Aadhaar file password

By Eric Fenton it's always a good idea to encrypt and protect password files and folders on your computer containing sensitive or personal information you don't want others to see. But things can turn ugly if you forget your password and find yourself locked out of your stuff! While you can choose to buy software that can hack into your files, this can be expensive and even then there is no guarantee the program will function quickly. The brute force methods that most programs apply can sometimes take days or weeks to do the job. Here is one method that allows you to do the job without any additional programs. Sign in to your computer as an administrator. Go to the Start menu and select Run. In the command prompt, enter /r:Eagent without quotation marks. Type the administrator's password when you're asked to do so. You're going to get a message saying that. CER and file. The PFX file was successfully created. Select to save files in the administrator's documents and settings folder, rather than another user folder. Go back to start, then run, and enter certmgr.msc. Right-click on the personal folder in the Certificate Manager menu and go to all tasks/import. When you're prompted by a list of folders, go to the folder you saved. CER and . PFX files. Select the file type, share personal information, mark .pfx, P12, open a file called Eagent.pfx. Enter the admin password again, and then continue until you click End. Return to run and enter secpol.msc to open the local security policy. Go to the folder's public key policy and search for the encrypted file system folder. Right-click and choose the add data recovery factor option. Select the Eagent file.cer from the same folder as in Step 3 and open it. Continue until you finish. The administrator is now assigned a recovery agent for locked files. Close the local security policy folder and go to encrypted files. Click on them to view their content and change passwords as necessary. If another user creates the files, log on to the computer as that user and then switch to the administrator. Files can now be accessed. Consider using a program to force through the encrypted file if this method does not work for your individual position. Some useful and free software to consider include zip password view from Last Bit Software, which is available in lastbit.com. Although it is not as fast or powerful as some of the most expensive options, it can get through most compressed files as long as the passwords are not too long. By Lindsay Howell virtual basic script is a file format used by Windows operating systems and Internet Explorer browser. View and edit VBS files in text editing apps such as Microsoft Word and Notepad. If the VBS file contains sensitive information, such as passwords, use windows encryption file system, included in Windows operating systems, to encrypt the file and protect it from unauthorized use. Click on Windows Explorer Located in the taskbar from your desktop; Click the Properties option. Select the dialogue box for advanced attributes within vbs file properties. Select the box called content encryption to enable file encryption. Click OK to save the changes you made to the VBS file, then click an application to encrypt the VBS file. Here's how to create a strong password or password that you'll remember and no one else can guess. It should be a strong password for your online accounts: randomly already, do not use 17 different characters for each online account that is changed every 90 days, and there are some password practices that should be avoided: do not use the word + common number format. Does not include personal information that is publicly available, such as your birthday. Do not use reduction and common substitutions (such as using @a). @MIRAHNEVA via Twenty20 while most passwords are groups of numbers, letters and symbols, the password consists of randomly grouped words. For example: StingrayCobaltLyingStimulusLiquid Passphrases are both easier to remember and harder to guess than standard passwords. Just try to save the first letter of each word, or turn it into a song in your head. To defend against dictionary attacks, you must use at least five words, and they should be really random. You don't want the phrase to look like a sentence to make sure that the words you choose are really random, use a free passphrase generator like Diceware or a secure passphrase generator. For a variety of random letters and numbers, use the Norton password generator or a random password generator Avast. Many online accounts have specific password requirements, so you may want to add numbers, special characters, or a combination of capital and small letters. Easy use to remember information such as your birthday or year you graduated from high school is not very encouraging. If you have trouble remembering traffic phrases, another strategy is to create a sentence shortcut. For example, gallons of milk used for a cost of 32 cents back in 1950 can be translated into: Agomutc$.32bi1950 It's generally not a good idea to write your passwords ; However, you can type the phrase as a reminder, and no one will know what it means if it finds it. If you have multiple online accounts, you must use a password manager to track your login credentials. Although it may be tempting, you should not use the same username and password in all your online accounts. Each account must have a unique and complex password. Fortunately, you don't have to remember them all individually. Alternatively, you can use password management. This way, you can sign in to any account by entering the password manager's primary password. Some The best password managers software also comes with built-in password generators. If you want to know how strong your password is, use a password checker like a password counter. Regardless of the strength of your password, it is always best to protect your online accounts by using binary authentication (2FA) when possible. When you turn on 2FA for Gmail and other services, you'll receive a verification code via text message or email every time you sign in. Most banking services and social media sites support a form of 2FA. In addition to your online accounts, you also need strong passwords for all your devices, especially if you carry them with you in public. In addition to passwords, most operating systems support some biometric verification. For example, Windows Hello uses facial recognition technology and Apple Touch ID uses a finger print scanner to determine who's trying to access your account. Passwords protect your online accounts from other people using the same computer. More importantly, it protects you from hackers who want to steal your personal information. If someone knows your email password, for example, they can know a lot about you including where you bank, where you work, and where you live. Stolen passwords are often sold on the black market for nefarious purposes. Hackers use several ways to steal passwords including: Brute Force Attacks: Brute Force Attack uses automated software to guess passwords using random combinations of characters. Dictionary attacks: Similar to brute force attacks, random word combinations are used to guess passwords. Phishing: Hackers solicit private information directly using emails, robocalls, or misleading links to get passwords from users. Recycle credentials: If a hacker has a username and password for one account, they are likely to try to use the same credentials on your other accounts. If you suspect that a password has been compromised: create a new, stronger password. Change passwords for any associated accounts. Update account recovery information. Keep an eye on your bank account for unauthorized purchase. Your usernames and passwords can be compromised by any error of their own. Many high-profile companies, such as Facebook and Sony, have been victims of data breaches that revealed user login credentials. You can visit The Avast Hack Check website and enter your email address to see if your privacy has been compromised. If so, you must change passwords for all accounts associated with this email. Set up security questions and account recovery information when possible to further protect your accounts. If you have a large set of files to compress and want to add password protection to each of them, what is the simplest or fastest way to do so? Today SuperUser Q&amp;A post has the answer to the curious reader's question. Today's Q&A session comes to us courtesy of SuperUser - a split of the stack A driven collection of question sasked and questioned sites. The superUser question the dae reader wants to know how zip and password protection files in as few steps as possible: I need a way to take a bunch of files and compress them into separate compressed files with each using the same password. I want to be able to do this in one simple step. I have created a push file that both of them using 7zip (which worked perfectly), but no password protect them. Is there anything I can add to the payment file that includes the password? Alternatively, how do I create a push file that protects password-compressed files? How do you zip and password protect files in as few steps as possible? SuperUser contributor DavidPostill's answer for us: How do I create a payment file that will protect the password compressed files? Use -p-option -p (set password) switch, which determines the password. Syntax {password} identifies examples of password squeezing * .txt files to archive.7z using a secret password. It also encrypts archive headers (-mhe switch) so that file names are encrypted. 7z Archive.7z -psecret-mhe* .txt if you compress folders: C:\Program Files (x86)\7-Zip\7z.exe a%x.zip -psecret%X\ extracts all files from the archive.zip using a secret password. 7z x archive.zip -psecret source: -p (set password) switch is there nothing to add to the explanation? Sound off in the comments. Want to read more answers from other tech-savvy Exchange stack users? Check out the full discussion topic here. In here.