Mobile Web Design : Password Strength Meter

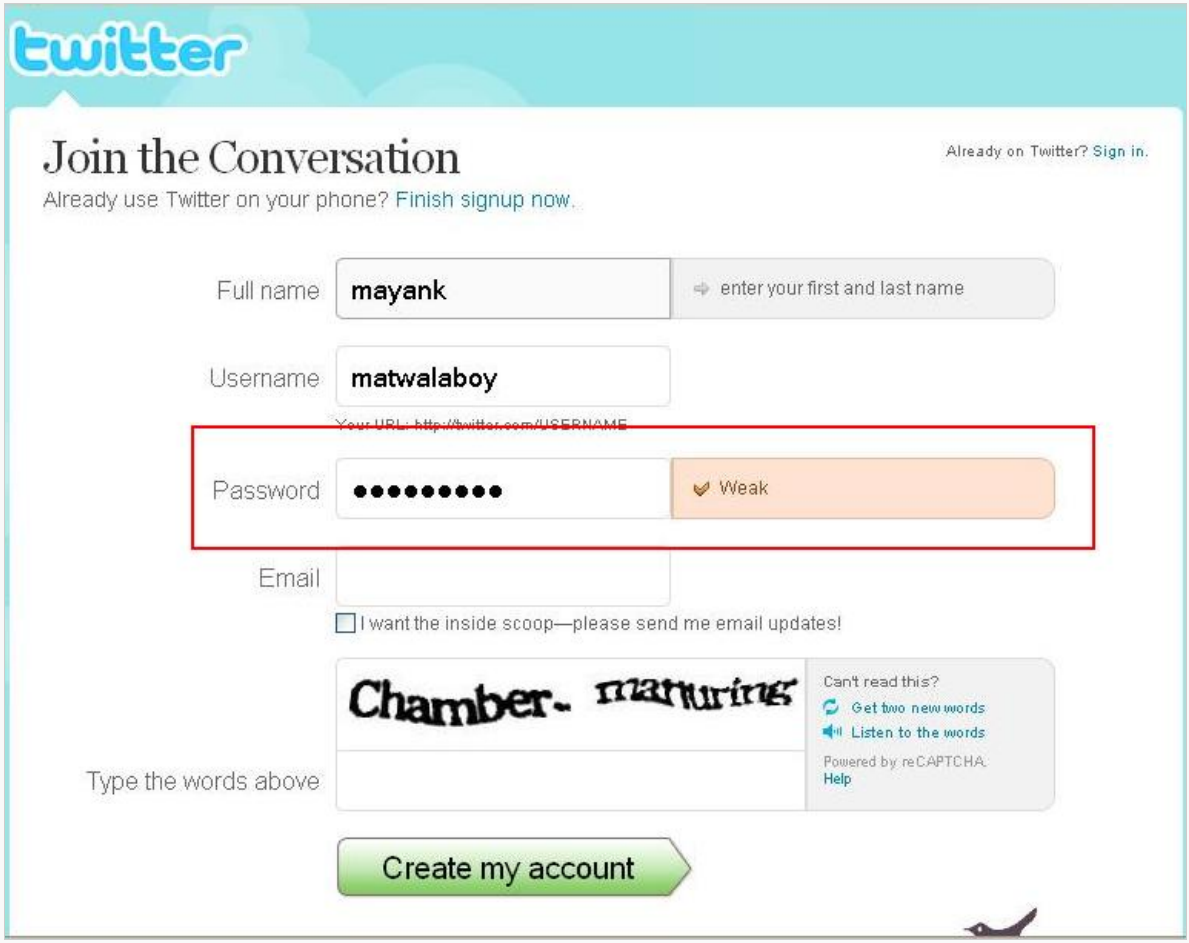
This design pattern is part of the Mobile Web Design series.

Introduction

Security remains one of the key desirability of any user, especially when they are interacting with a website that has access to their sensitive information like personal details like images/contacts, or other financial/individual details like credit card number, social security number etc. When designing a website which allows the user to do anything which they would want to protect from non-authorized persons zealously, it becomes very important that you have as many mechanisms as possible to ensure the safety of the user data. One such mechanism to protect the user account from being hacked easily is a **password strength meter**.

What is a password strength meter

Password strength meter is a visual/textual indication to the user to let them know how strong or weak their entered password is. The strength of a password is checked for a number of parameters with each of them having a rating assigned to them depending upon how tough it makes the password to be cracked by malicious elements. The password strength checker is a possible piece of code, which validates the password and then depending upon the cumulative score the password gets it lets the user know by either showing a bar or a text representation.



Use of password strength meter on twitter

(C) Copyright Nokia 2014. All rights reserved.

Use of password strength meter on twitter

When to use

Some of the websites/places where you should consider using a password strength meter are:-

- When the site you are developing has access to sensitive user data the security of which is critical from a user's standpoint.
- When you want to share the responsibility of data protection with the user by making them part of the process by allowing them to set stronger passwords for their accounts.
- When you want to make it tougher for unauthorized persons/spy wares to be able to infiltrate the user account.

