

# ***BVCC General Meeting***

July 8, 2024

**"Should I Allow My Browser To Manage My Passwords?"**

**Joel Ewing**

# Browser Management of Passwords?

- **These meeting presentation slides will be added to the BVCC website ( <https://bvcomputerclub.org> ) (under Information ► Presentations)**

# Should My Browser Manage My Passwords?

- **This is not about using a separate Password Manager (like LastPass) which uses browser extensions to save/insert passwords on logon webpages, but about password management capabilities that are a built-in component of the browser itself.**
  - **A feature of major browsers: Chrome, Firefox, Edge, Safari all have the ability to save and manage passwords.**
  - **From user's standpoint, looks very similar to the should-I-save-password interfaces of LastPass and similar browser extensions**
  - **Unlike separate Password Manager programs, the passwords of these internal password managers are only available within the context of those specific browsers.**

# Browser Password Management – Pros

- **Convenient – no additional software applications required**
  - Chrome, Firefox, Edge by default will ask to save passwords
- **Each browser provides options for syncing saved passwords and other browser data with a cloud service unique to that browser type**
  - Means if the same browser app is used from another device using the same cloud login, it will have access to the same saved data
  - Syncing browser data with the cloud is optional – it requires a login of some kind
    - *If passwords are synced, that login MUST have a secure password*
    - If your password is inadequate or can become compromised, having your passwords in the cloud (even if securely encrypted) does put you at wider risk.

# Browser Password Management – Cons

- **If you use multiple browser types, passwords saved on browser type "x" are not available from browser type "y"**
- **Can't save passwords that are not associated with a web page**
- **If cloud storage syncing across multiple devices is used, that means your encrypted passwords are potentially accessible on the Internet if they are protected by an inadequate master password**
- **Methods for backing up passwords saved by a browser are primitive: export to an unsecured, unencrypted .CSV file**

# Windows & OneDrive

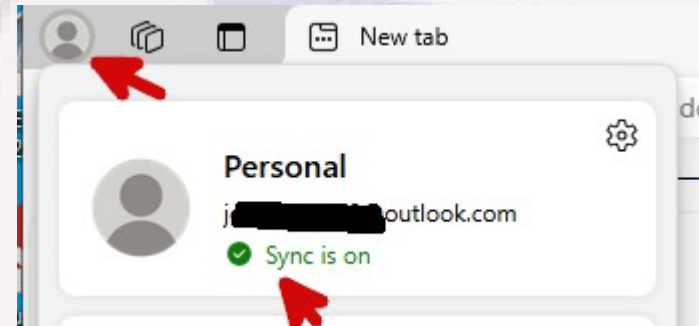
- **Windows 10 & 11 strongly push you toward using a MS email as login, which is associated with OneDrive cloud storage on the Internet**
  - **The idea is that active work and configuration settings will be stored in folders that are synced with OneDrive storage, so that if you define the same login on multiple devices you can access the same work on multiple devices.**
  - **The Edge browser can utilize cloud storage associated with a Windows login to make the same history, favorites, and other information available to the Edge browser on multiple devices.**

# Windows & OneDrive

- **If your Windows system logon is a MS account, that same account is probably the default OneDrive account for your Windows session.**
- **If your Windows system logon is a local-only account, Windows will periodically "suggest" that you supply a MS account for OneDrive so you can use the backup features of OneDrive cloud storage.**
- **If you have a MS account defined for OneDrive usage, that probably becomes the default MS account for cloud storage used by Edge.**
- **Or, you can explicitly supply to Edge a MS account to use for cloud storage,**

# Edge Browser Password Management

- Passwords saved by Edge are stored in your "Microsoft Wallet" which will be synced with MS servers on the Internet under your MS account cloud storage that is defined to Edge
  - You can check what MS account is being used by Edge by clicking on the "person" icon in the upper-left corner of the Edge browser – will show the current active profile, the associated MS account email, and whether Sync with the cloud is on. If there is no active account, you will be "encouraged" to supply a MS account, but Edge does seem to run successfully without one.
  - You can click the "Settings" icon under your profile and "sign out" to run Edge without cloud storage access, and Edge will remember that setting across a restart.



