

# Pepbase Security Update

June 3, 2019

Attn: PEP Coordinators

Hello,

Pepbase has an important security update. As of today, all staff member account passwords will be stored in an encrypted format, and removed from the Sign In Account listing (Tools->Security->Sign In Accounts), so no one (including Administrators, Coordinators, or myself) will be able to see other account passwords. Since passwords are no longer visible, I have written an "I forgot my password" routine available during sign in to prevent lock out or the need for another Administrator to look up your password. In order for this routine to work, all sign-in accounts must have a valid email address to send the reset password token.

Also, a drop down user menu was added, allowing staff members to update their own accounts. Staff members with the Host access level will only be able to change personal information about themselves (name, email, sign-in name, and password).

## What's New

- All sign in names and passwords remain the same, only the way they are saved has changed.
- Passwords are no longer visible to anyone using Pepbase (including myself).
- Only Administrators and Coordinators can create sign-in accounts.
- When a new account is created, an email is automatically sent to the new staff member with password setup instructions.
- An Activation field was added to each sign in account, so you can deactivate a staff member without deleting any of their data.
- To prevent lock-out, a password reset option is included on the Pepbase Sign In screen.

## What you need to do

- Sign in to Pepbase, click on Tools->Security->Sign In Accounts, and verify that all your staff members have a unique, valid email address.
- Request that all staff members add [admin@essentialspantry.org](mailto:admin@essentialspantry.org) to their email contacts. Large email servers like outlook and gmail have complex filters to prevent spam from reaching your inbox. Adding the [admin@essentialspantry.org](mailto:admin@essentialspantry.org) address to your contacts list will ensure alerts from Pepbase get through.
- Deactivate or delete any staff accounts that are no longer in use.

## Best Practices

- Don't share sign in accounts. You may have heard the phrase “Sharing is Caring”, but not in the case of internet password accounts. Many people use the same password and usernames for their smart phones, bank accounts, etc. Offering this information to others increases your risk of being compromised on other websites.
- Change your password often. There are two ways for all Pepbase users to update their passwords. The first way is to click the "I forgot my password or sign-in name" link on the Pepbase sign in page, and then follow the password reset instructions. There is also an edit account option in the new user drop down menu which allows you the option of changing your password.

This is a major step in making you more safe online, and I apologize for not coding this change earlier. Pepbase is not a full time job for me, so I do maintenance when I have the time. As far as I know, there haven't been any security breaches to our system, but this update will increase protection against any future compromises.

Let me know if you have any questions.

Best regards,

Michael Rolfsmeyer