

Bits and Bytes

August 2014

Arkansas' Premier Computer Club

Bella Vista Computer Club - John Ruehle Center

Highlands Crossing Center, 1801 Forest Hills Blvd, Suite 208, Bella Vista, AR 72715

Web Site: www.bvcompclub.org

E-mail: jrc@bvcc.arcoxmail.com

Richard Clark, President

Don Hood, Newsletter Editor

Open houses for Computer Repair & Help

Aug 20th (10 am—1 pm) (Wednesday)

Sept 3rd (1 pm — 4 pm) (Wednesday)

Sept 6th (10 am —1 pm) (Saturday)

“LASTPASS”

A PASSWORD MANAGER PROGRAM

A very high percentage of Computer Club users continue to use very simple passwords in their computer software programs installed with their personal computers. Many are short, simple, words with maybe a number or two attached and would be very, very easy for any individual to hack if they wanted to. Some of the club members don't have any idea how to compose a password let alone trying to remember it when its needed. Often at the open houses, club members can't remember what their password is or where they wrote it down long time ago.

This newsletter issue is dedicated to discuss a very simple password management program that will help develop strong, secure passwords and keep them safely stored for you and will even help you by logging in for you when you want to go to a specific web site.

Why Use a Password Manager?

We're often told we should use strong passwords, with a different one for each of our online accounts. But we know that the more accounts we have online the harder it becomes to keep track of all of those logins and passwords. So we end up using the same password here and there, or even everywhere! The danger with password reuse is that with the increasing number of big data breaches - like those of Target, eBay, LinkedIn, and others - if a password is leaked in one data breach it becomes much easier for a hacker to try that password on other sites, with the intent to get unauthorized access to people's accounts.

The solution to password reuse, and to keeping track of all of your online logins, is to use a password manager. A password manager, like LastPass, remembers all your passwords for you and keeps them in one "vault". You only have to remember your master password to login to your password manager, and the password manager remembers the rest.

The other major benefit to a password manager is that logging in to your online accounts will now only take seconds. Because the password manager remembers your logins for you, when you go to login to your accounts the password manager will just fill them in automatically for you, so you don't have to type the username or password in, or worry about trying to recall which password you happened to use for

that account. With logins so streamlined, you'll wonder why you weren't using a password manager sooner!

Once you've selected the password manager you want to use, you simply download it to your computer and follow the prompts to create your account. When the download is complete and you've finished all the steps to create the account, you can start saving your accounts to the password manager.

The other benefit of a password manager is that you can use the built-in password generator to create new passwords. As you sign up for new accounts, you can use the password generator to create a password for you. This way you'll know you have a strong password for each of your new accounts. You can also update the password of accounts you already have, to replace your old passwords with new, stronger ones.

Password managers often have a number of other features to help you with your online security and to improve your online browsing experience.

Downloading LastPass

Getting started with a password manager like LastPass is simple.

1. Open your browser.
2. Go to www.LastPass.com and select the "Download Free" option.
3. Once you've selected the download that best matches your computer and browser setup, you'll start the download.
4. You'll be prompted to create a LastPass account using your email address and a **new master password** just for your LastPass account. Make sure it's a strong one - this is the last password you'll have to remember!

The screenshot shows the LastPass account creation interface. It includes an 'Email' field with 'jason@howtogeek.com', a 'LastPass Password' field with a strength indicator showing a green bar and the text 'Fantastic job! Your password is very strong.' and a 'Password Reminder' field with 'Beefcake?'. At the bottom, there is a checkbox for 'I understand that my encrypted data will be sent to LastPass' and a note: 'No one at LastPass can read your confidential data since it is encrypted'.

Type in your primary email address and select a strong password which will become your **MASTER PASSWORD**. You'll only be using this password to access your web password vault and to login once every browser session to the local database.