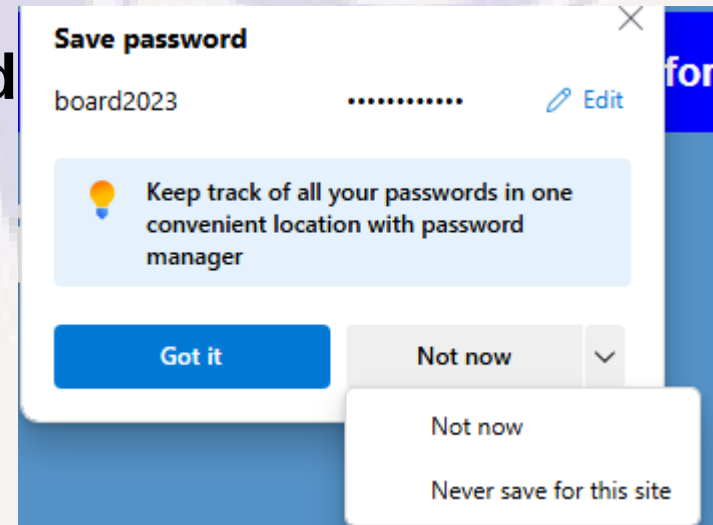


# Edge Browser Password Management

- **Passwords saved by Edge are stored in your "Microsoft Wallet" which by default will be synced with MS servers on the Internet under your account**
  - **It is possible to enter the Edge profile Settings → Sync and turn off syncing of passwords while allowing other Edge into to be synced – Not sure how useful.**
  - **Any one with access to your physical computer who can obtain your Windows login password can use and copy your saved login data.**
  - **Someone with access to your computer while it is in a logged-in state can login to websites with Edge-saved passwords, so you need to protect your login PIN as well.**
  - **If your MS Wallet is synced to the cloud and that MS login account is compromised, your cloud storage including your wallet is compromised and could potentially be used to access your websites even without access to your computer(s) – but if your account is setup with MFA, such as requiring a text code sent to your smart phone to login from a new device, that considerably reduces that risk.**

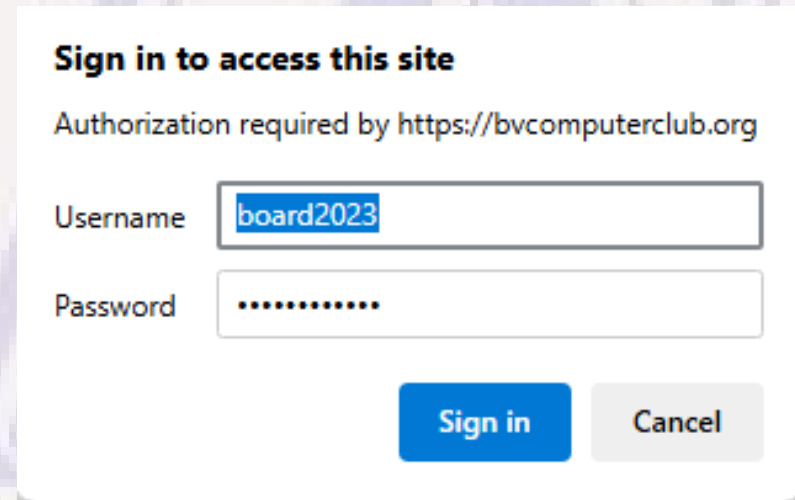
# Edge Browser Password Management

- **When you enter login information for a new website the first time, Edge will ask if you want it to save the account info: If you want Edge to save it, click "Got it". If you want to defer that decision to another time, click "Not now", and next time you logon you will be asked again. If you select "Never ...", the info won't be saved, and you won't be asked again for this same website.**



# Edge Browser Password Management

- The next time you login to a website for which Edge has saved login information, the username and password fields will be automatically primed with the saved values (with password hidden), and all you need to do is just click on the sign-on button.



**Sign in to access this site**

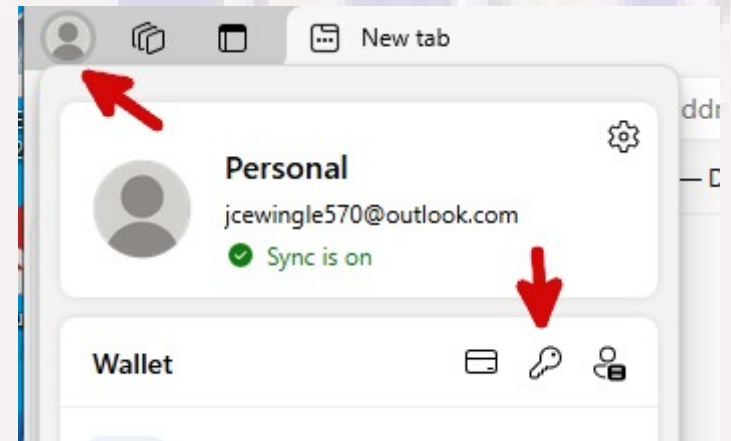
Authorization required by <https://bvcomputerclub.org>

Username

Password

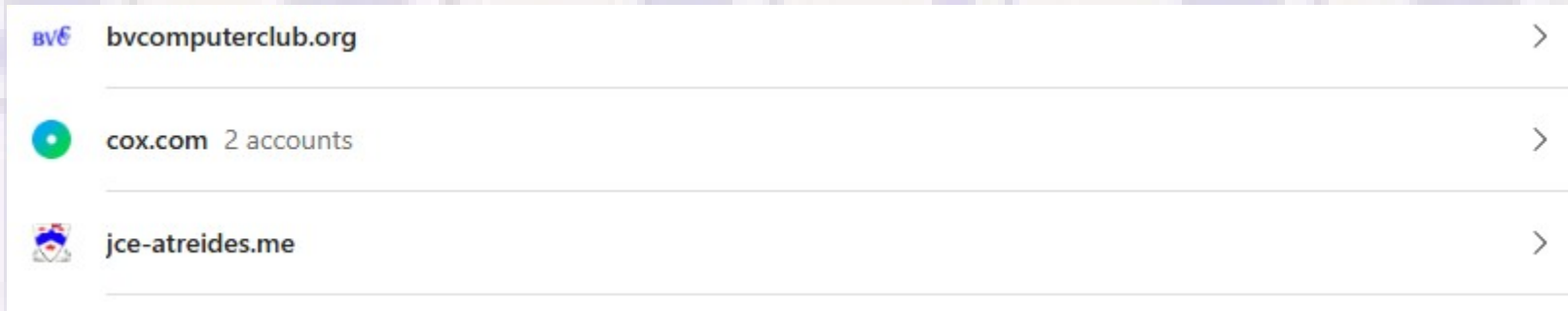
# Edge Browser Password Management

- If you want to view or modify passwords saved by Edge, click on the Profile icon (upper left corner), and then on the Wallet key icon:



# Edge Browser Password Management

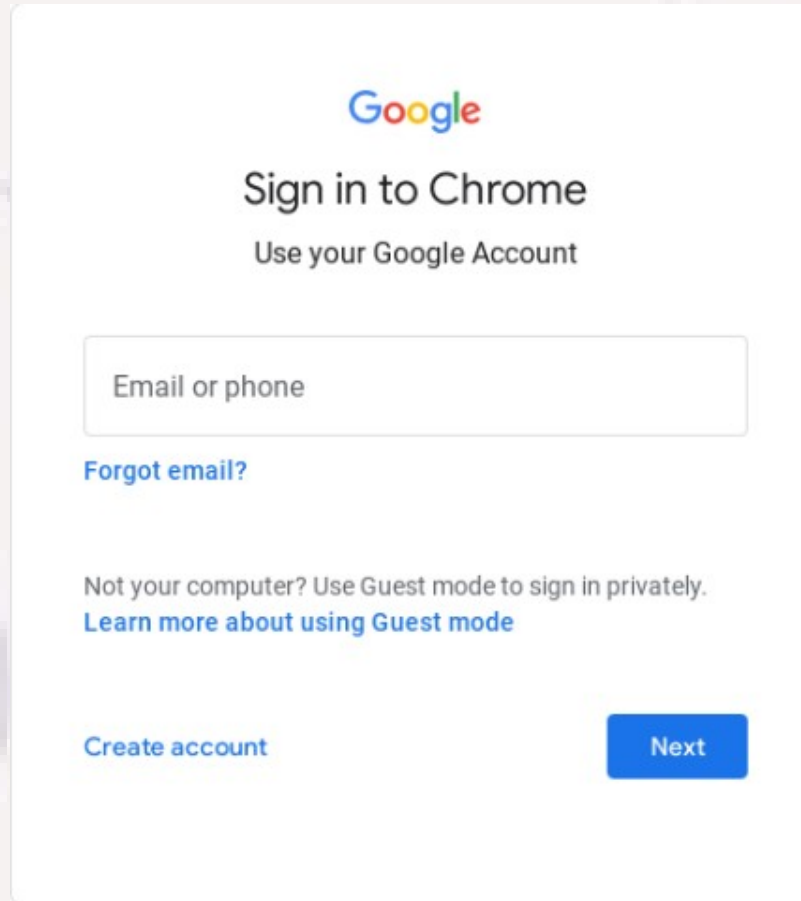
- To actually view or delete any of the saved entries, you have to click on the corresponding ">", and at that point you will be asked to supply the password for your current Windows logon – so at least there was some protection from copying down all your website logon info if you left your computer unattended for a few minutes while logged on to Windows.



# Chrome Browser Password Management

- **The Chrome browser native password support uses the Google Password Manager for saving passwords.**
- **Google Password Manager data and other Chrome browser data can be shared with Chrome browser running on other devices if you "Sign in to Chrome" using a Google account and elect to sync Chrome browser data using your Google account's cloud storage.**

# Chrome Browser Password Management

A screenshot of the Chrome browser's sign-in page. The page is white with a light blue border. At the top center is the Google logo. Below it, the text "Sign in to Chrome" is displayed in a large, dark font, followed by "Use your Google Account" in a smaller font. A text input field with a light gray border contains the placeholder text "Email or phone". Below the input field is a blue link that says "Forgot email?". Further down, there is a line of text: "Not your computer? Use Guest mode to sign in privately." followed by a blue link "Learn more about using Guest mode". At the bottom left, there is a blue link "Create account". At the bottom right, there is a blue button with the text "Next" in white.

