

FORCE (.FORCE) ransomware virus – removal and decryption options

 pcrisk.com/removal-guides/29391-force-ransomware

Tomas Meskauskas

Also Known As: **FORCE virus**

Type: **Ransomware**

Damage level: 



Written by [Tomas Meskauskas](#) on April 04, 2024 (updated)

▼ **REMOVE IT NOW (Mac)**. Get free scan and check if your computer is infected.

To use full-featured product, you have to purchase a license for Combo Cleaner. Limited seven days free trial available. Combo Cleaner is owned and operated by Rcs Lt, the parent company of PCRisk.com [read more](#).

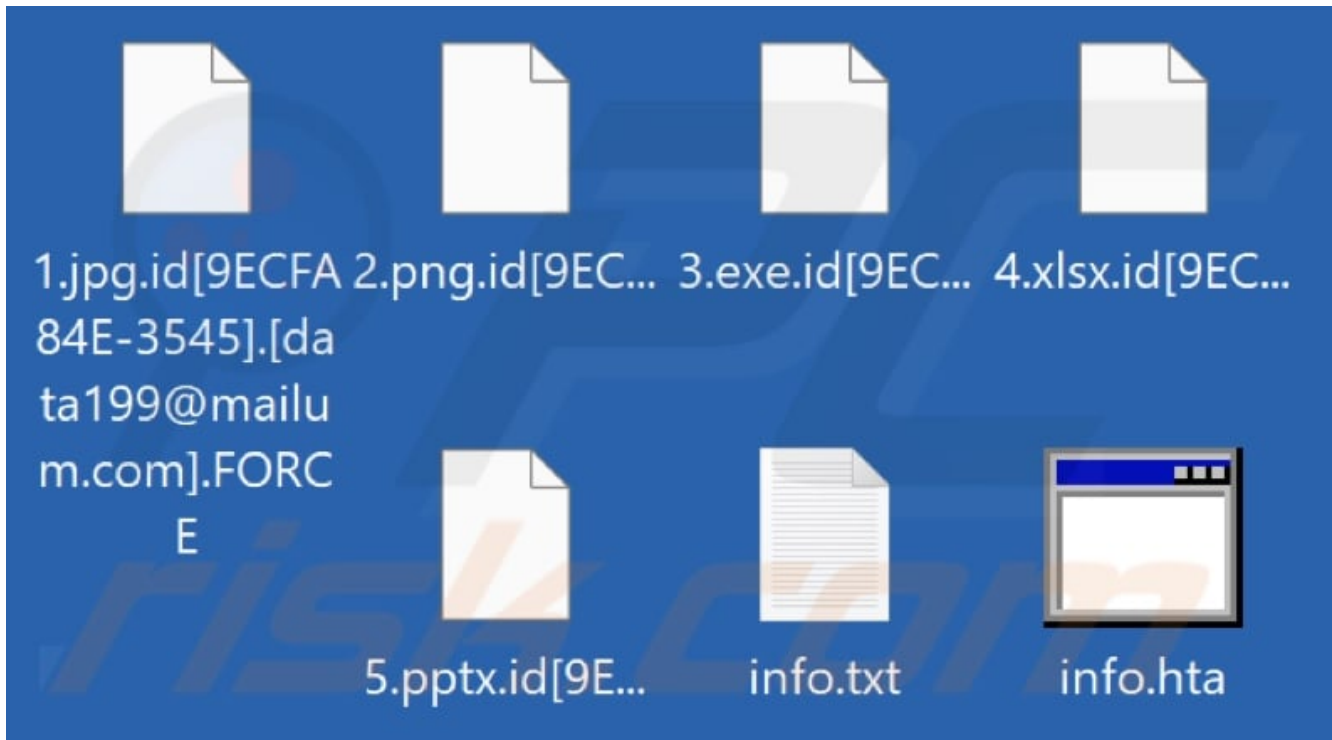
What kind of malware is FORCE?

Our researchers discovered the FORCE [ransomware-type program](#) during a routine review of new submissions to [VirusTotal](#). It is part of the [Phobos ransomware family](#).

On our test system, FORCE encrypted files and demanded payment for the decryption. The filenames of locked files were appended with a unique ID assigned to the victim, the cyber criminals' email address, and a ".FORCE" extension. For example, a file named "1.jpg" appeared as "1.jpg.id[9ECFA84E-3545].[data199@mailum.com].FORCE".

After the encryption process was completed, identical ransom notes were created – a pop-up ("info.hta") and a text file ("info.txt"). These messages were dropped onto the desktop and into all encrypted directories.

Screenshot of files encrypted by FORCE ransomware:



Ransom note overview

FORCE's ransom notes state that the victim's files were encrypted and vulnerable data was stolen. Decryption will require paying a ransom in Bitcoin cryptocurrency. If the victim does not meet these demands – the exfiltrated information will be sold. Prior to paying, the victim can test decryption for free (within certain limitations).

These messages warn against modifying the compromised files or using third-party recovery tools, as that may render the data undecryptable. Additionally, the victim is alerted that seeking aid from third-parties will increase their financial loss.

FORCE ransomware overview

This malicious program belongs to the Phobos ransomware family. Malware from this group does not render infected machines inoperable since they do not encrypt critical system files. These programs lock both local and network-shared files. They also end processes associated with open files (e.g., database programs, text file readers, etc.), thus ensuring no encryption exemptions due to files being considered "in use".

Phobos programs follow an exclusion list that includes popular ransomware so as to avoid double encryption (i.e., files locked by listed software remain unaffected). One recovery option is eliminated by Phobos deleting the Volume Shadow Copies.

This malware ensures persistence by copying itself to the %LOCALAPPDATA% path and registering with specific Run keys, as well as automatically starting upon each system reboot. The victim's geolocation data might determine whether this ransomware goes through with an attack. To elaborate, devices located in economically weak regions or ones in geopolitically-aligned countries could be excluded.

Based on our considerable experience researching ransomware infections, we can conclude that decryption is usually impossible without the cyber criminals' interference.

Furthermore, despite meeting the ransom demands – victims often do not receive the promised decryption keys/software. Therefore, we strongly advise against it since data recovery is not guaranteed, and paying also supports this illegal activity.

While removing ransomware from the operating system will prevent it from encrypting more data – removal will not restore already compromised files. The only solution is to recover them from a backup (if one is available).

The general advice for ensuring data safety is to keep backups in multiple different locations, such as remote servers, unplugged storage devices, and others.

Ransomware examples

We have analyzed thousands of ransomware-type programs; Vook, Looy, Nacugunder, Kool, and Payuransom are merely some examples. While the mode of operation for this malware is practically identical, there are two significant differences. Ransomware can use different cryptographic algorithms (symmetric or asymmetric) to encrypt data.

Ransoms can also vary drastically. The sums can range from three to eight digits in USD, depending on the intended victims – home users vs. companies, organizations, institutions, or other large entities. Cyber criminals often demand that the ransoms be paid using difficult-to-trace methods (primarily cryptocurrencies), as that decreases the chances of prosecution and victims retrieving their funds.

How did ransomware infect my computer?

Programs from the Phobos family typically infiltrate systems via vulnerable RDP (Remote Desktop Protocol) services. These infections commonly involve brute-force and dictionary attacks. It is noteworthy that systems with poor credential management are susceptible to these attacks. Phobos programs can also disable firewalls.

However, FORCE could infiltrate devices using other techniques, and the same is true of the methods used to distribute this software.

Generally, cyber criminals use phishing and social engineering tactics to proliferate malware. Malicious software is usually disguised as or bundled with ordinary programs/media. These files can be archives (ZIP, RAR, etc.), executables (.exe, .run, etc.), documents (Microsoft Office, Microsoft OneNote, PDF, etc.), JavaScript, and so forth.

The most widely utilized distribution techniques include: malicious attachments/links in spam (e.g., emails, PMs/DMs, social media/ forum posts, etc.), online scams, drive-by (stealthy/deceptive) downloads, malvertising, dubious download channels (e.g., freeware and free file-hosting websites, Peer-to-Peer sharing networks, etc.), illegal software activation ("cracking") tools, and fake updates.

What is more, some malicious programs can self-proliferate via local networks and removable storage devices (e.g., external hard drives, USB flash drives, etc.).

Name	FORCE virus
Threat Type	Ransomware, Crypto Virus, Files locker
Encrypted Files Extension	.FORCE (files are also appended with a unique ID and the cyber criminals' email)
Ransom Demanding Message	info.hta, info.txt
Free Decryptor Available?	No
Cyber Criminal Contact	Tox chat, data199@mailum.com
Detection Names	Avast (Win32:Phobos-D [Ransom]), Combo Cleaner (Trojan.Ransom.PHU), ESET-NOD32 (A Variant Of Win32/Filecoder.Phobos.C), Kaspersky (HEUR:Trojan-Ransom.Win32.Phobos.vho), Microsoft (Ransom:Win32/Phobos.PM), 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.
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 (Mac)	To eliminate possible malware infections, scan your Mac with legitimate antivirus software. Our security researchers recommend using Combo Cleaner. ▼ Download Combo Cleaner for Mac To use full-featured product, you have to purchase a license for Combo Cleaner. Limited seven days free trial available. Combo Cleaner is owned and operated by Rcs Lt, the parent company of PCRisk.com read more .

Threat Summary:

How to protect yourself from ransomware infections?

We highly recommend being careful while browsing, as fraudulent and dangerous online content usually appears legitimate and harmless. Caution must be extended to incoming emails and other messages. Attachments or links present in suspicious/irrelevant mail must not be opened, as they can be virulent.

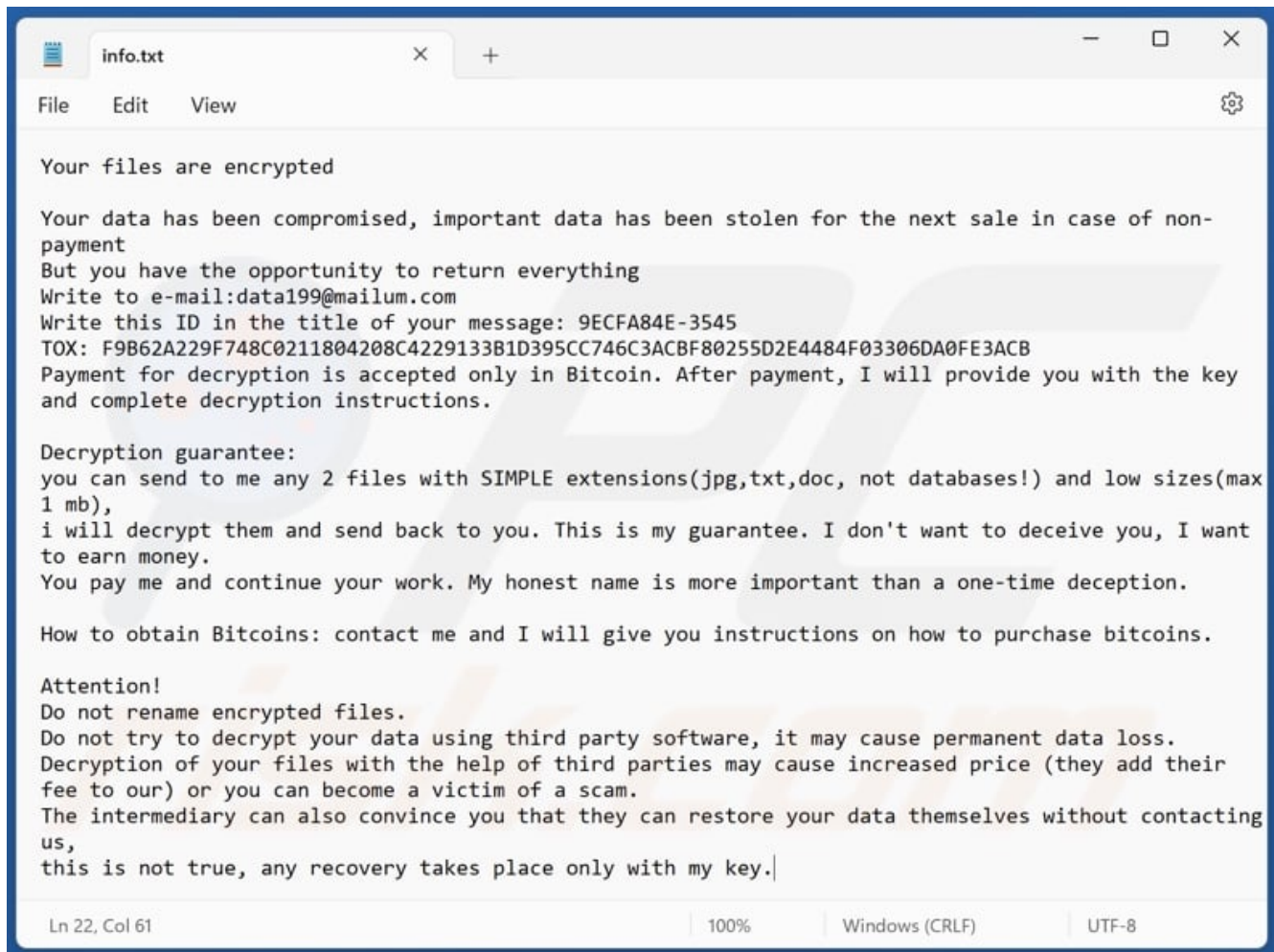
Furthermore, all downloads must be performed from official and verified sources. Another recommendation is to activate and update software using genuine functions/tools, as those obtained from third-parties can contain malware.

