Disk Encryption & Password Manager

zerosalarium.com/2024/12/store password securely how to password protect folder.html

Zero Salarium January 1, 2025

Keep something close to the vest: Disk Encryption & Password Manager

I. Overview

When you have some very important documents, and you start to care about the issue of protecting sensitive files on your computer. At this point, you may have considered how to make a folder password protected, or at a higher level, encrypting files on Windows.

Similarly, when you use various online services, it's likely that you'll have multiple account passwords corresponding to those services. The issue that arises at this point is how to store passwords securely and manage them effectively.

This is the sixth post in a series of articles on basic Operations Security (OPSEC) awareness. This time, I will introduce the following key points:

- Learn how to password protect files by using disk encryption software. This protective layer will help keep your personal data out of the sight of curious onlookers, even if they gain access to your computer.
- Learn how to use password managers to keep your passwords safe. It helps you avoid the situation of having to use one password for multiple accounts or using passwords that are too simple and easy to guess.

You can get the latest updates on this series of articles on X (Twitter): **Two Seven One Three** (@TwoSevenOneT)

II. Expanded insight

1. Encrypting files on Windows

When considering OPSEC, you may have thought about and sought ways to tackle the challenge of how to create a password-protected folder and file.

When you need a place that only you, the password holder, can access, disk encryption software will be the most suitable solution. Although it is called "disk encryption" we will use it to create encrypted container files that function like a regular drive.

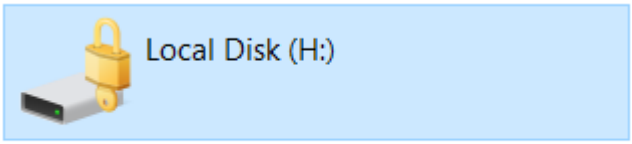
The two software programs I will introduce and guide you on how to use according to your needs are BitLocker and VeraCrypt.

A. BitLocker

A.1. What is BitLocker?

BitLocker is a full-disk encryption feature included with Microsoft Windows. It’s designed to protect data by providing encryption for entire volumes. BitLocker uses the Advanced Encryption Standard (AES) encryption algorithm to encrypt the data on your drive, making it nearly impossible for unauthorized users to access your information if your computer is lost or stolen.

Think of it as a digital lockbox that keeps your sensitive data safe from prying eyes. Whether it's personal files, business documents, or any other data, BitLocker ensures that only you, or those you authorize, can access it. It’s especially useful for safeguarding against physical threats, like device theft, or protecting sensitive information in a corporate environment.



The drive has been protected by BitLocker

BitLocker is built into certain editions of Windows. Specifically, it is available in Windows 10 Pro, Enterprise, and Education editions, as well as their Windows 11 counterparts.

A.2. How to use BitLocker to create an encrypted container

Because BitLocker's functionality only supports full-disk encryption, we will first create a Virtual Hard Disk (VHD) file. Then, we will proceed to encrypt and protect this file, and finally use it like a regular drive.

A VHD (Virtual Hard Disk) file is a disk image file format used by Microsoft Windows. It's essentially a file that acts like a physical hard drive. Think of a VHD file as a self-contained, portable virtual hard drive that you can easily move between different machines or environments.

How to create a VHD file using Disk Management

Please note that in order to use BitLocker, the newly created **VHD file must be at least 250 MB** in size.

Open Disk Management:

- **Right-click** on the **Start menu** and select **Disk Management**.
- Alternatively, you can press **Win + X** and then choose **Disk Management**.

Create VHD:

1. In the **Disk Management** window, click on the **Action** menu.

2. Select **Create VHD**.

Specify VHD Details:

1. Choose the location where you want to save the VHD file and give it a name.
2. Specify the size of the VHD (either in MB, GB, or TB).
3. Select whether you want a **Fixed size** or **Dynamically expanding** VHD.
4. Click **OK**.

Initialize the VHD:

1. After creating the VHD, it will appear in the **Disk Management** window as an **uninitialized disk**.
2. **Right-click** on the new disk (it will say "**Not Initialized**") and select **Initialize Disk**.
3. Choose the partition style (**MBR** or **GPT**) and click **OK**.

Create a Volume:

1. **Right-click** on the unallocated space of the new disk and select **New Simple Volume**.
2. Follow the **New Simple Volume Wizard** to format the VHD and assign a drive letter.

