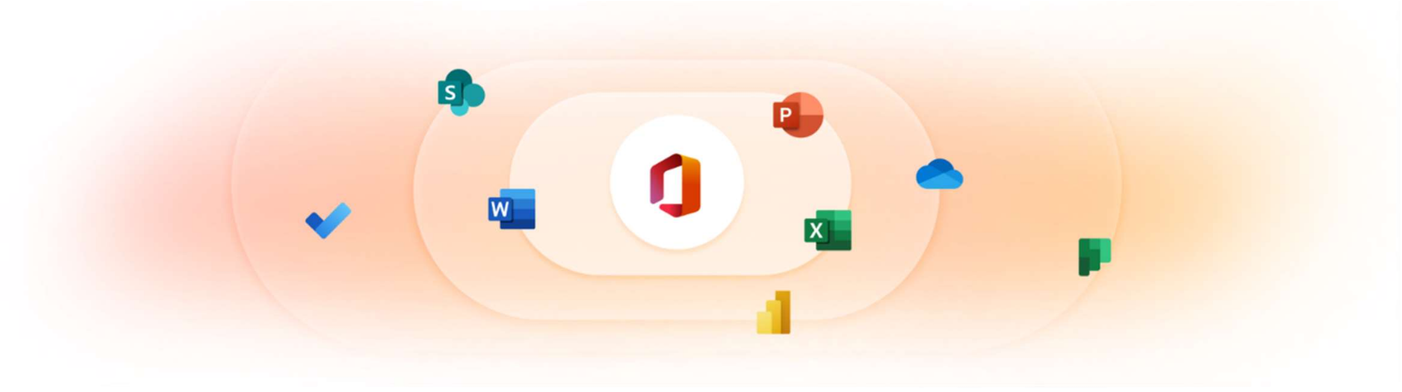


Dear Valuable Customer,

Around the world, PCs, Laptops are being caught under Ransomware attack.

With OneDrive (Subscription under Microsoft 365) stay protected.

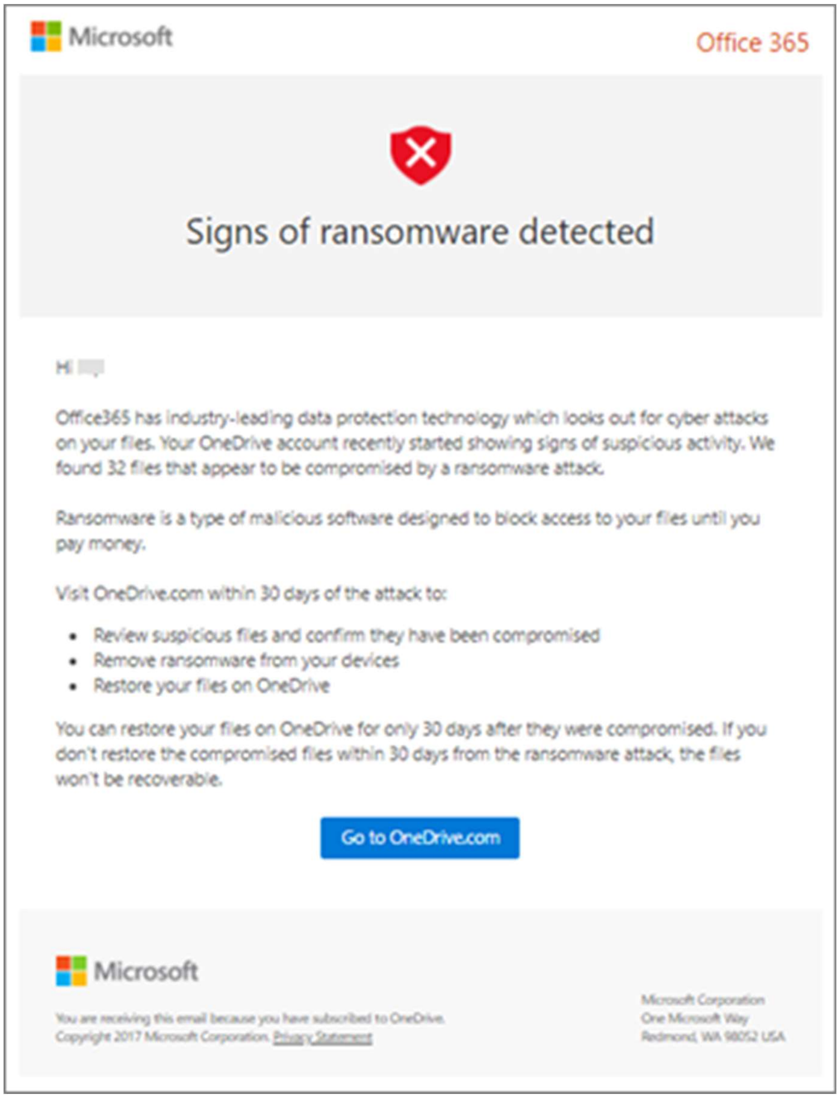
If you don’t have Microsoft 365 Subscription, get it today on VIJAYCO.CLOUD at:

https://vijayco.cloud/microsoft-365-business

Let’s understand the Ransomware detection and recovering your files in OneDrive.

Ransomware detection notifies you when your OneDrive files have been attacked and guides you through the process of restoring your files. Ransomware is a type of malicious software (malware) designed to block access to your files until you pay money.

When Microsoft 365 detects a ransomware attack, you'll get a notification on your device and receive an email from Microsoft 365.



Signs of ransomware detected

Hi [redacted]

Office365 has industry-leading data protection technology which looks out for cyber attacks on your files. Your OneDrive account recently started showing signs of suspicious activity. We found 32 files that appear to be compromised by a ransomware attack.

Ransomware is a type of malicious software designed to block access to your files until you pay money.

Visit OneDrive.com within 30 days of the attack to:

- Review suspicious files and confirm they have been compromised
- Remove ransomware from your devices
- Restore your files on OneDrive

You can restore your files on OneDrive for only 30 days after they were compromised. If you don't restore the compromised files within 30 days from the ransomware attack, the files won't be recoverable.

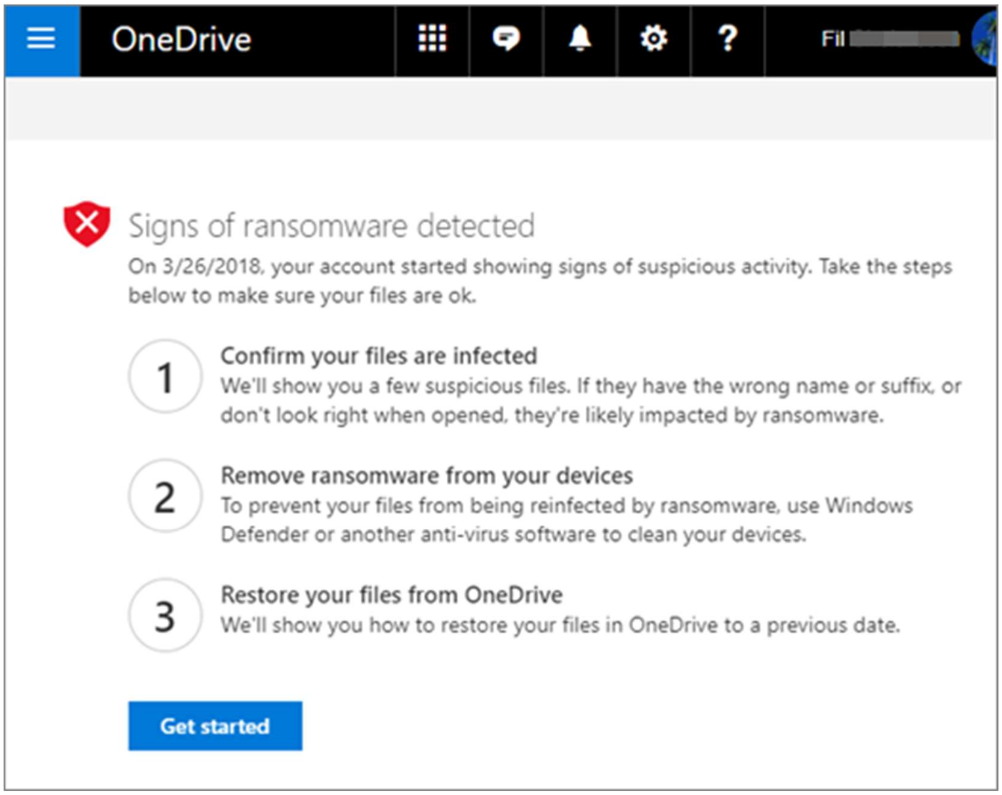
You are receiving this email because you have subscribed to OneDrive.
Copyright 2017 Microsoft Corporation. Privacy Statement

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052 USA

1. Click the link in the notification or in the email, or go to the OneDrive website, and Microsoft will walk you through the recovery process, which includes:
2. Confirm your files are infected.
3. Clean all your devices.
4. Restore your OneDrive.