We strongly advise having a reputable anti-virus installed and kept updated. Security programs must be used to run regular system scans and to remove detected threats/issues. If your computer is already infected with FORCE, we recommend running a scan with Combo Cleaner Antivirus for macOS to automatically eliminate this ransomware.

Screenshot of FORCE ransomware's pop-up window ("info.hta"):



Screenshot of FORCE's text file ("info.txt"):



Text presented in the pop-up and text file:

Your files are encrypted.

Your data has been compromised, important data has been stolen for the next sale in case of non-payment. But you have the opportunity to return everything.

Write to e-mail: data199@mailum.com

Write this ID in the title of your message -

Or write us to the TOX messenger:

F9B62A229F748C0211804208C4229133B1D395CC746C3ACBF80255D2E4484F03306DA0FE3ACB

You can download TOX messenger here <https://tox.chat/>

Payment for decryption is accepted only in Bitcoin. After payment, I will provide you with the key and complete decryption instructions.

Free decryption as guarantee

Decryption guarantee: you can send to me any 2 files with SIMPLE extensions(jpg,txt,doc, not databases!) and low sizes(max 1 mb), i will decrypt them and send back to you. This is my guarantee.

I don't want to deceive you, I want to earn money. You pay me and continue your work. My honest name is more important than a one-time deception.

How to obtain Bitcoins

Contact me and I will give you instructions on how to purchase bitcoins.

Attention!

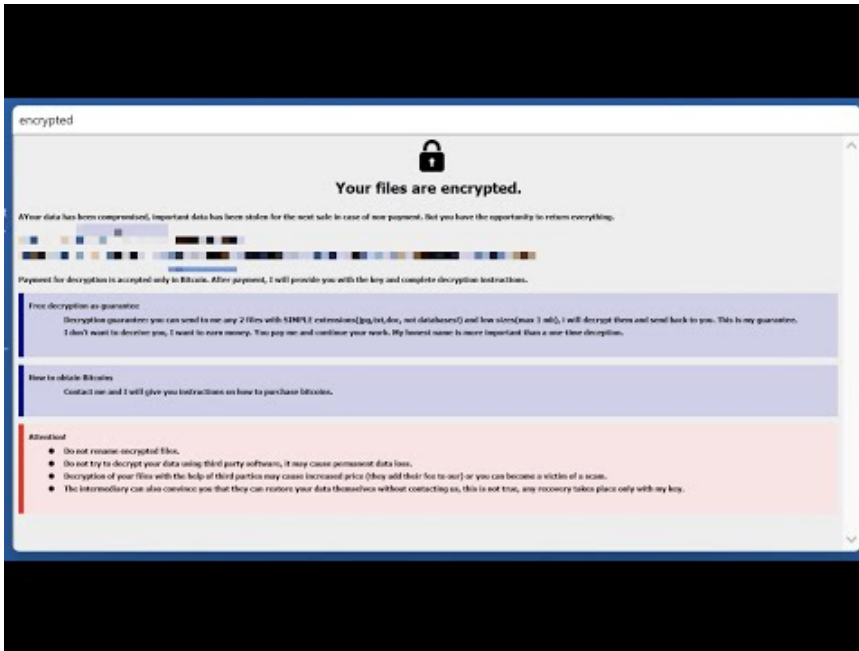
Do not rename encrypted files.

Do not try to decrypt your data using third party software, it may cause permanent data loss.

Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

The intermediary can also convince you that they can restore your data themselves without contacting us, this is not true, any recovery takes place only with my key.

Video showing how to remove FORCE ransomware using Combo Cleaner:



[Watch Video At:](#)

https://youtu.be/scW_JG2dv3Q

FORCE ransomware removal:

Instant automatic Mac 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 Mac malware. Download it by clicking the button below:
▼ DOWNLOAD Combo Cleaner for Mac 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. Limited seven days free trial available. Combo Cleaner is owned and operated by Rcs Lt, the parent company of PCRisk.com [read more](#).

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



Watch Video At:

<https://youtu.be/cMZ4apzfKjQ>

Quick menu:

- [What is FORCE 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):

-  **USA** - [Internet Crime Complaint Centre IC3](#)
-  **United Kingdom** - [Action Fraud](#)
-  **Spain** - [Policía Nacional](#)
-  **France** - [Ministère de l'Intérieur](#)
-  **Germany** - [Polizei](#)
-  **Italy** - [Polizia di Stato](#)
-  **The Netherlands** - [Politie](#)
-  **Poland** - [Policja](#)
-  **Portugal** - [Policía Judiciária](#)

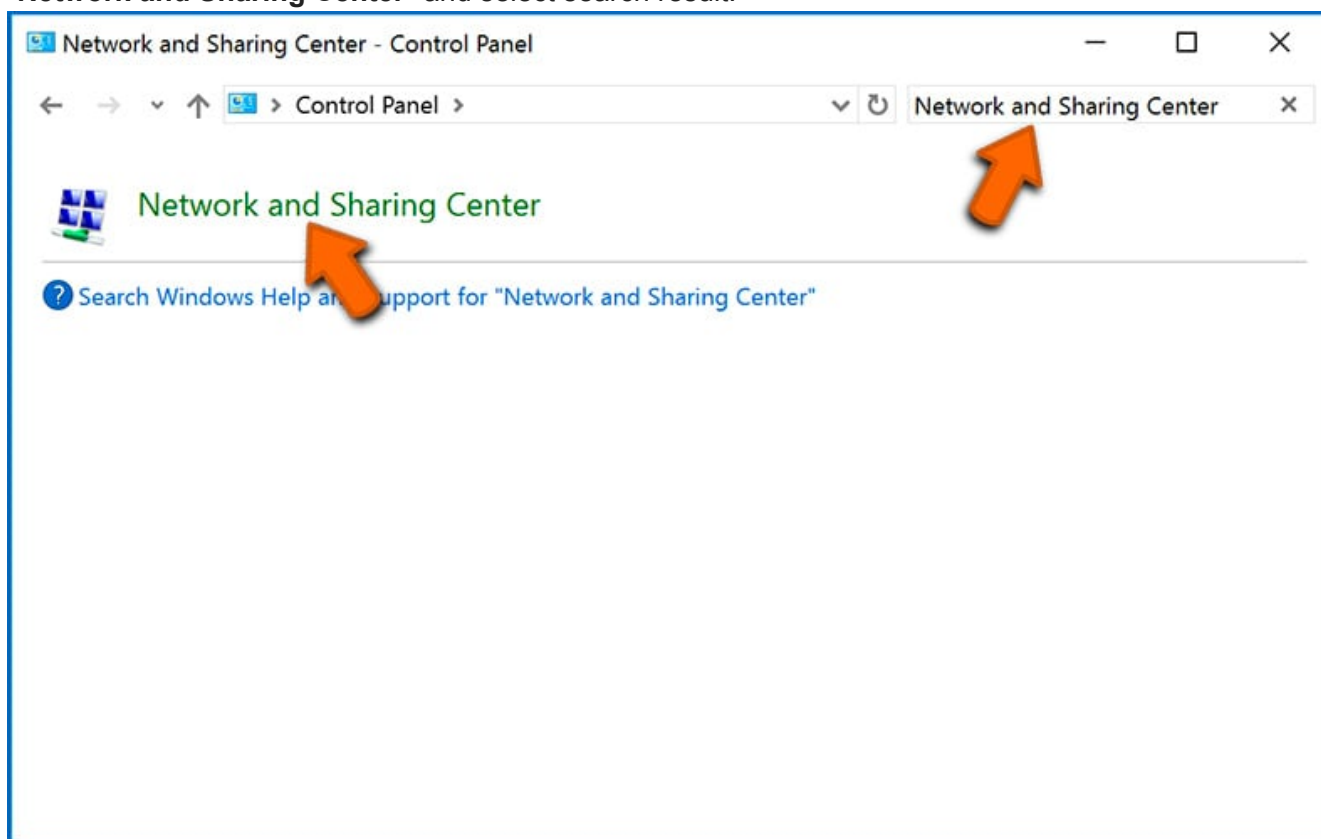
Isolating the infected device:

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.

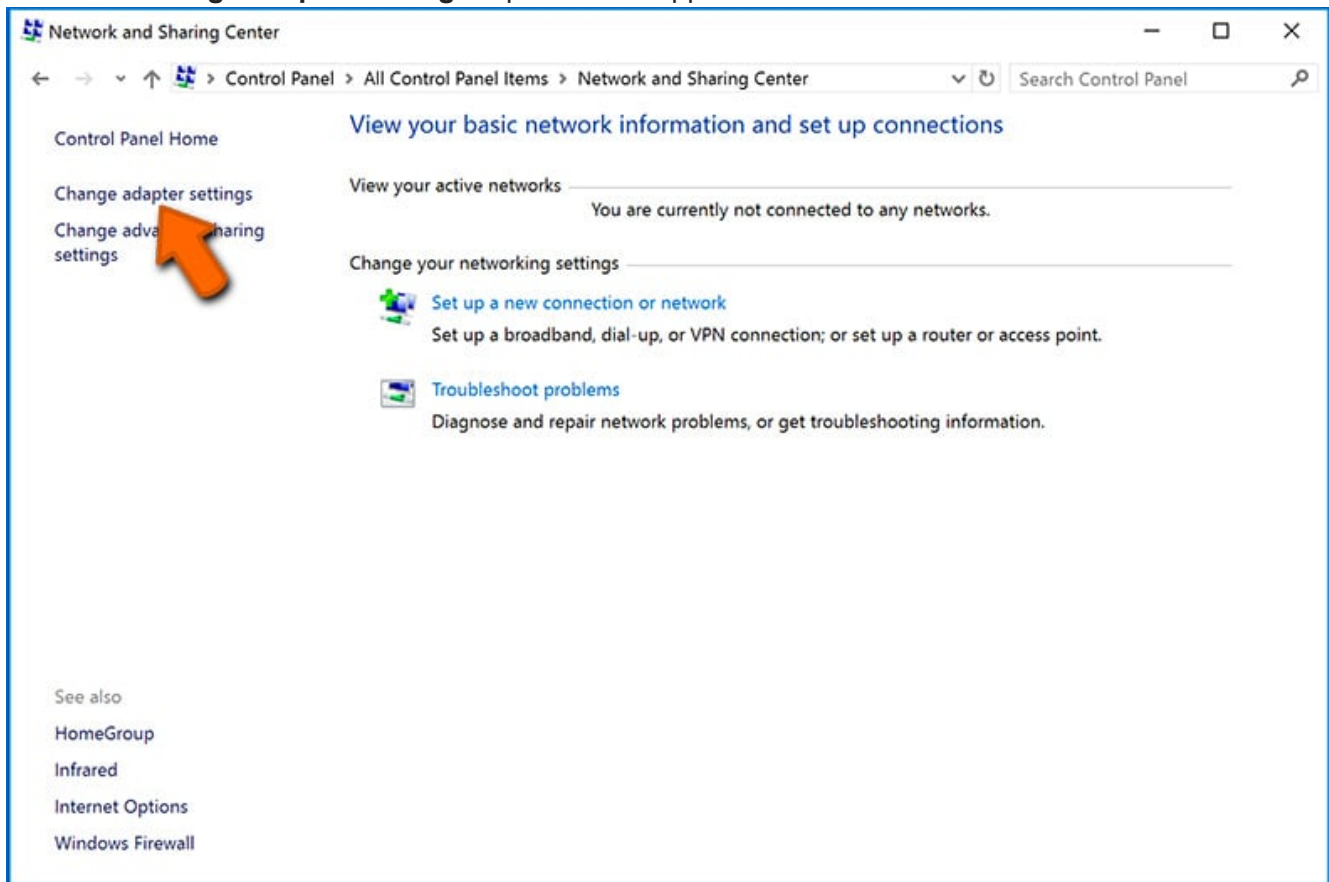
Step 1: Disconnect from the internet.