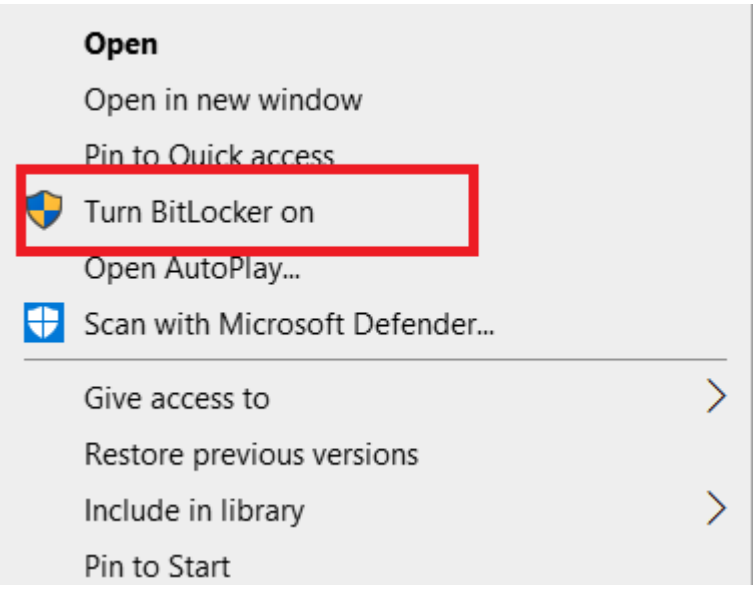
After initialization, whenever you want to use this virtual disk, you just need to double-click the newly created VHD file, and Windows will automatically mount it, allowing you to use it as usual.

You should not configure Windows to automatically mount a VHD file when it starts. Only interact with it when you need to use it.

A.3. How to use BitLocker to protect a drive

Using Context Menu to Enable BitLocker

1. Open **File Explorer**: Press Win + E to open File Explorer.
2. Locate the Drive: Navigate to This PC or Computer to see all your drives.
3. **Right-click** on the drive you want to encrypt with BitLocker.
4. Select **Turn on BitLocker** from the context menu.



Turn on BitLocker context menu

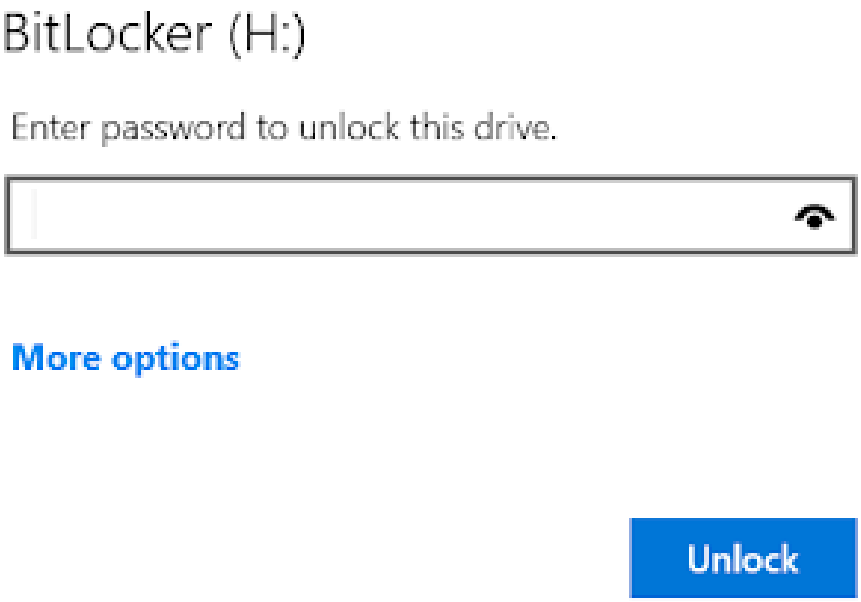
BitLocker Setup

1. **Choose How to Unlock the Drive**: You'll be prompted to choose how you want to unlock the drive. You can use a password or a smart card. Select your preferred method and follow the prompts.
2. **Save Your Recovery Key**: BitLocker will provide a recovery key that you should save in a secure location. You can save it to your Microsoft account, a USB drive, a file, or print it out.
3. Choose **How Much of Your Drive to Encrypt**: Decide whether to encrypt only the used disk space (faster) or the entire drive (slower but more secure).
4. Choose **Encryption Mode**: Select the encryption mode (new encryption mode for fixed drives or compatible mode for drives that might be moved to older Windows versions).
5. Start Encrypting: Click **Start Encrypting** to begin the encryption process. The time it takes will depend on the size of the drive and the amount of data.