Steps to the ransomware detection and recovery process on the OneDrive website

If Microsoft 365 detected a ransomware attack, you see the **Signs of ransomware detected** screen when you go to the OneDrive website (you might need to sign in first). Select the **Get started** button to begin.



Signs of ransomware detected

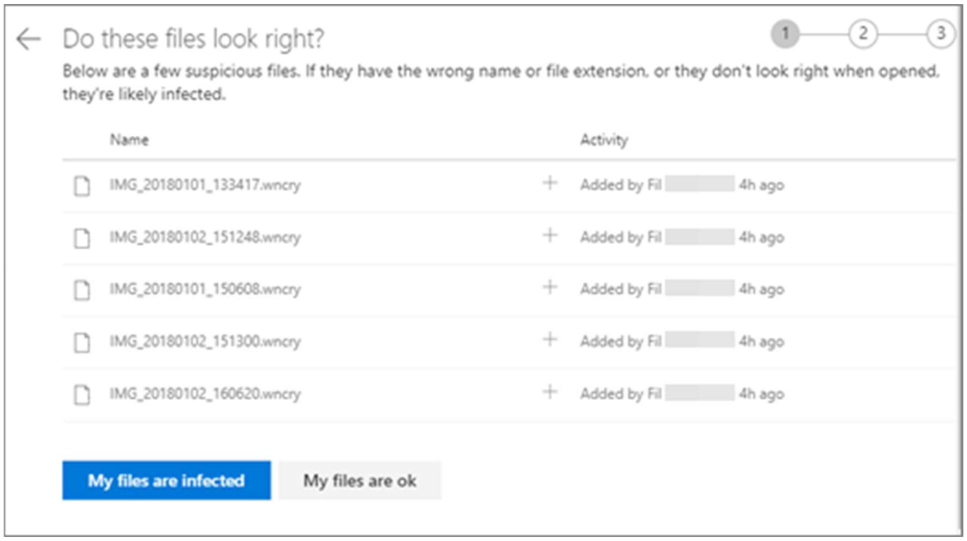
On 3/26/2018, your account started showing signs of suspicious activity. Take the steps below to make sure your files are ok.

1 Confirm your files are infected
We'll show you a few suspicious files. If they have the wrong name or suffix, or don't look right when opened, they're likely impacted by ransomware.

2 Remove ransomware from your devices
To prevent your files from being reinfected by ransomware, use Windows Defender or another anti-virus software to clean your devices.

3 Restore your files from OneDrive
We'll show you how to restore your files in OneDrive to a previous date.

<u>Step 1:</u> Confirm your files are infected



Do these files look right?

Below are a few suspicious files. If they have the wrong name or file extension, or they don't look right when opened, they're likely infected.

Name	Activity
IMG_20180101_133417.wncry	Added by Fil[redacted] 4h ago
IMG_20180102_151248.wncry	Added by Fil[redacted] 4h ago
IMG_20180101_150608.wncry	Added by Fil[redacted] 4h ago
IMG_20180102_151300.wncry	Added by Fil[redacted] 4h ago
IMG_20180102_160620.wncry	Added by Fil[redacted] 4h ago

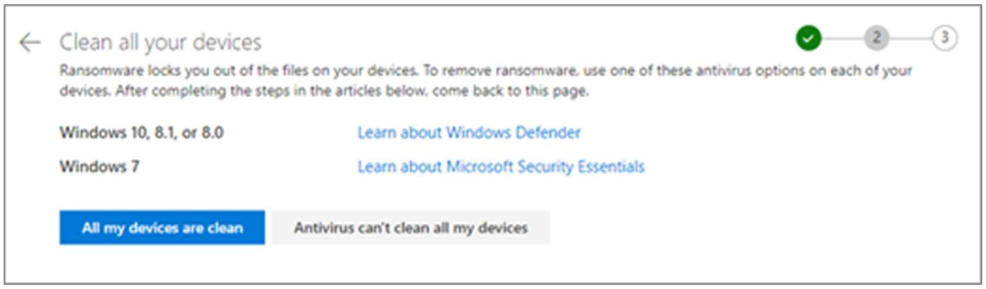
On the **Do these files look right?** screen, Microsoft shows you some suspicious files. If they have the wrong name or suffix, or don't look right when you open them from the list, they're likely compromised by ransomware.

