.harma (Ouroboros) Ransomware

By Tomas Meskauskas

Published: 2021-09-16 · Archived: 2026-04-05 23:22:53 UTC

What is .harma (Ouroboros)?

Discovered by malware researcher S!Ri, .harma (Ouroboros) is a ransomware-type malicious program belonging to the Ouroboros malware family. Systems infected with this software have data encrypted and victims receive ransom demands for decryption tools/software.

During the encryption process, all affected files are renamed with the "**.harma**" extension, which has been used by other ransomware from the Dharma family.

To elaborate on how files appear following encryption, a filename like "**1.jpg**" would appear as "**1.jpg.harma**". After this process is complete, two files ("**INFO.exe**" and "**ReadMe.txt**") containing the ransom messages are stored on the desktop.

The text file informs victims that their data has been encrypted. To restore files, users are instructed to establish contact with the ransomware developers via the email addresses provided. The subject line of their messages must include their unique IDs and personal keys.

The pop-up window (opened by "INFO.exe") is a more detailed ransom message, which repeats the information within "ReadMe.txt" and adds that victims can test decryption by sending one encrypted file to the cyber criminals behind .harma (Ouroboros).

This test file cannot exceed 1 MB or contain valuable information (e.g. databases, backups, large excel sheets or similar). The ransom size is not stated, however, it must be paid in the Bitcoin cryptocurrency. This message also lists links to websites detailing how to and from where to acquire Bitcoins.

It warns users that renaming the compromised files and attempting decryption with third party software can lead to permanent data loss. Unfortunately, in most cases of ransomware infections, decryption is impossible without the involvement of the criminals responsible, unless the malware is still in development and/or has bugs/flaws.

Whatever the case, you are strongly advised against meeting the ransom demands of cyber criminals. Despite paying, victims often receive none of the promised decryption tools/software. Therefore, their files remain encrypted and they also experience significant financial loss.

To prevent .harma (Ouroboros) ransomware from further encryption, it must be removed from the operating system, however, removal will not restore already affected data. The only solution is to recover files from a backup, if one was created prior to the infection and was stored in a different location.

Screenshot of a message encouraging users to pay a ransom to decrypt their compromised data:

Ragnarok, Devos, and Nosu are some examples of other ransomware infections. These malicious programs are designed to encrypt data and demand payment for decryption. Main differences include the cryptographic algorithm used (symmetric or asymmetric) for encryption and ransom size.

The latter typically ranges between three and four digit sums (in USD). Digital currencies (mainly cryptocurrencies) are preferred by cyber criminals, since these transactions are difficult/impossible to trace. To ensure data safety, you are advised to keep backups on remote servers and/or unplugged storage devices.

How did ransomware infect my computer?

Ransomware and malware are primarily spread through trojans, spam campaigns, illegal activation tools ("cracks"), fake updaters and untrusted download sources. Trojans are malware programs designed to cause chain infections (i.e. download/install additional malicious programs).

Spam campaigns are used to send deceptive emails on a mass scale. The mail is usually disguised as "official", "urgent", "important" and so on. The messages have infectious files attached (or contain links leading to them). The attachments come in various formats (e.g. archive and executable files, PDF and Microsoft Office documents, JavaScript, etc.).

When they are opened, the infection process starts. Software "cracking" (activation) tools can download/install malware.

Fake updaters infect systems by misusing weaknesses in outdated programs or simply by installing malware rather than the updates. Untrustworthy download sources (e.g. unofficial and free file-hosting websites, Peer-to-Peer sharing networks and other third party downloaders) can offer malicious content presented as normal software and/or bundled with it.

Threat Summary:

Name	.harma (Ouroboros) virus
Threat Type	Ransomware, Crypto Virus, Files locker.
Encrypted Files Extension	.harma
Ransom Demand Message	INFO.exe and ReadMe.txt
Cyber Criminal Contact	encryptor2020@protonmail.com and encryptor1996@protonmail.com
Detection Names	Fortinet (MSIL/Kryptik.QBJ!tr), McAfee (Artemis!01816325E9CB), ESET-NOD32 (A Variant Of MSIL/Kryptik.QBJ), Kaspersky (Trojan.Win32.DelShad.cgn), Full List Of Detections (VirusTotal)
Symptoms	Cannot open files stored on your computer, previously functional files now have a different extension (for example, my.docx.locked). A ransom demand message is displayed on your desktop. Cyber criminals demand payment of a ransom (usually in bitcoins) to unlock your files.
Additional Information	The added extension (.harma) has been used by ransomware from the Dharma malware family.
Distribution methods	Infected email attachments (macros), torrent websites, malicious ads.
Damage	All files are encrypted and cannot be opened without paying a ransom. Additional password-stealing trojans and malware infections can be installed together with a ransomware infection.
Malware Removal (Windows)	To eliminate possible malware infections, scan your computer with legitimate antivirus software. Our security researchers recommend using Combo Cleaner.

How to protect yourself from ransomware infections

Suspicious and/or irrelevant emails should not be opened, especially those received from unknown addresses. Any attachments or links found in dubious mail must never be opened, since doing so can trigger an infection. Use official and verified download channels.

All programs should be activated and updated with tools/functions provided by legitimate developers. Illegal activation tools ("cracks") and third party updaters carry a high risk of malware installation and should not be used. Have a reputable anti-virus/anti-spyware suite installed and kept updated.

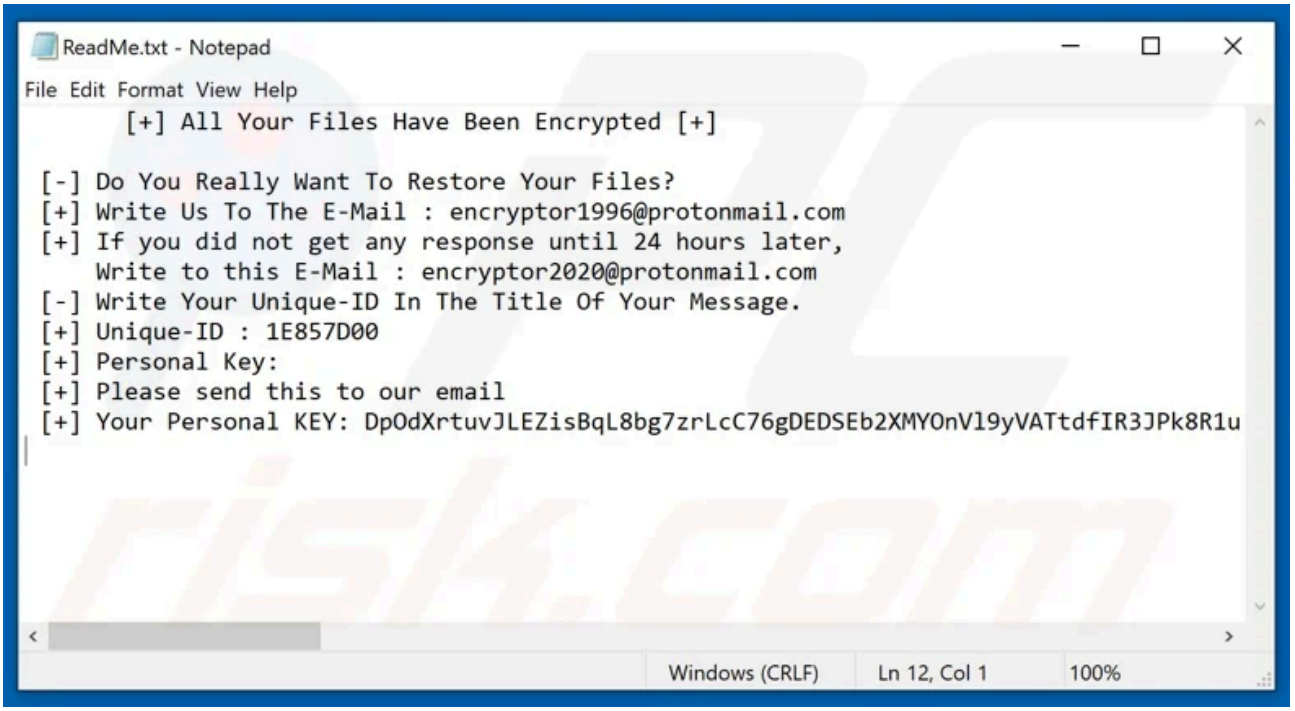
This software should be used for regular system scans and removal of detected/potential threats. If your computer is already infected with .harma (Ouroboros), we recommend running a scan with Combo Cleaner Antivirus for Windows to automatically eliminate this ransomware.

Text presented in .harma (Ouroboros) ransomware pop-up ("**INFO.exe**"):

> Your Files Has Been Encrypted
>
> How To Recover :
> Your Data Has Been Encrypted Due The Security Problem
> If You Want To Restore Your Files Send Email to Us
> Before Paying You Can Send 1MB file For Decryption Test to guarantee that your Files Can Be Restored
> Test File Should Not Contain Valuable Data (Databases Large Excels , Backups)
> Do Not Rename Files or Do Not Try Decrypt Files With 3rd Party Softwares , It May Damage Your Files
> And Increase Decryption Price
>
> Your ID : 1E857D00
> Our Email : encryptor2020@protonmail.com Or encryptor1996@protonmail.com
> How To Buy Bitcoin :
> Payment Should Be With Bitcoin

> You Can learn how To Buy Bitcoin From This Links :
> hxxps://localbitcoins.com/buy_bitcoins
> hxxps://www.coindesk.com/information/how-can-i-buy-bitcoins

Screenshot of .harma (Ouroboros) text file ("**ReadMe.txt**"):



Text presented in this file:

> [+] All Your Files Have Been Encrypted [+]
>
> [-] Do You Really Want To Restore Your Files?
> [+] Write Us To The E-Mail : encryptor1996@protonmail.com
> [+] If you did not get any response until 24 hours later,Write to this E-Mail : encryptor2020@protonmail.com
> [-] Write Your Unique-ID In The Title Of Your Message.
> [+] Unique-ID : 1E857D00
> [+] Personal Key:
> [+] Please send this to our email
> [+] Your Personal KEY: -

Screenshot of files encrypted by .harma (Ouroboros) ("**.harma**" extension):

.harma (Ouroboros) ransomware removal:

Instant automatic malware removal:

Manual threat removal might be a lengthy and complicated process that requires advanced IT skills. Combo Cleaner is a professional automatic malware removal tool that is recommended to get rid of malware. Download it by clicking the button below:

DOWNLOAD Combo Cleaner

By downloading any software listed on this website you agree to our Privacy Policy and Terms of Use. To use full-featured product, you have to purchase a license for Combo Cleaner. 7 days free trial available. Combo Cleaner is owned and operated by RCS LT, the parent company of PCRisk.com.

Video suggesting what steps should be taken in case of a ransomware infection:

Quick menu:

- What is .harma (Ouroboros) virus?
- STEP 1. Reporting ransomware to authorities.
- STEP 2. Isolating the infected device.
- STEP 3. Identifying the ransomware infection.
- STEP 4. Searching for ransomware decryption tools.
- STEP 5. Restoring files with data recovery tools.
- STEP 6. Creating data backups.

Reporting ransomware to authorities:

If you are a victim of a ransomware attack we recommend reporting this incident to authorities. By providing information to law enforcement agencies you will help track cybercrime and potentially assist in the prosecution of the attackers. Here's a list of authorities where you should report a ransomware attack. For the complete list of local cybersecurity centers and information on why you should report ransomware attacks, read this article.

List of local authorities where ransomware attacks should be reported (choose one depending on your residence address):

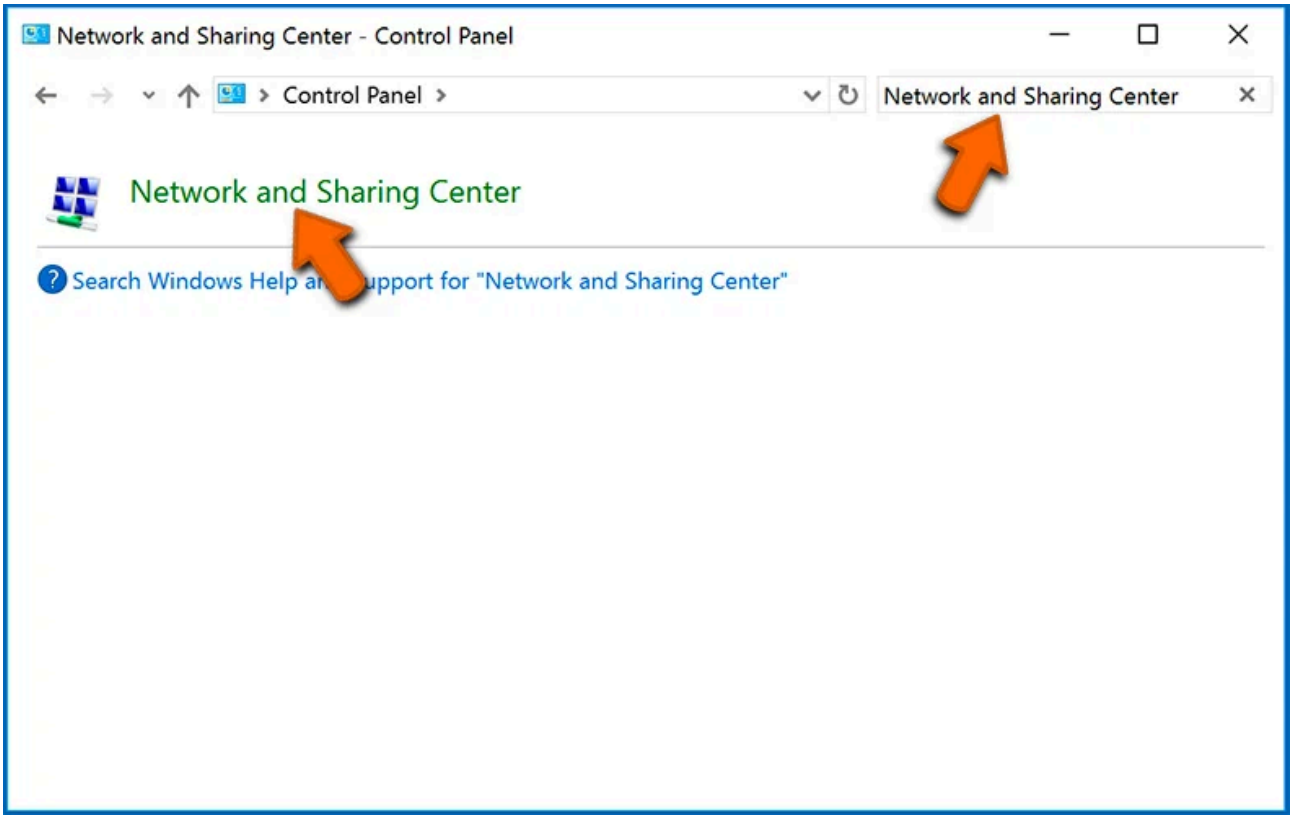
Isolating the infected device:

Some ransomware-type infections are designed to encrypt files within external storage devices, infect them, and even spread throughout the entire local network. For this reason, it is very important to isolate the infected device (computer) as soon as possible.

