Passwords

The key to your information kingdom

And what you must know to protect your information

Image source: http://www.ibtimes.com

Funny video on password

https://www.youtube.com/watch?v=Srh_TV_J144

Anonymous Leaked A Massive List of Passwords And Credit Card Numbers

Reported: Dec 27, 2014

Image source: http://knowyourmeme.com

Password Phishing

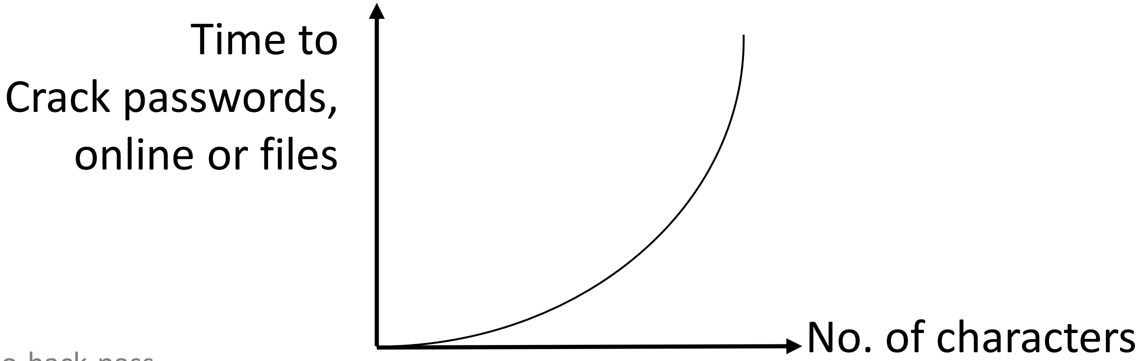
Responsible businesses will NOT use email to ask for personal information, especially user name and password

Any phone call or email requesting for your user name and password are SCAMS!

Why Complex Passwords?

Time to (brute force) crack passwords

	Lowercase	Upper & Lowercase	(Complex) Lowercase, Uppercase, No. & Symbols
10 char	13 hrs 48 mins		
9 char	31 min 52 sec		
8 char	1 min 13 sec		
7 char	2 sec	6 min 2 sec	6 hr 20 mins
6 char	< 1 sec	6 sec	4 mins 3 sec



Test done on random-ize.com/how-long-to-hack-pass

Creating Strong Passwords

- Start with a phrase

Phrase: my windows password was changed in quarter one 2017

- Extract the 1st letter of every word to form the password, with the following twist
  - Capitalize 1 or more letter(s)
  - Insert a symbol within the password

Phrase: my windows password was changed in quarter one 2017

mwPwciq#one17

- Just changed the variable part when system prompt for password change
  - E.g in quarter two: mwPwciq#two17

- Can be used on another system to achieve unique password
  - E.g. for HR system: mhPwciq#one17

DO NOT USE THIS PASSWORD!
Create your own system

- Come 2018, change “17” to “18”!

Creating Strong Passwords

- Start with a phrase

Phrase: my windows password was changed in quarter one 2017

- Extract the 1st letter of every word to form the password, with the following twist
  - Capitalize 1 or more letter(s)
  - Insert a symbol within the password

