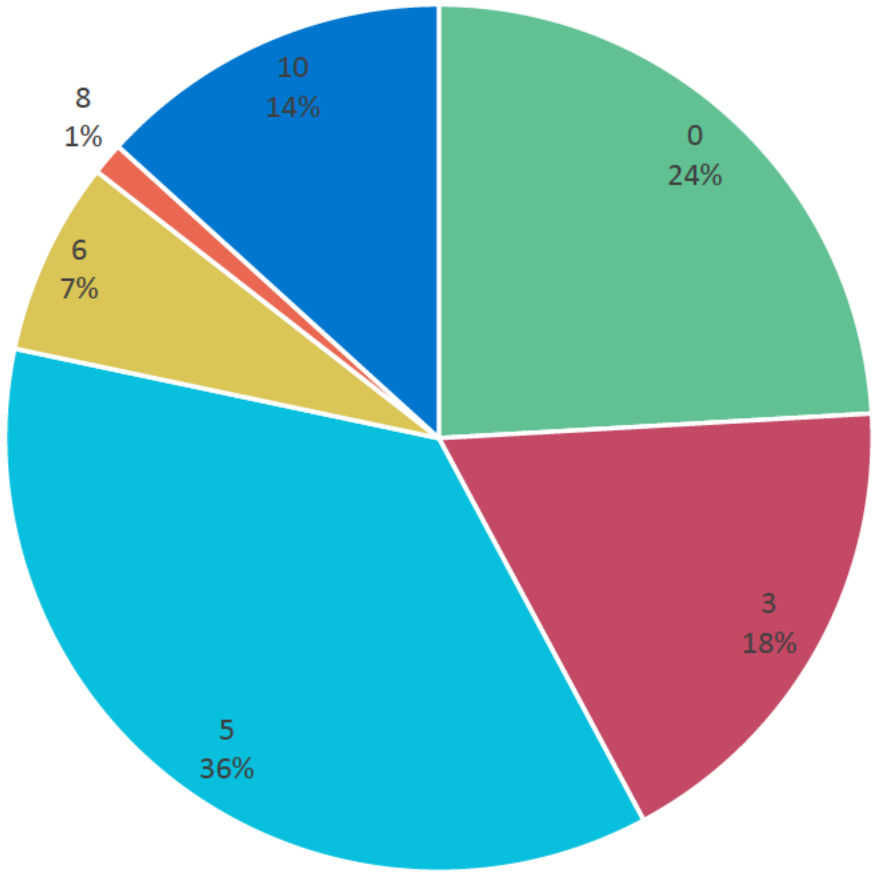
# “Our” average password policy – Lockout Duration




| STANDARD | Lockout Duration* |
|---|---|
| Microsoft | 15 |
| NIST | - |
| CIS | >15 |
| ISM | - |
| PCI DSS | >30 |