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:

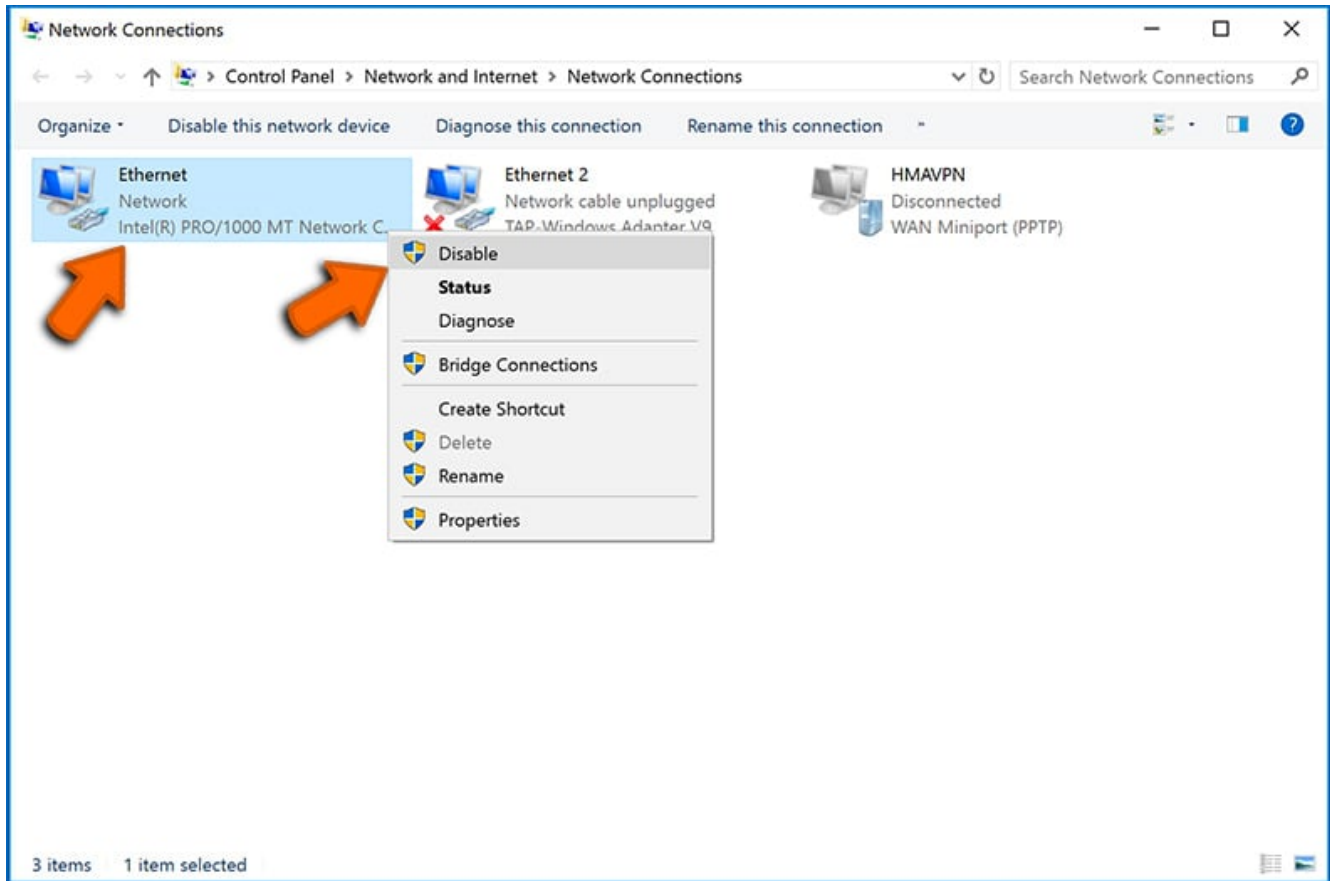
Navigate to the "**Control Panel**", click the search bar in the upper-right corner of the screen, enter "**Network and Sharing Center**" and select search result:



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



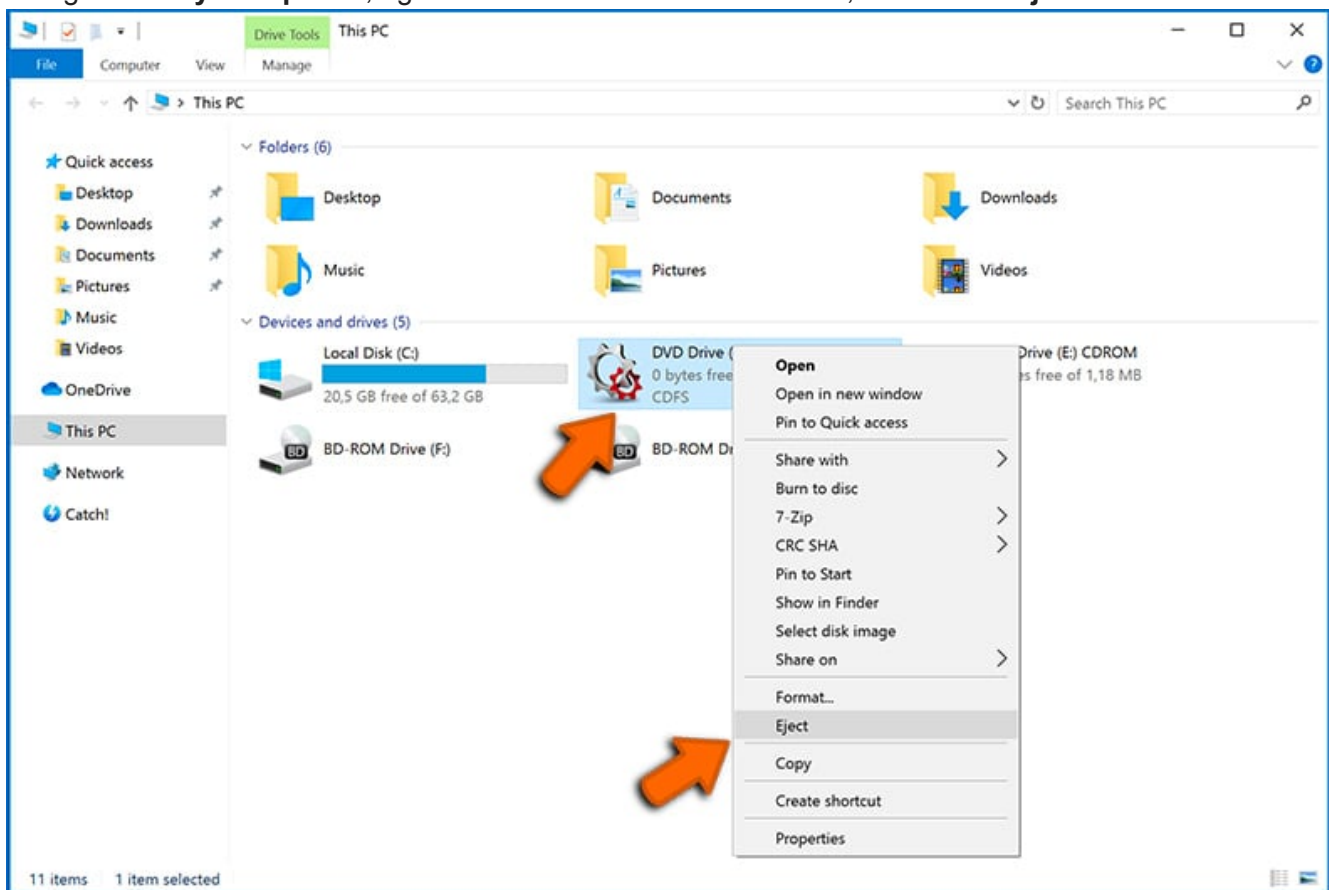
Right-click on each connection point and select "**Disable**". Once disabled, the system will no longer be connected to the internet. To re-enable the connection points, simply right-click again and select "**Enable**".



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).

```
READ_ME.txt - Notepad
File Edit Format View Help

[WALDO RANSOMWARE]

Oops!
Your computer has been infected by the Waldo Ransomware.
Your files have been encrypted to hex codes by AES and RSA algorithms.
The file extensions haven't changed, but the contents are encrypted.
They won't be recovered easily, but there is clearly a way to get them back.

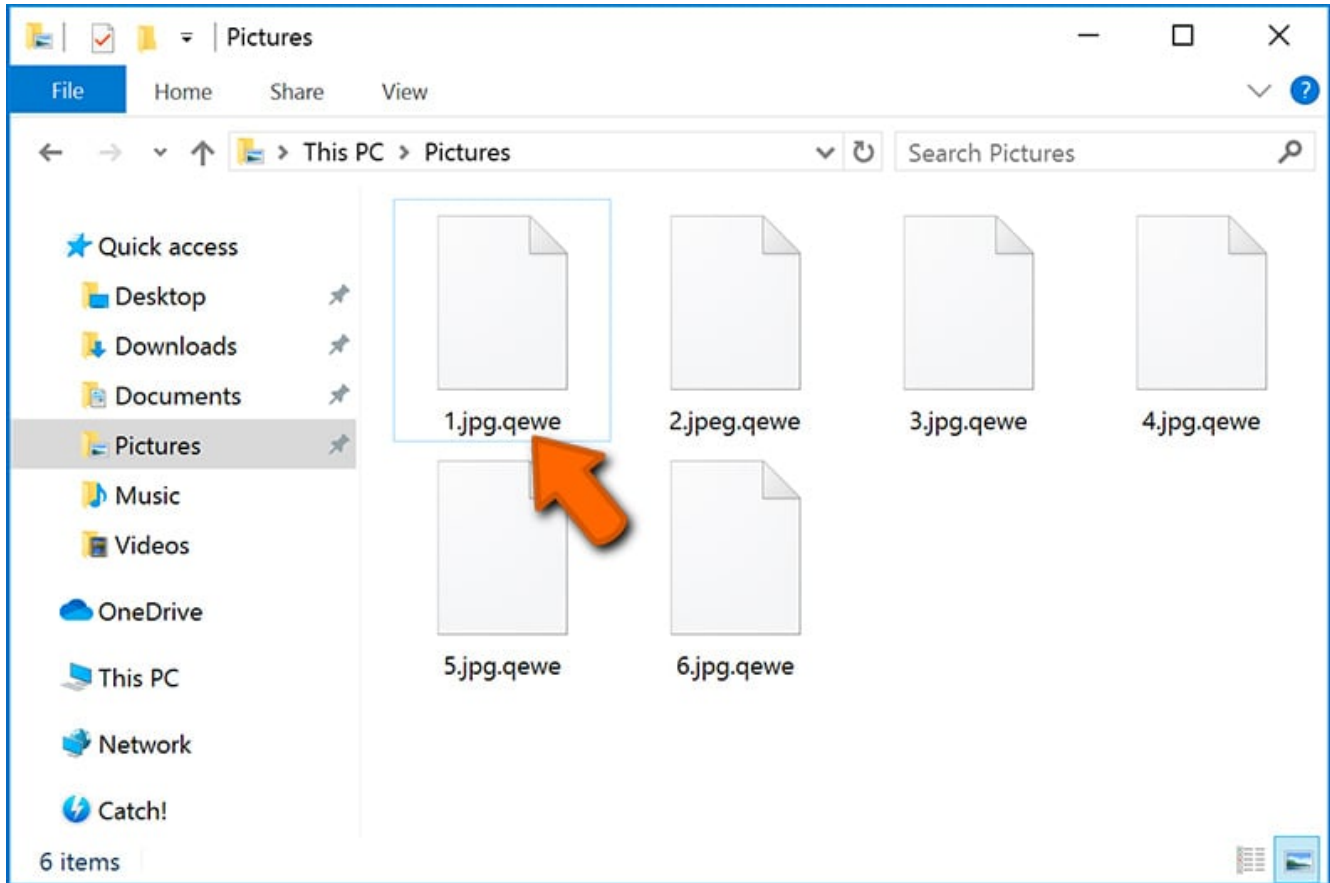
Contact me by email :
iamwaldo@tutamail.com

Your personal code :
5f149949b95d202c62c9e3c8c06f4d59c5dda8da0603de0c5e404785f02572ac47ba92d1b94fd0
2b3a9234a8dab64a87f0a12fcd7cfa9dfe7fb5b5610dba73c3dd0720b7683c2cd31396db55eff7f
8f5ce55076e277a665bb578dff9b90c62e56b222cf5562a29e92c2969d1951974e4e7147ce3698d
ce38b4b926f380af7993

You can't get your files back if you lose your personal code.
Good Luck!
```