If you lose your LastPass password you're totally out of luck. Instead of using a password, you may want to use a strong and memorable passphrase. If you have to, write it down and tape it to the bottom of your desk drawer or otherwise hide it away in a safe or someplace secure. **The Master Password is the ONLY password which you have to remember. This password along with your email address is absolutely necessary to get into your vault.**

Editors note: I devised my own password utilizing my military identification number and mixing in several letters both of upper and lower case as well as a couple of characters such as "" and "&".*

One of the greatest benefits of using LastPass is that it remembers all of your passwords for you, so you can [generate strong, unique passwords](#) without the hassle of recalling or typing them. Because you are storing all of your sensitive data in LastPass, though, creating a master password that is rock-solid while still being memorable is even more important.

Another approach is creating a long, non-dictionary-based, difficult-to-crack master

password: called “**passphrases**”.

What is a passphrase? A passphrase is typically a sequence of words or text strung together to create a password for logging in to an account. The difference between a passphrase and a password is that a passphrase is typically longer and uses whole words or variations of whole words to create nonsensical sentences or phrases that are easy for you to remember, but hard for someone else to guess or crack.

How to create your strong passphrase:

The key to creating a strong passphrase is to pick a string of words that's easy for you to remember but is not just a famous movie or literary quote, song lyric, piece of personal information, or a single word straight from the dictionary. The best passphrases will also include a mix of capitalization, punctuation, and numbers.

Given those parameters, let's look at an example, choosing words at random that don't really have a relation to each other but that hold meaning for you: **volkswagensummeryellowtulip**

That's a 27-character nonsensical phrase that will still be easy to remember. Now if we really want to increase the strength of the phrase, we can then add a better mix of character types:

VOLk\$wagenSummerYellow!Tulip

So now, we have a 28-character master password, with lowercase, uppercase, a number, and some symbols.

Of course the longer and more complicated you make the passphrase the more carefully you'll need to type, and the harder you may have to work at memorizing the master password at first. Even using "**volkswagensummeryellowtulip**" is far better than using "password" or one of the other common passwords or single dictionary words.

Whether you select a password or decide to have a passphrase as your Master Password, be sure it is a strong and easy to be remembered by you. You can use a feature in LastPass to test the strength of your

password when opening LastPass dialog box and clicking on “Tools” and bringing up “Taking the Challenge” which will test the strength of all your passwords and your master password. To be discussed to later.

5. Complete the installation steps - you can use the default install options as you go.

6. When you next launch your browser, you'll see a square button with a * icon. By clicking this button you'll be able to login to LastPass, and access other tools in the password manager. Ensure the icon is red while you're browsing - that means you're logged in and LastPass is active!

Saving a Site with LastPass

To save a site with LastPass, you would start by browsing to a site where you already have an account. Let's say you have a Facebook account and you want LastPass to remember that password for you.

1. Go to www.Facebook.com in your browser.

2. Enter your user name and password into the Facebook login fields.

3. You can now save the site one of two ways. You should see gray * icons in the field. You can click the * icon and then click the “Save Site” option, and then save the login.

4. Or, once you've entered the username and password you can click “Sign in” on the page,



and LastPass will then pop a notification bar at the top of your browser asking if it should remember that login for you. Click “Save Site”, and LastPass will store it in your vault.














NOTE: *Although all passwords are encrypted and saved in the vault, I still write*

down all my passwords in a little notebook for storage. I realize, all passwords can be retrieved on another computer if the user remembers the “Master Password” and your email address.....Editor

One of the greatest benefits of using LastPass is that it remembers all of your passwords for you, so you can [generate strong, unique passwords](#) without the hassle of recalling or typing them.

Import all present passwords

At this point you’ll be prompted to import secure or non-secure passwords from your web browsers into LastPass. There’s really no good reason not to import all passwords. Even if you’ve used “password” for all your passwords, it will at least build a list of sites you’ve been using insecure passwords so that you can later go back and update them.

