Existing Users Logging into Campus After Password Reset is Enabled

All users logging into Campus for the first time after Password Reset functionality is enabled are prompted to create their security preferences in order to comply with new Password Reset functionality (see Image 9).

Users will have three opportunities to log in without setting their password reset security email address and reset preferences.
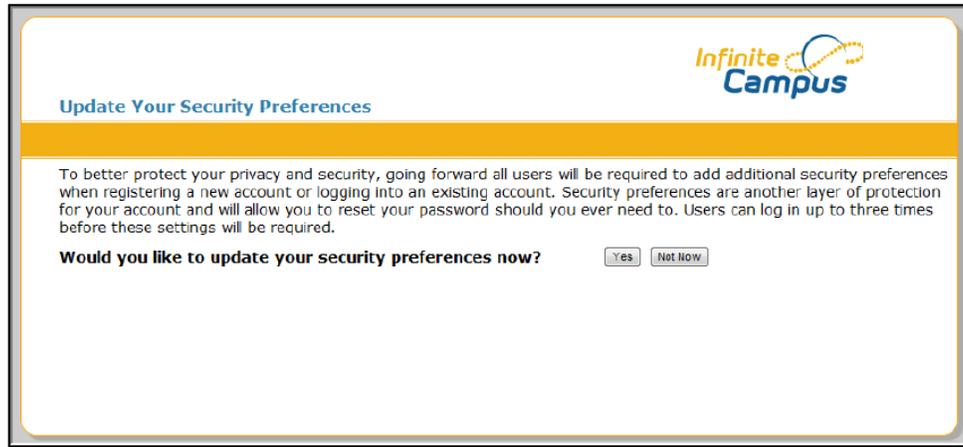

Image 9: Confirming Security Preference Updates

Selecting **Yes** will direct the user to the User Settings editor where preferences can be set (see Image 10).
Selecting **Not Now** will allow the user to access their account, however, the Update You Security Preferences confirmation screen will continue to appear for the user each time they log into their account. After the third login, the user will be forced to update their security preferences.
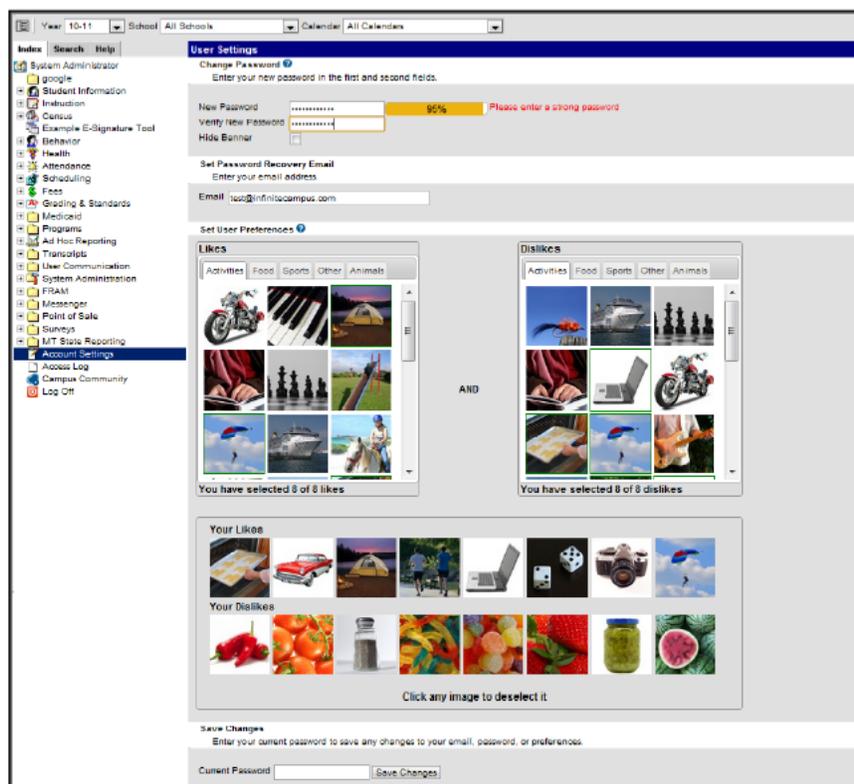

Image 10: Establishing Account Security Preferences

In order for a user to recover their forgotten password, a valid **Security Email** address must be provided and eight **Dislike** and **Like** images must be selected. Dislike and Like images are used to confirm the user's identity during password recovery.

Users must select eight Dislike images and eight Like imagines in order to save. The email address entered must be valid in order to recover a forgotten password.