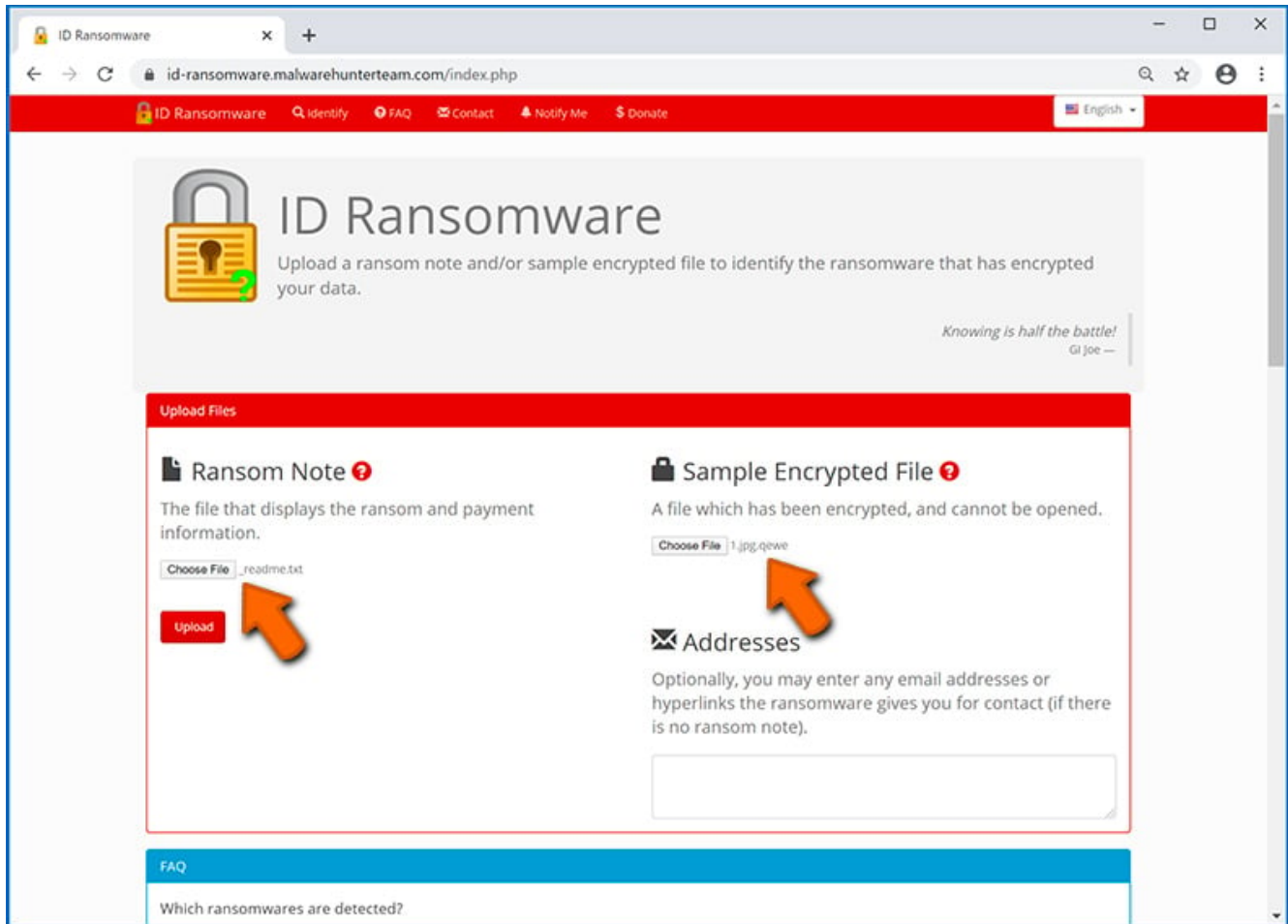
This, however, is rare. In most cases, ransomware infections deliver more direct messages simply stating that data is encrypted and that victims must pay some sort of ransom. Note that ransomware-type infections typically generate messages with different file names (for example, "**_readme.txt**", "**READ-ME.txt**", "**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):


ID Ransomware
 Upload a ransom note and/or sample encrypted file to identify the ransomware that has encrypted your data.

Knowing is half the battle!
— GI Joe —

⚠ Warning: SMB port 445 was found to be exposed on your IP! This is a commonly exploited service for ransomware and other malware.
 * Data provided by Shodan.

1 Result

STOP (Djvu)

⚠ This ransomware may be decryptable under certain circumstances.

Please refer to the appropriate guide for more information.


Identified by

- ransomnote_email: he1pdatastore@firemail1.cc
- sample_extension: .qevv
- sample_bytes: [0x1F9C - 0x1FC2]
0x783336413639384239204436374320344530372042453832203045433542313442344446357D

Click here for more information about STOP (Djvu)

Ransomware Got Past Your Antivirus?

Emsisoft Anti-Malware



100% PROTECTION.
DUAL VIRUS SCANNER.
FAST & THOROUGH.

FREE TRIAL

* This is an affiliate link, and I receive commission for purchases made. I do honestly recommend Emsisoft and their products even without this affiliation.

© Copyright 2020 MalwareHunterTeam. All rights reserved. App v1.9.13, Updated 04/27/2020
Coded by Demonslay335

Example 2 (.iso [Phobos] ransomware):

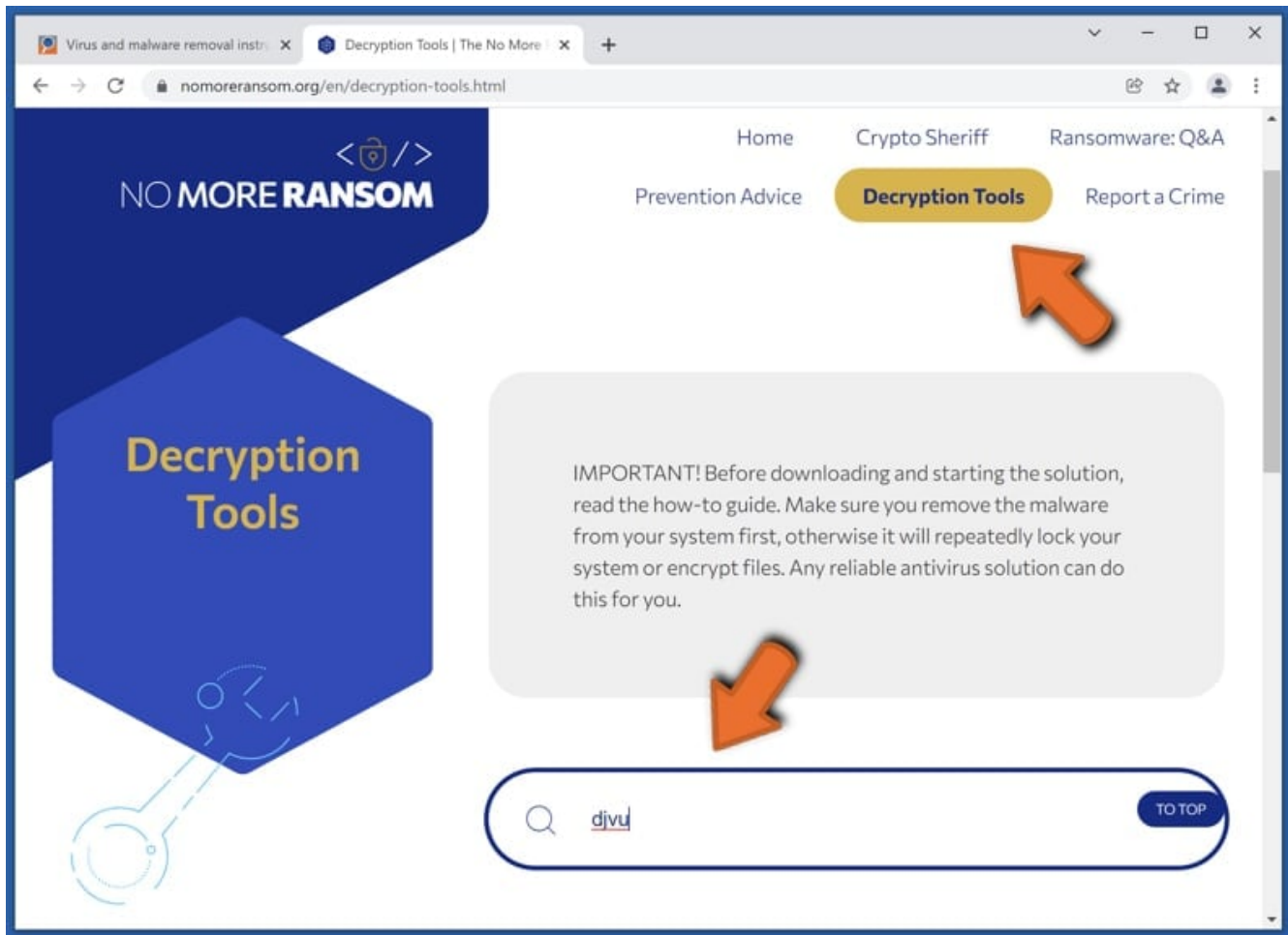
The screenshot shows a web browser window with the URL `id-ransomware.malwarehunterteam.com/identify.php?case=313d30808caec6c2b81ccb61ad532365b2c4bdb5`. The page header includes navigation links for 'Identify', 'FAQ', 'Contact', 'Notify Me', and 'Donate', along with a language selector set to 'English'. The main content area features a large padlock icon and the text 'ID Ransomware' with the instruction 'Upload a ransom note and/or sample encrypted file to identify the ransomware that has encrypted your data.' Below this, a search result for 'Phobos' is displayed. The result text states: 'This ransomware has no known way of decrypting data at this time. It is recommended to backup your encrypted files, and hope for a solution in the future.' It also identifies the ransomware as being identified by 'ransomnote_email: backup_iso@aol.com' and provides a link for more information. To the right of the result is an advertisement for 'Emsisoft Anti-Malware' with a 'FREE TRIAL' button. The footer contains copyright information for MalwareHunterTeam and version details for the application.

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.