1. Select a file to open it in the online viewer. (This won't download the file to your device.)
2. If you don't see the file, you'll have the option to download it to your device so can open it.
3. Repeat steps 1 and 2 for as many files as you want to see.
4. If your files are infected, select **My files are infected** to move to the next step in the ransomware recovery process. Otherwise, if your files look fine and you're confident they aren't infected with ransomware, select **My files are ok**.

If you choose **My files are ok**, you'll exit the ransomware recovery process and you'll go back to using OneDrive as usual.

Step 2: Clean all your devices

On the **Clean all your devices** screen, you'll see instructions for cleaning all your devices where you use OneDrive. Before you restore your files, it's important to use antivirus software to clean all your devices. Otherwise, your files could get encrypted again when you restore them.

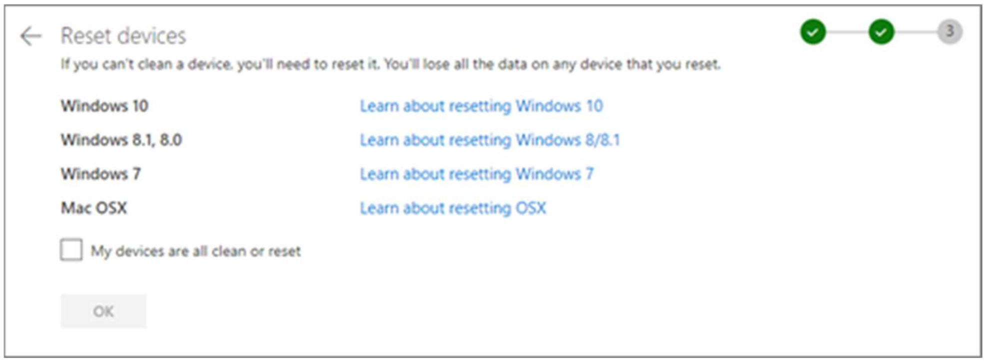


Clean all your devices

Ransomware locks you out of the files on your devices. To remove ransomware, use one of these antivirus options on each of your devices. After completing the steps in the articles below, come back to this page.

Windows 10, 8.1, or 8.0	Learn about Windows Defender
Windows 7	Learn about Microsoft Security Essentials

1. Select the link for the version of Windows that you're using and follow the instructions in the article.
2. Repeat step 1 for all the other devices where you use OneDrive.
3. After completing the steps in the articles, return to the **Clean all your devices** page on the OneDrive website and choose one of these buttons:
   - **All my devices are clean**. Select this button when you've finished cleaning all your devices, and you're ready to move to the last step in the recovery process, which is to restore your files from OneDrive.
   - **Antivirus can't clean all my devices**. Select this button after you're tried to clean your devices and discovered that you can't clean all your devices for whatever reason. You'll now be on the **Reset devices** page, which lists information about how to reset your devices.



Reset devices

If you can't clean a device, you'll need to reset it. You'll lose all the data on any device that you reset.

Windows 10	Learn about resetting Windows 10
Windows 8.1, 8.0	Learn about resetting Windows 8/8.1
Windows 7	Learn about resetting Windows 7
Mac OSX	Learn about resetting OSX

□ My devices are all clean or reset

Follow the links based on your operating system. When you've cleaned or reset all your devices, go back to the OneDrive website to return to the **Reset devices** page, select the **My devices are all clean or reset** box, and then select **OK**.

Step 3: Restore your files from OneDrive

The final step after all your devices are clean is to restore your OneDrive.

You can follow below steps

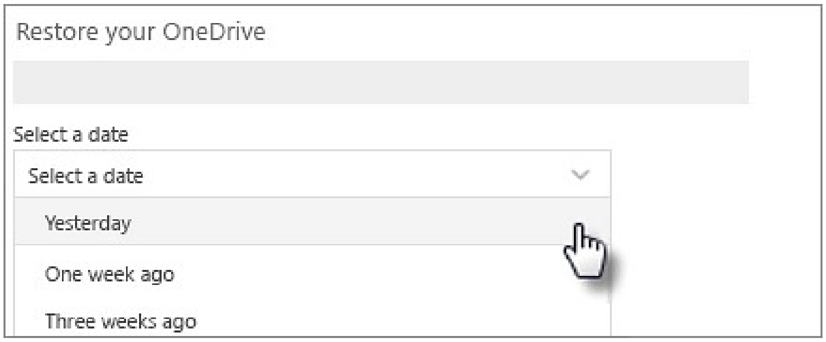
Restore OneDrive to a previous time

To restore your OneDrive, you'll need to have Microsoft 365. Otherwise, you'll be redirected to this article when you try to follow the steps below.