* Recommended values by the standards

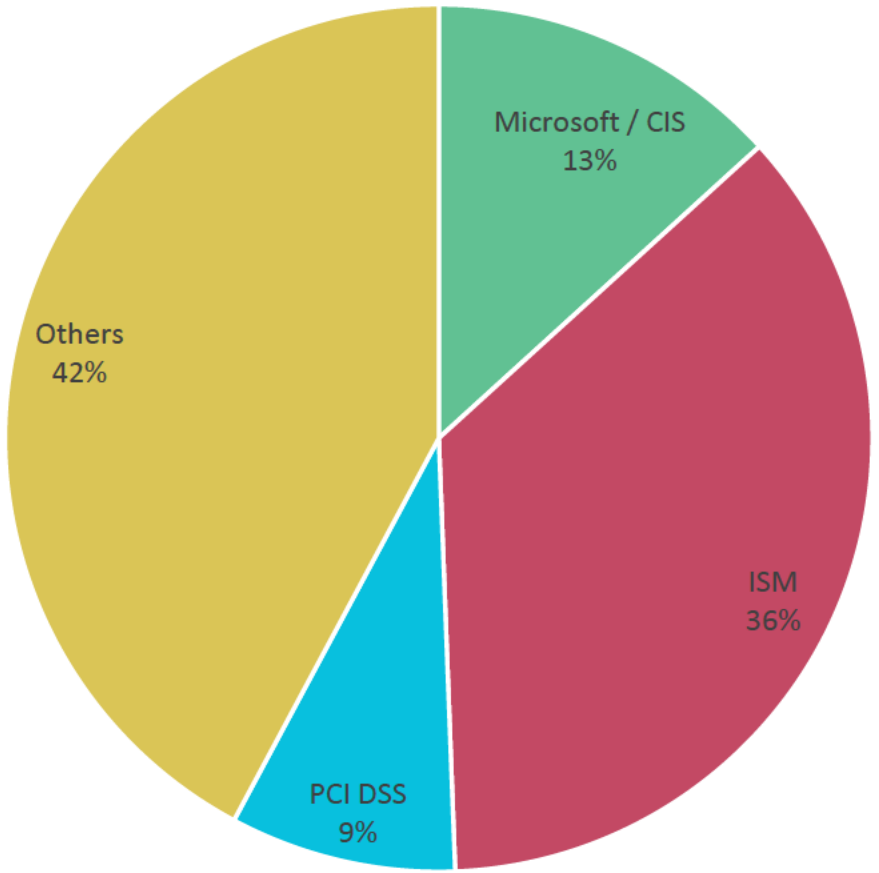
# “Our” average password policy – Lockout Threshold




| STANDARD | Lockout Threshold* |
|---|---|
| Microsoft | 10 |
| NIST | - |
| CIS | 10 |
| ISM | 5 |
| PCI DSS | 6 |

* Recommended values by the standards

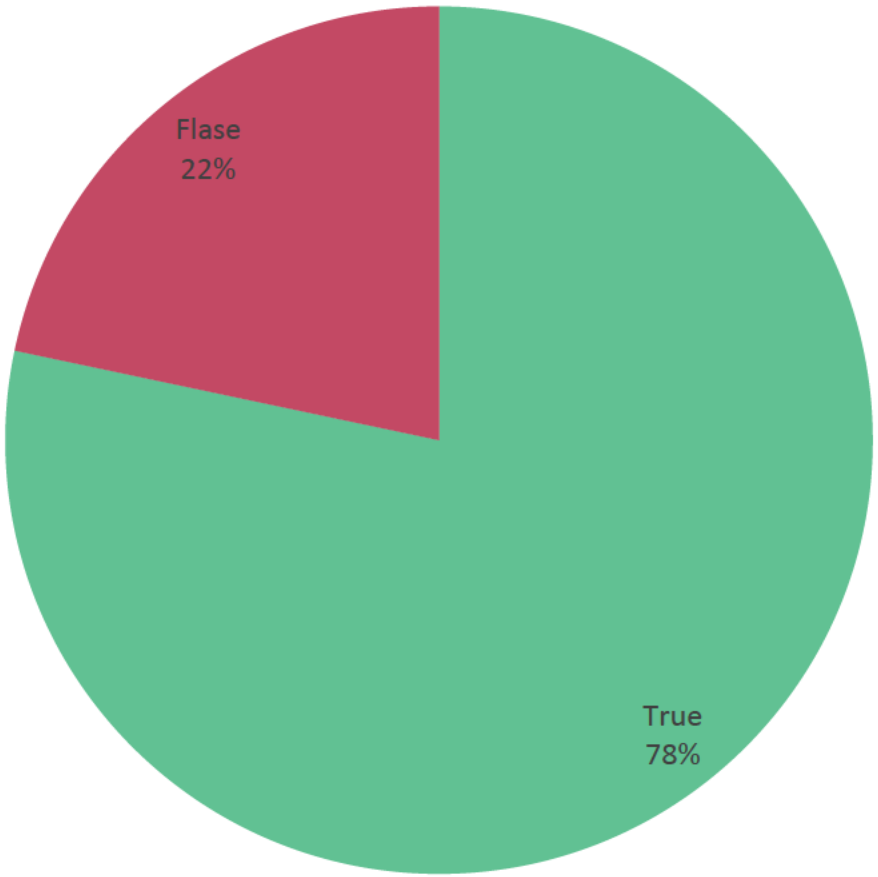
# “Our” average password policy – Lockout Threshold