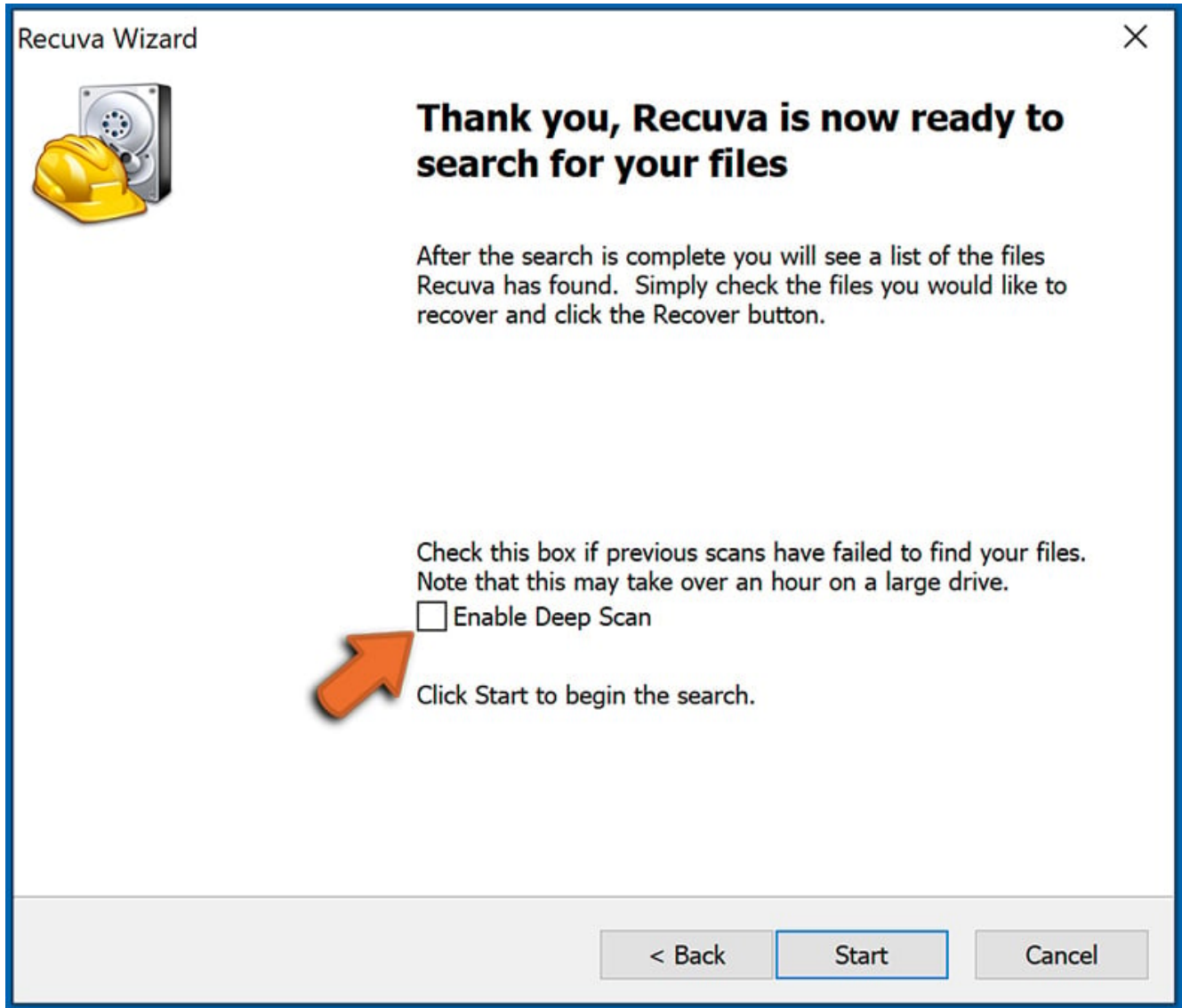


Restore files with data recovery tools:

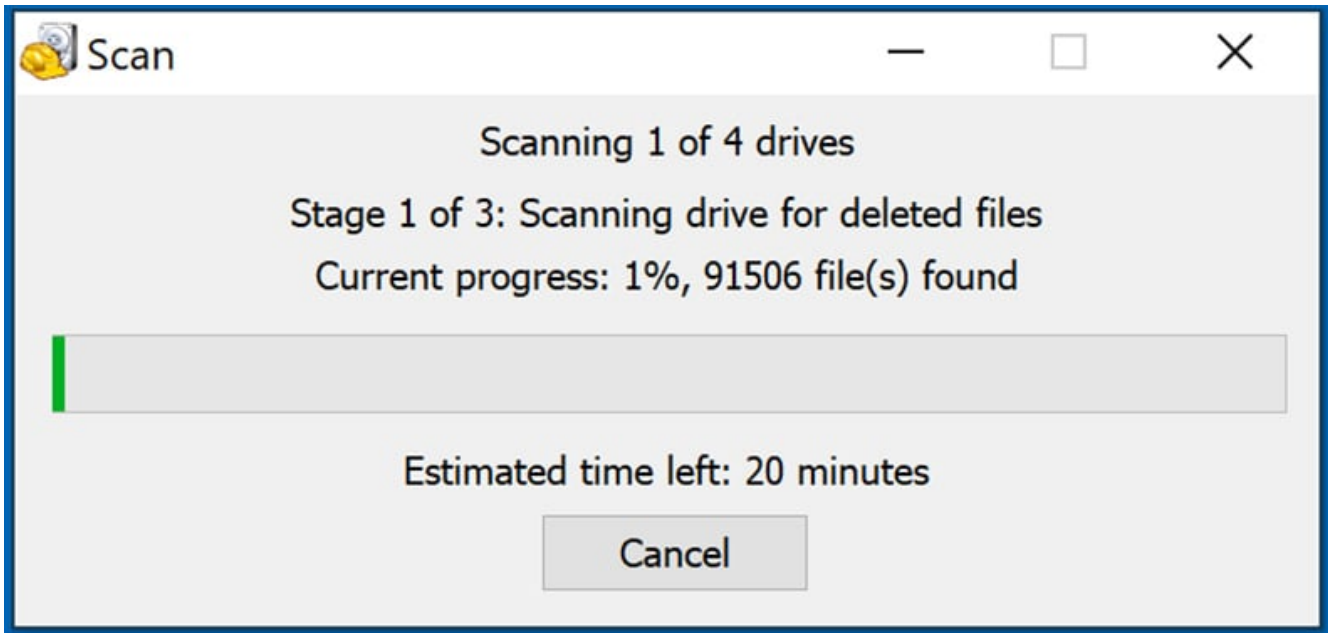
Depending on the situation (quality of ransomware infection, type of encryption algorithm used, etc.), restoring data with certain third-party tools might be possible. Therefore, we advise you to use the [Recuva tool developed by CCleaner](#). This tool supports over a thousand data types (graphics, 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.

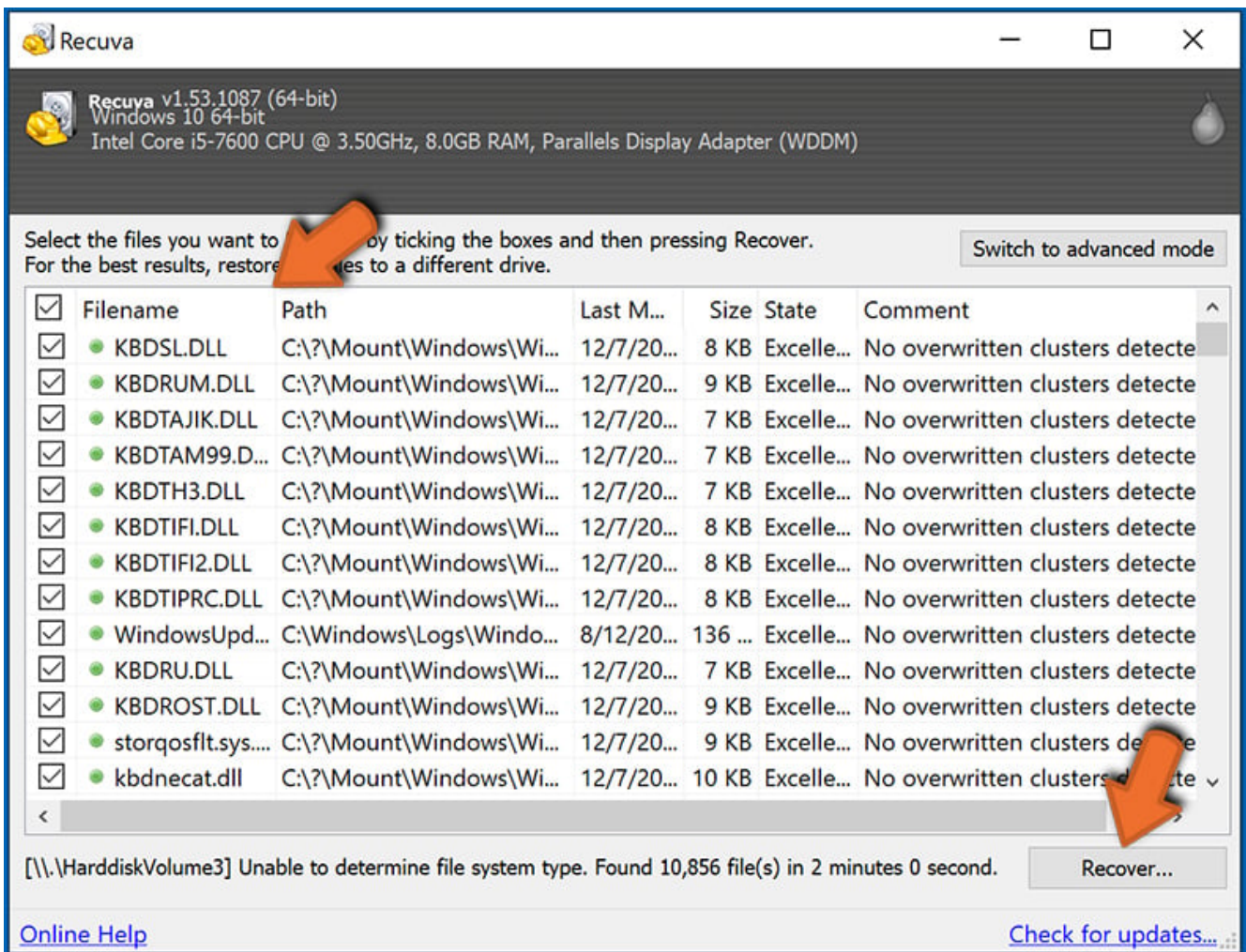


Wait for Recuva to complete the scan. The scanning duration depends on the volume of files (both in quantity and size) that you are scanning (for example, several hundred gigabytes could take over an hour to scan). Therefore, be patient during the scanning process. We also advise against modifying or 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.

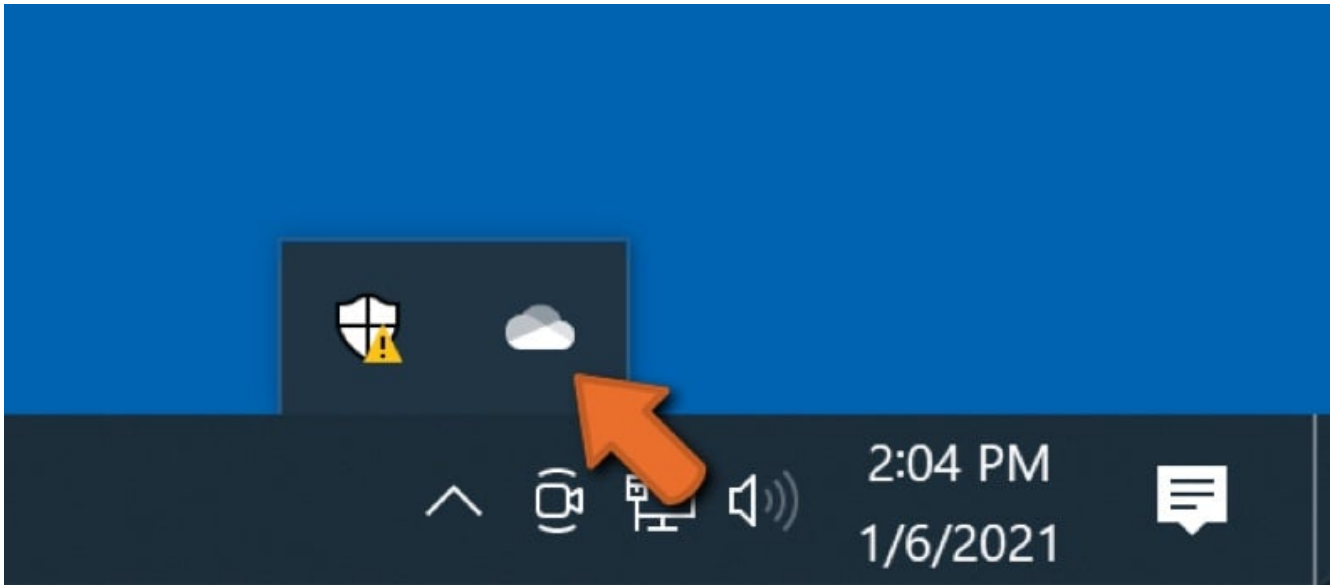
The service is built using HTML5 technologies and allows you to upload files up to 300 MB via drag and drop into the web browser or up to 10 GB via the [OneDrive desktop application](#). With OneDrive, you can download entire folders as a single ZIP file with up to 10,000 files, although it can't exceed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