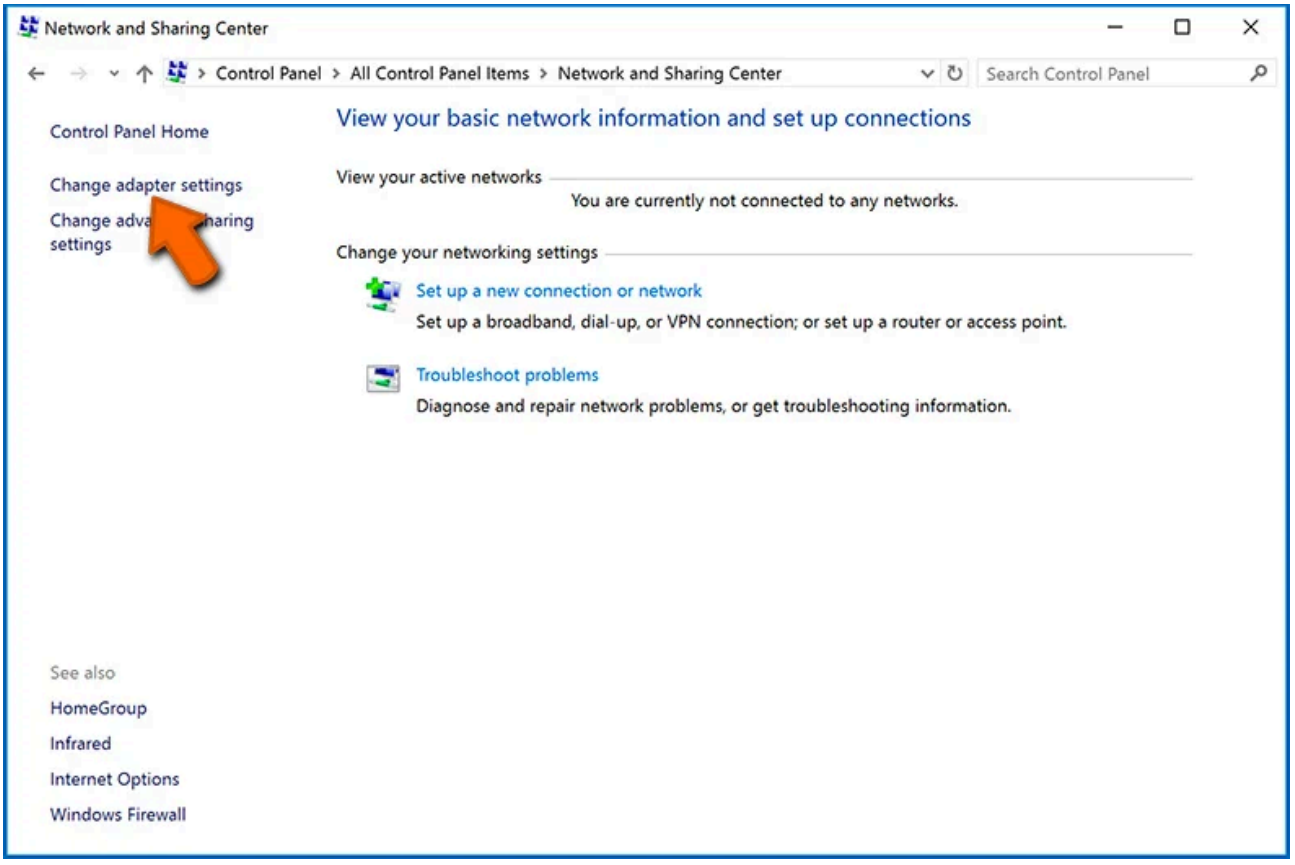
Step 1: Disconnect from the internet.

The easiest way to disconnect a computer from the internet is to unplug the Ethernet cable from the motherboard, however, some devices are connected via a wireless network and for some users (especially those who are not particularly tech-savvy), disconnecting cables may seem troublesome. Therefore, you can also disconnect the system manually via Control Panel:

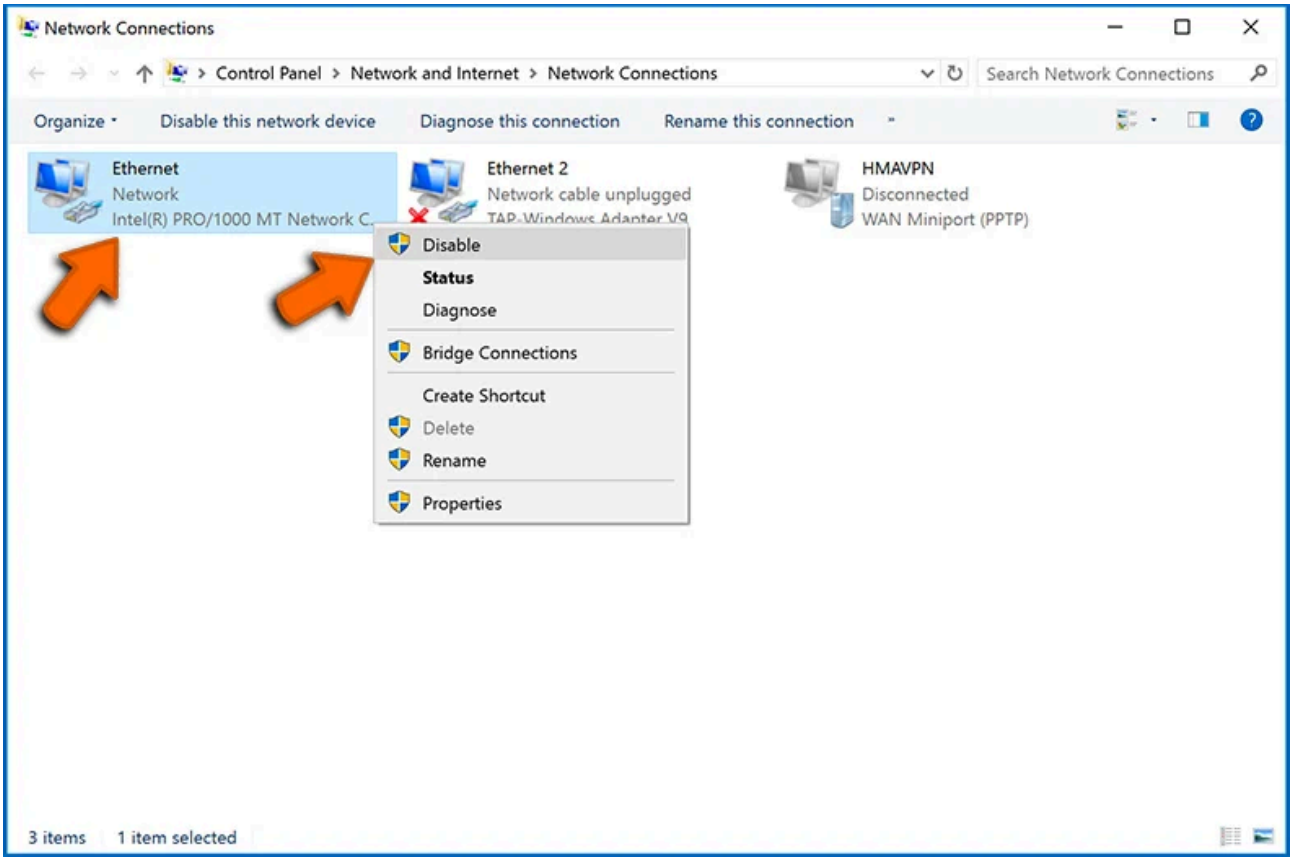
Navigate to the "**Control Panel**", click the search bar in the upper-right corner of the screen, enter "**Network and Sharing Center**" and select search result:



Click the "**Change adapter settings**" option in the upper-left corner of the window:



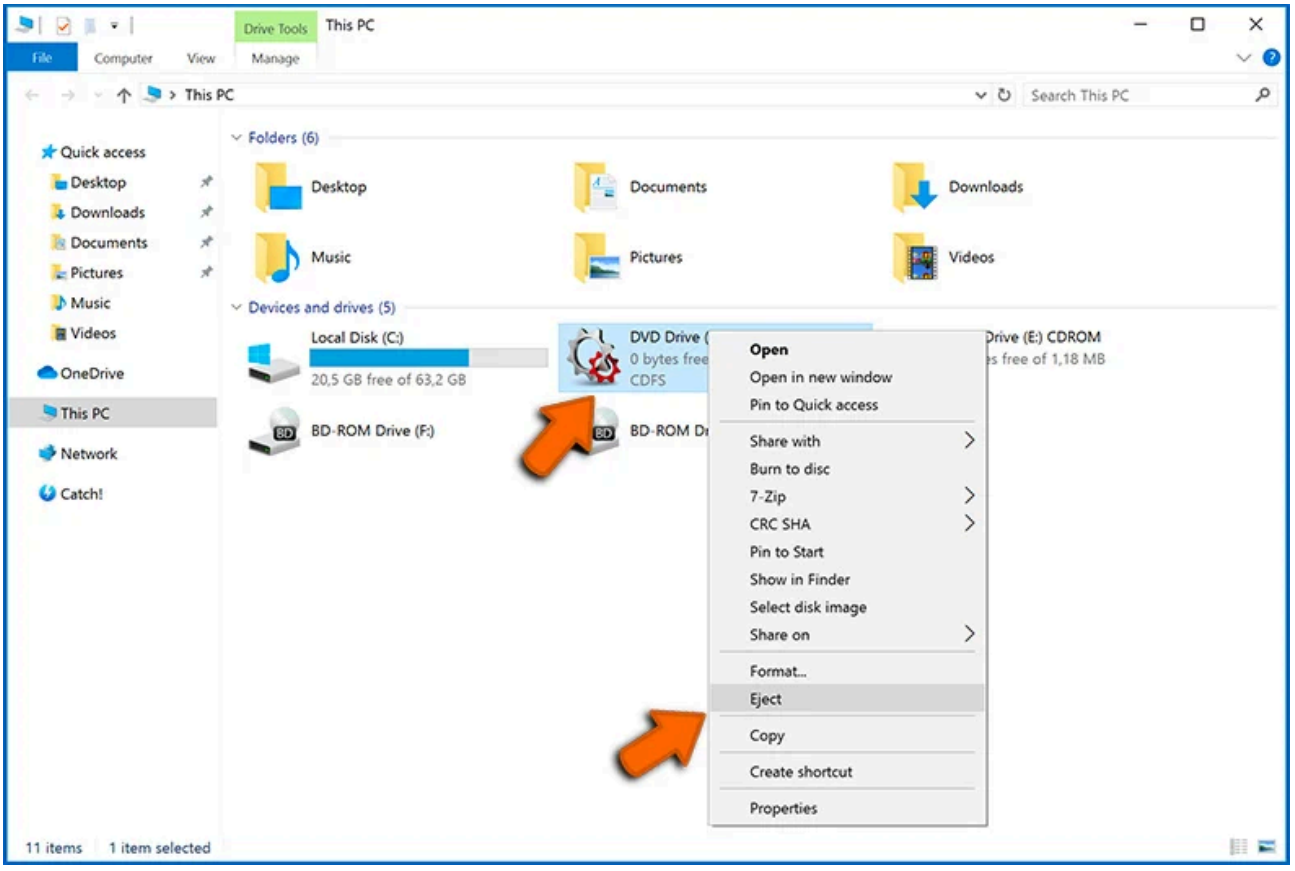
Right-click on each connection point and select "**Disable**". Once disabled, the system will no longer be connected to the internet. To re-enable the connection points, simply right-click again and select "**Enable**".