What is a strong password

Some of the key elements on which the strength of a password can be measured are as follows:-

1. Number of characters entered, should be more then 10 characters
2. The case used, should be a combination of upper and lower cases
3. Numeric/Special characters used should be a combination of numbers, special and alphanumeric characters.
4. Uniqueness of the password should not be obvious to guess things like spouse name/DOB/place of residence etc.
5. Spacing between the numbers/alphanumeric characters, should not be consecutive numbers or alphabets.

How to measure password strength

Based on the above mentioned elements defining a strong/weak password, the strength of the password entered can be tested and displayed to the user.

Some additional resources on how to measure the password strength, with source code and guidelines for a strong password creation can be found at the links below:-

- Microsoft Password Strength Checker
- codeassembly.com
- passwordmeter.com
- geekwisom.com

Usability guidelines

(C) Copyright Nokia 2014. All rights reserved.

From usability standpoints of using a password strength meter are as under:-

- **Always indicate to the user the strength of the password possibly with a strength number/percentage/visual notification etc.**

Incremental password strength checking on youtube

Visual notification of password strength on youtube

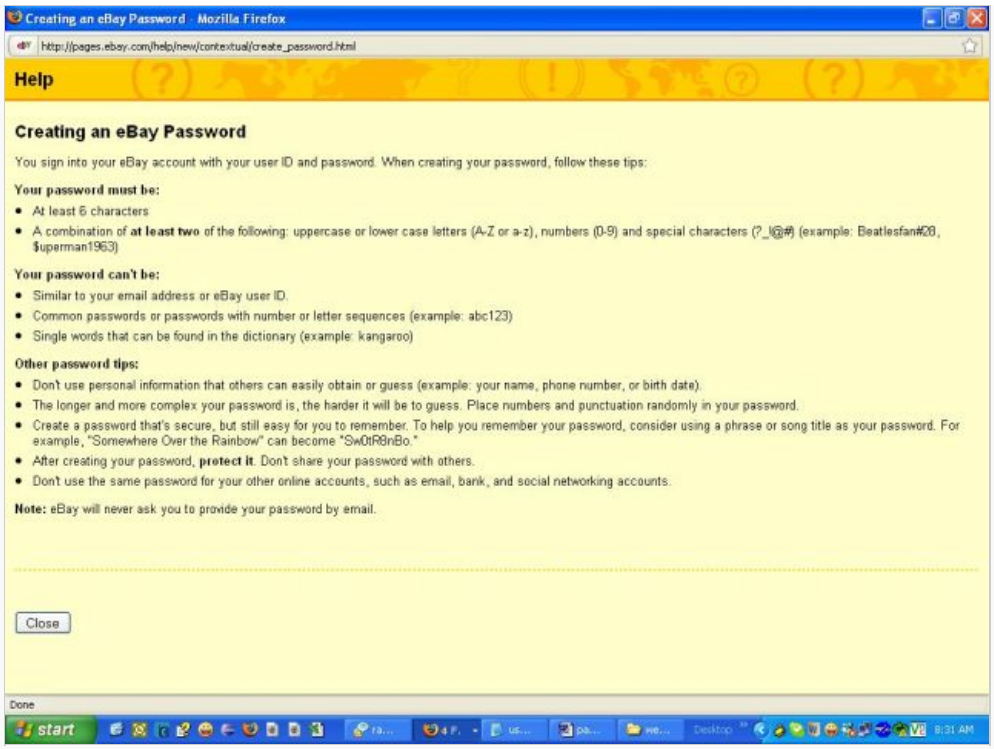
(C) Copyright Nokia 2014. All rights reserved.

Visual notification of password strength on youtube

- **Provide help guidelines to the user to make them understand what constitutes a strong password, so that they don't end up grappling with the strength meter trying to crack it.**

Educating user on what is a strong password on ebay

(C) Copyright Nokia 2014. All rights reserved.



Help manual detailing what makes a strong password on ebay

- Provide live examples of what is a strong v/s weak password and then let the user decide their password choice.
- Do not be rigid on the strength of the password to allow registration/change of password, if the user decides to ignore the warnings/alerts on password strength, let it be their choice.
- Decide on the strength of the password requirements depending upon what you are trying to guard, for instance if it's a fun site, you possibly don't want a password strength testing to be done.
- Do not stress on the user fulfilling all the parameters of making a good password, sometimes only a few parameters are good enough to make a strong password.

Final Word

The password strength meter not only makes the user data safer and less prone to malicious attack/intrusion, it also gives the user a sense of confidence when conducting business with the site. The user always wants to get some sort of a comfort feeling while sharing their privy information that the latter would be in safe hands. Other security mechanisms should also be considered though as password strength meter is not a sure sought guarantee to safeguarding user data, but surely goes a long way in helping towards meeting that objective.

--- Added by Mayank on 30/06/2009 ---

(C) Copyright Nokia 2014. All rights reserved.