After encryption is complete, Windows will automatically unlock it for you to use the first time. For subsequent uses, after double-clicking the VHD file to mount the drive, you will need to provide the decryption password to access the mounted drive.

Thus, you now have a safe place to store personal files like photos and documents. Even if someone obtains your VHD file, they will not be able to access the contents without the password, which only you know. This ensures that you will not encounter issues related to sensitive data exposure.

You can also transfer this VHD file to other machines that support BitLocker and use it as usual.



BitLocker password prompt

B. VeraCrypt

B.1. What is VeraCrypt?

VeraCrypt is a free, open-source disk encryption software that provides strong security for your data. It's a fork of the discontinued TrueCrypt project and offers several advanced features for encrypting files, partitions, and entire storage devices.

VeraCrypt supports various encryption options such as AES, Serpent, Twofish, Camellia, and Kuznyechik. It also supports creating a virtual encrypted disk within a file, which functions just like a regular disk. This is the feature we are interested in.

VeraCrypt offers hidden volumes and hidden operating systems, allowing you to deny the existence of encrypted data if you are forced to reveal a password.

B.2. Creating a Virtual Encrypted Disk with VeraCrypt

You can download and install VeraCrypt from the GitHub link: VeraCrypt.

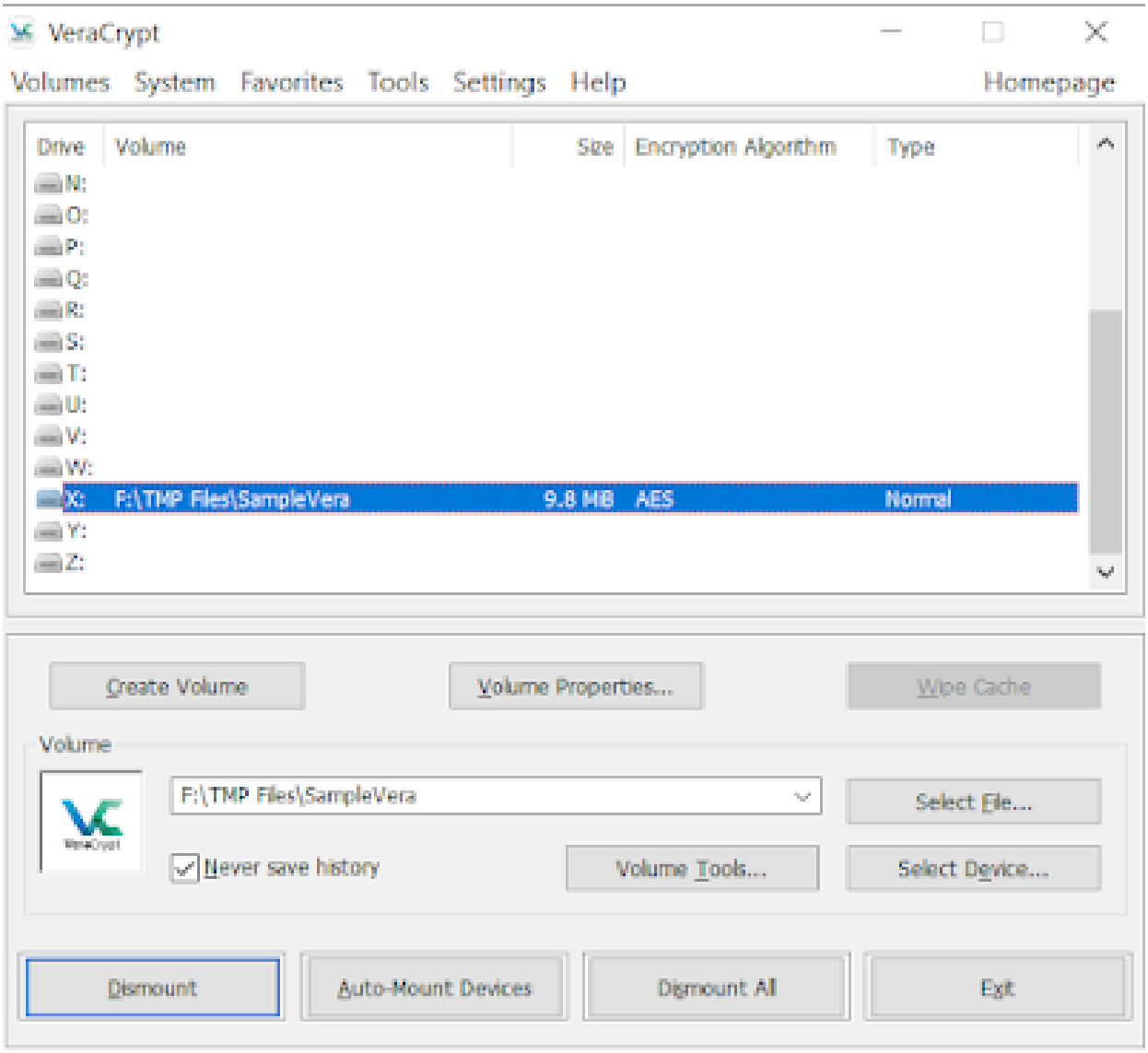
How to create an encrypted container with VeraCrypt:

1. **Launch VeraCrypt**: Open VeraCrypt from the Start menu or desktop shortcut.
2. Create a New Volume: In the VeraCrypt main window, click on **Create Volume**.
3. Volume Creation Wizard: Select "**Create an encrypted file container**" and click **Next**.
4. Choose "**Standard VeraCrypt volume**" and click Next.

5. Volume Location: Click “**Select File**” to choose the location and name for your encrypted volume. Make sure to choose a file name and save location that’s easy to remember. Click **Save** and then **Next**.
6. Encryption Options: Choose the encryption algorithm and hash algorithm you want to use. The default settings (**AES and SHA-512**) are a good balance between security and performance. Click Next.
7. Volume Size: **Specify the size of the volume you want to create**. Enter the desired size (e.g., 1 GB) and click Next.
8. Volume Password: **Create a strong password for your encrypted volume**. This password will be used to unlock the volume, so make sure it’s something you can remember but hard for others to guess. Click **Next**.
9. Format Options: **Select the file system for your encrypted volume** (e.g., NTFS for Windows). You can leave the cluster size at the default setting.
10. Volume Format: **Move your mouse randomly** within the VeraCrypt window to generate some random data for the encryption. This improves the cryptographic strength of the encryption keys. Click **Format** to create the encrypted volume.
11. Wait for VeraCrypt to process and notify you of completion.

Mount the Volume:

1. In the VeraCrypt main window. Select a drive letter from the list (e.g., X:).
2. Click **Select File** and navigate to the encrypted volume file you just created. Select it and click **Open**.
3. Click **Mount** and enter the password you set earlier. Click **OK**.
4. Access the Encrypted Volume: The encrypted volume will now appear as a new drive under This PC or Computer. You can use it just like a regular drive to store files securely.



The VeraCrypt drive has been successfully mounted

Similar to the VHD file mentioned above, you can also copy this VeraCrypt encrypted container file to other machines and use it as usual. The prerequisite is that you must have the decryption password.

2. How to use password managers

When you have more than 10 accounts of various types, how would you manage them? Would you use a single username and password, or would you use different passwords and then save them in a file called "accounts.txt" on your Desktop? When faced with a similar situation, you would need a secure password management app.

A. List of password managers

Below is a list of commonly used password managers.

- KeePass: An open-source option that works as a portable application, meaning it doesn't need to be installed and can be carried around on an external device

- KeePass XC: KeePassXC is a powerful, cross-platform, and open-source password manager. It is based on the original KeePass program but includes more advanced features and enhancements.
- Password Safe is a simple and secure password manager designed to help you store and manage your passwords and other sensitive information.
- Enpass is a versatile and secure password manager that offers both offline and cloud-based storage options.
- Sticky Password is a secure and user-friendly password manager with a range of features designed to keep your passwords and sensitive information safe.

Some criteria you should prioritize when choosing a password manager include:

- **Offline functionality and local storage**: This software must be capable of operating offline and should not connect to the Internet, except for updates. Most importantly, it must store the database on your own device.
- **Open source**: Given the sensitivity of the data, it is essential for the software to be open source, allowing the community to monitor how the software handles data and whether it secretly sends tracking information to the provider.
- **Free**: Naturally, financial considerations are always very important.

You should not use browser add-ons as password managers, as browsers are the most susceptible to risks such as vulnerability exploitation and phishing attacks on your device, because they must interact with the Internet environment. So why would you place your secret treasure in the most attack-prone location?

The password management software I will introduce to you is "KeePass XC" It perfectly meets your needs and the criteria for a secure password management app.

B. KeePass XC

What is KeePass XC?