Step 2: Unplug all storage devices.

As mentioned above, ransomware might encrypt data and infiltrate all storage devices that are connected to the computer. For this reason, all external storage devices (flash drives, portable hard drives, etc.) should be disconnected immediately, however, we strongly advise you to eject each device before disconnecting to prevent data corruption:

Navigate to "**My Computer**", right-click on each connected device, and select "**Eject**":

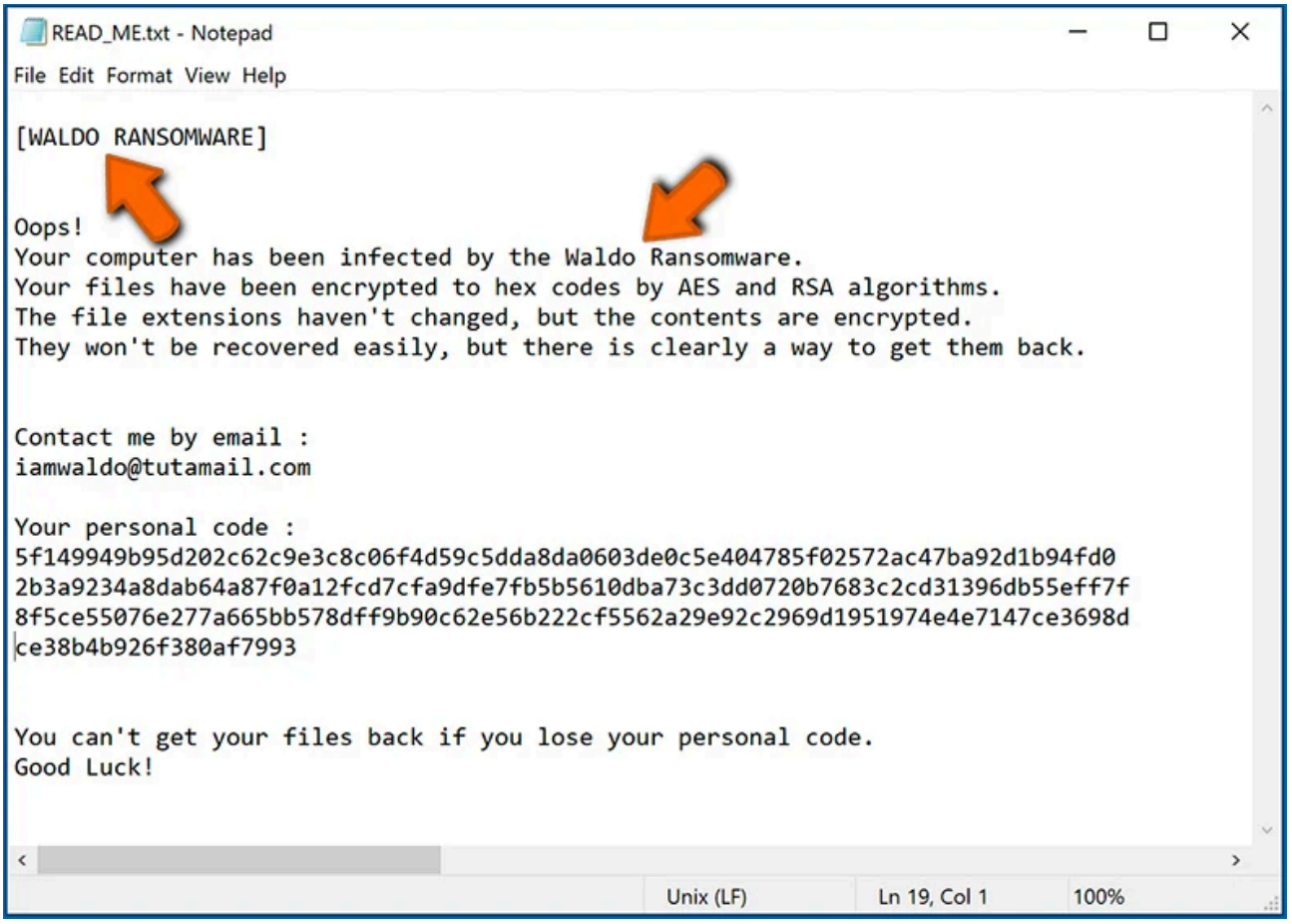


Step 3: Log-out of cloud storage accounts.

Some ransomware-type might be able to hijack software that handles data stored within "the Cloud". Therefore, the data could be corrupted/encrypted. For this reason, you should log-out of all cloud storage accounts within browsers and other related software. You should also consider temporarily uninstalling the cloud-management software until the infection is completely removed.

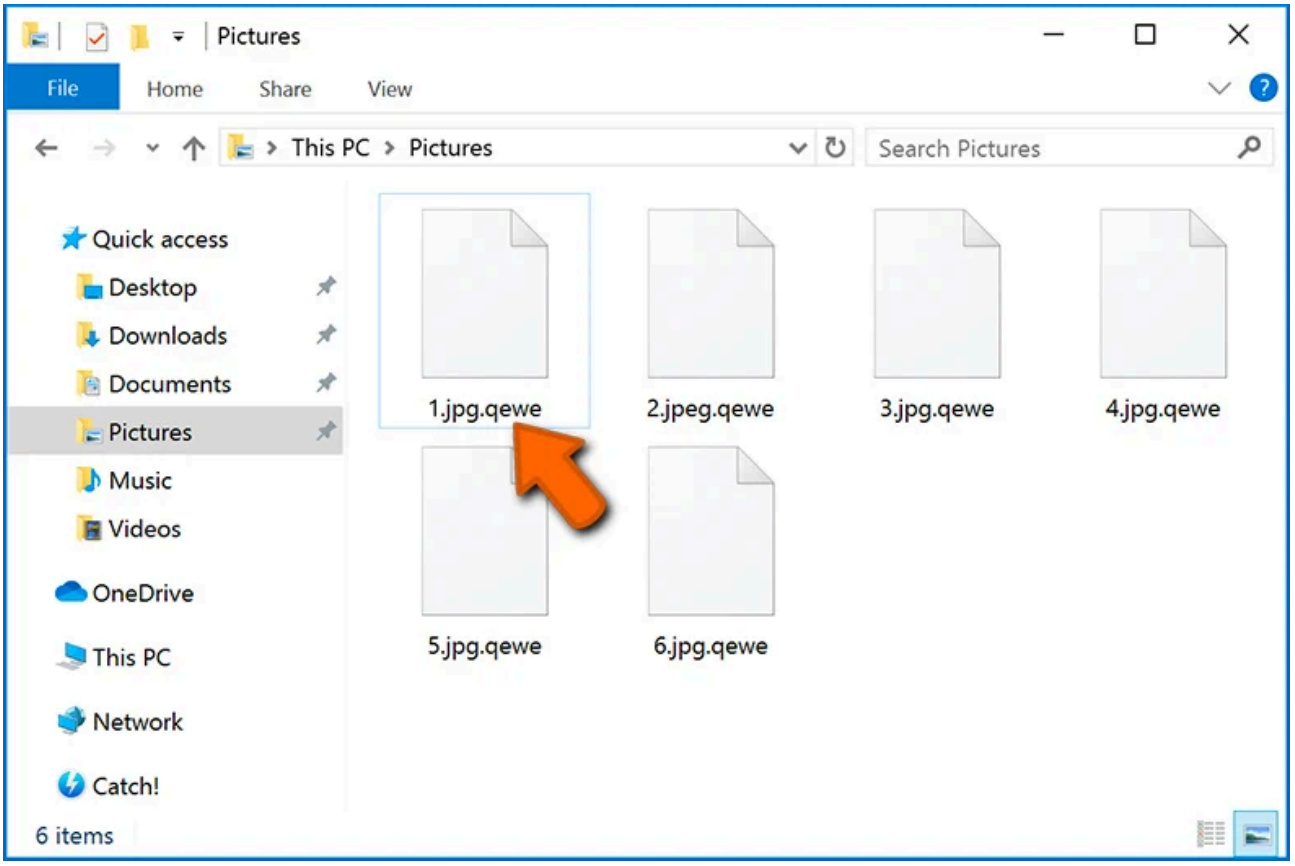
Identify the ransomware infection:

To properly handle an infection, one must first identify it. Some ransomware infections use ransom-demand messages as an introduction (see the WALDO ransomware text file below).



This, however, is rare. In most cases, ransomware infections deliver more direct messages simply stating that data is encrypted and that victims must pay some sort of ransom. Note that ransomware-type infections typically generate messages with different file names (for example, "**_readme.txt**", "**READ-ME.txt**", "**DECRYPTION_INSTRUCTIONS.txt**", "**DECRYPT_FILES.html**", etc.). Therefore, using the name of a ransom message may seem like a good way to identify the infection. The problem is that most of these names are generic and some infections use the same names, even though the delivered messages are different and the infections themselves are unrelated. Therefore, using the message filename alone can be ineffective and even lead to permanent data loss (for example, by attempting to decrypt data using tools designed for different ransomware infections, users are likely to end up permanently damaging files and decryption will no longer be possible even with the correct tool).

Another way to identify a ransomware infection is to check the file extension, which is appended to each encrypted file. Ransomware infections are often named by the extensions they append (see files encrypted by Qewe ransomware below).

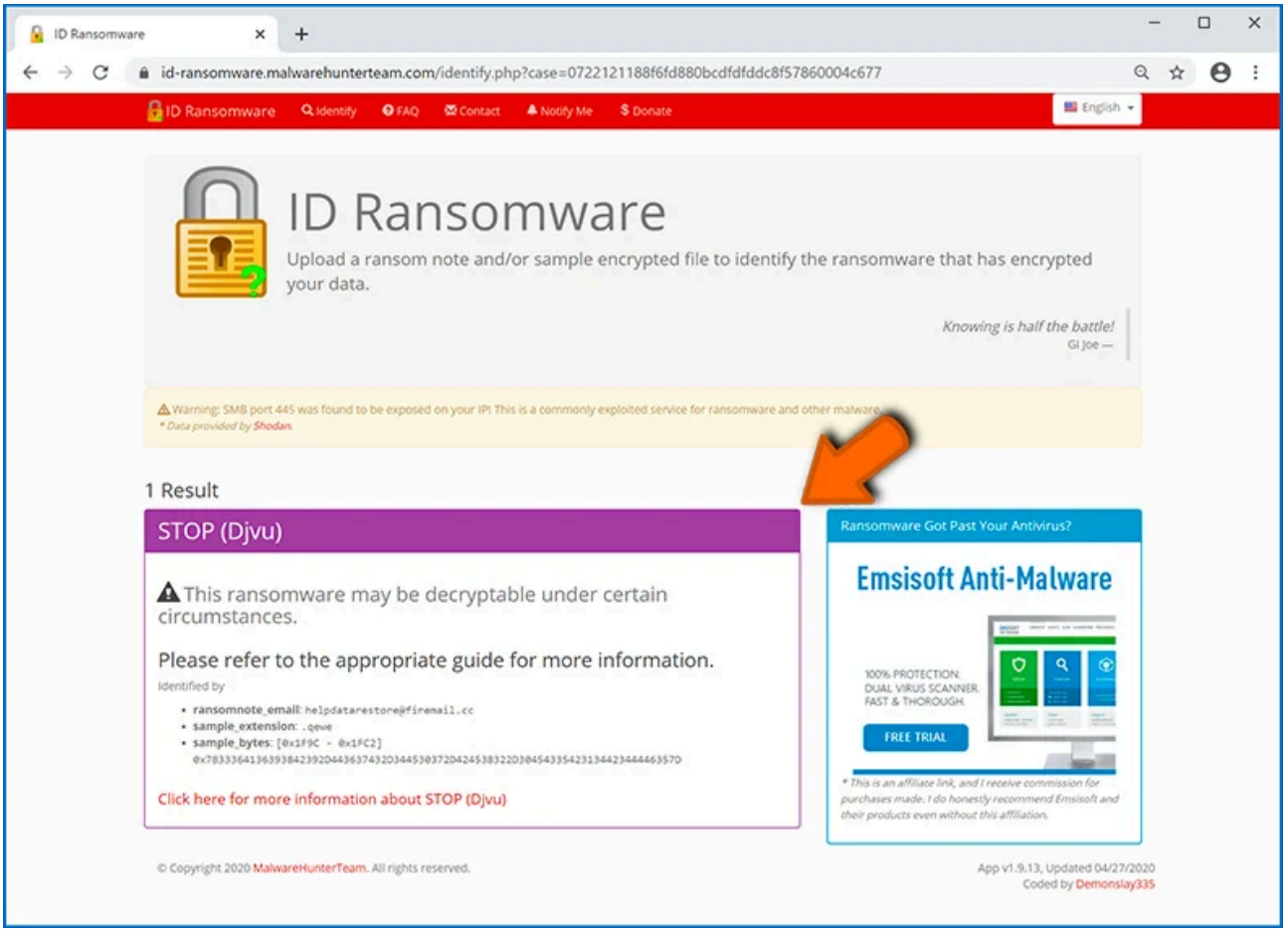


This method is only effective, however, when the appended extension is unique - many ransomware infections append a generic extension (for example, "**.encrypted**", "**.enc**", "**.crypted**", "**.locked**", etc.). In these cases, identifying ransomware by its appended extension becomes impossible.