Google

Sign in to Chrome

Use your Google Account

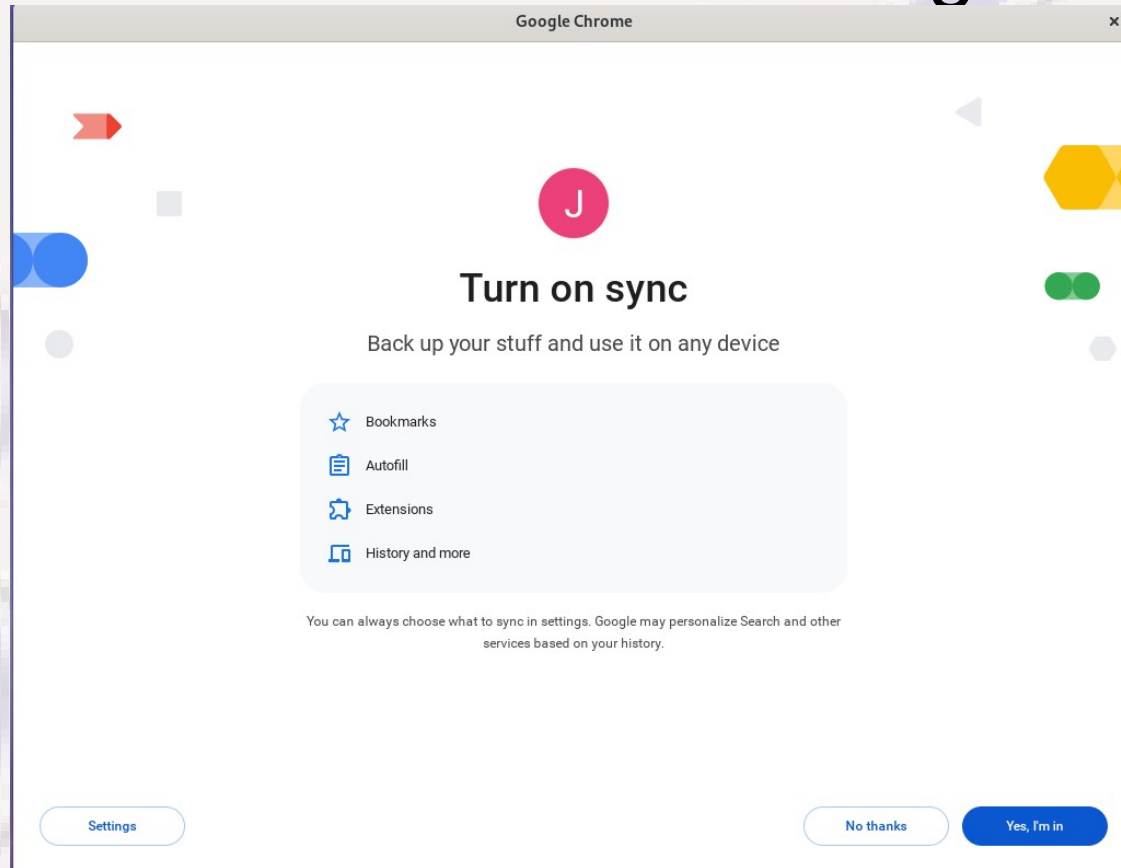
Email or phone

[Forgot email?](#)

Not your computer? Use Guest mode to sign in privately.  
[Learn more about using Guest mode](#)

[Create account](#) [Next](#)

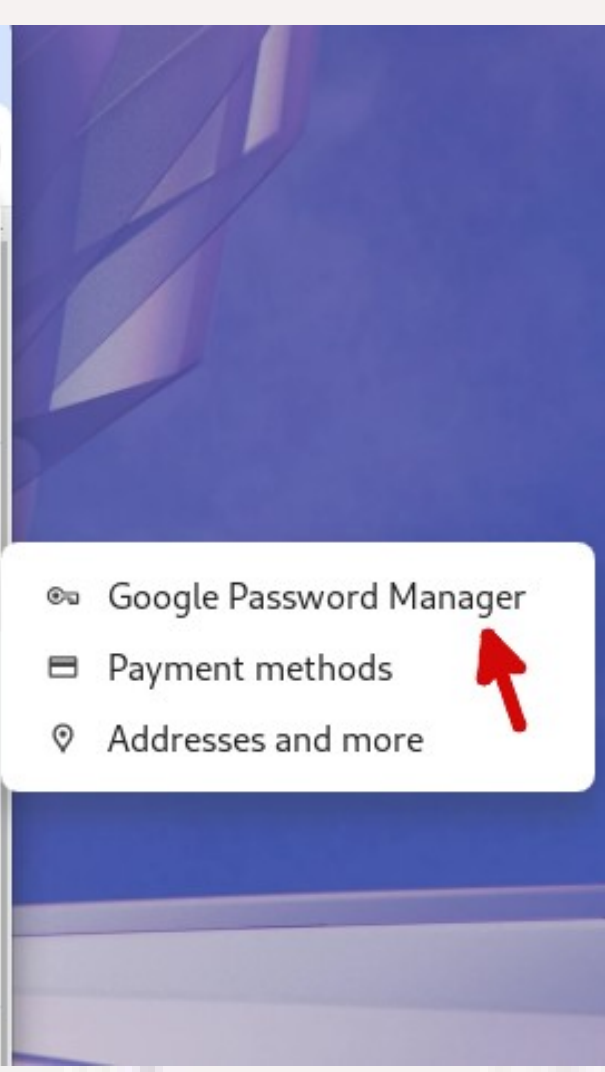
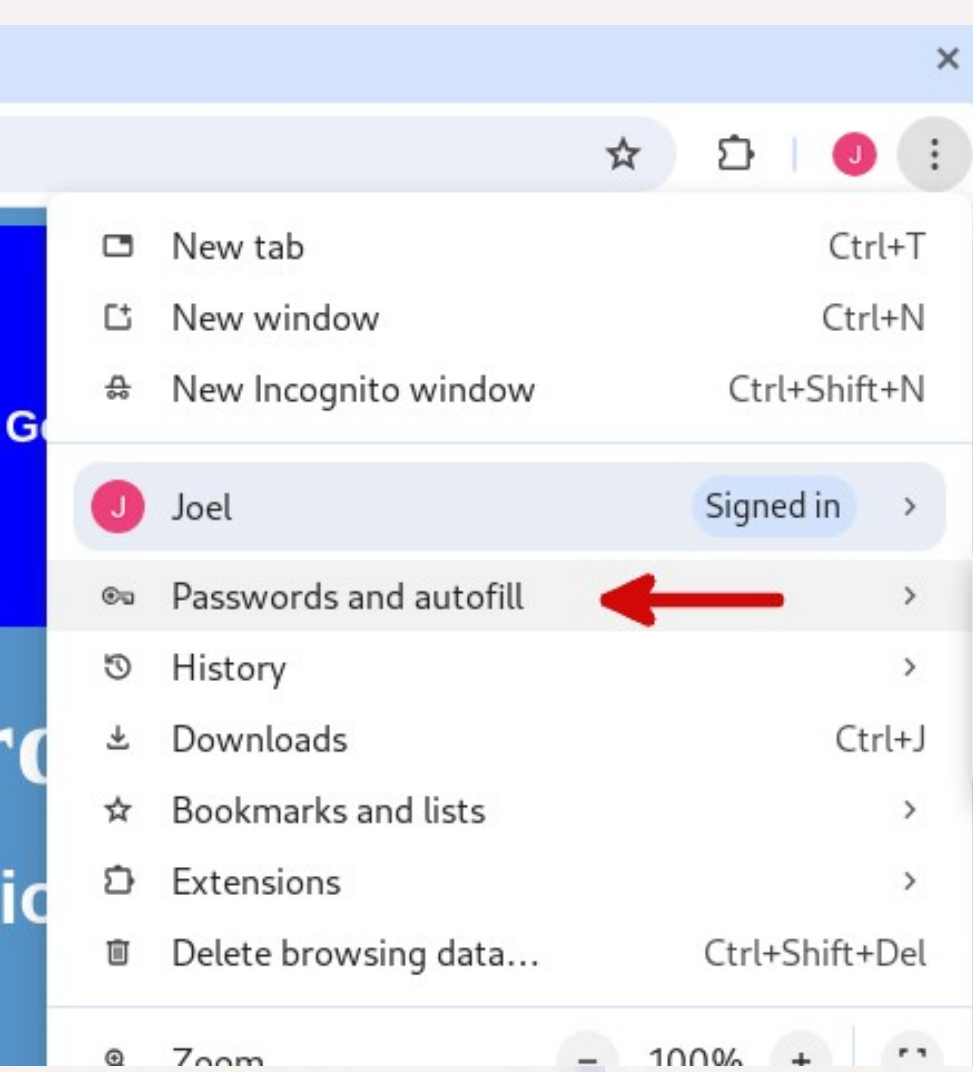
# Chrome Browser Password Management