KeePass XC is a modern, secure, and open-source password manager derived from the popular KeePass program. It is designed to manage your passwords and other sensitive information in a user-friendly way.

- Cross-Platform: KeePassXC runs on Windows, macOS, and Linux, making it versatile and accessible across different operating systems.
- Local Storage: It stores all your encrypted data locally on your device, which means your information isn't stored in the cloud, ensuring your data remains private and secure.
- Open Source: The source code of KeePassXC is available for anyone to inspect, verify, and improve, promoting transparency and trustworthiness.
- Strong Security: It uses AES-256 encryption to keep your data safe. Additionally, it supports multi-factor authentication using key files or hardware tokens.
- ~~Browser Integration: KeePassXC provides browser extensions that allow for easy auto-fill and management of your login credentials on websites.~~

- Password Generator: The application includes a built-in, customizable password generator to help create strong and unique passwords.

You may be wondering about the question of KeePass vs KeePass XC.

KeePass

- Original Version: KeePass is the original version, which has been around for a longer time.
- Plugins and Extensions: Highly extensible with a vast array of plugins to add new features.
- Windows Focused: Primarily designed for Windows, but can also run on macOS and Linux with the help of Mono.

KeePass XC

- **Modern Fork**: KeePassXC is a modern fork of KeePass, integrating many features from the start.
- Cross-Platform: Natively supports Windows, macOS, and Linux without requiring additional frameworks.
- User Interface: Offers a more polished and user-friendly interface compared to KeePass.
- Built-In Features: Includes many features that would require plugins in KeePass, such as ~~browser integration~~ and a more advanced password generator.
- **Community-Driven**: Actively maintained and developed by a community of contributors.

C. How to use KeePass XC.

C.1. Download and Install.

Visit the official KeePassXC website and download the version for your operating system Install the application following the on-screen instructions. Prioritize selecting the portable version (download the file with the .zip extension).

KeePassXC download link: KeePass XC

C.2. Create a New Database.

Start a New Database:

1. Launch the application.
2. Click on the "**Database**" menu at the top.
3. Select "**New Database...**"

Set Up Your Database:

1. **Database Name and Description**: Enter a name and an optional description for your database.

2. **Master Password**: Create a strong master password. **This is crucial because this password will protect all your other passwords**. Ensure it's something you can remember but difficult for others to guess.
3. Key File (Optional): You can enhance security by using a key file in addition to your master password. This key file can be any file (e.g., a photo), and it must be present whenever you want to unlock your database.

Choose Encryption Settings:

KeePass XC uses strong encryption by default (AES-256), so you can leave the encryption settings as they are unless you have specific requirements.

Save Your Database:

Choose a location on your device to save the database file (.kdbx). **Make sure this location is secure and remember the path to it.**

C.3. Add Entry to the newly created KeePass XC database.

Add New Entry:

1. Open KeePassXC: Launch the KeePassXC application and open your existing database by entering your master password (and key file if you use one).
2. Click on the "**Entries**" menu at the top.
3. Select "**Add New Entry**" or click the plus (+) icon on the toolbar.

Fill in Entry Details:

1. **Title**: Enter a descriptive title for your entry, like "Gmail" or "Bank Account".
2. **Username**: Type in your username or email address associated with the account.
3. **Password**: Generate a strong password using the built-in password generator by **clicking the dice icon**. Alternatively, you can **type in your existing password**.
4. **URL**: Enter the URL of the website associated with this entry.
5. Notes: Add any additional information or notes relevant to this entry.

Save the Entry:

Click "**OK**" to save the entry to your database.

Remember to save your database regularly to ensure your data is up-to-date.

Organize Your Entries:

You can drag and drop the new entry into different groups or create new groups to keep your entries organized.

