Important: Changes coming to your HRmony system login as of

Thursday June 25, 2015!

Who is NOT impacted with these changes:

Employees that ONLY clock in/out from a web address ending with .clock (i.e., web clock) and/or use a physical time clock will NOT have to change anything unless those users attempt to login to their respective system account (i.e., click 'login'), only then will they need to perform the following:

The security changes are as follows:

1. <u>Enhanced Password Standards</u>:
Going forward, user account passwords must contain a **minimum of 8 characters and include** EACH of the following:

- **Uppercase (Capital) Letter,**
- **Lowercase (Small) Letter,**
- **Number, AND a**
- **Symbol**

An example would be: Password1$

2. <u>Multi-factor Authentication</u>:
Multi-factor Authentication adds an additional level of security. After you enter your username/password and click login, if the system does not recognize this computer as one you have used in the past, the system will require a second form of authentication before you can continue. In that case, a 6-digit verification code will be texted, emailed, or voice called to you. Then, you simply enter that 6-digit code on the login screen and are then granted access to your system account.

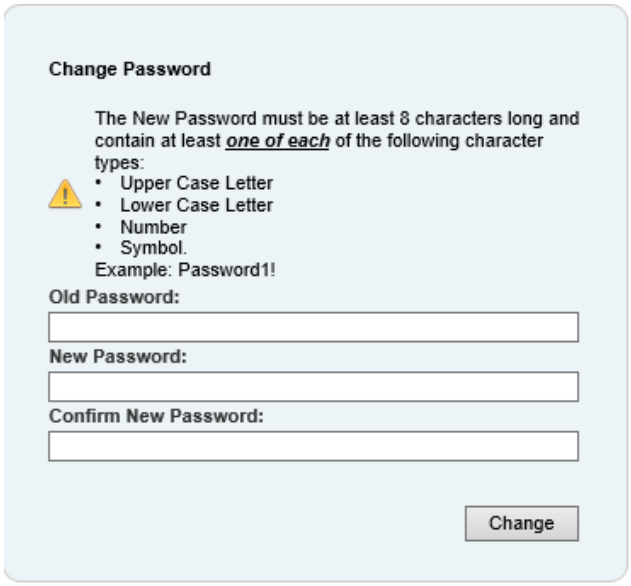
The following pages describe (with screen shots) what will happen on Thursday, June 25, 2015 when users login to their respective accounts.

<<<<<<AGAIN – those using the web clock (i.e., '.clock' web address) for clocking in/out are not impacted at all, unless those same users attempt to login to their respective user

account>>>>>

What Will Happen On Thursday Morning, June 25, 2015?

Step #1: Users should start the login process as usual. After you enter successfully the username and password, the system will prompt you for a new password. The password criteria will have to meet the new standards outlined above. The dialog box shown below will appear:



Step #2: After changing the password, you will be prompted to configure the Multi-Factor Authentication Settings. Up to three methods can be configured for receiving the code, as follows:

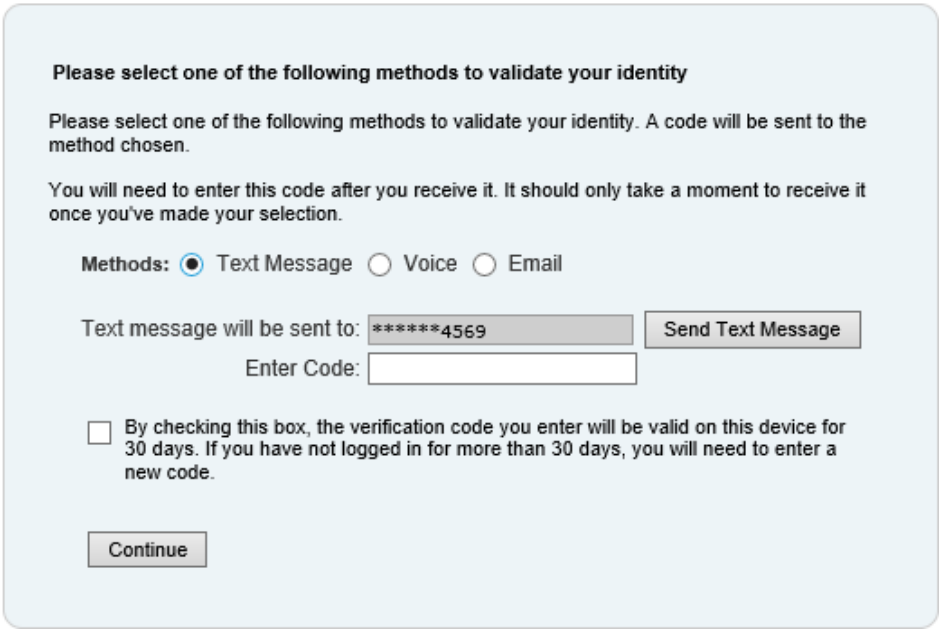
- **Text Mobile #**: Will be used to send codes via **text message**<<<**preferred method**
- **Email**: Will be used to send codes via email address (check your spam folder, if using this)
- **Voice Phone #**: Will be used to send codes via automated phone call

WE SUGGEST POPULATING AT LEAST 2 OF THE ABOVE NOTED OPTIONS AND IDEALLY ALL 3 WITH ACCURATE DATA UNIQUE TO THE USER.

In the previous screen shot (Configure Multi Factor Authentication) - the system will have pre-filled any phone or email that is already listed in your system account – **VERIFY CONTACT INFORMATION SHOWING IS CORRECT, OR TYPE IN WHAT IS ACCURATE FOR YOU AND CLICK 'SAVE'.** Once this step is completed, you will be logged in to the system.

***Please note**: if you change your email or phone number in this process, it will not replace or update information entered in your employee profile. Information entered on Multi Factor Authentication setup screen is used strictly for system security.*

Next time you login (after changing password and setting up multi-factor authentication), the system will list the methods you have selected in the multi-factor authentication setup process; you will be able to select one of those, THEN CLICK 'SEND CODE'. The system will generate a random 6-digit code and send it to you, after entering the code you received, click "Continue" and the system will validate the code and grant access to the application.



Important TIP! If this is your office or home computer that you will use in the future to login, you should check the box *"Remember This Device" (see screen shot above),* this will avoid the verification code requirement on future logins from "this computer."

Mobile Application Users

Mobile application users will be forced to change their password to the new password requirements. Multi-factor authentication is NOT currently required on the mobile application.

Time Clocks (Physical clocks mounted on walls):

This security does not effect the punching on a physical time clock, only accessing your respective user account in the system.

IMPORTANT INFORMATION ABOUT FUTURE MULTI-FACTOR AUTHENTICATION CHANGES BY EMPLOYEES IS AVAILBLE IN A SEPARATE DOCUMENT.