| STANDARD | Lockout Threshold* |
|---|---|
| Microsoft | 10 |
| NIST | - |
| CIS | 10 |
| ISM | 5 |
| PCI DSS | 6 |

* Recommended values by the standards

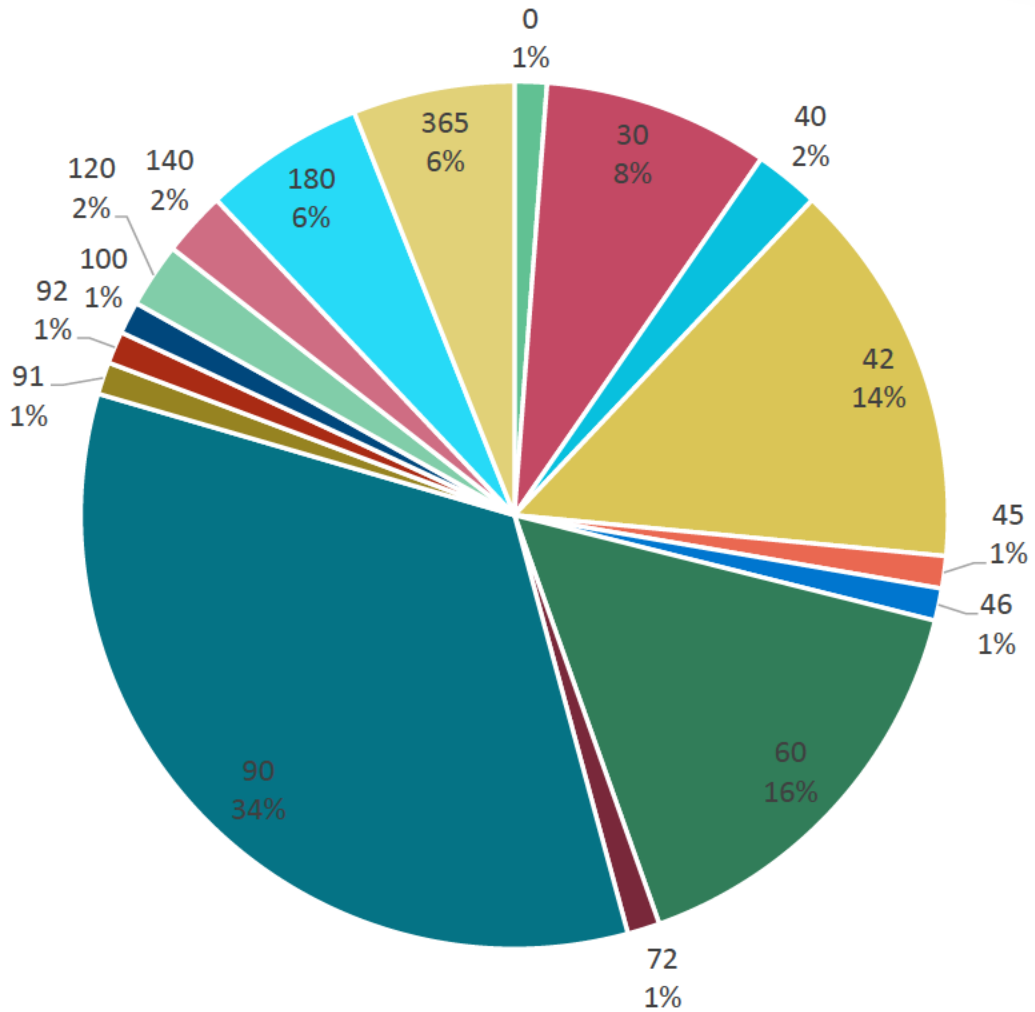
# “Our” average password policy – Complexity




| STANDARD | Complexity* |
|---|---|
| Microsoft | Yes |
| NIST | - |
| CIS | Yes |
| ISM | Yes |
| PCI DSS | Yes |