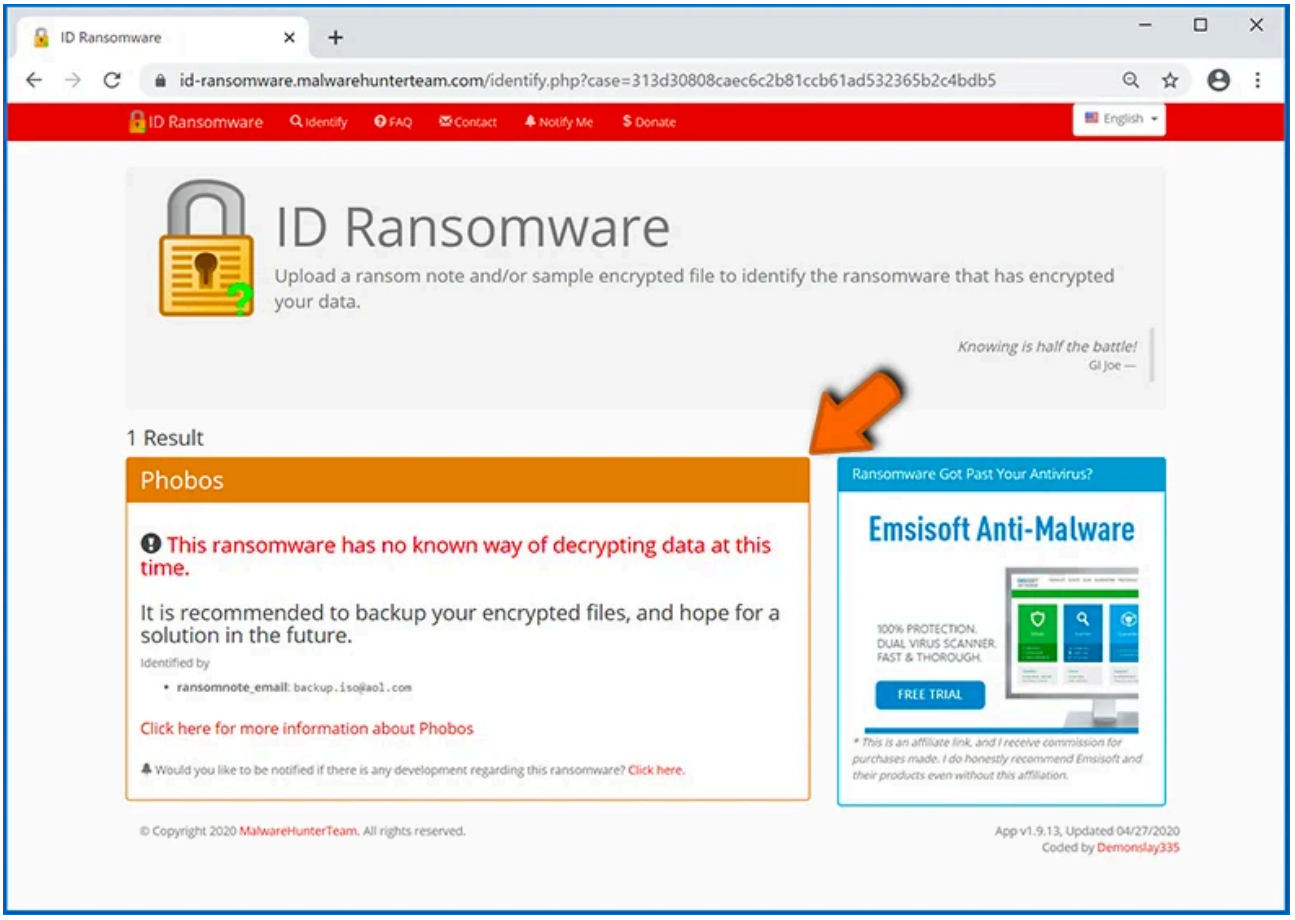
One of the easiest and quickest ways to identify a ransomware infection is to use the ID Ransomware website. This service supports most existing ransomware infections. Victims simply upload a ransom message and/or one encrypted file (we advise you to upload both if possible).

The ransomware will be identified within seconds and you will be provided with various details, such as the name of the malware family to which the infection belongs, whether it is decryptable, and so on.

Example 1 (Qewe [Stop/Djvu] ransomware):



Example 2 (.iso [Phobos] ransomware):

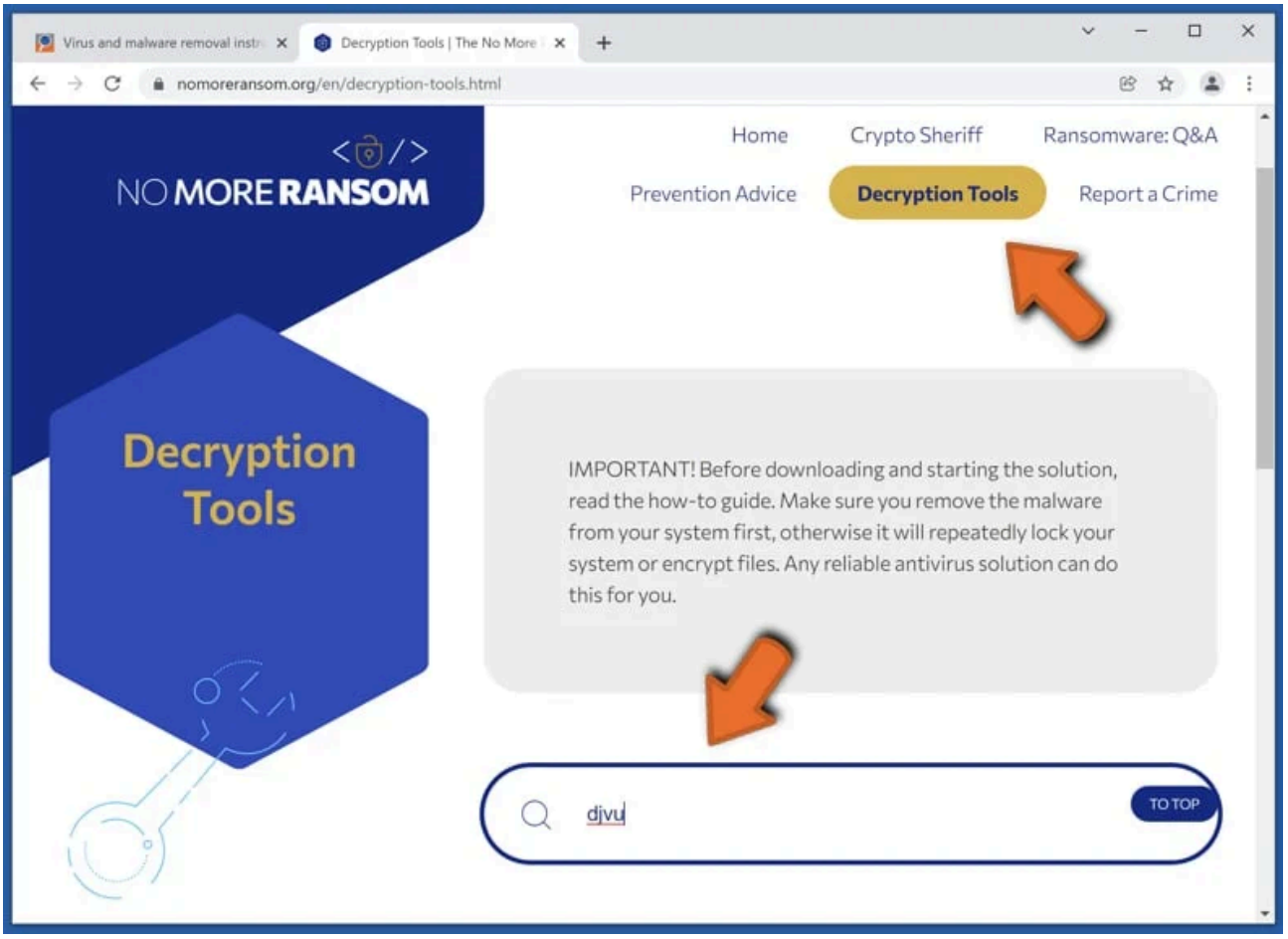


If your data happens to be encrypted by ransomware that is not supported by ID Ransomware, you can always try searching the internet by using certain keywords (for example, a ransom message title, file extension, provided contact emails, crypto wallet addresses, etc.).

Search for ransomware decryption tools:

Encryption algorithms used by most ransomware-type infections are extremely sophisticated and, if the encryption is performed properly, only the developer is capable of restoring data. This is because decryption requires a specific key, which is generated during the encryption. Restoring data without the key is impossible. In most cases, cybercriminals store keys on a remote server, rather than using the infected machine as a host. Dharma (CrySis), Phobos, and other families of high-end ransomware infections are virtually flawless, and thus restoring data encrypted without the developers' involvement is simply impossible. Despite this, there are dozens of ransomware-type infections that are poorly developed and contain a number of flaws (for example, the use of identical encryption/decryption keys for each victim, keys stored locally, etc.). Therefore, always check for available decryption tools for any ransomware that infiltrates your computer.

Finding the correct decryption tool on the internet can be very frustrating. For this reason, we recommend that you use the No More Ransom Project and this is where identifying the ransomware infection is useful. The No More Ransom Project website contains a "Decryption Tools" section with a search bar. Enter the name of the identified ransomware, and all available decryptors (if there are any) will be listed.

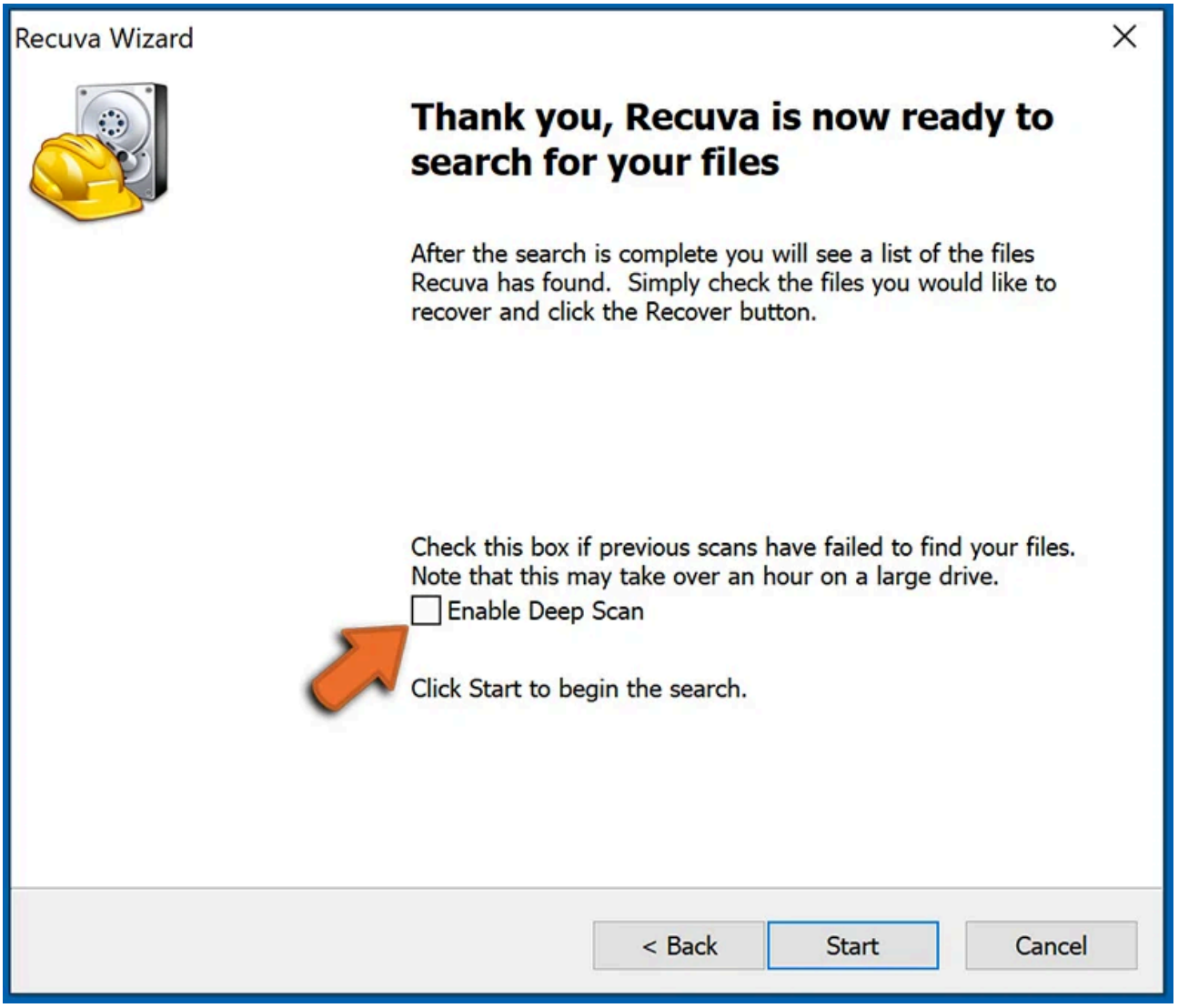


Restore files with data recovery tools:

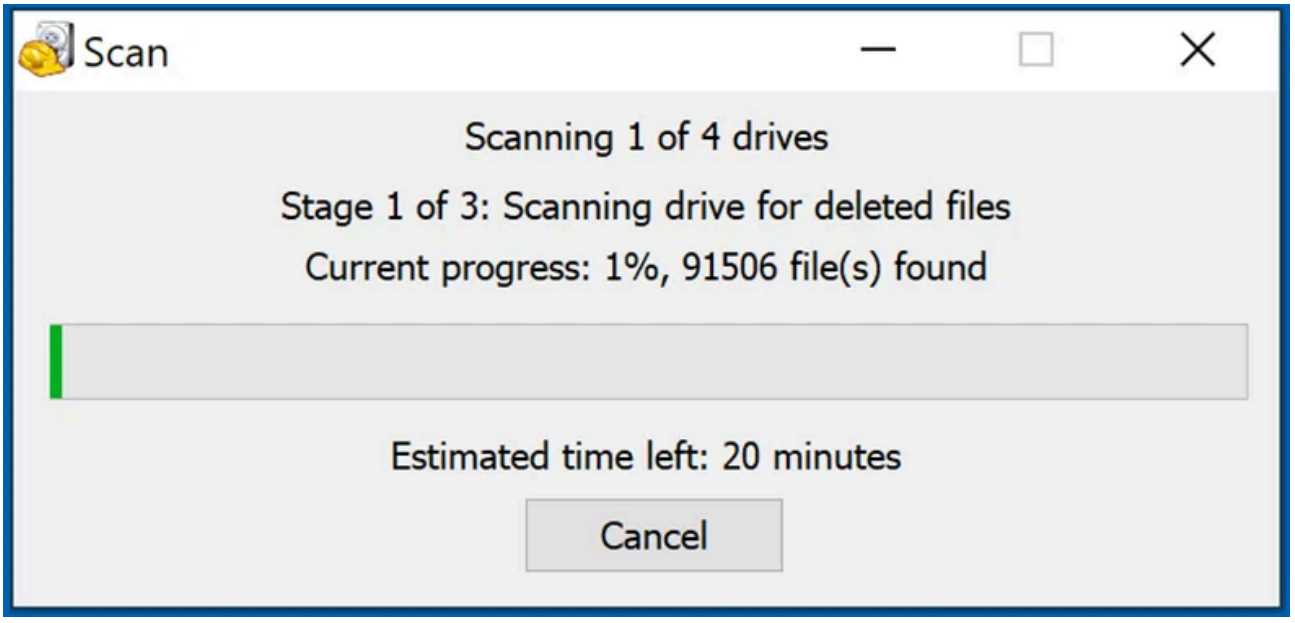
Depending on the situation (quality of ransomware infection, type of encryption algorithm used, etc.), restoring data with certain third-party tools might be possible. Therefore, we advise you to use the Recuva tool developed by CCleaner. This tool supports over a thousand data types (graphics, video, audio, documents, etc.) and it is very intuitive (little knowledge is necessary to recover data). In addition, the recovery feature is completely free.

Step 1: Perform a scan.

Run the Recuva application and follow the wizard. You will be prompted with several windows allowing you to choose what file types to look for, which locations should be scanned, etc. All you need to do is select the options you're looking for and start the scan. We advise you to enable the "**Deep Scan**" before starting, otherwise, the application's scanning capabilities will be restricted.

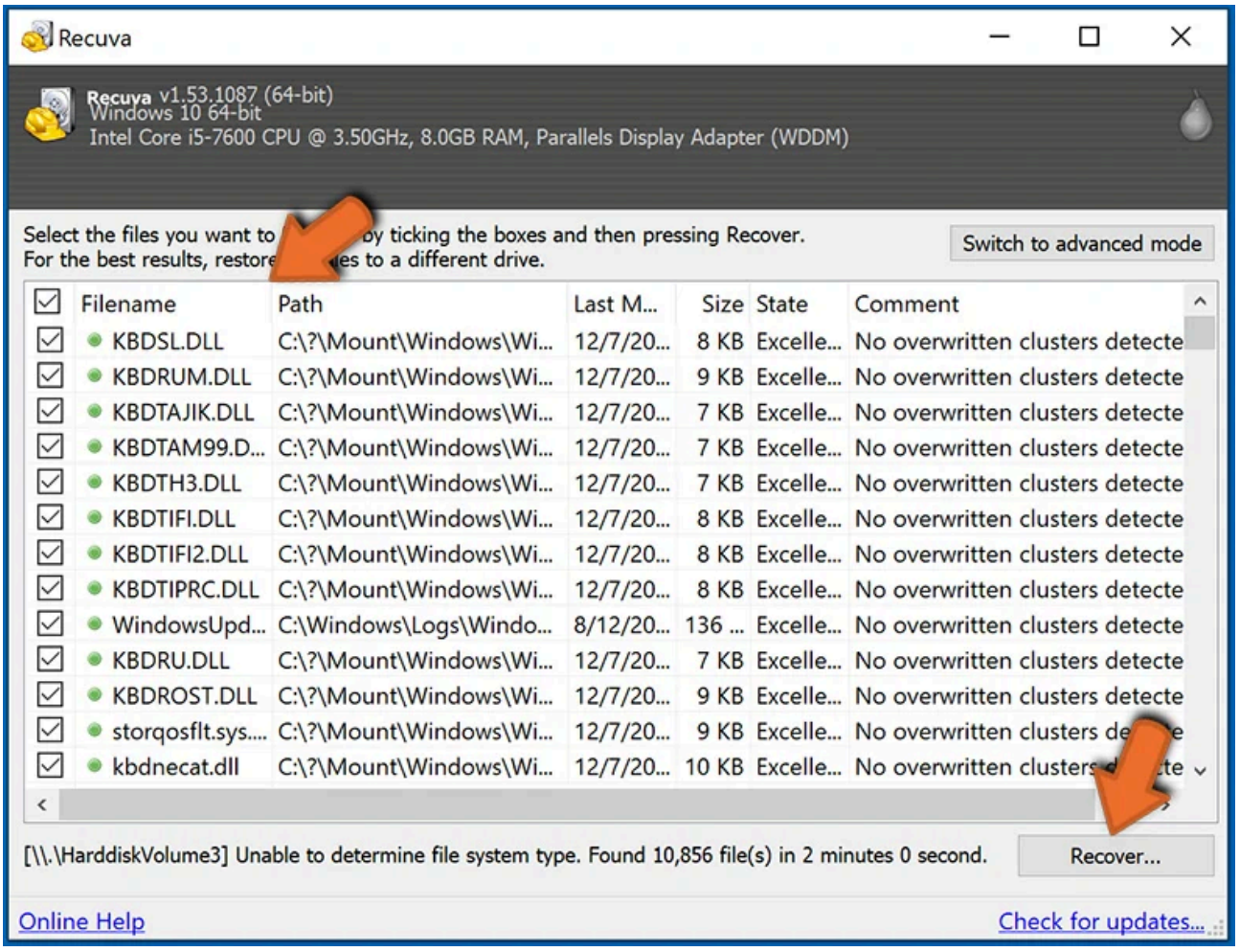


Wait for Recuva to complete the scan. The scanning duration depends on the volume of files (both in quantity and size) that you are scanning (for example, several hundred gigabytes could take over an hour to scan). Therefore, be patient during the scanning process. We also advise against modifying or deleting existing files, since this might interfere with the scan. If you add additional data (for example, downloading files/content) while scanning, this will prolong the process:



Step 2: Recover data.

Once the process is complete, select the folders/files you wish to restore and simply click "Recover". Note that some free space on your storage drive is necessary to restore data:



Create data backups:

Proper file management and creating backups is essential for data security. Therefore, always be very careful and think ahead.

Partition management: We recommend that you store your data in multiple partitions and avoid storing important files within the partition that contains the entire operating system. If you fall into a situation whereby you cannot boot the system and are forced to format the disk on which the operating system is installed (in most cases, this is where malware infections hide), you will lose all data stored within that drive. This is the advantage of having multiple partitions: if you have the entire storage device assigned to a single partition, you will be forced to delete everything, however, creating multiple partitions and allocating the data properly allows you to prevent such problems. You can easily format a single partition without affecting the others - therefore, one will be cleaned and the others will remain untouched, and your data will be saved. Managing partitions is quite simple and you can find all the necessary information on Microsoft's documentation web page.

Data backups: One of the most reliable backup methods is to use an external storage device and keep it unplugged. Copy your data to an external hard drive, flash (thumb) drive, SSD, HDD, or any other storage device, unplug it and store it in a dry place away from the sun and extreme temperatures. This method is, however, quite inefficient, since data backups and updates need to be made regularly. You can also use a cloud service or remote server. Here, an internet connection is required and there is always the chance of a security breach, although it's a really rare occasion.

We recommend using Microsoft OneDrive for backing up your files. OneDrive lets you store your personal files and data in the cloud, sync files across computers and mobile devices, allowing you to access and edit your files from all of your Windows devices. OneDrive lets you save, share and preview files, access download history, move, delete, and rename files, as well as create new folders, and much more.

You can back up your most important folders and files on your PC (your Desktop, Documents, and Pictures folders). Some of OneDrive’s more notable features include file versioning, which keeps older versions of files for up to 30 days. OneDrive features a recycling bin in which all of your deleted files are stored for a limited time. Deleted files are not counted as part of the user’s allocation.

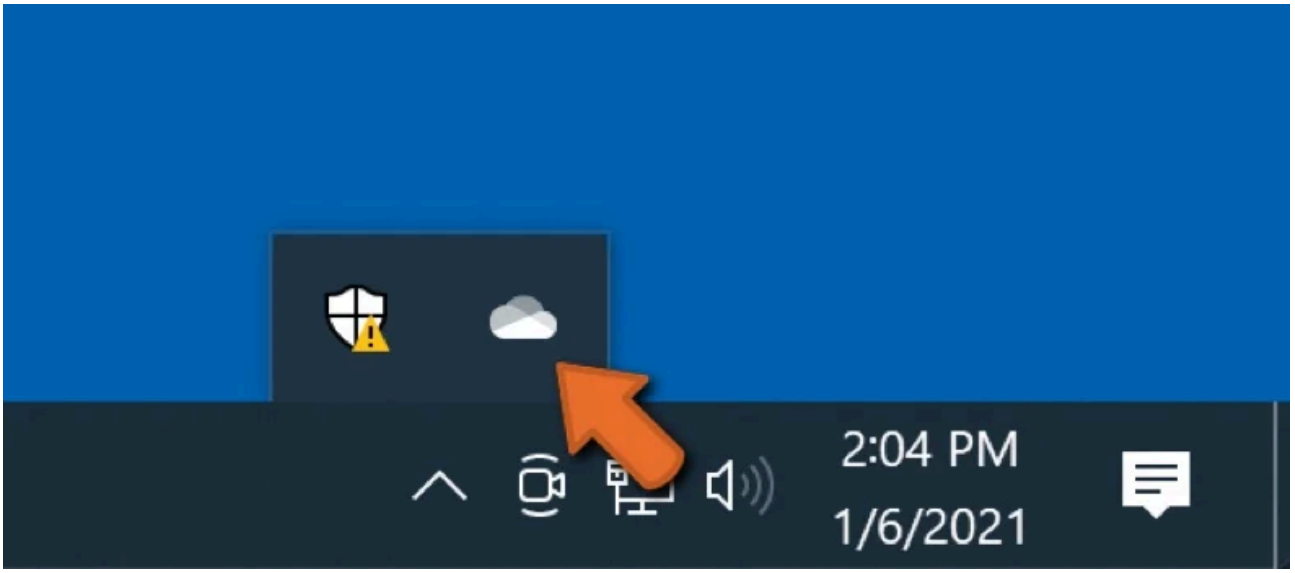
The service is built using HTML5 technologies and allows you to upload files up to 300 MB via drag and drop into the web browser or up to 10 GB via the OneDrive desktop application. With OneDrive, you can download entire folders as a single ZIP file with up to 10,000 files, although it can’t exceed 15 GB per single download.

OneDrive comes with 5 GB of free storage out of the box, with an additional 100 GB, 1 TB, and 6 TB storage options available for a subscription-based fee. You can get one of these storage plans by either purchasing additional storage separately or with Office 365 subscription.