Name	Last touch	Username	Actions
favorites			
account.live.com	1 month ago	donest@cox.net	  
accounts.google.com	1 day ago	donest	  
amazon.com	1 day ago	donest@cox.net	  
Canon	4 months ago	donest	  
ebay	2 months ago	donest479	  
emissoft.com	1 year ago	donest@cox.net	  
facebook.com	7 hours ago	deh863@cox.net	  
Generated Password for belk.com		1 year ago	 
idm.east.cox.net	1 hour ago	donest	  

Managing Your Accounts

Once you store passwords with LastPass, you’ll be able to view everything you’ve stored in your LastPass Vault. The LastPass Vault allows you to centrally

manage all of your passwords, logins, notes, and more in one secure place. To open the vault, you would click the LastPass button in your browser toolbar and select “My LastPass Vault”. Your sites can be organized into Folders, and you can create as many as you want. Once you create a Folder you can drag and drop your sites from one folder to another.

There is also a “search” field in the vault so that you can easily search by website name or keyword to find the login you need.

In the Vault, you can easily manage and administer your sites easily. Simply click “edit” for a site in order to view the stored login information, or use the ‘delete’ option to remove a login.

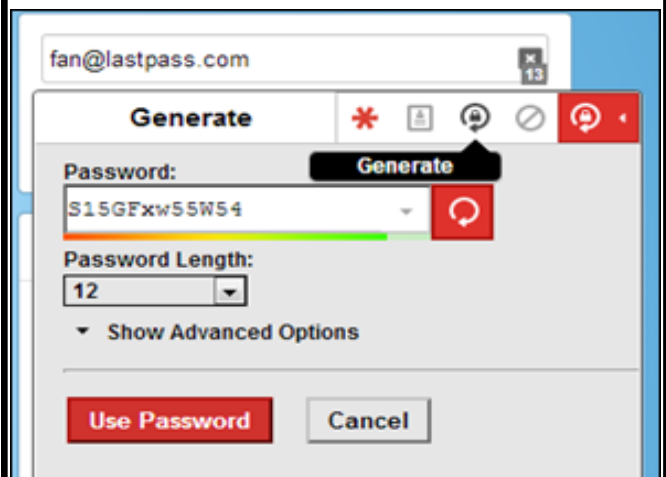
Now you have a “Vault” of web sites where passwords have been used.

Generating a Password

LastPass gives you tools to generate very secure, non-guessable passwords, helping you to have the safest web experience possible. You can also use LastPass to replace old passwords with unique, randomly generated ones.

Let’s say you’re registering for a new site. When you are on the site:

1. LastPass sees that you need a new password and shows a “generate” icon in the new password field.



2. You click the generate icon, and “accept” the newly-generated password that LastPass has created for you.

3. Complete the other registration steps and submit the information to create your new account.

4. LastPass will prompt you to save your new login, with the newly-generated password.



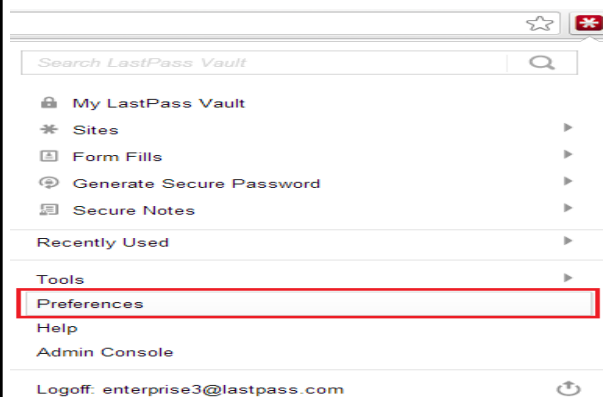
We're almost done! The last setup step is to specify whether or not LastPass should log you out when the browser closes and whether or not your LastPass Vault should be your homepage. We recommend setting it to log you out and not using your vault as your homepage. We double recommend against those things if you're using LastPass on a portable computer or mobile device.



After you finish the LastPass installation, launch one of the web browsers you specified in the first step of the setup. In the toolbar of the browser will be a dark LastPass icon (which looks like an asterisk). Login using your email and LastPass password. We let LastPass remember our login but leave the password blank. Once you login the LastPass logo should switch from dark gray to red and white. Clicking on the logo yields a drop-down menu filled with LastPass goodies. The first thing we want to

do is hit up the Preferences menu. Click on it now.