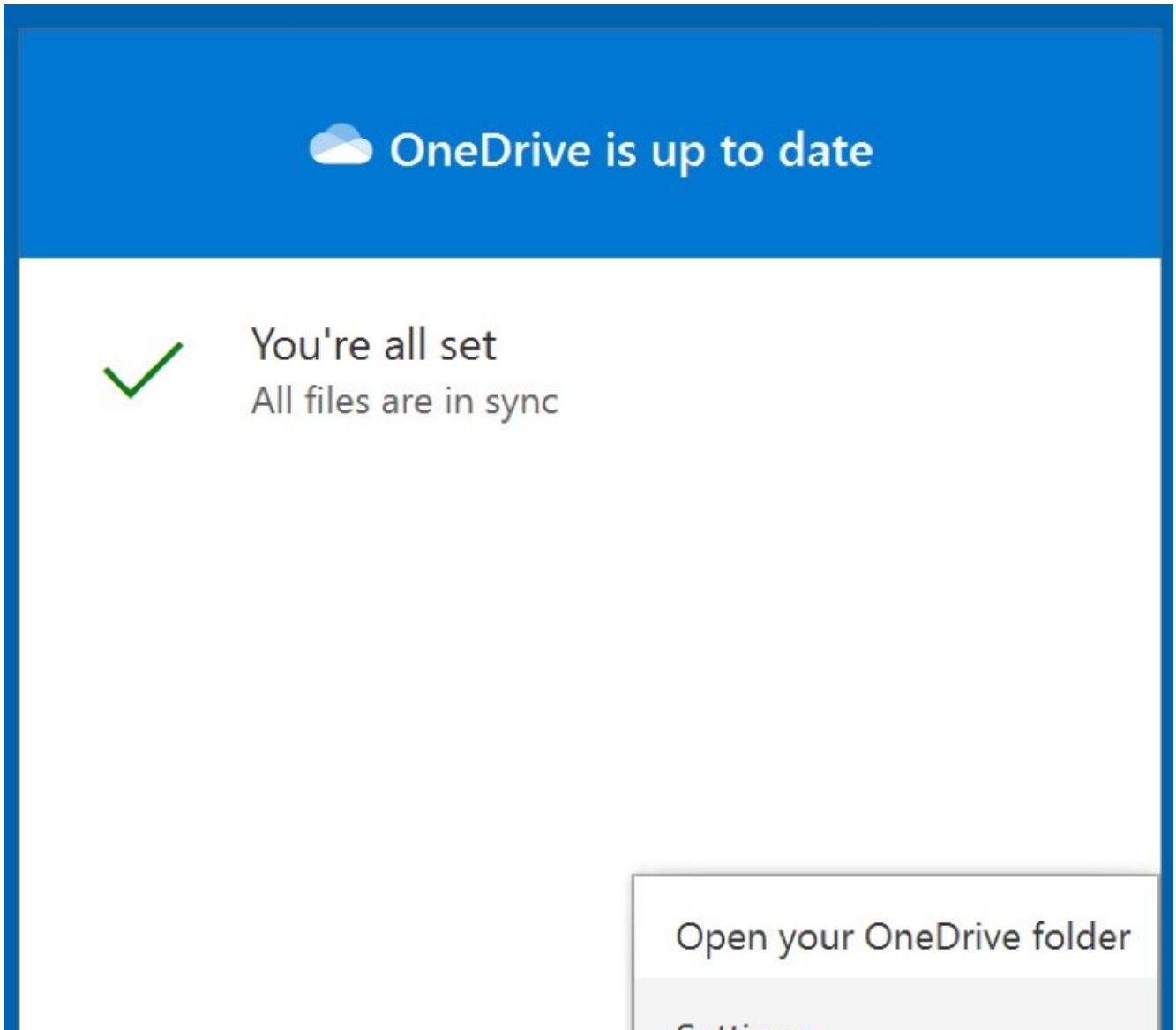
Creating a data backup:

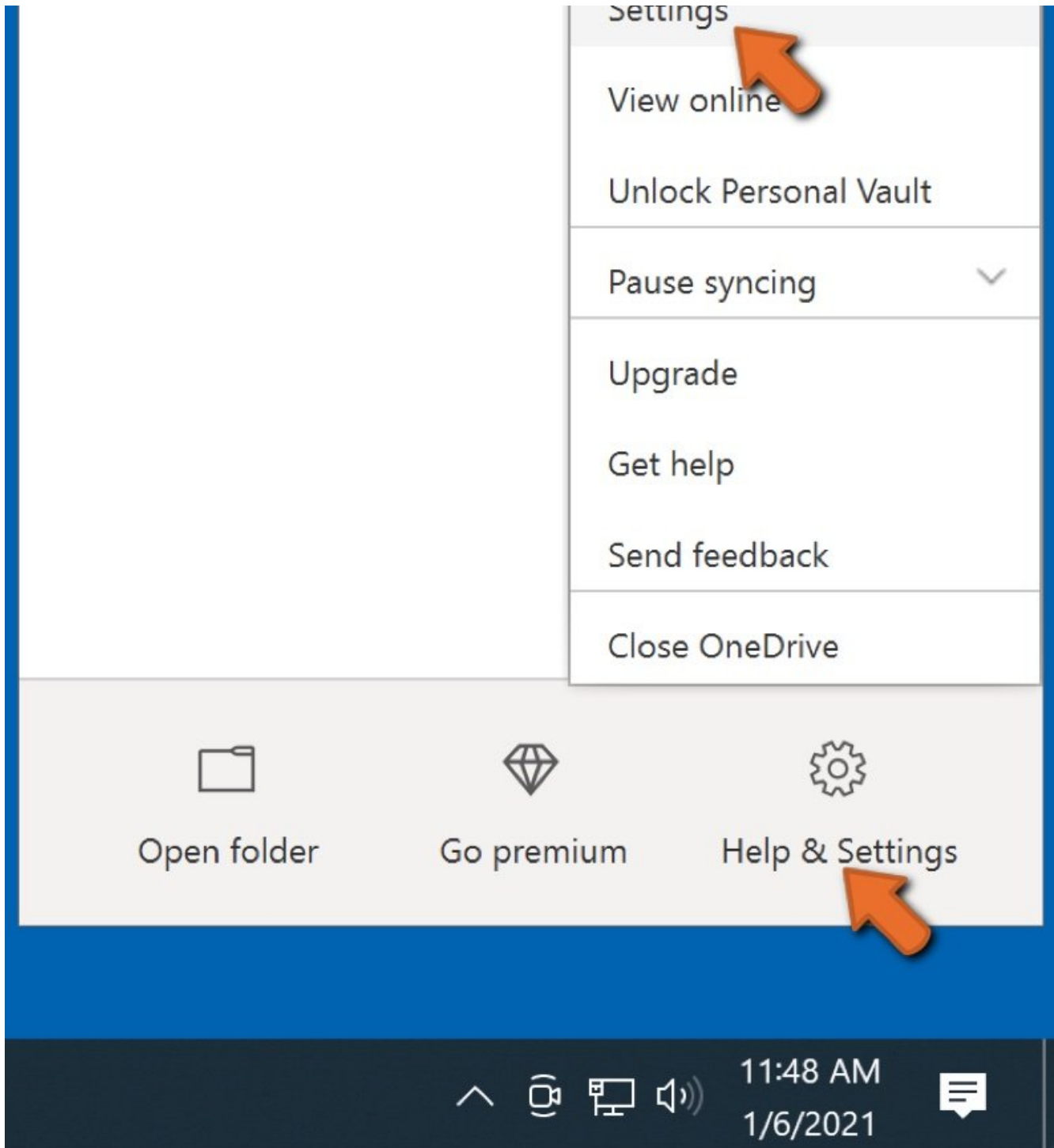
The backup process is the same for all file types and folders. Here's how you can back up your files using Microsoft OneDrive

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

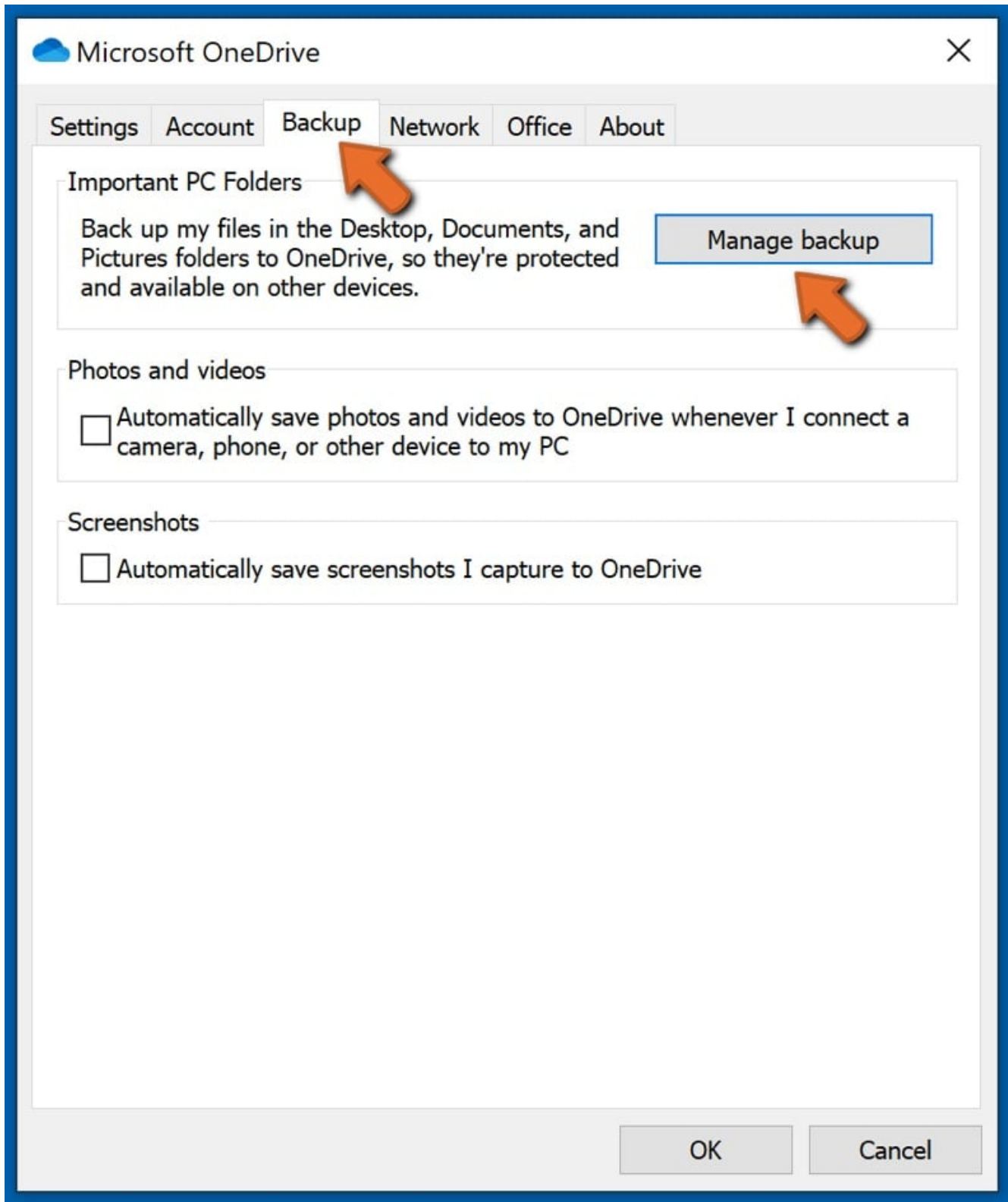


Click the **OneDrive cloud icon** to open the **OneDrive menu**. While in this menu, you can customize your file backup settings.





