

# *Creating a **STRONG** Password*



# IN A WORLD...

- Where you don't have any access to your online life, how would you cope?
- What would you miss the most?
  - What If someone else using your FB/Gmail...???



# IS That...???



YAHOO!

Linked 



what

would

you

do?



Use & Create Strong  
Passwords for your online  
Life and Be Safe...



Your Password is like  
your Home Key...  
So Treat as it is....



“Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months”

-Clifford Stoll-



# Quick Look

- What is a password
- Characteristics of a weak password
- Creating a strong password(Tips)
- An example(With Steps)
- Password attacks
- Self test



# What is a Password?

- What is a password?

Simply, a secret word or phrase that must be used to gain admission to a place

– “A password is information associated with an entity that confirms the entity’s identity.”



# What is a Password? Cont...

- Why do we need passwords?
  - Passwords are used for *authentication*
    - Authentication can be thought of as the act of linking yourself to your electronic identity within the system you are connecting to
      - Your password is used to verify to the system that you are the legitimate owner of the user/account identifier
    - Commonly referred to as “log in”



# What is a Password? Cont...

- Passwords/Identity/Privacy
  - Attackers who obtain your password can authenticate themselves on various systems and in turn ...

Access your personal information  
(**invade Your Privacy**)

Impersonate you by acting on your behalf  
(**steal Your Identity**)



# WORST PASSWORDS OF 2013

rank	password	change from 2012
#01	123456	⤴1
#02	password	⤵1
#03	12345678	—
#04	qwerty	⤴1
#05	abc123	⤵1
#06	123456789	new
#07	111111	⤴2
#08	1234567	⤴5
#09	iloveyou	⤴2
#10	adobe123	new



**NEVER use these as your passwords**

legend:

unchanged — up ⤴# down ⤵#



<http://splashdata.com/press/worstpasswords2013.htm>



# Length of time to crack passwords of varying complexity

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

GOOD

Average

Bad

<http://www.inetsolution.com/turnleft/image.axd?picture=password-cracking-table>



# Characteristics of a *weak* password

- based on common dictionary words
  - Including dictionary words that have been altered:
    - Reversed (e.g., “terces”)
    - Mixed case (e.g., SeCrEt)
    - Character/Symbol replacement (e.g., “\$ecret”)
    - Words with vowels removed (e.g., “scrt”)
- based on common names (e.g., “john”, “jack”)
- based on user/account identifier (e.g., “admin”, “user”)



# Characteristics of a *weak* password

- short (under 6 characters)
- based on keyboard patterns (e.g., “qwerty” “zxcvbnm”)
- composed of single symbol type (e.g., all characters)
- resemble license plate values or phone numbers
- are **difficult** for you to **remember**



# *Weak* password practices

- recycling passwords (using the same password again)
- recording (writing down) passwords
- use of previously recorded passwords (combination of above practices)
- use of password on two or more systems/contexts
  - Especially risky when passwords are reused in low-trust systems (e.g., online gaming) since increased exposure



# CREATING STRONG PASSWORDS

- A strong password is an important part of keeping your information safe online
- Lets get ready to learn some tips for creating a strong password