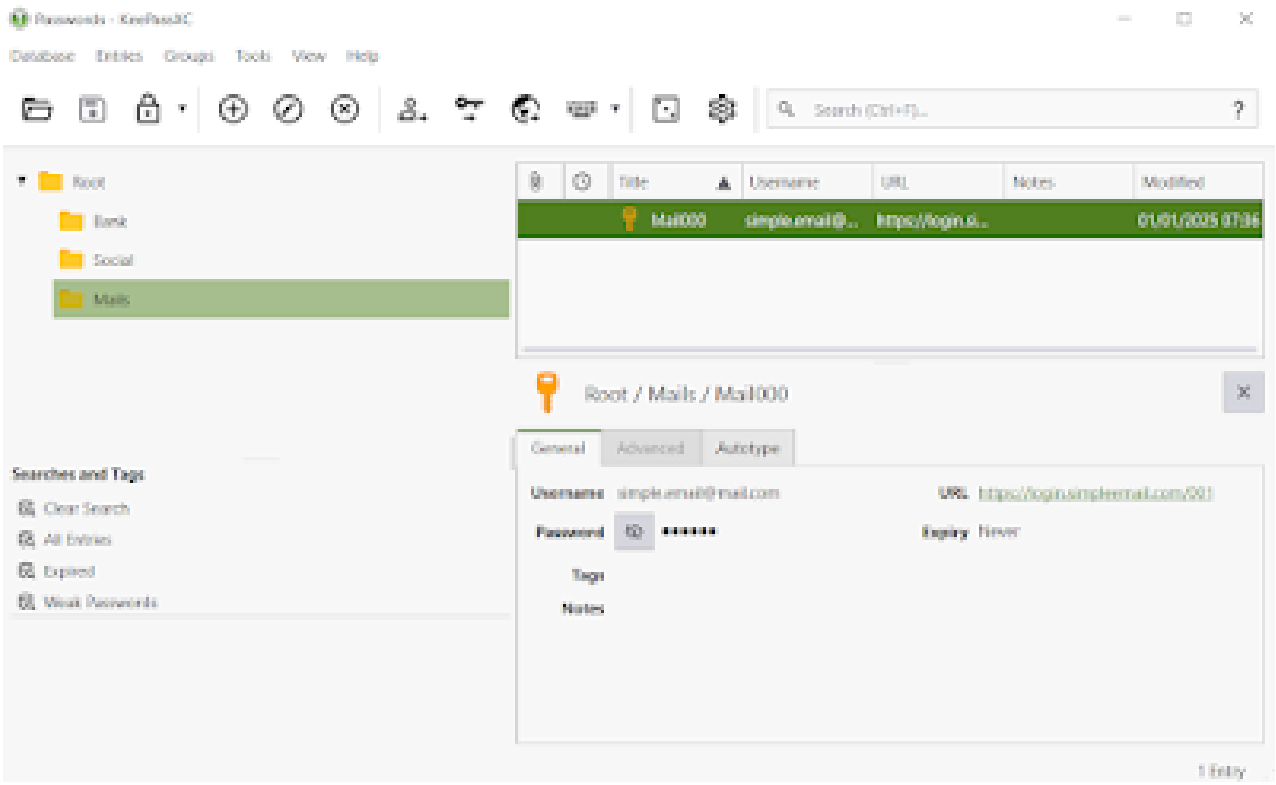
C.4. Use an entry in KeePass XC.

Select the Entry:

Browse through your groups to find the entry you want to use. You can also use the search bar at the top to quickly locate the entry.

Copy Username and Password:

- Once you've found the entry, right-click on it. You'll see options to copy the username and password.
- Select "**Copy Username**" to copy your username to the clipboard. Go to the login page of the website and paste it into the username field.
- Similarly, select "**Copy Password**" to copy your password to the clipboard and paste it into the password field.



III. Summary

To address the question "how to password protect a folder" the two software options, BitLocker and VeraCrypt, will be highly suitable solutions.

VeraCrypt is a robust open-source encryption software that offers a high level of security for your data. While BitLocker is a full-disk encryption feature included with Windows (Professional and Enterprise editions).

Both BitLocker and VeraCrypt allow you to create encrypted containers to store your sensitive files. These containers can be mounted as virtual drives.

With the level of OPSEC you require, along with ease of use, encrypted containers will be the most balanced solution. If you need a higher level of top-tier security, then full disk encryption, whole operating system encryption, hidden drives, and hidden operating systems would be more appropriate options.

By implementing the policy of encrypting files on Windows, you will add an extra layer of defense, preventing data breaches even if your computer is lost.

When you use multiple accounts, it will be safer and more convenient to have a password management app to keep your passwords secure.

KeePass XC will address common account management issues: ensuring each account has a unique password, maintaining an acceptable password strength, and eliminating the need to remember passwords for all accounts.

By using disk encryption software your personal data will be protected and managed through a strong layer of encryption. These locations will become a safe place to store personal files like photos and documents.

By using password manager software, you will no longer have to remember long, complex passwords. Strong passwords play a significant role in helping you stay safe on the Internet.

Disk encryption and password manager software play an extremely important role in the basic OPSEC (Operational Security) checklist.