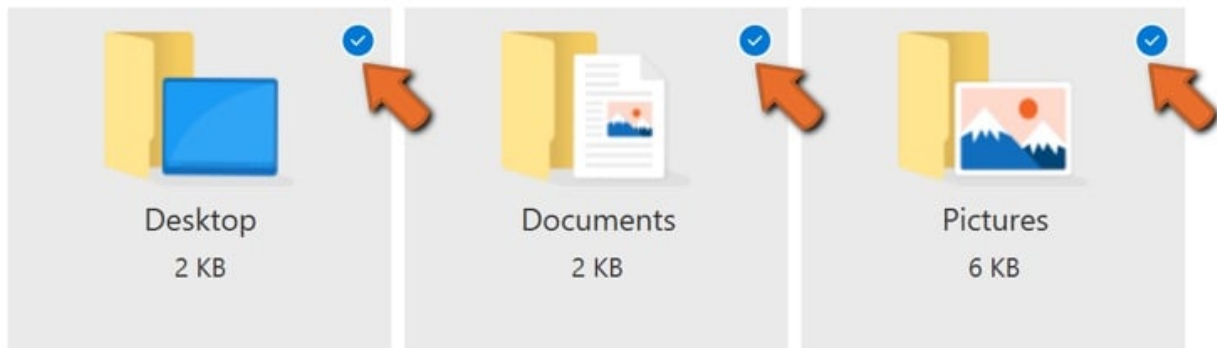
Click **Help & Settings** and then select **Settings** from the drop-down menu.



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

Manage folder backup

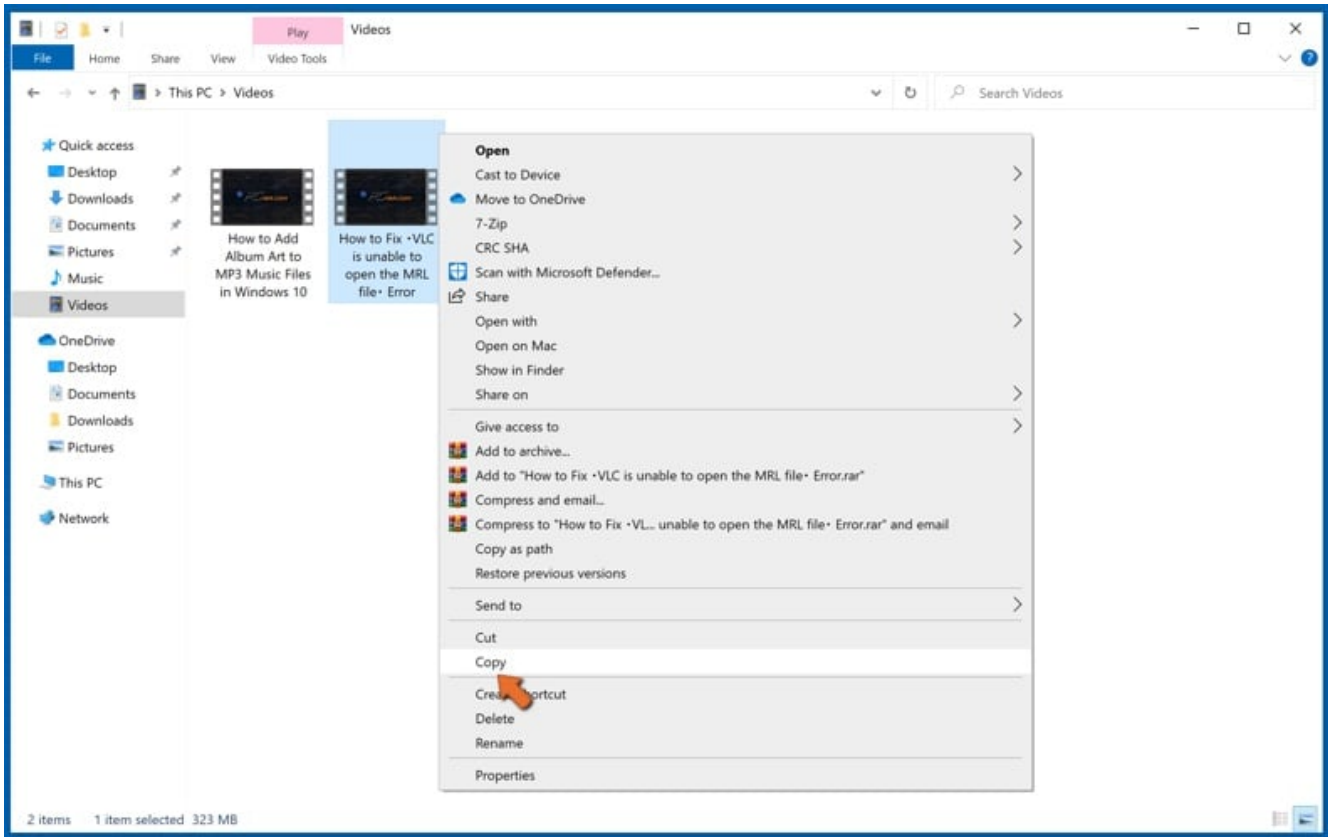
These folders are syncing in OneDrive. New and existing files will be added to OneDrive, backed up, and available on your other devices, even if you lose this PC.



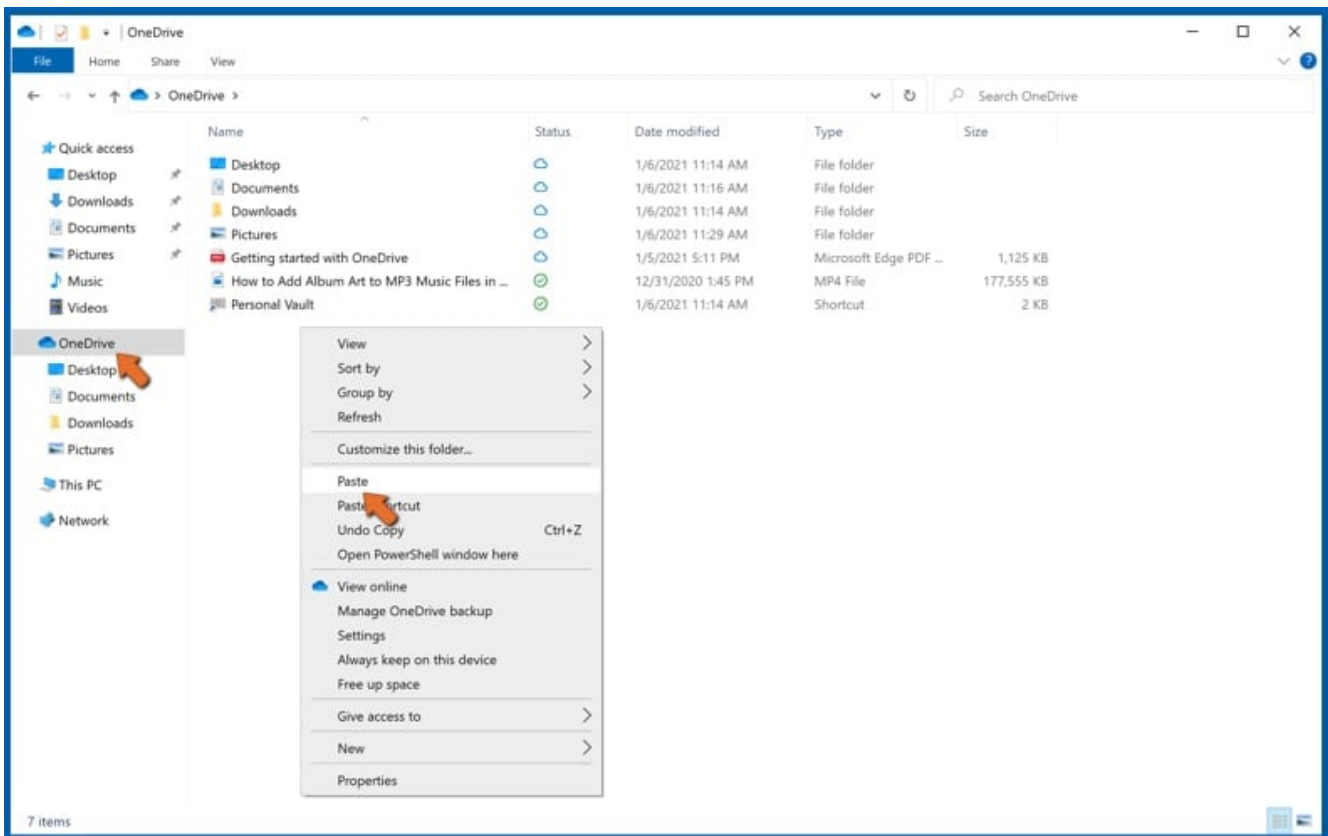
In this menu, you can choose to backup the **Desktop** and all of the files on it, and **Documents** and **Pictures** folders, again, with all of the files in them. Click **Start backup**.

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

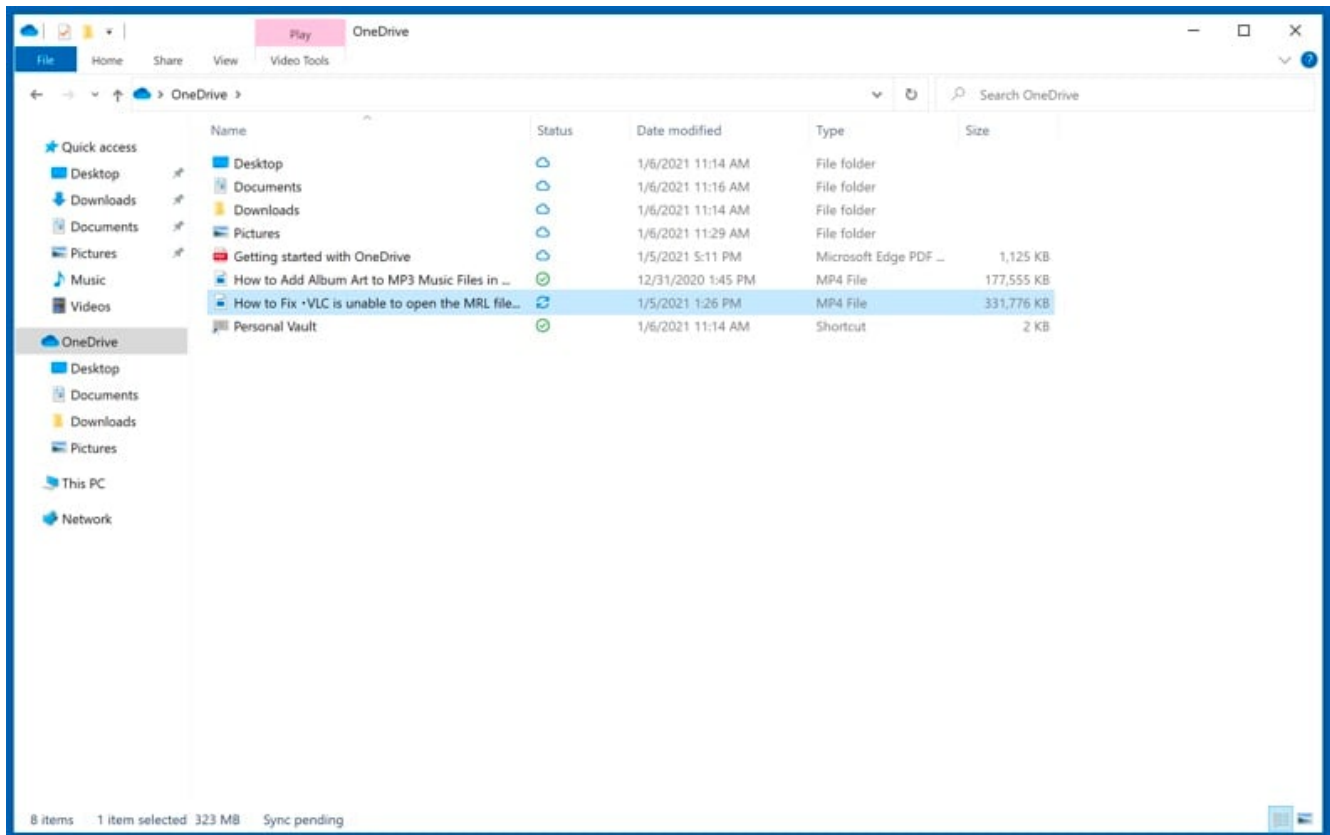
To add folders and files, not in the locations shown above, you have to add them manually.



