

INDEX

Introduction to password management	Page 3
How passwords get compromised	Page 3
Guidelines for a safe password	Page 4
Examples of a good password	Page 6
Scenario Study	Page 8
Conclusion	Page 9
About RCOM	Page 10



Introduction to Password Management

With the internet penetration growing everyday and most of our activities getting dependent on computers and internet, it is increasingly becoming a little difficult to make sure we are safeguarding ourselves from hackers and criminals. Such people can have various intentions and motives. Some have simple knowledge seeking intentions to defame some one and some have more serious monetary motives. Here we will try to tackle the problem of password management. Let us see how to choose and maintain the right password.

How passwords get compromised?

One physically writes it down somewhere and keeps it where it can be seen like desk, wallet etc. Various permutations and combinations can be worked out by person known to you or program to crack a password. These passwords can be as simple as the name of one's child or wife. On the internet, passwords can be tracked which transit in encrypted or plain text format. Even on computers, servers and backup machines passwords are stored in encrypted or plain text which can be easily obtained.

The above are most of the problems which are required to be tackled. These problems would not require so much of attention if we were able to create, remember & safeguard multiple difficult-to-crack passwords. Also change these passwords frequently.

Due to interfaces with multiple sites & gateways it can be at times difficult to remember all the passwords. But without it safe on-line activities is impossible. Hence Password Management requires some serious thoughts.

We may be able to sometimes guess the username & password of accounts of people known to us. For example our children's email account or our wife's bank account because we to a great extent know what they could be thinking. Under unknown scenarios where complex passwords of high importance accounts there still is the threat of professional hackers operating in market. The bottom line is that a password needs to be very difficult to guess either by human or machine



Guidelines for a safe password

- The password character length must be at least 7 characters.
- Password must contain at least:
 1. One Lowercase Letter
 2. One Uppercase Letter
 3. One Digit
 4. One Symbol
- If your system is advanced and if the option is available then try to include a symbol or punctuation mark in your password.
- A very good practice is not to repeat a character more than twice. Example: password112 is better than having password111 since the digit '1' is used thrice in the later.
- It is always suggested not to use your password same as your username or login ID.
- Few other common passwords like – 'password', '123456', 'qwerty', 'administrator', your own name etc should never be used.
- Words straight from the English dictionary should be strictly avoided. For any hacker or attacker it is very easy to crack such passwords.
- However words from other language dictionaries should be tried to be included if the system supports it. The most popular trends seen these days are use of Latin and Chinese characters and symbols as passwords. At the moment these are considered to be very secure and difficult to compromise.
- One should always remember that a password is his/her personal property and should not be shared with any one no matter how close the other person may be. There are high chances that the other person becomes careless and in turn your password gets compromised. Generally young children are often seen sharing their passwords with their friends.
- Users are lot of times fooled (by spam or phishing) in to typing their password in to websites and systems which look legitimate. You must be able to identify if the website or system is genuine or not. Make sure you are using the latest version of a trust browser like Internet Explorer, Mozilla, Opera, etc with pop-up blocker enabled. Also make sure you have active, updated Anti-spyware and Anti-spam installed in your computer.



White Paper Series- Password Management

RELIANCE
Broadband

- ❑ Many people use one single strong password which is common for all the applications or systems they use. This is called as 'synchronizing the password'. Synchronized passwords reduce security because if one system is compromised then as a result all systems are compromised. However on the other hand unsynchronized passwords are difficult to remember and people end up writing it some where which in the end again makes it less secure. So it is a personal choice based on how many passwords one can remember & on which all fronts synchronized passwords could be maintained.
- ❑ You can also make password depending on the importance (may be financial) of the application, system or website. For example your email account or bank account password needs to be stronger than the password for a daily news subscription website. Thus reducing your load to remember multiple complicated passwords.
- ❑ The most important thing that one needs to remember is that, a password which is safe today may not be safe tomorrow or day after or after a year. Some one may try continuously to crack your password and in matter of days or weeks might even get successful. The best practice is such a scenario is to change your password very often. Most systems have an auto password change policy after 45, 60 or 90 days. You can manually change your passwords more often to make them more secure.
- ❑ When you change passwords it is very important not to use passwords which have been previously used. This makes the system very vulnerable incase the old password is already compromised.



Examples of a good password

You can make a good password based on something which is relevant to you or by creating logic for every alphabet, number, punctuation mark or even a character. By doing so it will be easy for you to remember it but extremely difficult for others to crack.

Here we are either replacing a particular character or moving to one (or more) characters in alphabetical order/ key board.