Phrase: my windows password was changed in quart

mwPwciq#one17

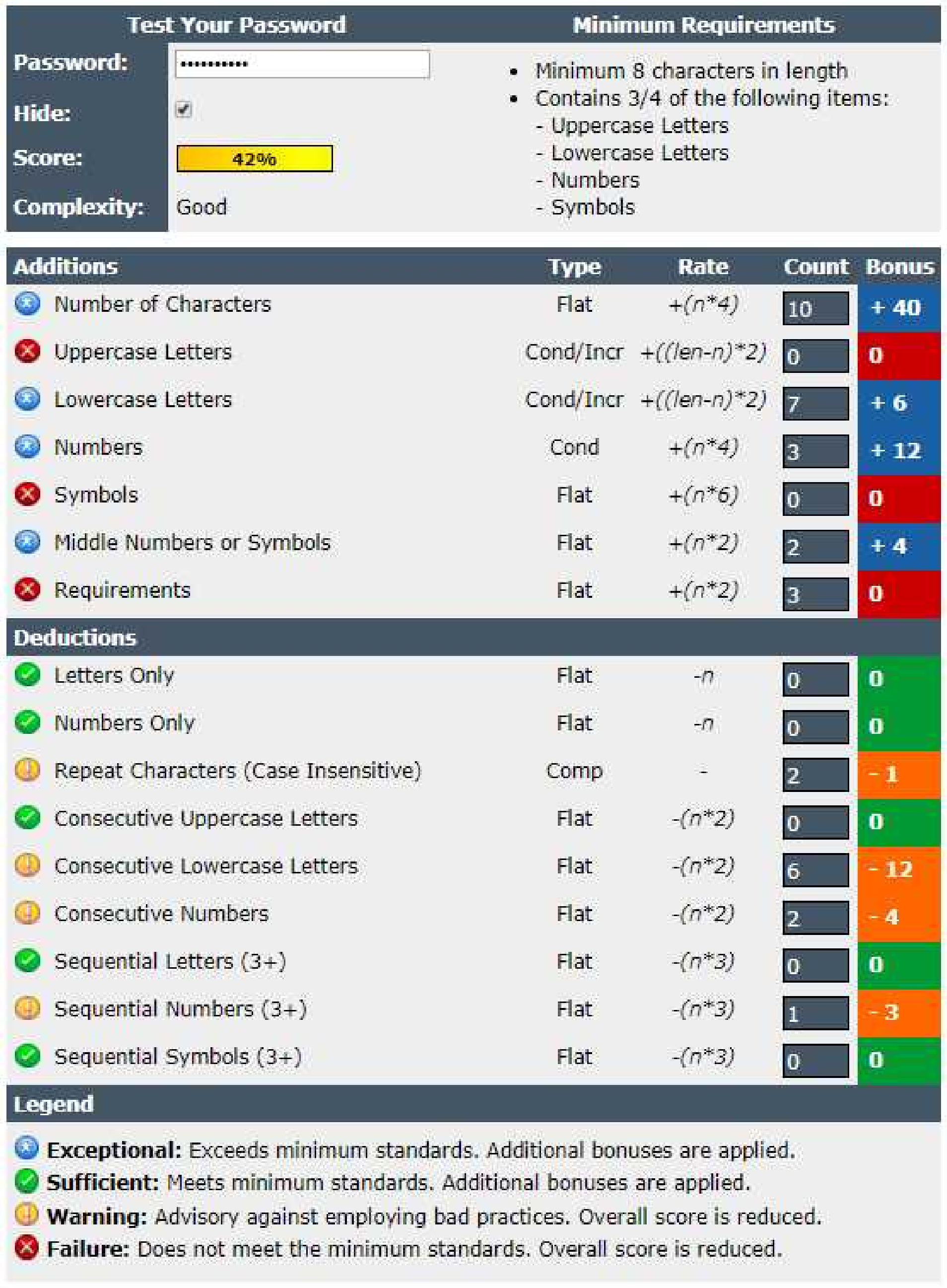
506,637,647 years, 7 months!

- Just changed the ange
  - E.g in quarte

How long does it take to crack this password?

- Can be used on another system to achieve unique password
  - E.g. for HR system: mhPwciq#one17

- Come 2018, change "17" to "18"!