* Recommended values by the standards

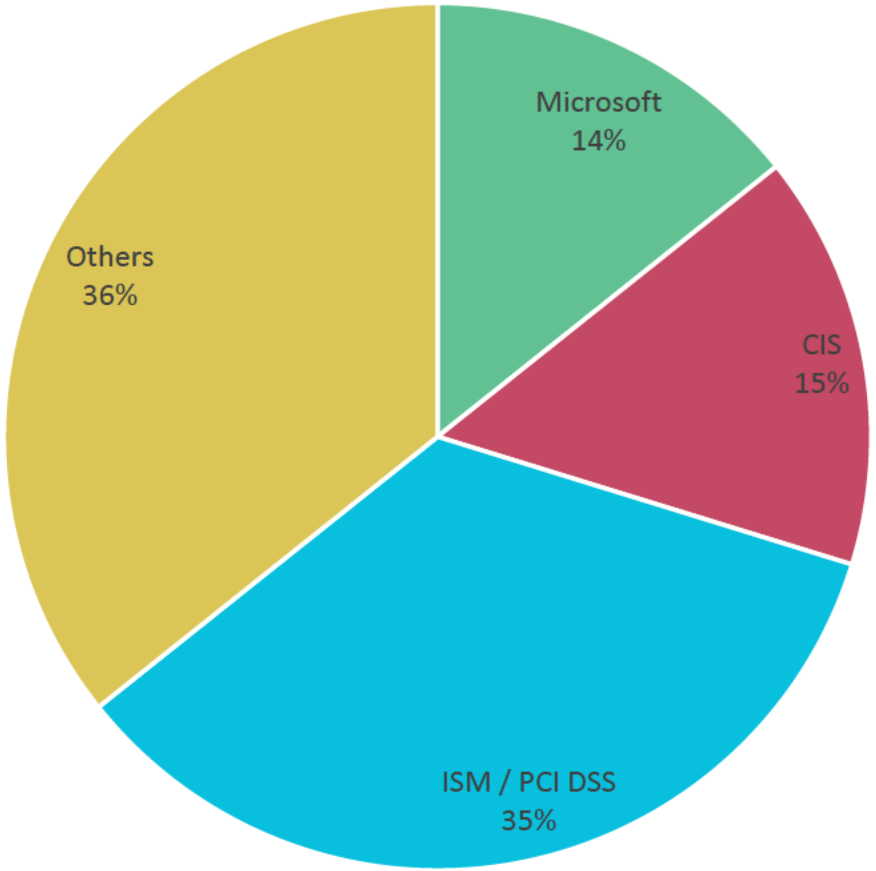
# “Our” average password policy – Max Age (Expiry)




| STANDARD | Max Age* |
|---|---|
| Microsoft | 42 |
| NIST | - |
| CIS | 60 |
| ISM | 90 |
| PCI DSS | 90 |

* Recommended values by the standards

# “Our” average password policy – Max Age (Expiry)




| STANDARD | Max Age* |
|---|---|
| Microsoft | 42 |
| NIST | - |
| CIS | 60 |
| ISM | 90 |
| PCI DSS | 90 |

* Recommended values by the standards

# Who does it better? (on paper)

| Sector | Avg Min Length | Avg Expiry | Avg Pass History |
|---|---|---|---|
| Other | 9 | 100 | 12 |
| Government | 9 | 64 | 12 |
| Technology | 9 | 60 | 19 |
| Insurance | 9 | 45 | 17 |
| Utilities & Energy | 8 | 98 | 24 |
| Health Care | 8 | 88 | 9 |
| Banking and Financial Services | 8 | 71 | 17 |
| Food Services | 8 | 42 | 24 |
| Industrial | 7 | 98 | 11 |
| Education | 5 | 63 | 7 |