1. Go to the OneDrive website. (Make sure you're signed in with the correct account.)
2. If you're signed in with:
   - A personal account with a Microsoft 365 subscription, at the top of the page, select **Settings** ⚙ > **Options**, and then select **Restore your OneDrive** from the left navigation.
   - A work or school account, select **Settings** > **Restore your OneDrive**.

Note: The **Restore your OneDrive** option isn't available in the classic experience of OneDrive for work or school or without a Microsoft 365 subscription.

3. On the Restore page, select a date from the dropdown list—such as **Yesterday**—or select **Custom date and time**. If you're restoring your files after automatic ransomware detection, a suggested restore date will be filled in for you.



Restore your OneDrive

Select a date

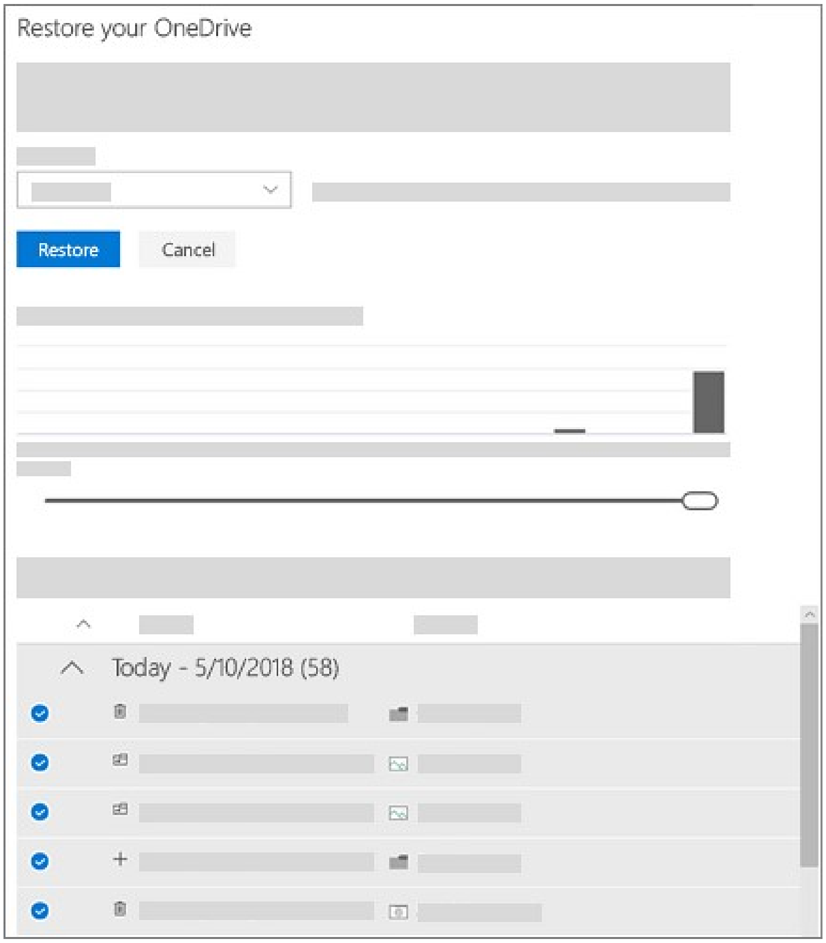
Select a date

Yesterday

One week ago

Three weeks ago

4. Use the activity chart and activity feed to review the recent activities that you want to undo.



The daily activity chart shows the volume of file activities in each day for the last 30 days. It gives you an overview of what has happened to your OneDrive over time and it can help you identify any unusual activities. For example, if your OneDrive was infected by malware, you can look for when it happened.

The activity feed shows individual file and folder operations in reverse chronological order. You can scroll down to see previous days or move the slider below the daily activity chart to quickly move to a specific day.

> ***Tip:*** *Use the expand and collapse arrow next to each day in the activity feed to show or hide activities for that day.*

5. If you selected **Custom date and time**, select the earliest activity that you want to undo. When you select an activity, all other activities that occurred after that are selected automatically.