Test Your Password		Minimum Requirements
Password:	••••••••••	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	42%	
Complexity:	Good	

Additions	Type	Rate	Count	Bonus
★ Number of Characters	Flat	+(n*4)	10	+ 40
✖ Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
★ Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 6
★ Numbers	Cond	+(n*4)	3	+ 12
✖ Symbols	Flat	+(n*6)	0	0
★ Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
✖ Requirements	Flat	+(n*2)	3	0

Deductions				
✓ Letters Only	Flat	-n	0	0
✓ Numbers Only	Flat	-n	0	0
! Repeat Characters (Case Insensitive)	Comp	-	2	- 1
✓ Consecutive Uppercase Letters	Flat	-(n*2)	0	0
! Consecutive Lowercase Letters	Flat	-(n*2)	6	- 12
! Consecutive Numbers	Flat	-(n*2)	2	- 4
✓ Sequential Letters (3+)	Flat	-(n*3)	0	0
! Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
✓ Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

★ **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.

✓ **Sufficient:** Meets minimum standards. Additional bonuses are applied.

! **Warning:** Advisory against employing bad practices. Overall score is reduced.

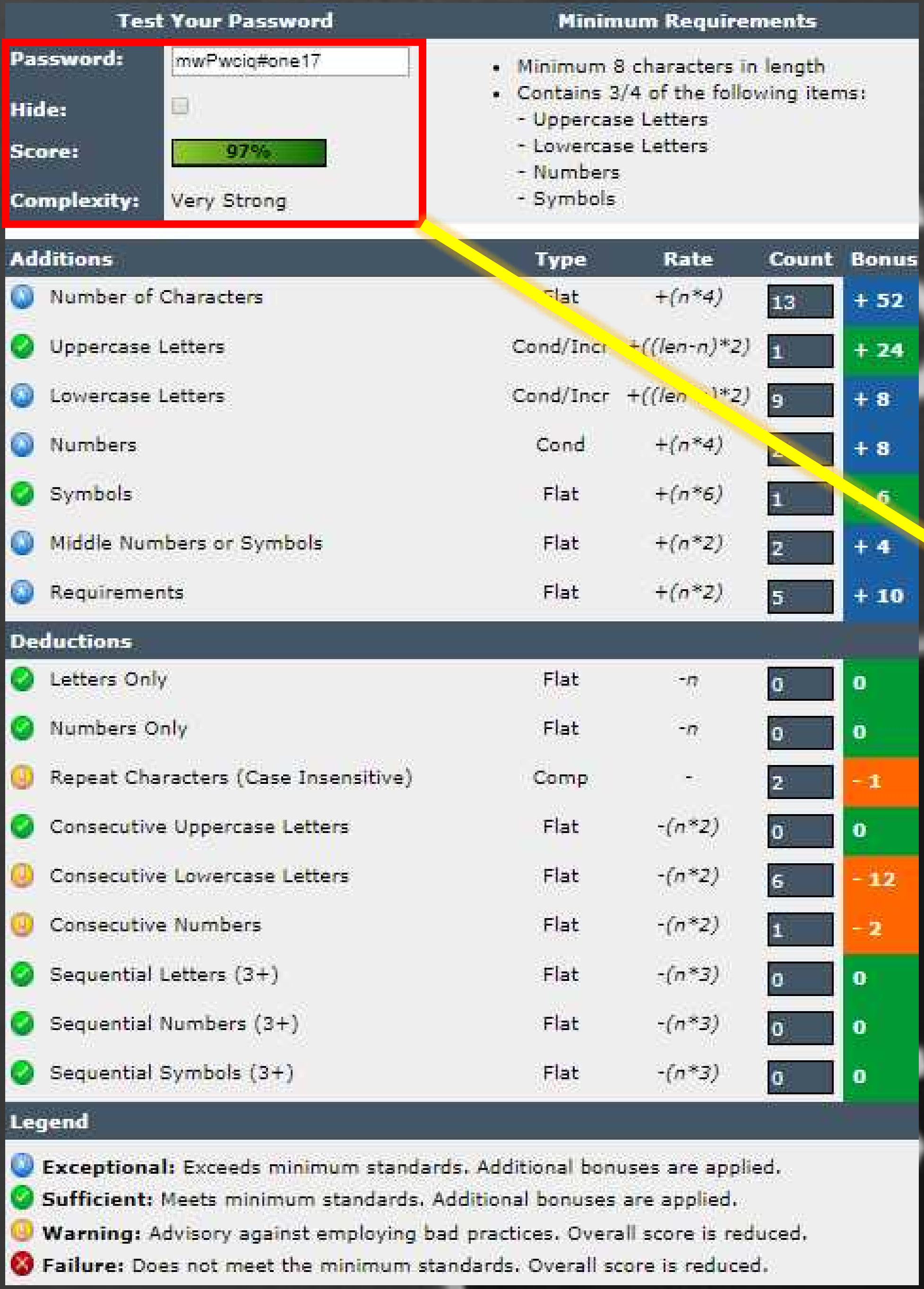
✖ **Failure:** Does not meet the minimum standards. Overall score is reduced.