# What do the bad guys think of this?

- Short 8-9 length creates potential for weak / guessable passwords
- High lockout threshold aids attackers during brute forcing
- Long lockout timeouts increases the effect of mass account lockouts
- Short password history increases likelihood of password recycling

RSAConference2020 APJ
A Virtual Learning Experience

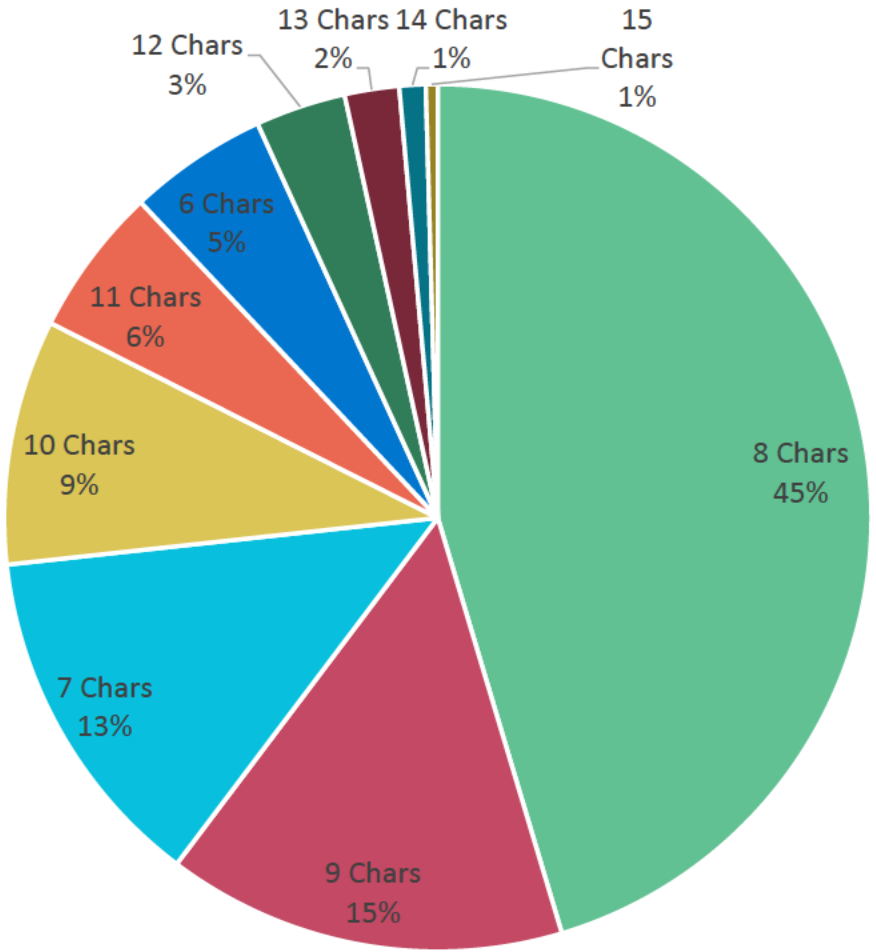
# Bad Passwords...