# Chrome Browser Password Management

- **To look at Google Password Manager, go to vertical ellipses icon : (upper right), select "Settings", select "Autofill and passwords", select "Google Password Manager"**
  - **Can view / edit/ delete saved passwords**
  - **Can go to GPM "Settings" to turn off "Offer to save passwords" or "Sign in automatically"**

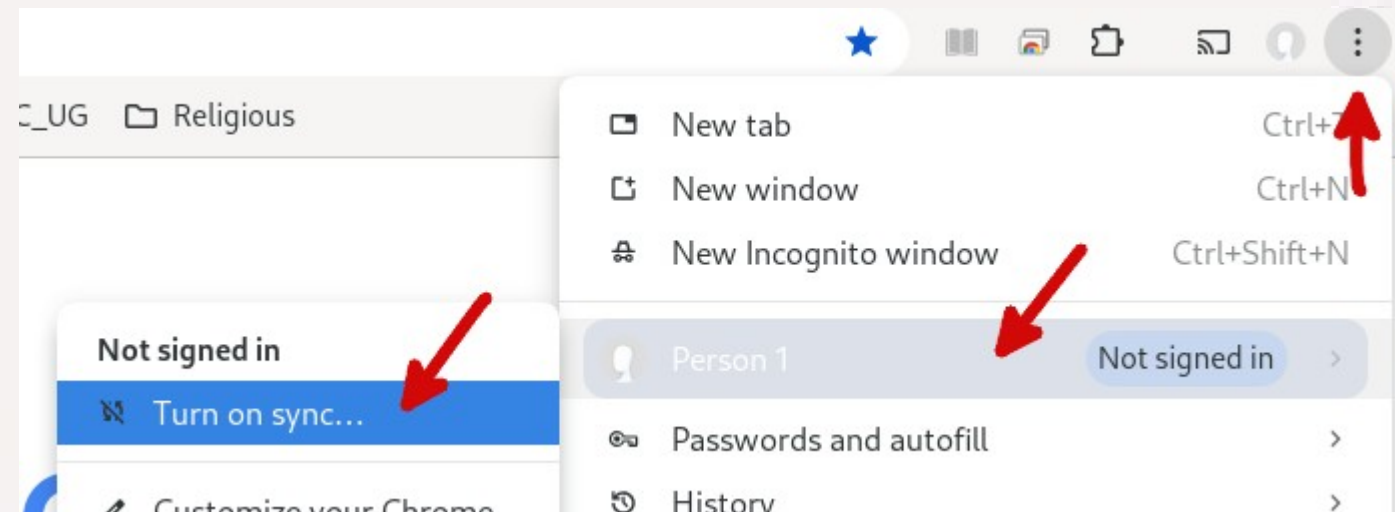


Also note the menu line that shows Chrome is "Signed in", meaning sync is available