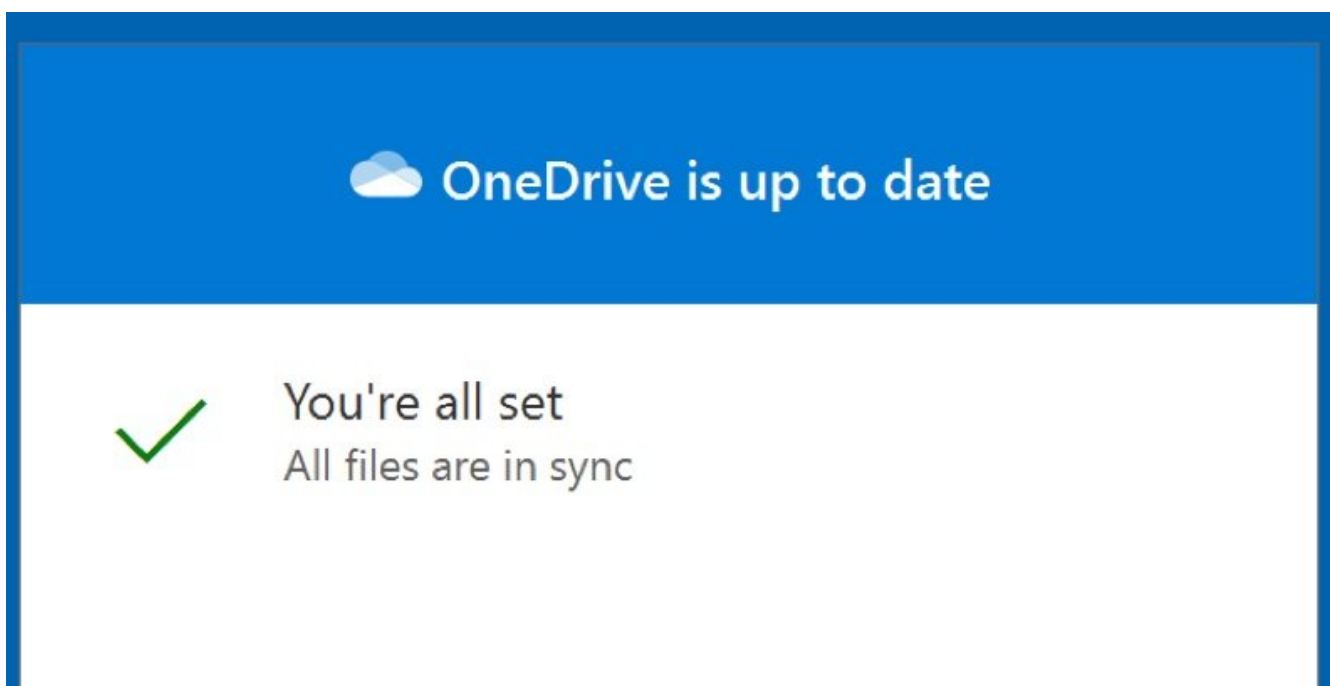
Open File Explorer and navigate to the location of the folder/file you want to backup. Select the item, right-click it, and click Copy.



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.



Open your OneDrive folder

Settings

View online

Unlock Personal Vault

Pause syncing



Upgrade

Get help

Send feedback

Close OneDrive



Open folder



Go premium

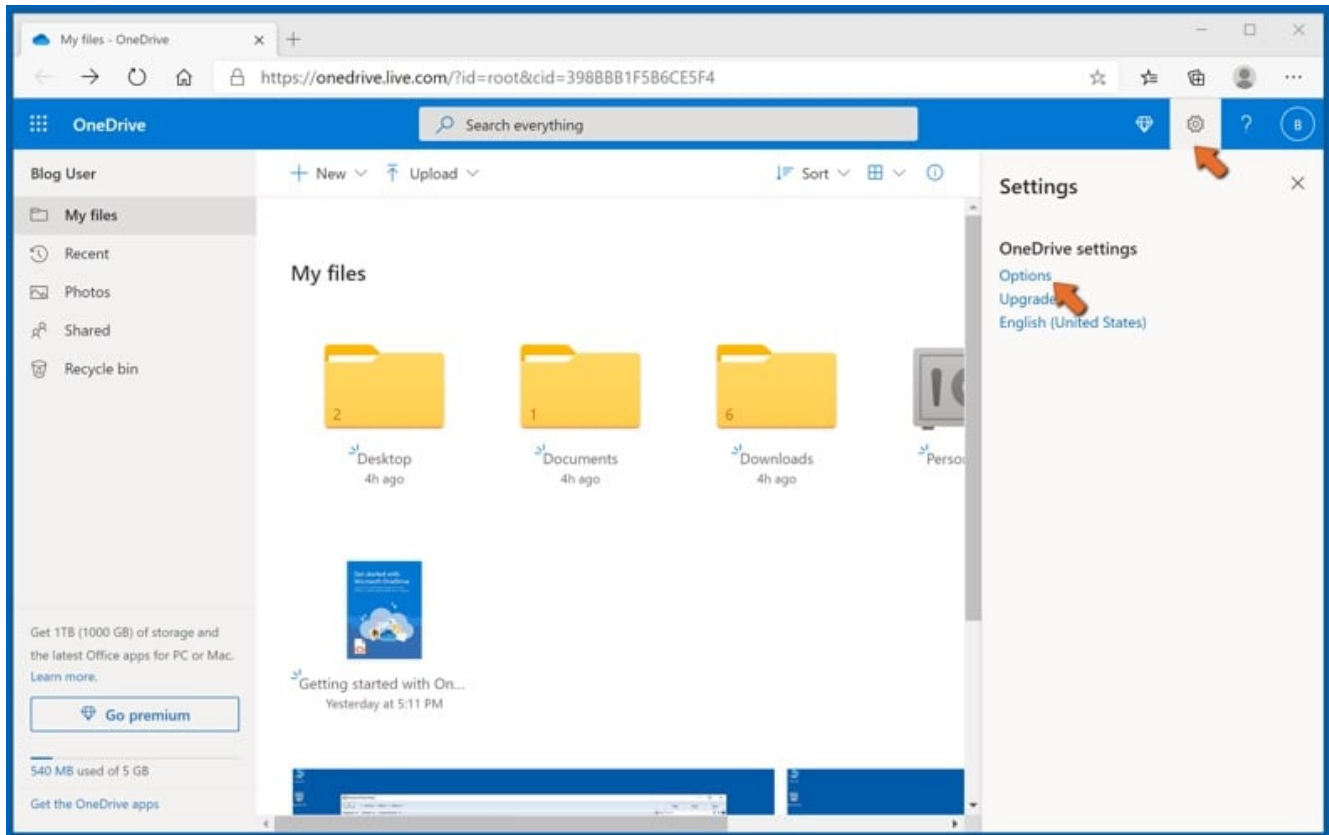


Help & Settings

2:34 PM



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

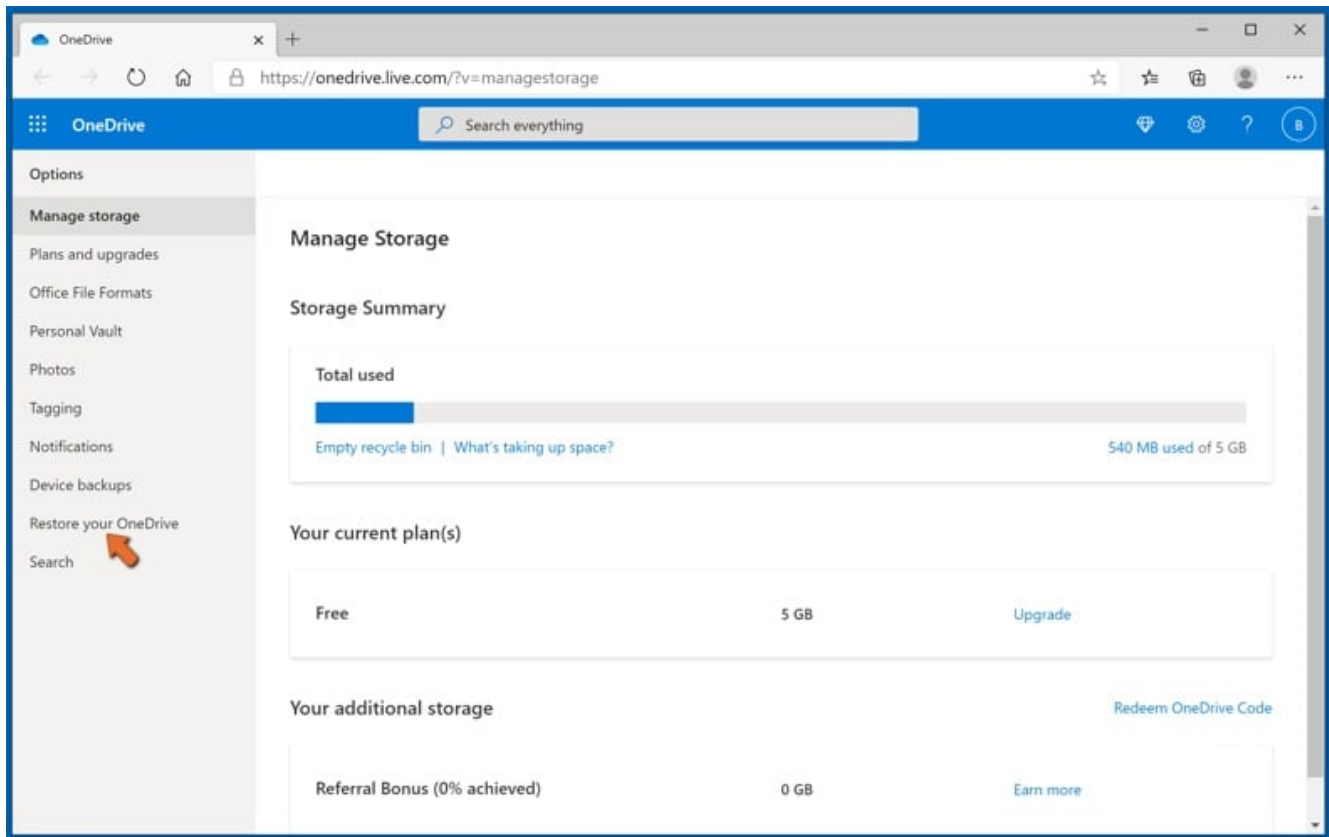


Step 2: Restore corrupted files.

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.

Frequently Asked Questions (FAQ)

How was my computer hacked and how did hackers encrypt my files?

FORCE is part of the Phobos ransomware family. These programs often infiltrate systems via vulnerable RDP services and rely on brute-force and dictionary attacks. Other infiltration/proliferation techniques are possible. Malware is most commonly spread via drive-by downloads, untrustworthy download sources (e.g., freeware and third-party sites, Peer-to-Peer sharing networks, etc.), illegal program activation tools ("cracks"), fake updaters, spam mail, online scams, and malvertising.

How to open ".FORCE" files?

Encrypted files cannot be opened/used unless they are decrypted.

Where should I look for free decryption tools for FORCE ransomware?

If you have experienced a ransomware infection, we recommend checking out the [No More Ransom](#) project website ([more information above](#)).

I can pay you a lot of money, can you decrypt files for me?

We do not provide decryption services. In fact, aside from cases involving deeply flawed ransomware, decryption is usually impossible without the attackers' interference. Hence, third-parties offering paid decryption are often scams or aim to act as middlemen between victims and criminals.

Will Combo Cleaner help me remove FORCE ransomware?

Yes, Combo Cleaner can scan systems and eliminate active ransomware infections. It must be mentioned that while using an anti-virus program is the first step in ransomware recovery – security software is incapable of decrypting files.

▼ Show Discussion

[Back To Top](#)