Passwordmeter.com

- Real time feedback & advice to help create better password
- Warning: Do not use your actual password to test
  - Replace each character of your password to be tested. If testing mdiT45?a, test using nelR23!b

Passwordmeter.com

- Score of our password example “mwPwciq#one17”



Test Your Password	
Password:	mwPwciq#one17
Hide:	□
Score:	97%
Complexity:	Very Strong

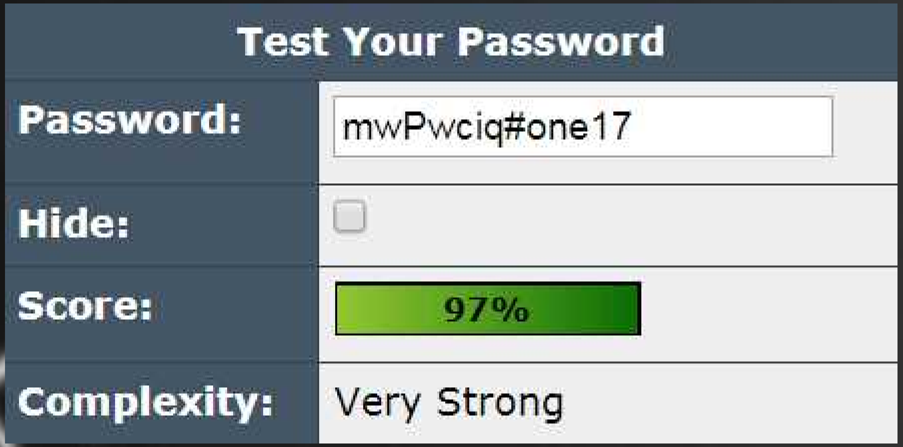
Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	13	+ 52
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 24
Lowercase Letters	Cond/Incr	+((len-n)*2)	9	+ 8
Numbers	Cond	+(n*4)	2	+ 8
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	6	- 12
Consecutive Numbers	Flat	-(n*2)	1	- 2
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.



Test Your Password	
Password:	mwPwciq#one17
Hide:	□
Score:	97%
Complexity:	Very Strong

Two-Factor Authentication

Something you KNOW

Please Sign In

Sign in using your username and password.
Fields are case sensitive.

Username/Email:
Password:
Remember Me
LOGIN

Can be stolen

+

Your Security PIN is

768334

Something you HAVE (2FA Token)