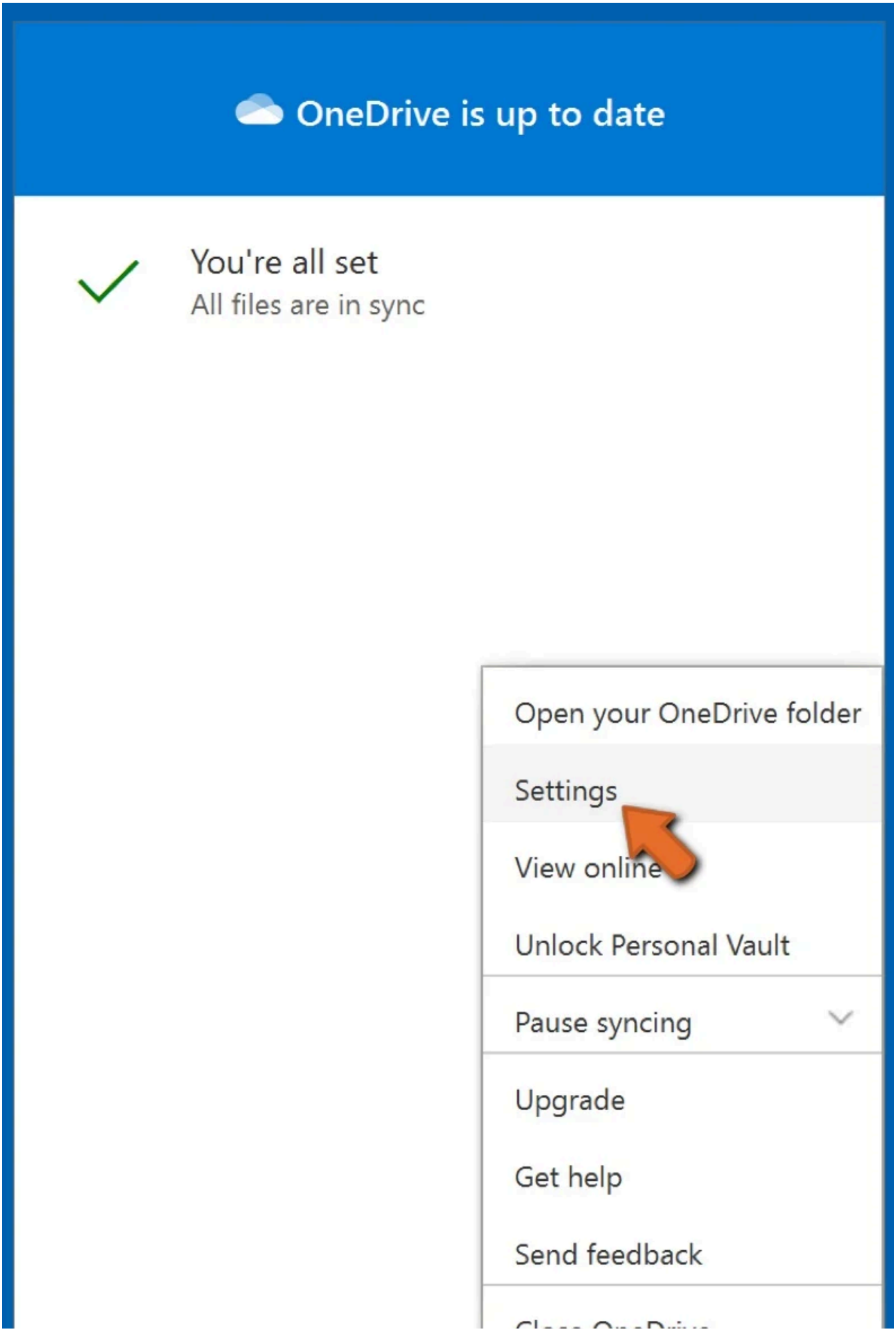
Creating a data backup:

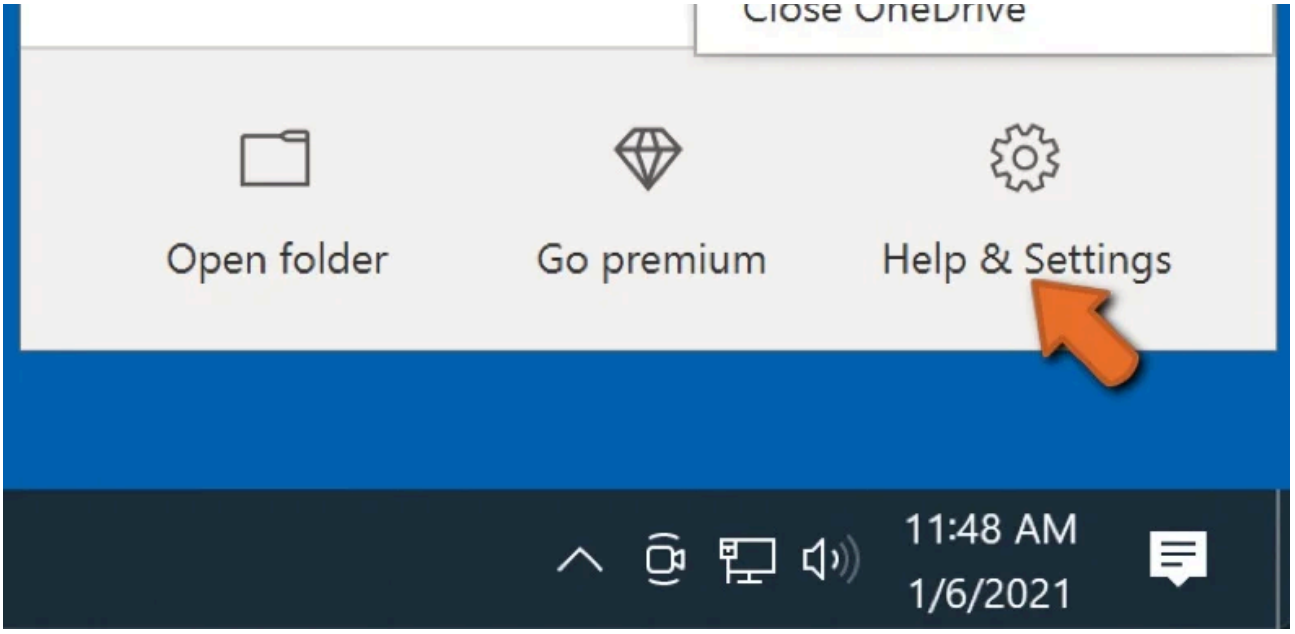
The backup process is the same for all file types and folders. Here’s how you can back up your files using Microsoft OneDrive

Step 1: Choose the files/folders you want to backup.

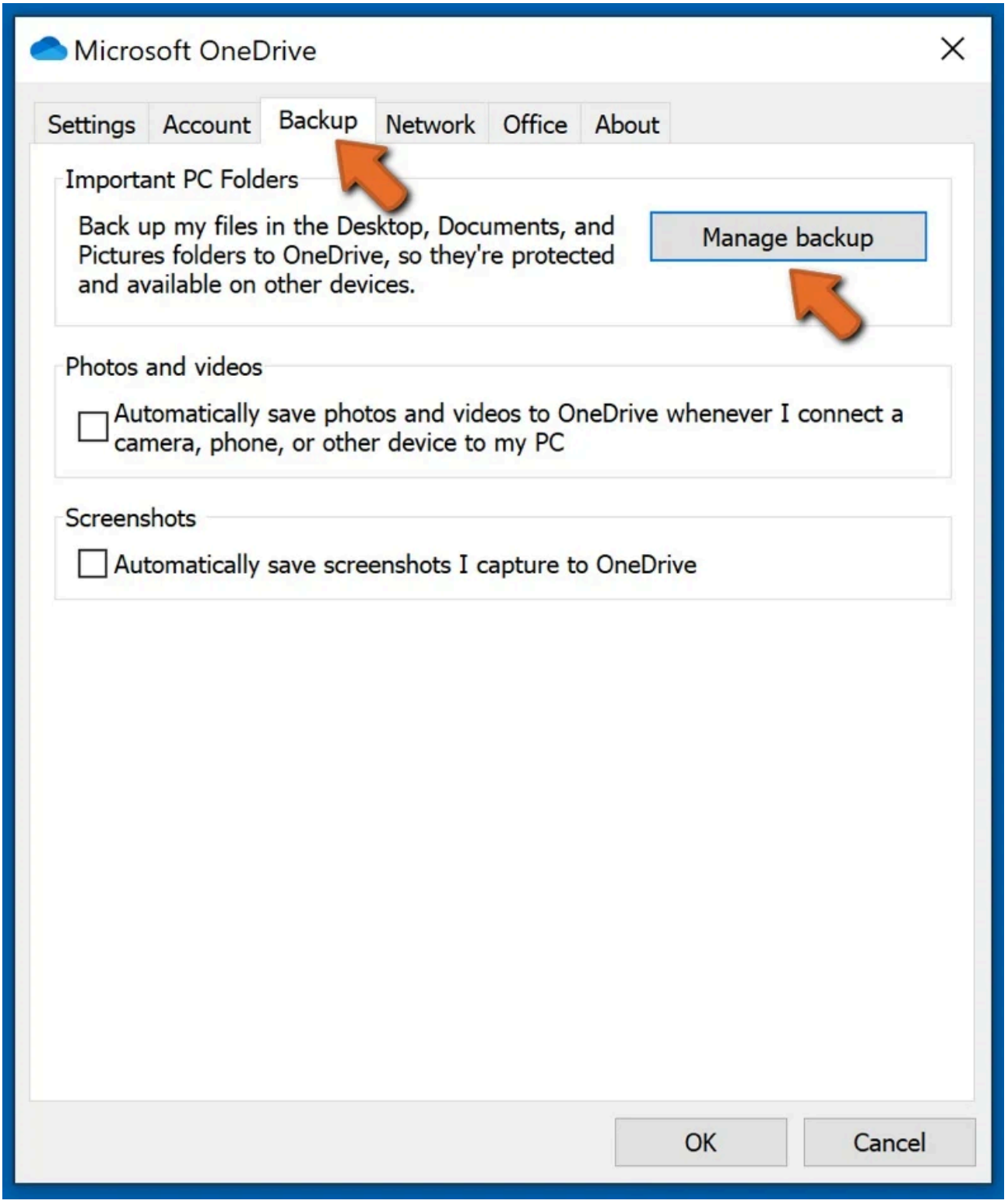


Click the **OneDrive cloud icon** to open the **OneDrive menu**. While in this menu, you can customize your file backup settings.

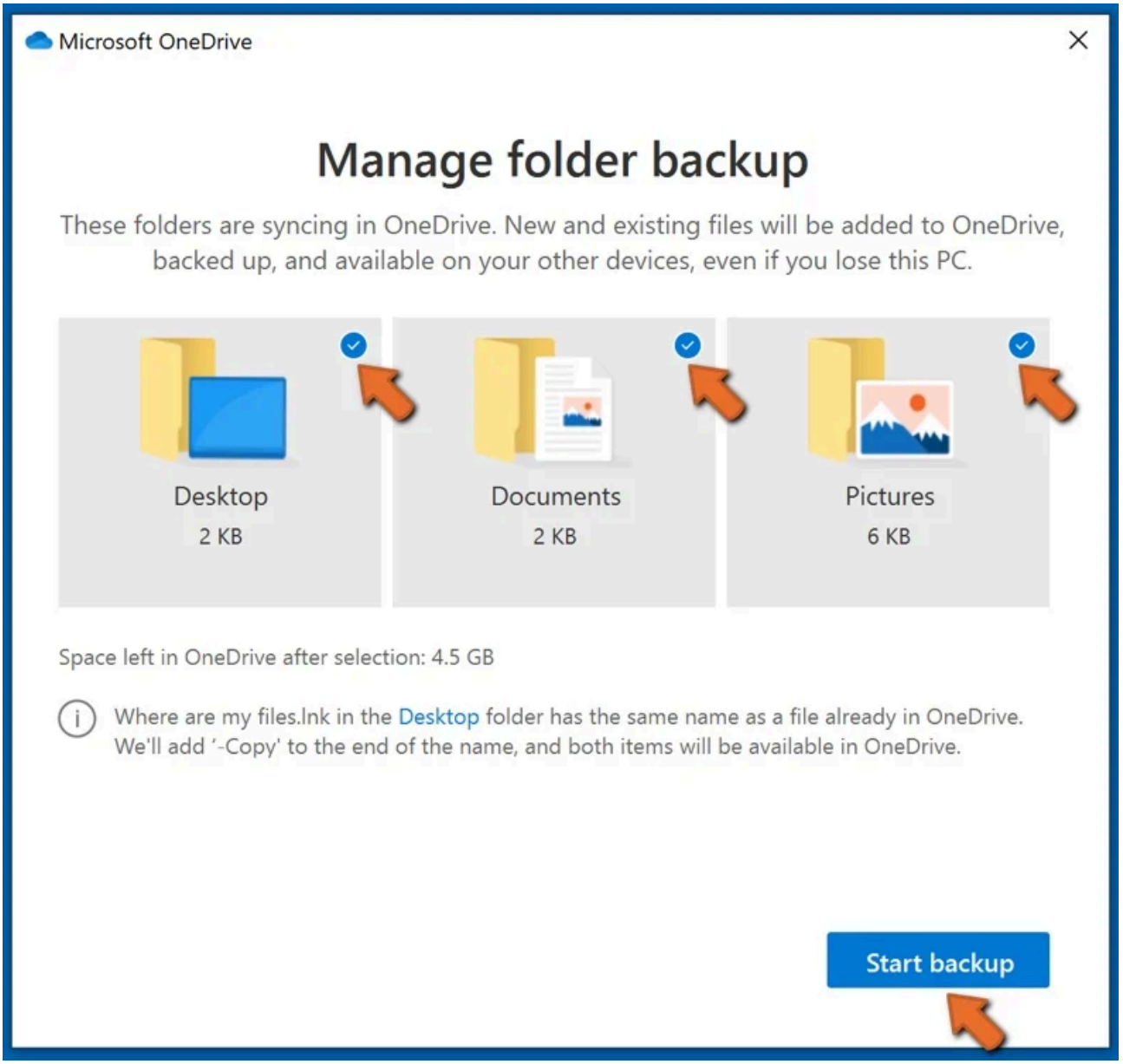

OneDrive is up to date
You're all set
All files are in sync
Open your OneDrive folder
Settings
View online
Unlock Personal Vault
Pause syncing
Upgrade
Get help
Send feedback



Click **Help & Settings** and then select **Settings** from the drop-down menu.