   > **Note:** Before you select **Restore**, scroll to the top of the activity feed to review all the activities you are about to undo. When you pick a day in the activity chart, the more recent activities are hidden in the feed, but they're still selected when you select an activity.

6. When you're ready to restore your OneDrive, select **Restore**. This action will undo all the activities you selected.

Your OneDrive will be restored to the state it was in before the first activity you selected.

Note: If you change your mind about the restore you just did, you can undo the restore by running Files Restore again and selecting the restore action you just did.

Limitations and troubleshooting

- When version history is turned off, Files Restore can't restore files to a previous version. For information about versioning settings, see Enable and configure versioning for a list or library. Files Restore uses version history and the recycle bin to restore OneDrive, so it's subject to the same restrictions as those features.
- You can't restore deleted files after they've been removed from the site collection recycle bin—either by manual delete or by emptying the recycle bin. A SharePoint site collection administrator may be able to view and restore those deleted items.
- Albums are not restored.
- If you upload a file or folder that you deleted, Files Restore will skip the restore operation for that file or folder.
- If some files or folders cannot be restored, a log file will be generated at the root folder of your OneDrive to capture the errors. The name of the file will begin with "RestoreLog" followed by an ID (for example, RestoreLog-e8b977ee-e059-454d-8117-569b380eed67.log). You can share the log file with our support team to troubleshoot any issues that may occur.

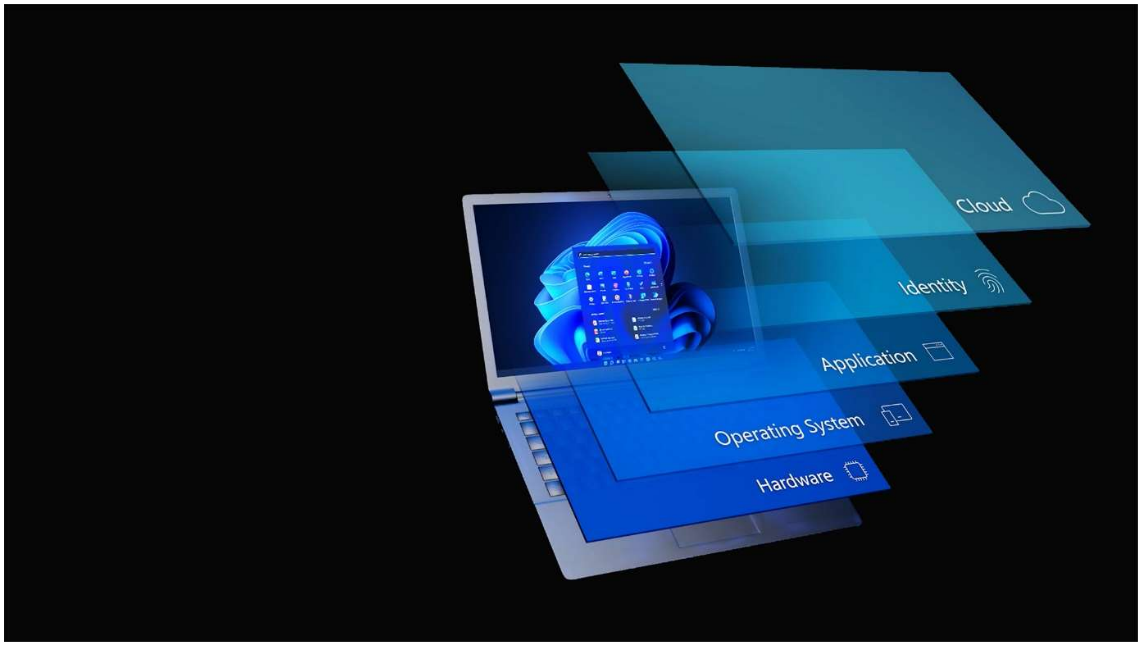
When you reach this step, the time and date that ransomware was detected will automatically be selected for you.

VIJAYCO.CLOUD recommends using Windows 11 Professional. Get your Genuine Windows 11 Professional License at:

https://vijayco.cloud/shop/ols/products/windows-11-professional-wnd-11-prf-wth

With Genuine Windows Operating System, you get latest and updated Security patches from Microsoft.

Windows 11 Professional



Regards,

VIJAYCO.CLOUD Team.