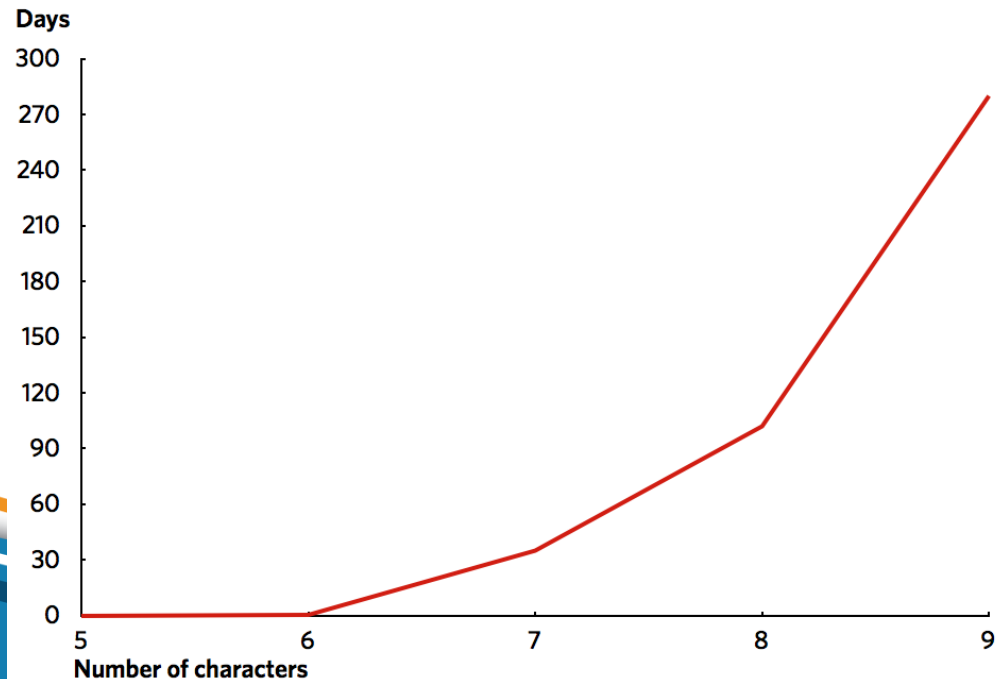


# TIP #1 - LENGTH

- Make your passwords long
- 10 or more characters is a good length



Time to brute force entire alphanumeric + symbols keyspace



# ***TIP #2 - COMPLEXITY***

- Include letters, punctuation, symbols, and numbers (a-z) , (, . ” ’ ? ) , ( ! @ \$ % ^ & \* ) , ( 0 - 9)
- Use the entire keyboard, not just the letters and characters you use or see most often.



## *TIP #2 – (Cont...)*

- The greater the variety of characters in your password, the better.
- However, password hacking software automatically checks for common letter-to-symbol conversions, such as changing
  - "and" to "&"
  - "to" to "2."



# ***TIP #3 - VARIETY***

- Don't use the same password for everything!  
(e.g. – Gmail / Facebook etc...)
- Cybercriminals steal passwords on websites that have very little security, and then they use that same password and user name in more secure environments, such as banking websites.



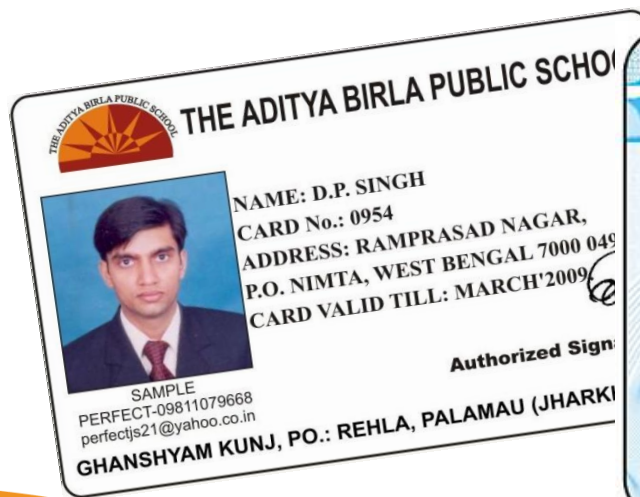
# ***TIP #4 - VARIATION***

- To keep strong passwords effective, **change them often.**
- Remind yourself to change your passwords every six months or so.



# TIP #5 – THINGS TO AVOID

- Personal information. Your name, birthday, driver's license, student number, passport number, or similar information.



# ***TIP #6 ADD AN EXTRA LAYER OF SECURITY***

- Once you've created a smart password, you can add an extra layer of security by enabling [2-Factor Verification](#)
- Not all Internet accounts have this security option, but Google/Facebook /yahoo etc..Account does.
- 2-Step Verification requires you to have access to your device(phone/tab/etc...), as well as your username and password, when you sign in.



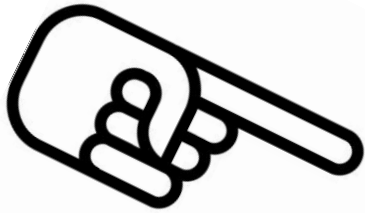
# *AN EXAMPLE*

- There are many ways to create a long, complex password.  
Here are some suggestions that might help you to remember it easily:



## Step 1

- Lets get a sentence/phrase like this...



“me gase boho pani dodam thibe, wadiya kadana naraka lami hema nowe api“

## Step 2

- Remove the space of the sentence & get the first letter of each word

mgbpdtwknlna



## Step 3

- Then alternate them Randomly  
(Capital/Simple)

# MgbpdtWknlhna



## Step 4

- Finally substitute a symbol like a ! For **l** and 6 for **b**

Mg6pdtWkn!hna



# TESTING THE STRENGTH

- Click on the link below to test how long it would take to crack it.

<https://www.grc.com/haystack.htm>

GRC's Interactive Brute Force Password "Search Space" Calculator  
*(NOTHING you do here ever leaves your browser. What happens here, stays here.)*

2 Uppercase   9 Lowercase   1 Digit   1 Symbol   13 Characters

**Mg6pdtWkn!hna**

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	$26+26+10+33 = 95$
Search Space Length (Characters):	13 characters
Exact Search Space Size (Count): <small>(count of all possible passwords with this alphabet size and up to this password's length)</small>	51,880,316, 927,184,027,554,126,495
Search Space Size (as a power of 10):	$5.19 \times 10^{25}$