This will bring up the following menu. We'd recommend leaving the default notifications in place as they serve as excellent reminders to use LastPass and to generate secure passwords. As you get more comfortable using LastPass and need fewer reminders, go ahead and



return to this menu and toggle some of



them off. As you become familiar with using LastPass, you may or may not want to use three additional features involving letting LastPass help complete online shopping forms in seconds. A second program is "Sharing Passwords" and a third is "Storing More than Passwords" which is allowing the user to store personal information as encrypted information.

Some computer club members may be somewhat skeptical of storing personal information in this manner even though it is encrypted material and is just as safe as using a credit card in a grocery store,

restrauntant or banking on line like so many of us do.

LastPass also provides a unique service when clicking on “Tools” in the dropdown menu and taking the “Secure Challenge”. LastPass will check all of your passwords making sure of no duplicates, and measure the secure strength of each password. In addition, LastPass will give you the following results: **A check of your vault for Heartbleed-vulnerable sites**

1) A free, fast on-the-spot analysis of your LastPass vault. 2) An easy to interpret score from 1 to 100. 3) Easy, actionable ways to increase your security right now. 4) A comparison of your score against all other LastPass Security Challenge participants to date. 5) Results of a vault check for vulnerable sites that may have been involved in recent compromises. 6) All of your email addresses will be checked for any security breaches and results will be emailed to you.

Using LastPass will give you a very secure feeling of using the internet knowing your information is very, very safe. You can't go wrong with “**LastPass**”.

<https://lastpass.com/>
Amber Gott, Marketing Manager,
<http://www.howtogeek.com/77319/the-how-to-geek-guide-to-getting-started-with-lastpass/>

FOUR GREAT WINDOWS TIPS

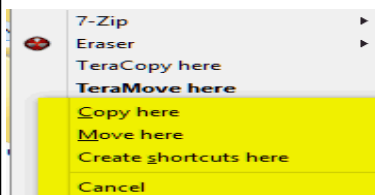
1. Click your mouse wheel to close a browser tab. You can do it, yes you can. Most of us use the mouse wheel to scroll pages and other common mouse wheel stuff. But if you press down on your mouse wheel you'll notice it depresses just bit. Well, did you know that just a bit is enough to allow you to close a browser tab. Try it and see. Position your mouse pointer in the middle of a browser tab and press down on the control wheel. See?

WELCOME NEW COMPUTER CLUB MEMBERS

Alta Ramsey
Tom Throne
Roger Zemlicka
Barbara Westfall
Bob Clark
Ralph Malatesta

Mark Hawkins
Pamla Throne
Lynn Zemlicka
Robert Westfall
Paul Gaconnier
Juanita Clark

2. Holding down the right mouse button while dragging a file or folder gives you more options, If you drag a file or folder while holding down the left mouse button, you'll get the “move here” option. If you drag a file or folder while holding down the right mouse button and release it over the target (the folder you're copying or moving to) you'll get several options including: Copy here Move here Create shortcuts here



3. Using the Shift key to select text. Most of you know that you can select files and folders by holding the Shift key and clicking on the first and then the last file/ folder. But this also applies to selecting text in documents like MS Word docs as well as text files (and Web pages).

All you have to do is click on the first character in the text you want to copy, then point to the last character, click and release the shift key. All the text between the first click and the last click is selected. Now just press CTRL + C to copy the selected text and CTRL+V to paste it wherever you want...like a Word doc or an email or a text file.

4. Maximize any program with a double-click Instead of fumbling around looking for the maximize button between the – and the X in the top-right corner of most program and file windows, just double-click anywhere on the title bar to maximize the window. (The title bar is the top-most part of the program window and usually contains the program name.)

copyright 2008 by Cloudeight Internet. <http://thundercloud.net/infoave/index.htm>

The Bella Vista Computer Club assumes no responsibility for the accuracy of information contained herein and will accept no liability for its application