## Recovering Passwords via the Forgot Your Password Link

If a user is part of a school or district which has Password Reset functionality enabled, they may recover their password using the **Forgot Your Password?** link (see Image 11).
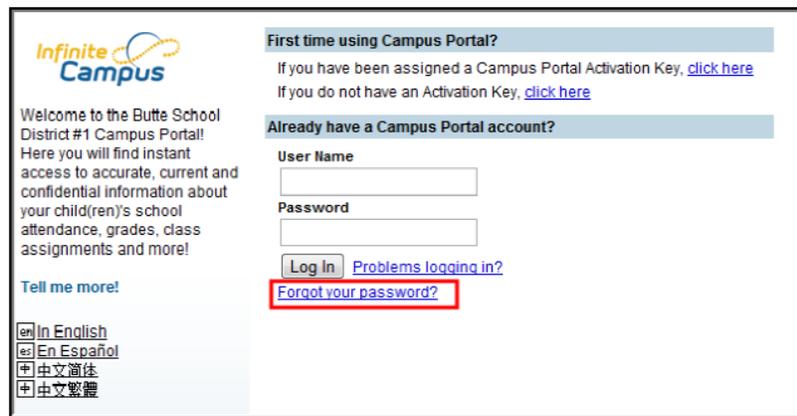
Image 11: Forgot Your Password Link

Once the **Forgot Your Password?** link is selected, the Reset Your Password editor will appear (see Image 12).
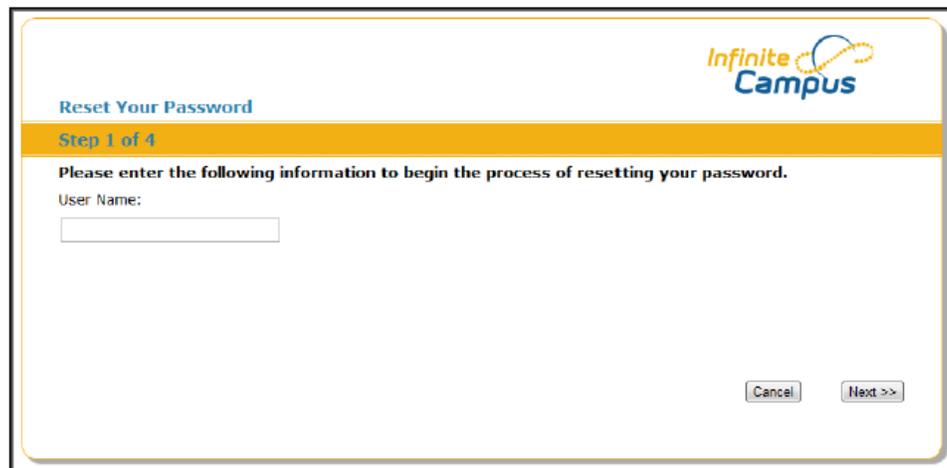
Image 12: Entering Your User Name

Enter your **User Name** and select the **Next** button. The Reset Your Password editor will refresh and inform you to check your email for a unique URL which needs to be selected in order to move on to the next step.

It is critical the email address established on the user account is valid. Users with an invalid email address will be unable to finish the password recovery process. The user account email address is established during the initial setting of preferences as well as managed on the Account Management tool.

This message is in response to a request made in Infinite Campus for an account password. If you did not make this request, please contact your district at (555)123-1234x456789.

You can begin the reset process by clicking the URL below. You can also copy and paste the URL into your browser:

http://▮▮▮▮▮▮▮▮▮/SIS-46568-I90-E/unique-link/5s3pUsgST0UKuwpa?appName=ieMTd1&errorPath=/password/reset/invalidLink.jsp

Image 13: Example of an Email Containing a Unique Password Reset URL

The image above (Image 13) is an example of the email a user will receive. Select the URL or copy/paste it into a web browser to continue the password recovery process. A district contact phone number will also be provided in case additional help is needed.
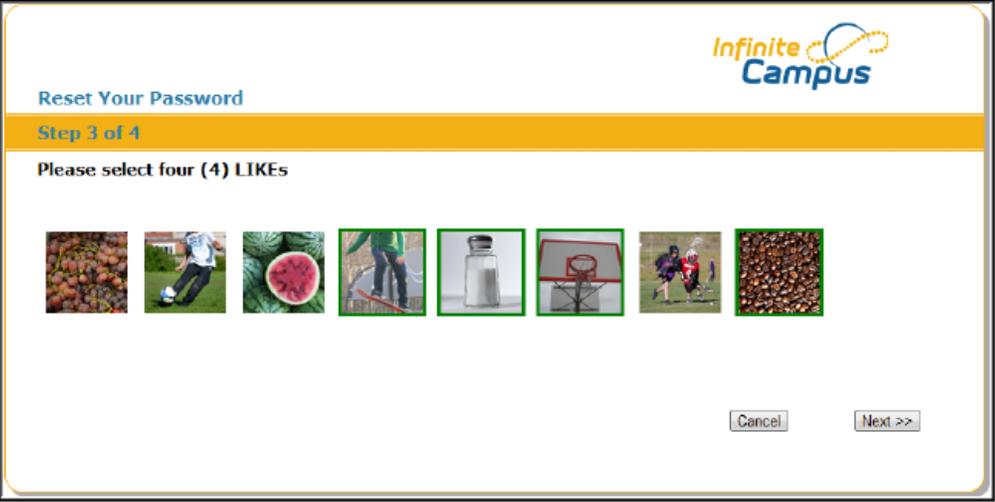