## ... and where to find them

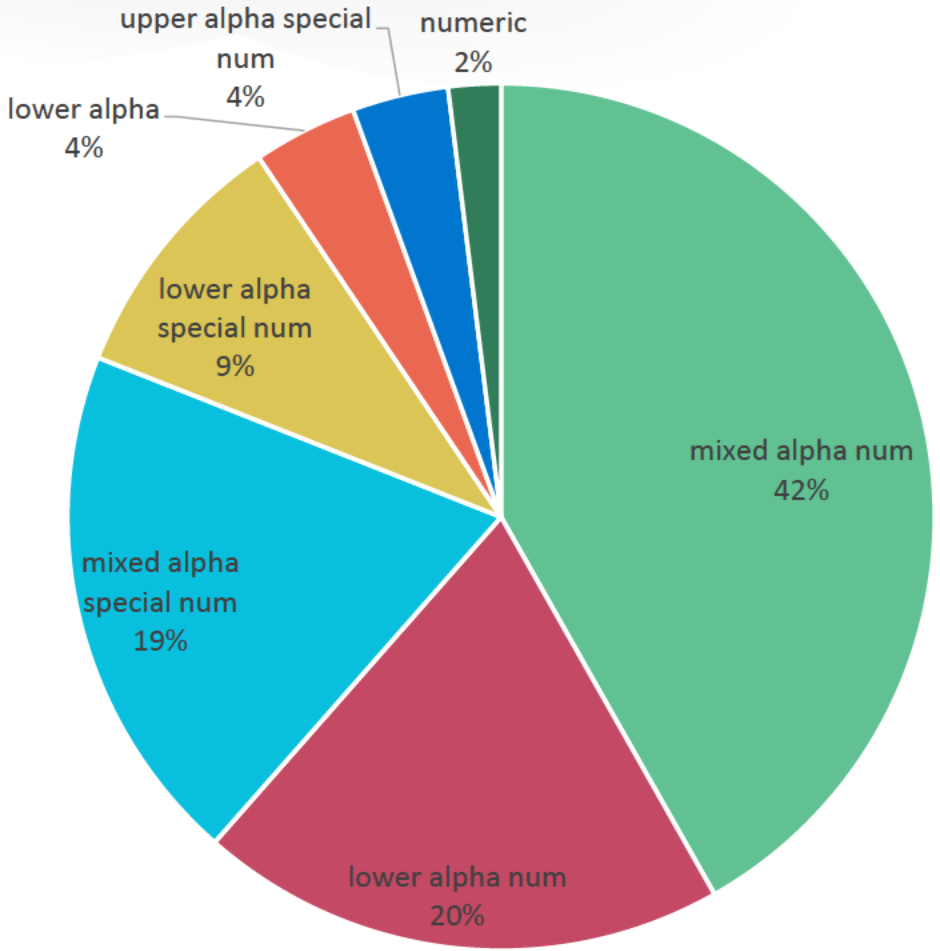
# Policy is all well and good but…

- Educate users
- Lack of MFA, misconfigured MFA
- Weak passwords

# P@55w0rd by any other name…



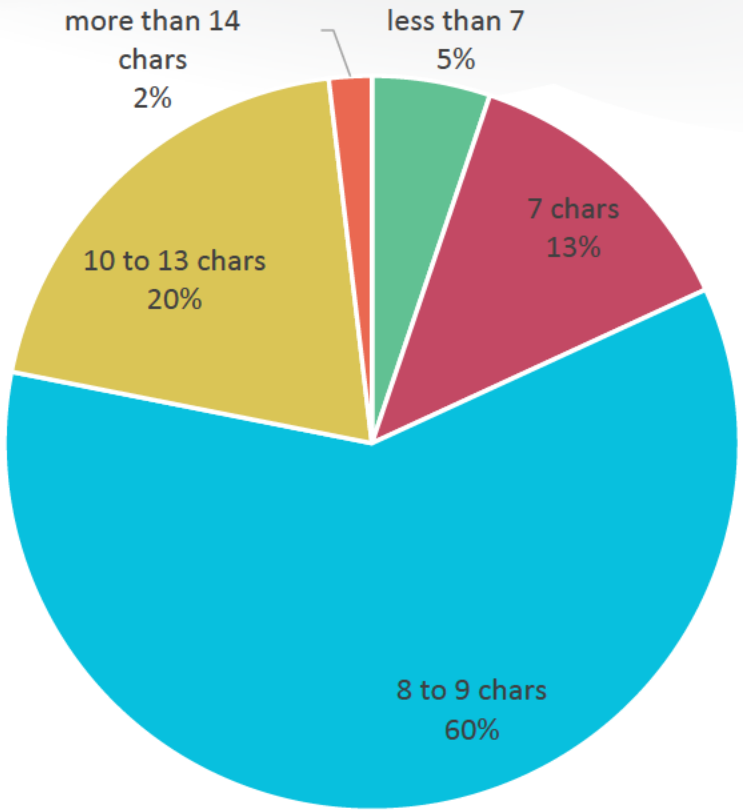

Password length




Character sets

# Does ~~size~~ length really matter?

- Password brute-force
- Less than 7 chars
- 7 chars len
- 8 to 9 for Microsoft/NIST
- 10 to 13 for ISM
- More than 14 chars CIS




| STANDARD | MIN LEN* |
|---|---|
| Microsoft | 8 (default 7) |
| NIST | 8 |
| CIS | 14 |
| ISM | 10 |
| PCI DSS | 7 |

* Recommended values by the standards

# P@55w0rd by any other name…

- Top 10 passwords
  - {Company}-1234
  - {Company}123
  - {Company}@2020
  - {Company}@2019
  - Welcome1
  - Password1
  - 1Welcome
  - 12345678
  - Password01#
  - P@55w0rd
- Top 10 base words
  - {company}
  - welcome
  - password
  - pass
  - summer
  - monday
  - spring
  - tuesday
  - winter
  - friday

# When in doubt “Summer2020”

- First capital last number (43.9%)
- Two digits on the end (21.05%)
- Single digit on the end (15.68%)
- Three digits on the end (10.96%)
- First capital last symbol (9.57%)

- Last 4 digits (Top 10)
  - 1234
  - 2020
  - 2019
  - 2017
  - 2018
  - 2345
  - 5678
  - 2016
  - 3456
  - 2015

RSAConference2020 APJ

A Virtual Learning Experience

# So where do we use all of this

# Some common mistakes and blind spots

- Passwords obtained from previous breaches
- Dictionary words
- Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’).
- Context-specific words, such as the name of the service, the username, and derivatives thereof …

# I hear you say MFA?

While MFA is a very effective counter measure, some common mistakes are frequently made:

- SMS/Email based MFA
- Bad configuration
  - Excessive number of MFA attempts
  - Small MFA key space
- Missing / inconsistent MFA requirements