# Chrome Browser Password Management

- **Chrome's default when signed-in is to sync everything (which includes passwords)**
  - **If you don't want any passwords to be synced to the cloud, you need to turn off syncing passwords before having chrome save any passwords. If you have any saved passwords while synced and then turn off password syncing, they remain in the cloud and can't be deleted from the cloud from that device (and can still be used to sign in).**

# Chrome Browser Password Management

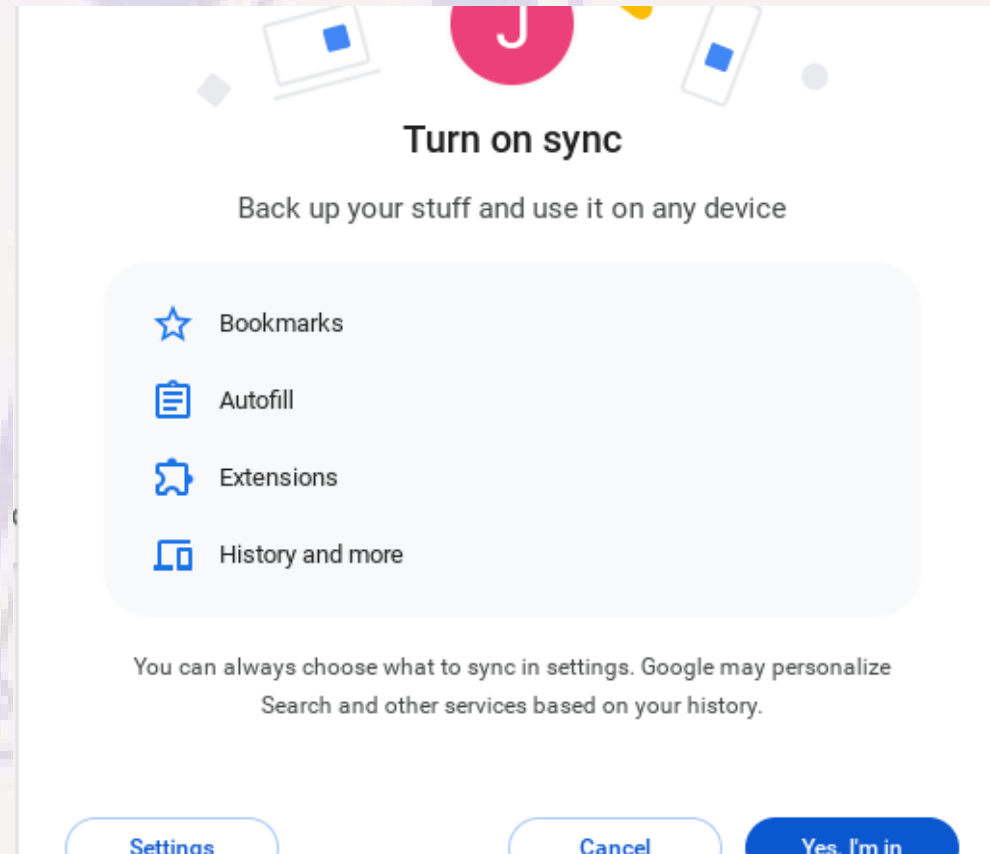


**If menu shows you are not signed in, there is no syncing with cloud, but passwords can still be saved on this local device.**

**If you want to sync any Chrome data with other devices you must first start from : and "Turn on sync" (which asks you for a Google login)**

# Chrome Browser Password Management

- When you first sign-in to sync Chrome, if you don't want to sync passwords, select "Settings", then under that select "Manage what you sync", select "Customize sync", then turn off the switch for "Passwords and passkeys". Use ← to back up to the "Sync and Google services" and confirm the setup of your Chrome sign in.



# Chrome Browser Password Management

- **The user interface for saving and using passwords is very similar to the Edge browser**
  - **The first logon to a new website will result in popup asking if you want Chrome to save the password. Response is either to "Save" or "Never ask again" for that website, or just close the popup window to not save the password this time.**
  - **When visiting the login page for a website with a saved login, values for the username and password will be primed and all you need is "Enter" to login.**