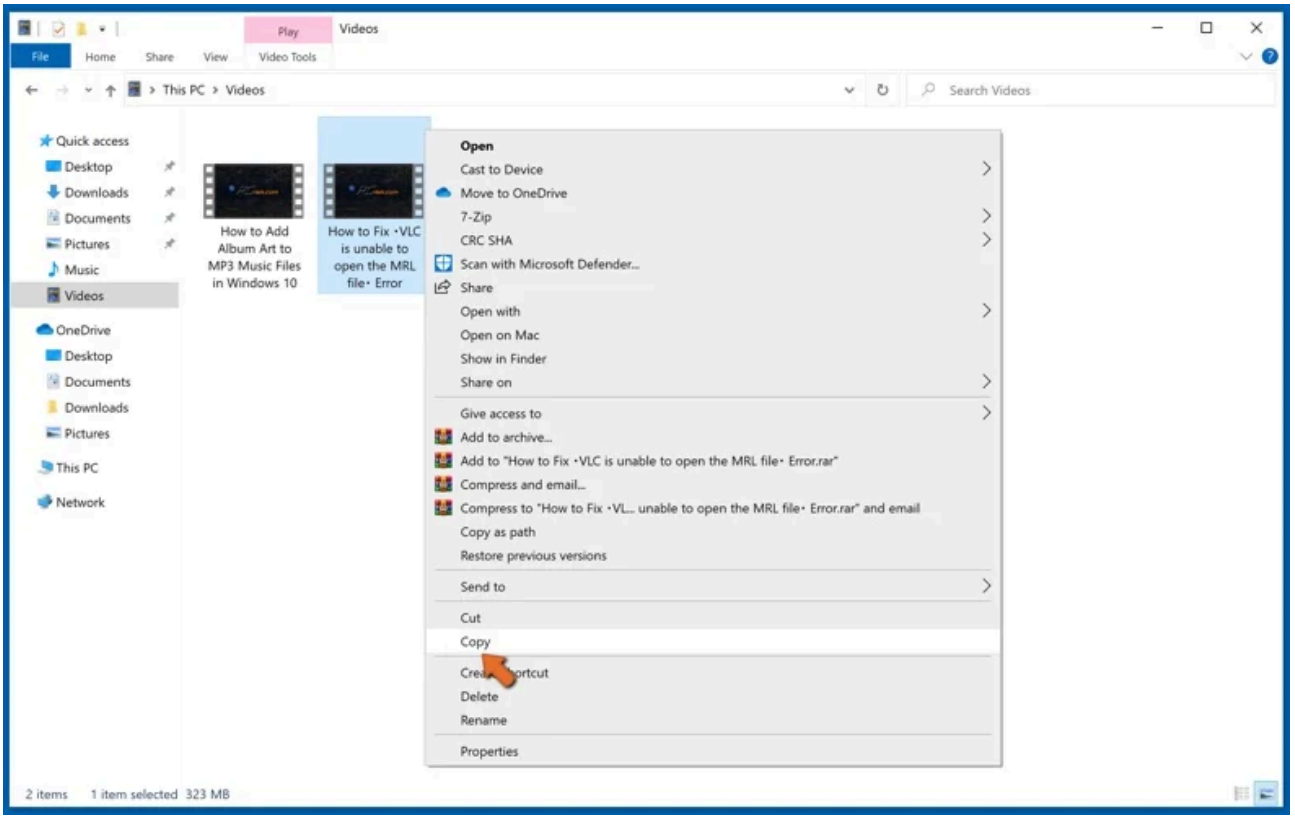
Go to the **Backup tab** and click **Manage backup**.



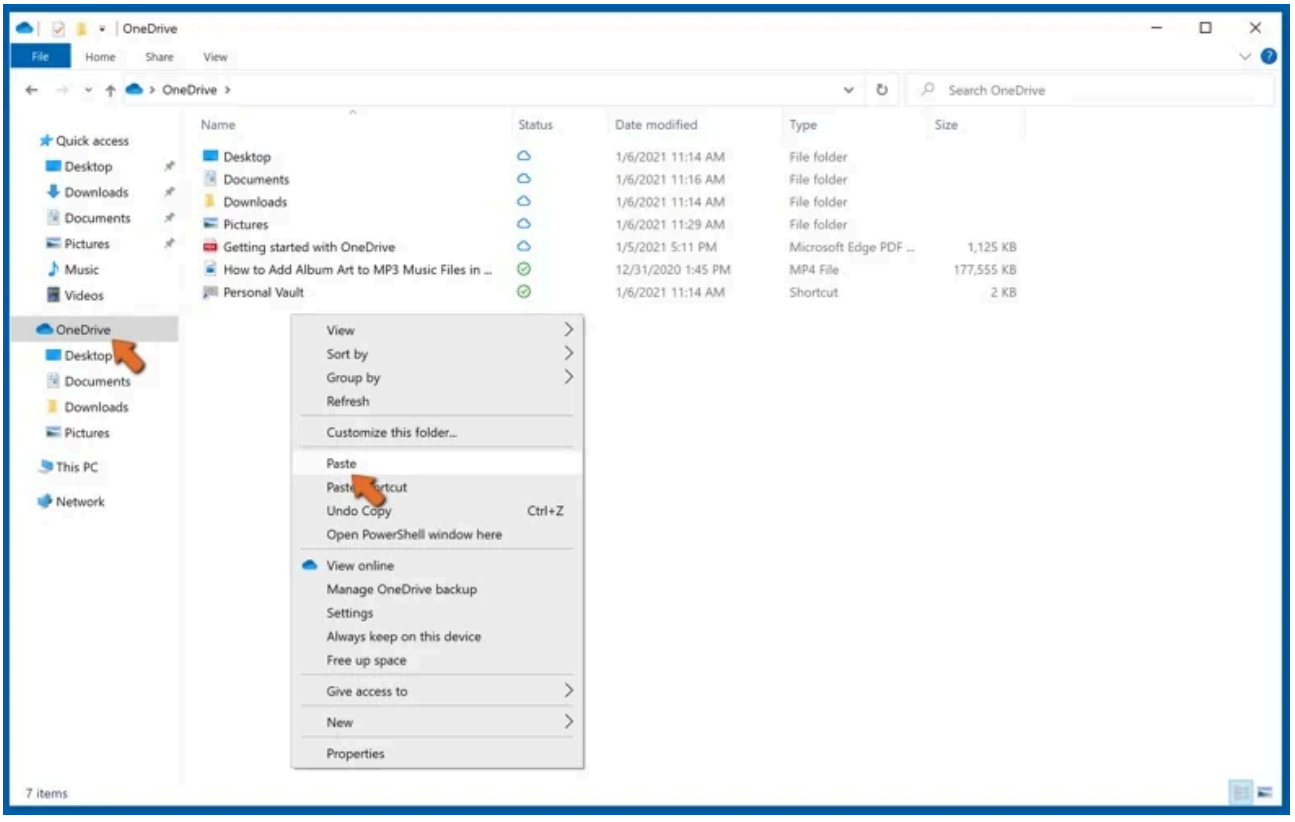
In this menu, you can choose to backup the **Desktop** and all of the files on it, and **Documents** and **Pictures** folders, again, with all of the files in them. Click **Start backup**.

Now, when you add a file or folder in the Desktop and Documents and Pictures folders, they will be automatically backed up on OneDrive.

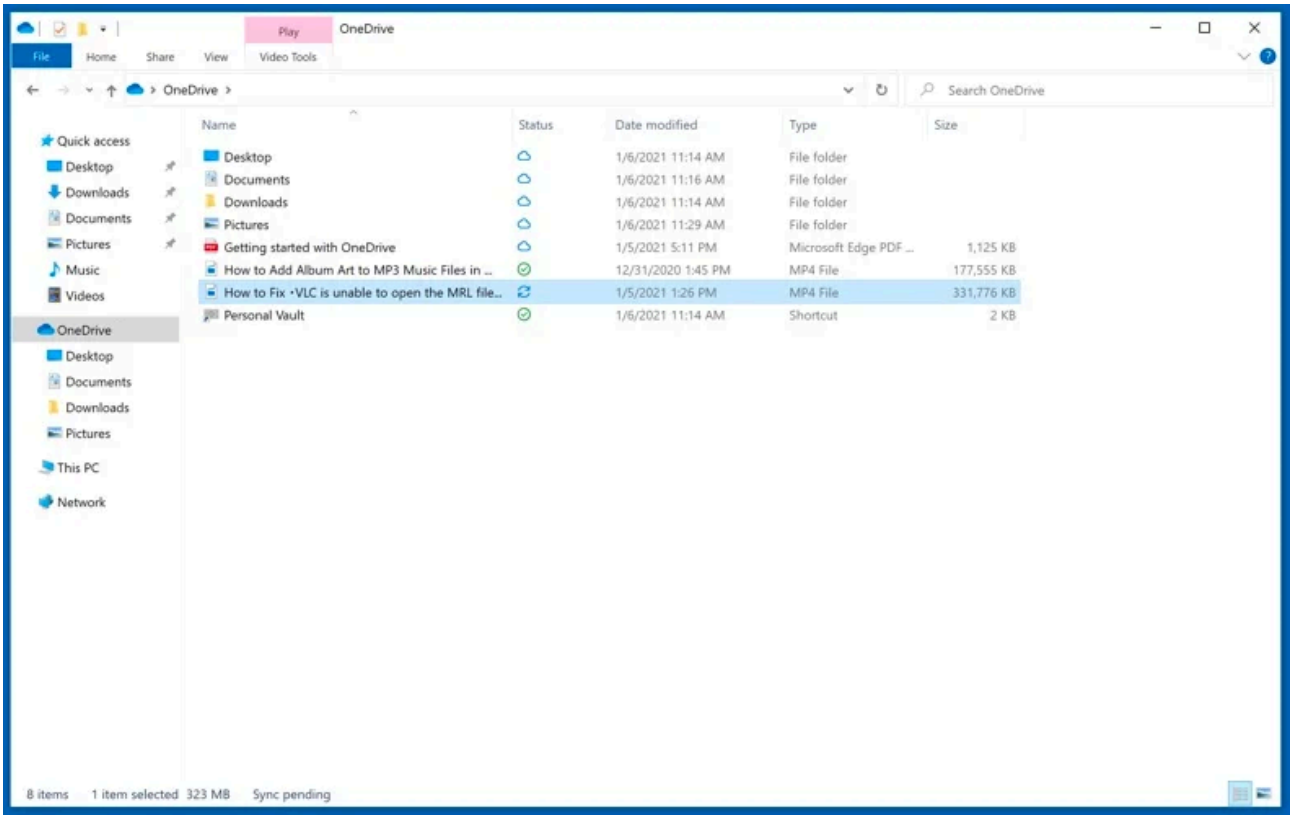
To add folders and files, not in the locations shown above, you have to add them manually.



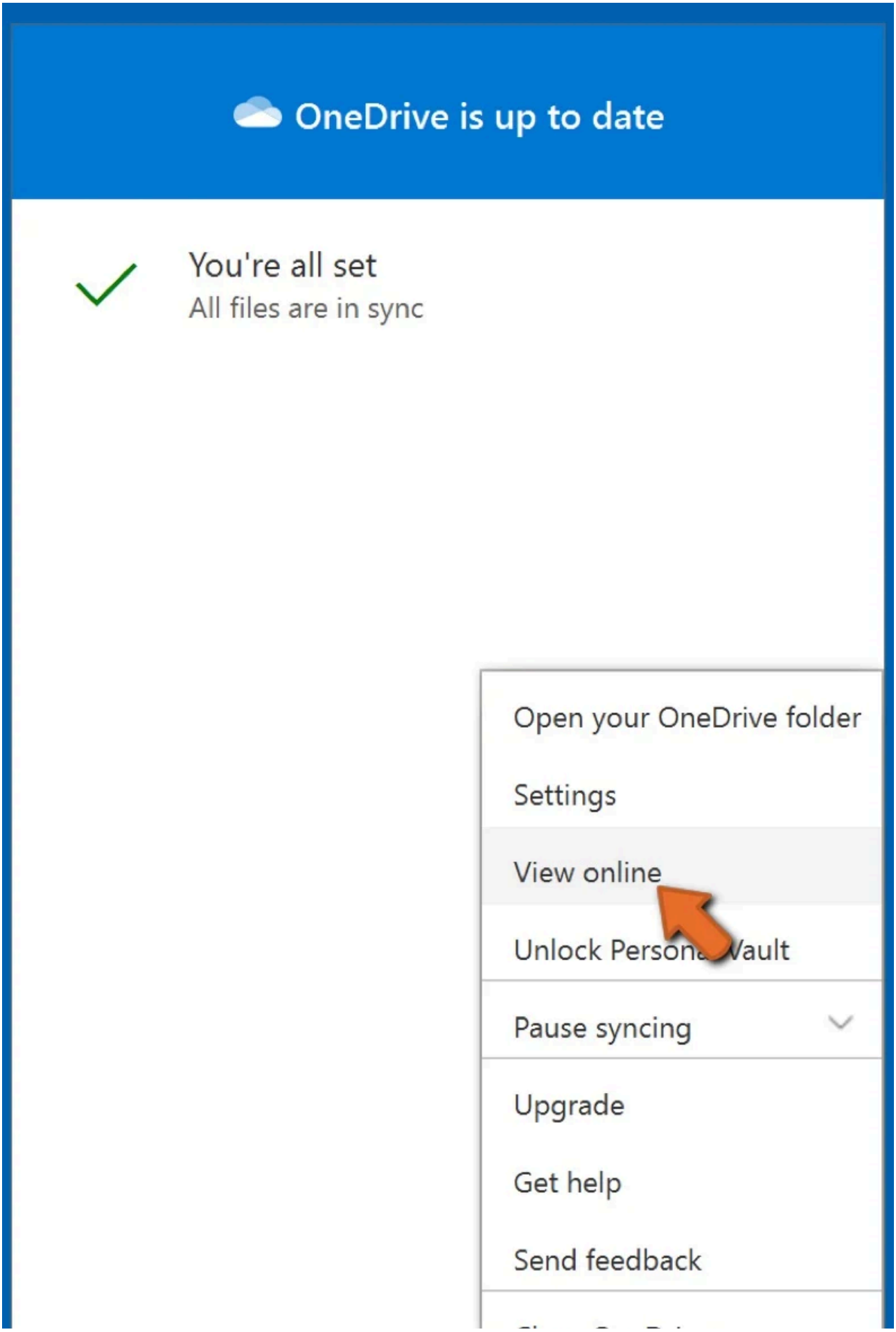
Open File Explorer and navigate to the location of the folder/file you want to backup. **Select the item, right-click it**, and click **Copy**.