Image 14: Confirming Identity via Like and Dislike Images

Once a user accesses the URL provided in the email, Step 3 of the Reset Your Password editor appears. Users must either select four of their **Like** or four of their **Dislike** images (depending on the question asked) and select the **Next** button. Like and Dislike images are used to confirm the user's identity.
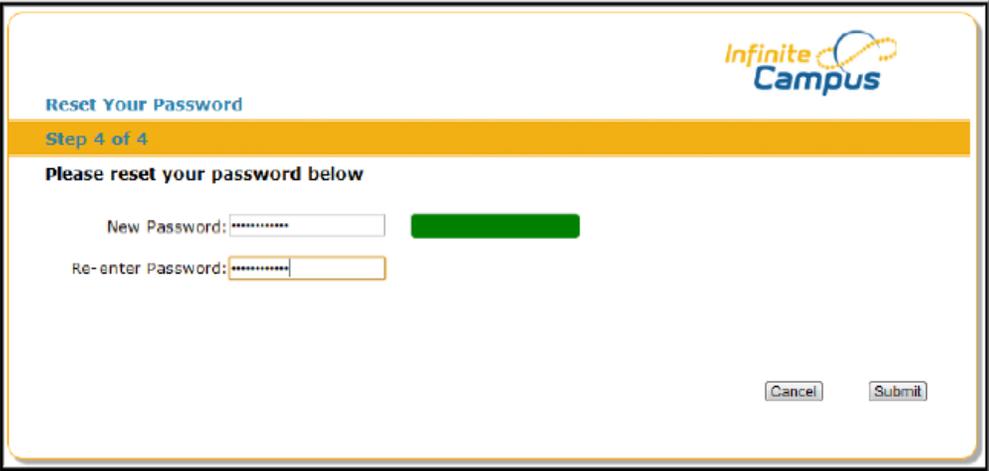

Image 15: Resetting the Account Password

Once four correct images are selected, the user can enter a **New Password** and **Re-enter the Password** to ensure its accuracy. The box to the left of each field indicates the strength of the password. Red indicates weak, yellow indicates medium and green indicates strong. Users cannot save a weak or medium (red or yellow) password. Once an appropriate new password is entered, select the **Submit** button. The account password is now reset and the user can log into their account using the password.

User Incorrectly Attempts to Log Into Campus Multiple Times

Users who incorrectly log into their account multiple times will be required to enter a CAPTCHA each time they attempt to log in. This feature prevents users from being locked out of their account after several failed login attempts and protects accounts from malicious bots and scripts.
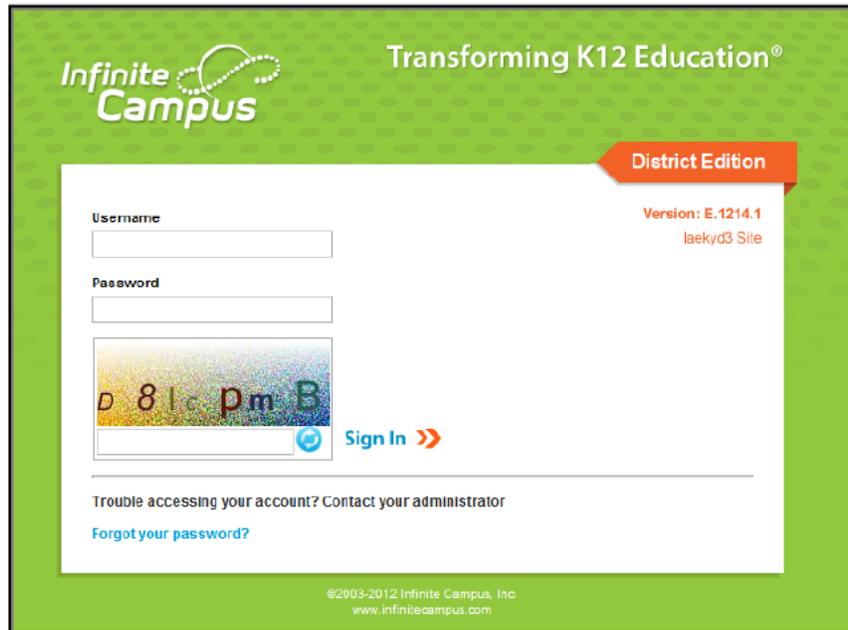

Image 17: Entering a CAPTCHA (E.1222 and greater)