# Firefox Password Manager

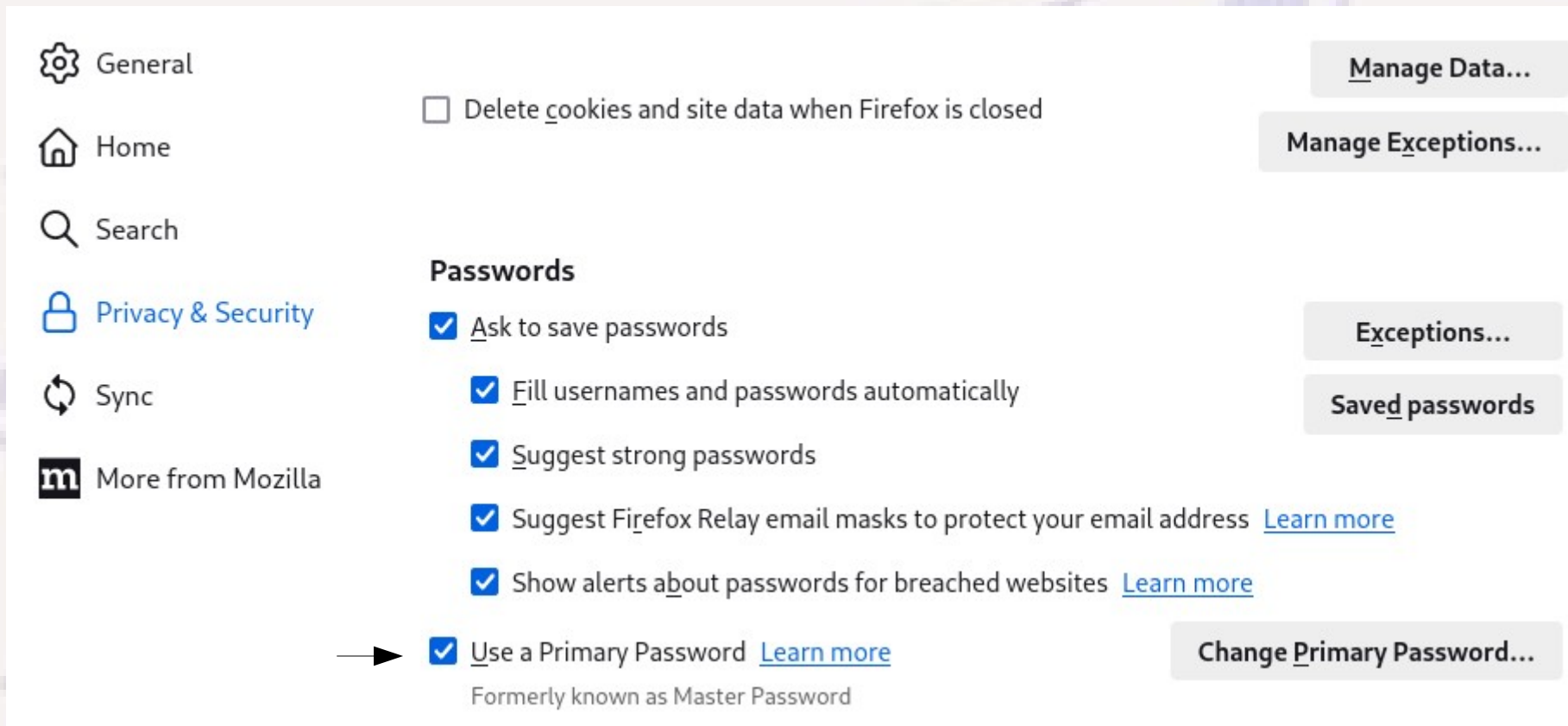
- **Like other browsers, Firefox has both password management capabilities and the ability to sync Firefox data, including passwords, to Firefox browsers running on other devices by using cloud storage at Mozilla.**
  - **By default Firefox Sync is not enabled. Firefox Sync requires setting up a Mozilla account using an existing email account – see <https://accounts.firefox.com/> to setup a new account .**
  - **By default, Firefox Password Management is enabled, but a "Primary password" is not enabled. Without Firefox Sync enabled, Firefox only saves passwords on the local device. if Firefox Sync is enabled, then by default all data including passwords are synced to a Mozilla cloud service.**

# Firefox Password Manager

- **If you are going to allow Firefox to save passwords, the first thing you should do is set up a primary password**
  - **Select the upper-right "burger" ☰ menu icon, select "Settings", select "Privacy & Security" in left navigation frame, and then under the "Passwords" section turn on "Use a Primary Password", create and securely record a good Primary Password. This will be used to securely encrypt all passwords saved by Firefox, and you will be asked to enter this password once each time Firefox is started before it will allow you to access any saved passwords.**
  - **That same Passwords section allows you to turn off "Ask to save passwords" if you never want Firefox to save any passwords.**



# Firefox Password Manager



The image shows the Firefox Password Manager settings page. On the left is a navigation sidebar with icons and labels for General, Home, Search, Privacy & Security (highlighted in blue), Sync, and More from Mozilla. The main content area is titled 'Passwords' and contains several settings, each with a checkbox. The 'Use a Primary Password' setting is highlighted with a blue arrow pointing to its checkbox. To the right of the settings are several buttons: 'Manage Data...', 'Manage Exceptions...', 'Exceptions...', 'Saved passwords', and 'Change Primary Password...'. The 'Use a Primary Password' setting includes a link to 'Learn more' and a note that it was formerly known as the Master Password.

General

Home

Search

Privacy & Security

Sync

More from Mozilla

Delete cookies and site data when Firefox is closed

**Passwords**

Ask to save passwords

Fill usernames and passwords automatically

Suggest strong passwords

Suggest Firefox Relay email masks to protect your email address [Learn more](#)

Show alerts about passwords for breached websites [Learn more](#)

→  Use a Primary Password [Learn more](#)  
Formerly known as Master Password

Manage Data...

Manage Exceptions...

Exceptions...

Saved passwords

Change Primary Password...

