Broken Authentication Prevention in PHP

a) Vulnerabilities in authentication (login) systems can give attackers access to user accounts and even the ability to compromise an entire system using an admin account. For example, an attacker can take a list containing thousands of known username/password combinations obtained during a data breach and use an automated script to try all those combinations on a login system to see if there are any that work.

b) Or an automated attack, such as brute force, while an attacker can brute force and try every possible combination of the admin password for an example.

c) Or also an attacker might try all possible default admin passwords, some people forget to change their system's default password, so hackers take advantage of that.

Prevention:

1. Google reCaptcha:

Basically captcha will limit the automated tools to test all possible login credentials and will make life harder for the hacker to guess the right password.

Because in login page, sometimes some malicious users try to guess or brute force admin or other users' password, which they use automated tools to do that, so google reCaptcha prevents accessing these tools to the web site/app by asking them to solve humanly solvable simple puzzles.

Go here to get started with Google reCaptcha:
https://www.google.com/recaptcha/

reCaptcha v3 PHP code and step by step:
https://stevencotterill.com/articles/adding-google-recaptcha-v3-to-a-php-form

reCaptcha v2 PHP code and step by step:
http://acmeextension.com/integrate-google-recaptcha-with-php/

Toolkit Scans if any input form doesn't have reCaptcha and Notifies Developer about it.

2. Some Verbal Advices

a. Make sure you change default admin password
b. Use complex non famous passwords (at least 10 chars)
c. Implement Multi-Factor Authentication
d. Implement strong Temporary Token based or Multi-Factor Authentication based Forgot-Password Process.
e. Make sure no Session IDs are exposed in URLs and/or during redirects.
f. Make sure to auto logout users after sometime of inactivity.
g. Limit Failed Logins.

To learn more about Broken Authentication:
https://www.youtube.com/watch?v=mruO75ONWy8
https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A2-Broken_Authentication