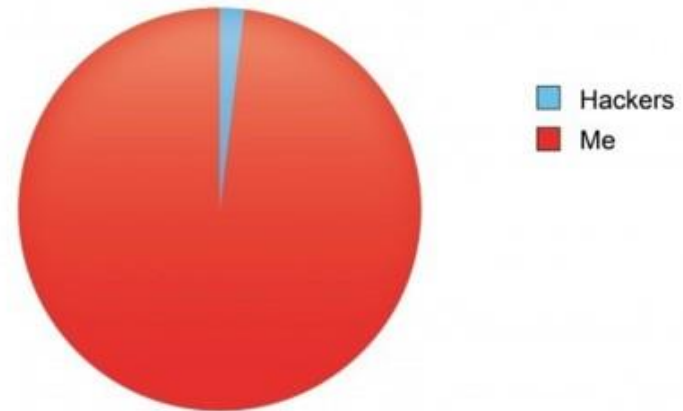
Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: <small>(Assuming one thousand guesses per second)</small>	16.50 trillion centuries
Offline Fast Attack Scenario: <small>(Assuming one hundred billion guesses per second)</small>	1.65 hundred thousand centuries
Massive Cracking Array Scenario: <small>(Assuming one hundred trillion guesses per second)</small>	1.65 hundred centuries

# ***REMEMBER YOUR PASSWORDS***

- Having multiple complex passwords can be complicated
- You must find the best way to remember them (but always keep your passwords secret!)

**People who can't log in to my account  
because of my ultra high security password**



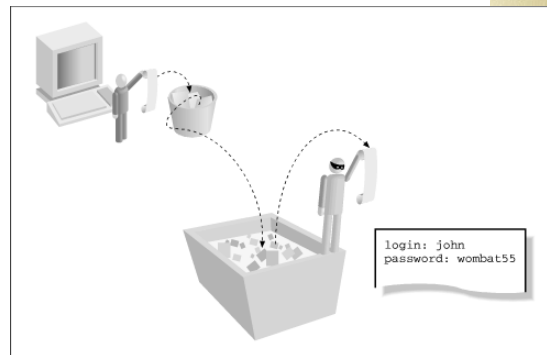
# PASSWORDS ATTACKS

- Most successful attacks are based on:
  - **Dictionary attacks**
    - “The guessing [often automated] of a password by repeated trial and error.”
  - **Social engineering**
    - “Social engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.”



# >>Social Engineering<<

- Social engineering is a technique used by criminals to gain access to your computer
- Social Engineering methods
  - Friendships:
  - E-Mail:
  - Dumpster Diving:
  - Office Snooping:
  - Trust:
  - Time:



# Key Things To Remember !!!

- Remember to **Create a Long/Complex Password** using learned [Tips](#)
- **Do Not Reuse** your passwords
- **Never Share Your Passwords** with anyone and keep them Safe
- **Change Passwords** periodically (at least by six months)



# Self Test



# Question 1

Strong passwords and password practices contribute to protection of identity and privacy.

- A. TRUE
- B. FALSE



✓ Correct!

Excellent, **Answer – A(True)**

strong passwords and password practices do contribute  
to protection of identity and privacy

Now let's move onto the next question ...



## Question 2

Which pair contains both a *weak* and a **strong** password?

- A. cs101ra, ME11111
- B. WYSIWYG, passwd
- C. ig\*hh4klsd, f9%Wfsdfh
- D. abc123, on\$7musdfr

(choose/click one)



✓ Correct!

Excellent, **Answer - D**

**A. cs101ra, ME11111**

**(weak, common), (weak, license #)**

**B. WYSIWYG, passwd**

**(weak, common acronym), (weak, common)**

**C. ig\*hh4klsd, , f9% Wfsdfh**

**(strong), (strong)**

**D. abc123, on\$7musdfr**

**(weak, common ), (strong)**



Now let's move onto the next question ...



## Question 3

What is the role of passwords in authentication?

- A. to identify the user
- B. to verify you are the legitimate owner of the user/account identifier
- C. to provide security
- D. none of the above

(choose/click one)



✓ Correct!

Excellent, Answer - B

B. the role of passwords in authentication is to verify you are the legitimate owner of the user/account identifier

Now let's move onto the next question ...



## Question 4

Which of the followings are **not** a characteristic of a weak password?

- A. based on common dictionary words
- B. short (under 6 characters)
- C. based on keyboard patterns (e.g., “qwerty” “zxcvbnm”)
- D. Included letters, symbols, and numbers with length of 10 or more characters

(choose/click one)



✓ Correct!

Excellent, Answer - D

D. Included letters, symbols, and numbers with length of 10 or more characters

Now let's move onto the next question ...



## Question 5

Social engineering is the process of using social skills

- A. To find more friends online
- B. To search information via internet
- C. to convince people to reveal access credentials or other valuable information to the attacker

(choose/click one)



✓ Correct!

Excellent, Answer – C

C. to convince people to reveal access credentials or other valuable information to the attacker

Congratulations, you have answered all questions correctly ...



Remember, it is ...

**Y**our Password  
our Identity  
our Privacy





training@nic.lk