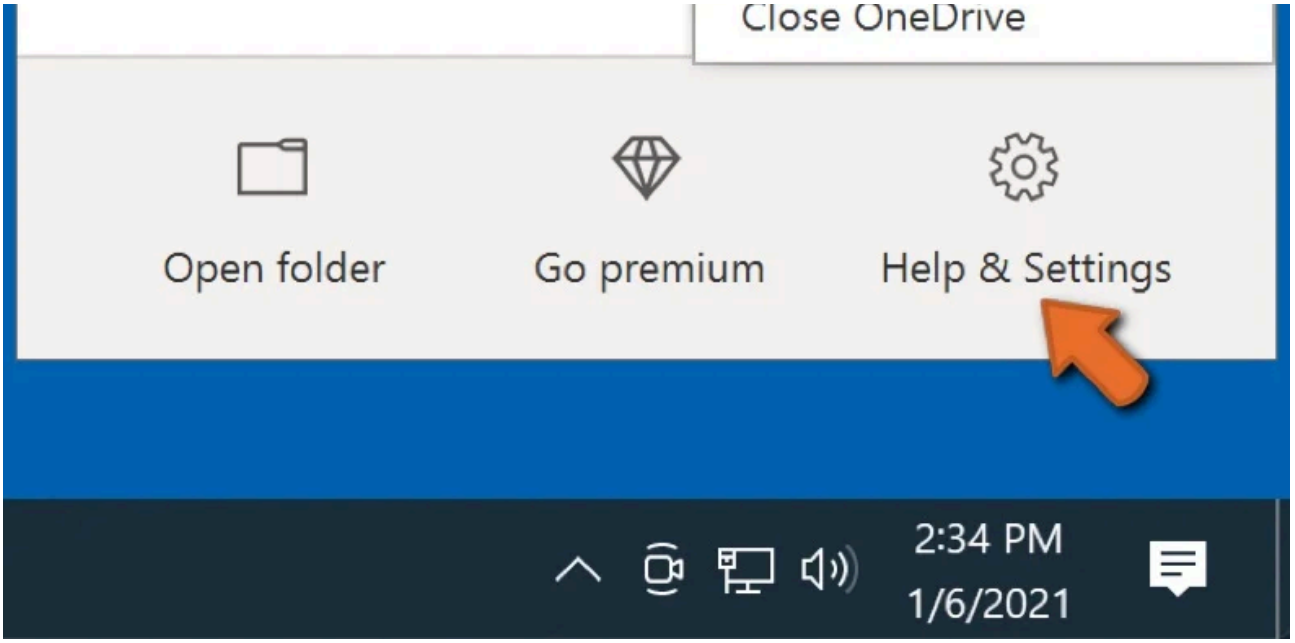


Then, **navigate to OneDrive, right-click** anywhere in the window and click **Paste**. Alternatively, you can just drag and drop a file into OneDrive. OneDrive will automatically create a backup of the folder/file.

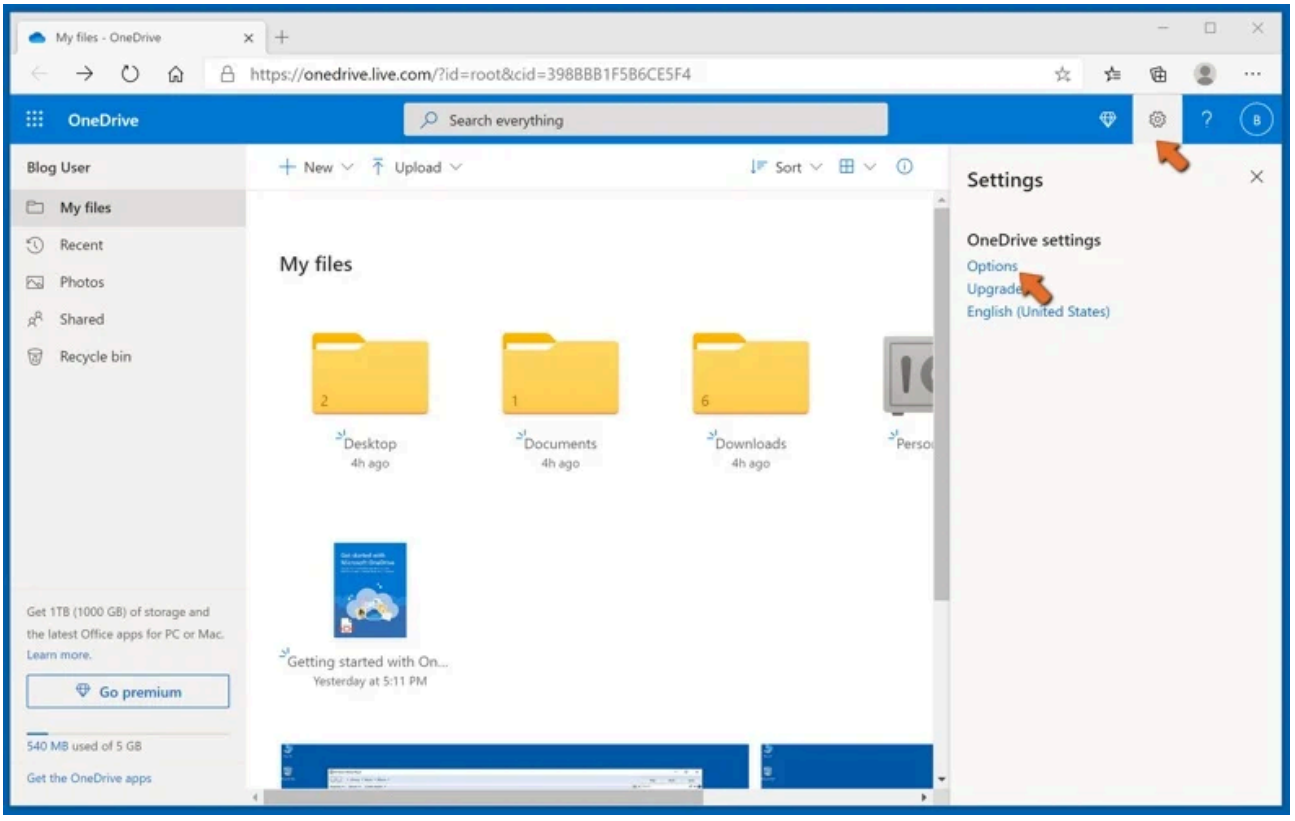


All of the files added to the OneDrive folder are backed up in the cloud automatically. The green circle with the checkmark in it indicates that the file is available both locally and on OneDrive and that the file version is the same on both. The blue cloud icon indicates that the file has not been synced and is available only on OneDrive. The sync icon indicates that the file is currently syncing.


OneDrive is up to date
You're all set
All files are in sync
Open your OneDrive folder
Settings
View online
Unlock Personal Vault
Pause syncing
Upgrade
Get help
Send feedback



To access files only located on OneDrive online, go to the **Help & Settings** drop-down menu and select **View online**.

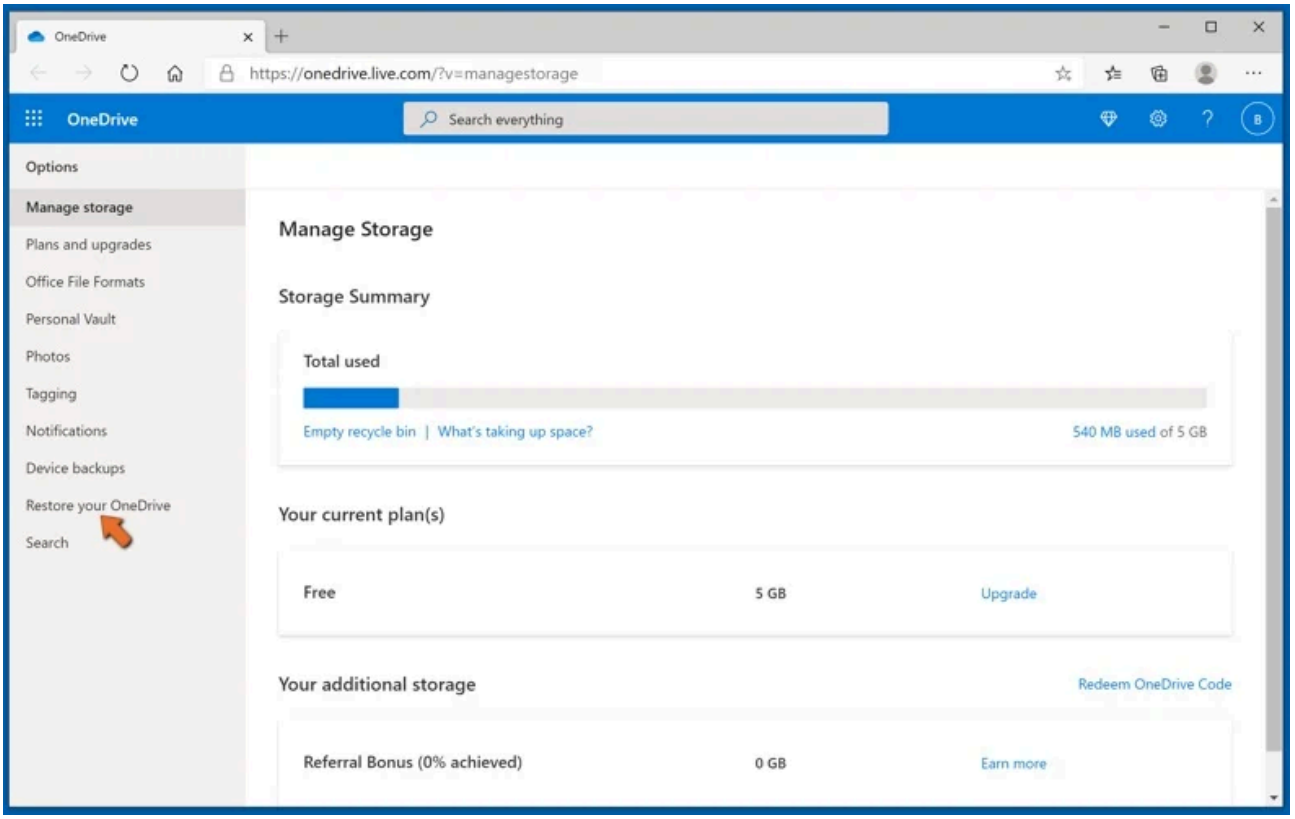


Step 2: Restore corrupted files.

OneDrive makes sure that the files stay in sync, so the version of the file on the computer is the same version on the cloud. However, if ransomware has encrypted your files, you can take advantage of **OneDrive's Version history** feature that will allow you to **restore the file versions prior to encryption**.

Microsoft 365 has a ransomware detection feature that notifies you when your OneDrive files have been attacked and guide you through the process of restoring your files. It must be noted, however, that if you don’t have a paid Microsoft 365 subscription, you only get one detection and file recovery for free.

If your OneDrive files get deleted, corrupted, or infected by malware, you can restore your entire OneDrive to a previous state. Here’s how you can restore your entire OneDrive:



1. If you're signed in with a personal account, click the **Settings cog** at the top of the page. Then, click **Options** and select **Restore your OneDrive**.

If you're signed in with a work or school account, click the **Settings cog** at the top of the page. Then, click **Restore your OneDrive**.

2. On the Restore your OneDrive page, **select a date from the drop-down list**. Note that if you're restoring your files after automatic ransomware detection, a restore date will be selected for you.

3. After configuring all of the file restoration options, click **Restore** to undo all the activities you selected.

The best way to avoid damage from ransomware infections is to maintain regular up-to-date backups.

Source: https://www.pcrisk.com/removal-guides/16844-harma-ouroboros-ransomware