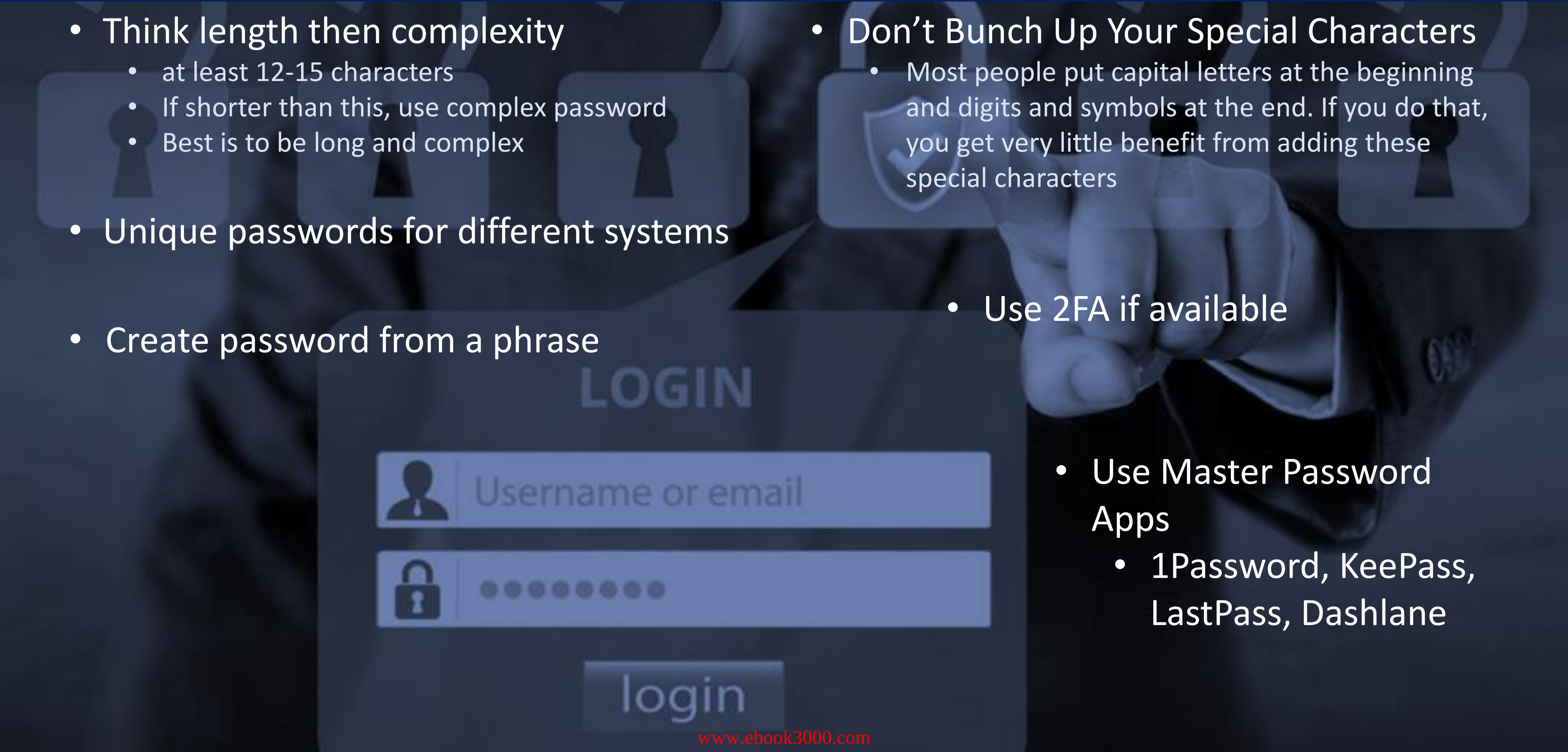
Hard to steal

- Traditionally, only user name and password is required to access any system
  - Both can be stolen easily

- 2FA adds an extra layer of security
  - Something that only the user has e.g. 2FA token
- Also known as multi factor authentication

How to Protect yourself?

- Think length then complexity
  - at least 12-15 characters
  - If shorter than this, use complex password
  - Best is to be long and complex
- Unique passwords for different systems
- Create password from a phrase
- Don’t Bunch Up Your Special Characters
  - Most people put capital letters at the beginning and digits and symbols at the end. If you do that, you get very little benefit from adding these special characters
- Use 2FA if available
- Use Master Password Apps
  - 1Password, KeePass, LastPass, Dashlane



PASSWORDS ARE LIKE UNDERWEARS

Keep Them
Out of sight

Change Them
Regularly

Don't Share
Them

Link to editable Powerpoint version of this ebook

- https://1drv.ms/p/s!AsPU2WUrSYsmpXtBKAn2jur9w03m or
- **https://tinyurl.com/y8gvvcqj**