# Firefox Password Manager

- **If you want to view, edit, or remove any previously saved passwords from Firefox, use the same path as before, except as the final step select the "Saved Passwords" button. If this is the first time saved passwords have been accessed, you will be prompted to supply your Firefox Primary Password.**
- **By selecting the upper right ... icon on the password list display, you will also find the options for exporting and importing passwords (as an unencrypted .CSV file). Doing an export will also require supplying your Firefox Primary Password.**

# Firefox Password Manager

Search Passwords +

Sort by: **Name (A-Z)** 50 passwords

- jcewing@acm.org
- bentonvilleford.com (no username)
- blackhillsenergy.com jcewingawg
- bpl.tlcdelivers.com 20296000643585
- bvcomputerclub.org (Board\_Files)** board2023
- bvcomputerclub.org (Member S... surveymember
- cart.pcusastore.com jcewing.pcusastore.com
- classicalarchives.com

Get your passwords on your other devices **Sign in to sync** ...

**bvcomputerclub.org (Board\_Files)** Edit Remove

Website address <https://bvcomputerclub.org>

Username board2023 Copy

Password ●●●●●●●● Copy

on your other devices **Sign in to sync** ...

Remove

- Import from Another Browser...
- Import from a File...
- Export Passwords...
- Remove All Passwords...
- Options
- Help

Jul 6, 2023 Created Mar 15, 2024 Used

# Firefox Browser Password Management

- **The user interface for saving and using passwords is very similar to the Edge and Chrome browsers**
  - **The first logon to a new website will result in popup asking if you want Firefox to save the password. Response is either to "Save", "Don't save", or "Never save" for that website.**
  - **When visiting the login page for a website with a saved login, values for the username and password will be primed and all you need is "Enter" to login.**

# Other Browsers

- **Haven't experimented with other browsers and their saved password support.**
  - **I use Safari on iPhone and iPad, but only for general searches, not for accessing websites that require a login account.**

# General Thoughts

- **How secure are passwords saved by these browsers on a local device?**
  - **One would hope passwords saved on disk are always in an encrypted state, but documentation is a little fuzzy whether they are vulnerable at other times.**
    - **When Firefox has a Master Password, you are in control of encryption security**
    - **Chrome has an option setting for providing your own "local" encryption password. Not clear how local encryption works by default.**
    - **Unclear whether the means by which MS and Google arrive at encryption keys could provide any avenue of attack.**
    - **My instinct puts greater trust in an application designed from the ground up as a password manager, rather than a sub function of much larger browser app.**

# General Thoughts

- **What about security when passwords are synced with the vendors cloud storage?**
  - **If you are concerned about password managers like LastPass that sync copies of your password database in the cloud, you should at least be equally concerned about a browser's password manager that syncs such data in the cloud. If you have to replicate password data for two or more browser types each with their own cloud storage, that multiples the exposure.**
  - **The description of local encryption passwords for Google Password Manager implies that without that, Google might be able to recover your passwords – if true, a court order or threats from a rogue imperial President without a court order could force Google to reveal your passwords, possibly without your knowledge.**

# General Thoughts

- **If you don't trust putting encrypted passwords in the cloud, is it still possible to sync browser history, favorites, cookies and other browser data across different devices, just not the passwords?**
  - **Yes. Edge, Chrome, and Firefox all have [different] ways to explicitly disable syncing passwords via the cloud. In all cases, if syncing is enabled, syncing passwords is the default; so, if that's not what you want, you have to be sure to set the correct options to disable it.**



# General Thoughts

- **Could I manually sync browser password data on two devices without using syncing via cloud storage?**
  - **Yes.** They all seem to support exporting and importing password data as a **.CSV** file, so if passwords don't change often, you could export the data on one device and import on another. Might even work across browser types, provided their **.CSV** files expect data in the same order.  
**\*BUT...\***, be **VERY** sure to keep those **.CSV** file around for the minimum time possible, not even in Trash, because they reveal all your saved logins and passwords in clearly readable form.

# General Thoughts

- **Can browser-based password managers replace a password manager program?**
  - **Not really**
    - They can't handle logon info that is needed outside that specific browser type.
    - They can't save useful data like security questions, associated recovery phone numbers and emails that may be needed to manage or recover an on-line account.
    - They can't support account logins on multiple browser types without replication of work.
    - The user interfaces for organizing, viewing, and editing login info is more restrictive.
    - Password managers add more security by requiring by default more than just a successful login to the Operating System to access your password information.
    - With a separate Password Manager application, the decision of whether or where to put password data in cloud storage is independent from the decision of sharing less sensitive browser information across devices.

# Recommendations

- **Rather than trying to track changes and possible exposures in the internal password managers of multiple browsers, my personal preferences are:**
  - **Use a separate password manager as the primary repository for keeping track of all my on-line accounts and any changes to on-line accounts.**
  - **Use saved passwords in browsers as a time convenience for accounts that are frequently used but have no financial exposure – no ability to purchase arbitrary items on credit or transfer assets; and similarly avoid saving in a browser any credentials for my primary email accounts that can be used to recover (change passwords for) other on-line accounts. That way, it's not a serious problem if any account passwords stored by the browser are exposed.**

# Recommendations

- **I believe Edge, Chrome, and Firefox all have versions that run on smart phones and other mobile devices that are capable of sharing synced browser data on those devices.**
  - **Since mobile devices are more susceptible to theft or loss and there are more avenues of attack if you can get physical control of a device, that might also influence whether you want to install those browsers and configure the browser on that mobile device to share browser cloud data.**

Questions?

BYSS