In the first example below of 'maple tree'

- Passwords generally being case sensitive we can change 'm' by 'M' and reduce chances of it being cracked
- 'a' can be by '4' – since it looks a little similar.
- 'p' can be mirrored and replaced by 'q'.
- Lower case 'l' can be replaced by 'L'.
- 'e' can be replaced by '3' – again based on a little similarity.
- The space is replaced by '_'
- 't' can be replaced by '7'.
- 'r' can remain unchanged.
- 'e' can again be replaced by '3'.
- Finally 'maple tree' is converted to 'M4qL3_7r33'.

Few more examples are shown below which shows how each character in a meaningful word is replaced by a similar looking character to make a complicated password.

The last example in the below table of 'apple' shows a very old encryption technique of transmitting data. Here each alphabet is moved sequentially one space ahead forming 'bqqmf'. Hence again converting a meaningful word into a complicated password. Instead of moving one space it can be moved multiple spaces and the complexity can be further increased.



broadband plan as per TRAI.

White Paper Series- Password Management

RELIANCE
Broadband

Base of Password	Actual Password	Remarks
maple tree	M4qL3_7r33	a → 4 p → q e → 3 space → _ t → 7
reliance	R31i@n63	L → 1 a → @ c → 6
Commercial	60ww3Rc1@L	o → 0 m → w i → 1
password	P#55M0rd	a → # s → 5 w → M
internet	!n73rN3t	i → !
apple	bqqmf	Each alphabet sequentially moved one space ahead. a → b, p → q, l → m, e → f.



Scenario Study

It is probably by now very easy for you to make a single difficult-to-crack password, remember and keep it safely. However it may seem challenging to make multiple such passwords and remember them. In such a scenario making relevant passwords proves to be of great help. For example, if you have 3 banks accounts then passwords you can choose can be

- ❑ My first bank account → wyF1r5tb@nk@660unt
- ❑ My second bank account → wy5360ndb@nk@660unt
- ❑ My third bank account → wy7h1rdb@nk@660unt

Below is the table showing the character replacement guide for the 3 complicated passwords created out of simple statements.

Original Character	Replaced Character – based on physical similarity
M	w
i	1
s	5
a	@
c	6
o	0
e	3
t	7

In case you forget any of the passwords it is very helpful to use the ‘forgot password’ functionality. Most of these functionalities work on the basis of a secret question and answer format, where a pre-chosen question needs to be answered to give you access by generating a new password or revealing your current password. The new password is either emailed or is sent as a SMS to the user. Care must be taken that the answer selected for the question is not known to your family, friends or associates. For example, questions like ‘what is your car model?’ or ‘what is your mother’s maiden name?’ etc. These answers will be known to most of your surrounding people or are easy to find. Even if the answers are common by using techniques showed above even the obvious answers or words can be converted into strong passwords.



White Paper Series- Password Management

RELIANCE
Broadband

Conclusion

No password can guaranty 100 percent security however the probability can be decreased and time taken to attempt crack can be increased by a well managed password.

A strong password is the only wall between your data & hackers. Building a strong on-line wall is dependent upon your rating of data on level of importance & privacy and creating equally difficult-to-crack, well managed, easily recallable & most important regularly changed password.

About RCOM

Reliance Communications Limited founded by the late Shri Dhirubhai H Ambani (1932-2002) is the flagship company of the Reliance Anil Dhirubhai Ambani Group. The Reliance Anil Dhirubhai Ambani Group currently has a net worth in excess of Rs. 64,000 crore (US\$ 13.6 billion), cash flows of Rs. 13,000 crore (US\$ 2.8 billion), net profit of Rs. 8,400 crore (US\$ 1.8 billion).

Reliance Communications is India's foremost and truly integrated telecommunications service provider. The Company, with a customer base of 105 million including over 2.5 million individual overseas retail customers and nearly 3 million DTH customers, ranks among the Top 5 Telecom companies in the world by number of customers in a single country. Reliance Communications corporate clientele includes 2,100 Indian and multinational corporations, and over 800 global, regional and domestic carriers.

Reliance Communications has established a pan-India, next generation, integrated (wireless and wireline), convergent (voice, data and video) digital network that is capable of supporting best-of-class services spanning the entire communications value chain, covering over 24,000 towns and 600,000 villages. Reliance Communications owns and operates the world's largest next generation IP enabled connectivity infrastructure, comprising over 190,000 route kilometers of fibre optic cable systems in India, USA, Europe, Middle East and the Asia Pacific region.