RSAConference2020 APJ

A Virtual Learning Experience

# Apply

# Some practical advice

- Human factor
  - Ongoing user education
  - Do not use corporate credentials on public websites
  - Monitor and inform
  - Encourage users to protect themselves (haveibeenpwned)
  - Password manager software (Dashlane, 1Password, etc.)

# Some practical advice

- Strong password policy
  - Length over complexity
  - Encourage the use of phrases rather than words
  - Longer password expiry periods
  - Enforce password history
  - Considered lockout
- Multi-Factor Authentication
  - Have it everywhere
  - For everybody
  - Make it less disruptive

# Some practical advice

- No default/weak passwords
  - Password blacklist
  - No passwords from known breaches
  - No internal default passwords such as Company123
- Lest we forget the devices/software
  - Service accounts
  - Local machine account account
  - Password re-use/LAPS
  - IoT
  - Network devices / software
  - CMSs

# Some practical advice

- Identity audit
  - Regular password audits
  - Reviewing inactive, dormant unused accounts
- Authentication behavioural analysis
  - monitor fail logins
  - Suspicious logins
  - Impossible travel

# Some practical advice

- This week you should:
  - Check your password in password dumps (i.e. https://haveibeenpwned.com/Passwords)
  - Get rid of all default/weak passwords
- In the first three months following this presentation you should:
  - Define a strong password policy
  - Implement MFA everywhere
  - Implement/enable authentication behavioural analysis
- Within six months you should:
  - User education
  - Implement identity audit

RSAConference2020 APJ

A Virtual Learning Experience

**Hamed Merati**
**Senior Security Consultant**

**Willem Mouton**
**Principal Security Consultant**

**Sense of Security Pty Ltd (a CyberCX Company)**
**senseofsecurity.com.au**