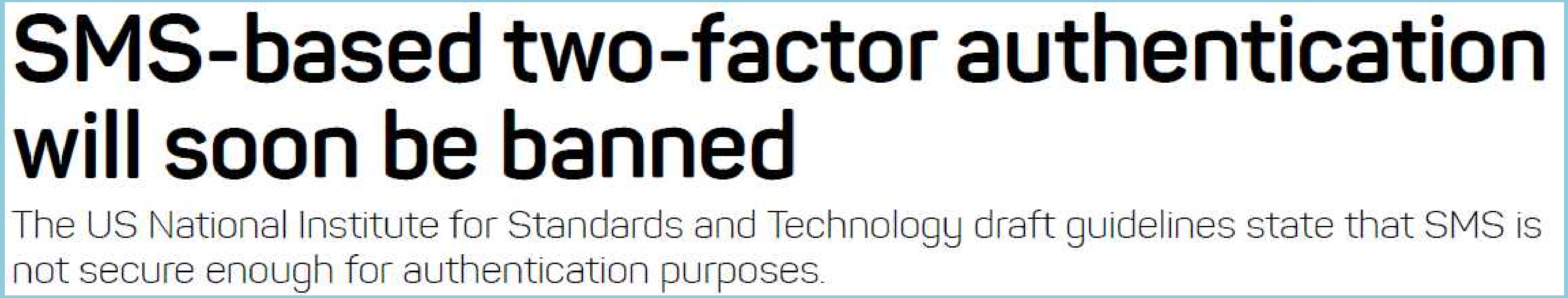
The author can be contacted at mobileapps4u@gmail.com

Password Quiz

1. Is SMS two-factor authentication safe?

   a. Yes

   [✓ b. No]



SMS-based two-factor authentication will soon be banned

The US National Institute for Standards and Technology draft guidelines state that SMS is not secure enough for authentication purposes.

Sep 2016

Image source: https://www.indusface.com

Password Quiz

2. Password – Which is more important?

[✓ a. Length]

b. Complexity

Length is Strength.

However, Length + Complexity is Super Strength!

Image source: https://www.indusface.com

Password Quiz

3. Which of the following passwords is the most secure?

   a. 123Goat

   [✓ b. ZSb6ed!]

   c. 567890

   d. my69*pi

This password contains the basic elements of a strong password. It contains a combination of letters, numbers and symbols; it includes both upper and lower case letters; and it does not contain any words from the dictionary.

Image source: https://www.indusface.com

Passwords - The key to your information kingdom

This was created for busy IT Security folks, who have to juggle with daily operations, project advisories, incident response, audits AND IT security awareness. As an IT Security professional myself, I fully understand the amount of time required to create (and update) a good set of IT Security awareness presentation slides. The slides (the link to the actual editable Powerpoint slides is in the PDF) come with suggested speaker's note so it's a ready-to-present material. This is the first part of a multi-part series that will be published by me.

My approach to IT Security Awareness training is to focus about 75% of the training content on areas that audience can relate to - things that they can apply in their personal life. I firmly believe that once that's achieved, the effect of the awareness will flow over to what they do in their office work.

My audience has appreciated and enjoyed (very much) the content in this training material, especially the part where they were made to guess the time required to crack 8-10 character passwords of different complexities. You will get the sense of achievements when you see their jaws dropped!

I hope the content in this 15-slide training material (including a quiz with 3 questions) – 2FA, tips on how to protect oneself, how to create strong password from a phrase, why regular change of password is important and the fun part on the time required to crack passwords, will help my security counterparts in their preparation for a IT Security Awareness presentation.

Jeremy Ong currently heads the Corporate IT Security arm of a Service Integrator in Singapore, which has more than 300 clients. He was also the former IT Security head of one of the largest Utility companies in Singapore.