P.O. Box 95
Pine Grove Mills, PA 16868
814-206-0000
814-207-4323
mas@tekresults.com
www.tekresults.com

TekResults Newsletter (May 2025)

To unsubscribe send an email to UnsubscribeNewsletter@tekresults.com with unsubscribe to Newsletter in the subject line or click here UnsubscribeNewsletter@tekresults.com

Dear Clients and Friends

Welcome to another edition of our newsletter. Today we have some helpful hints about encrypting data you store in the cloud. Specifically, we're going to take a look at a free app called Cryptomator that keeps your data safe, even if you should (shudder!) get compromised. We're going to look at backing up your Microsoft 365 data and, finally we're going to show you how to find out if your computer is eligible to upgrade from Windows 10 to Windows 11 and then show you how to do it. Sounds like fun! Let's get started.

## Computer sale!

With Windows 10 quickly approaching the end of its supported life, now is an excellent time to replace those aging computers. We have many desktops and laptops in stock! We specialize in refurbished Dell systems that look great and come nicely appointed with a solid state drive, at least 16GB memory (we can add more if necessary) and an Intel Core i5 or i7 processor. We bench test each of our systems to ensure they are working in top-notch order before presenting them for sale, and each one comes with our 30-day warranty and we normally have replacements and spare parts on hand if there are problems. Allt of our systems feature Windows 11 Professional. We always have laptops and desktops in stock and we can order custom systems from our reliable vendors if you have unique needs

## Referrals

TekResults owes much of its success to our loyal and enthusiastic clients. It's those of you who tell your friends about us that keep our company growing, and we'd like to say thanks. Just telling someone about us is all it takes. Just let us know you dropped our name, and we'll drop a gift card in the mail. See, who said talk is cheap!

### Businesses Who Need Our Referrals

Any business needing a better disaster recovery strategy including backups for mission-critical devices (servers, essential PCs, etc.), equipment redundancy,
Any business requiring help upgrading existing IT infrastructure due to obsolescence
Any business who has slow computer systems
Any business who has slow network
Any business that needs better email services
Any business that needs to migrate to a new software platform
Any business that needs help with its industry vertical market software
Any business that has employees and compliance questions

Any business that needs help with employees working from home
Any business that needs reliable IT service
Any business that is purchasing another business and needs IT help
Any business that is being sold or is being dissolved
Any business with human resource issues as they pertain to IT
Any business that wants to save money and improve functionality by utilizing a VoIP Business phone systems
Any business needing a better security infrastructure
Any business needing remote desktop applications
Any business needing help migrating to Microsoft 365
Any business that would benefit from monitoring of performance, security, etc. of their IT infrastructure
Any business that would like an IT department that will visit and report on each device on a scheduled basis
Any business that would like to read our newsletter or other mail tips and blasts

## Is your cloud data really safe?

Many of our clients are Microsoft 365 subscribers. Microsoft handles their email and, in most cases, backs up their desktops, documents and pictures using OneDrive on their workstations. A while back, we published a newsletter article titled **Backing Up Your Email**. You can read it here. To summarize the article, if Microsoft loses your data (email, SharePoint, OneDrive, etc.), they can't be held responsible. This should make us all tremble with fear! Imagine all your vital documents, gone in an instant as a result of some unforeseen disaster. You know, like one of Microsoft's data centers catches fire and burns to the ground.

To be fair, Microsoft does an excellent job of maintaining their infrastructure, employing multiple redundancies in case of disaster, but regardless of how good they are, they won't take responsibility if something happens to your precious data.

Part of the agreement you sign when you use Microsoft services clearly states that it is you who bears the responsibility of backing up and securing your data. Microsoft has provided a Shared Responsibility Model to help their customers understand where Microsoft's responsibility ends and theirs begins. The model clearly displays that the responsibility of protecting your data ultimately lies in your hands, and not in Microsoft's. So, what does Microsoft provide? Microsoft is responsible for maintaining the infrastructure of its services, ensuring it's accessible and protected from service-side issues. They are also responsible for many other elements, but your data is incidental to them.

We bring this up because for the past two years we have been highly recommending to all our clients that they subscribe to Zix/AppRiver's Cloud-to-Cloud backup. For about $2 a month per user, C2C Backup will back up all your users' data stored with Microsoft, allowing you to automatically back up and recover email, OneDrive, SharePoint, and Teams data. We believe that every day brings us closer to the day "it could happen to you" and we really want you to be safe.

Did we mention recover data? Yep! C2C Backup provides the ability to recover deleted emails, lost OneDrive folders and so much more. Run full searches on your daily snapshots and choose a point-in-time and/or hierarchy (mailbox, site, folder, doc, etc.) of the exact data you want to retrieve.

Still not convinced? Here are 7 reasons every business needs cloud backup. Please give us a call and allow us to schedule a demo of Zix Cloud-to-Cloud backup.

# Why the files you've stored in the cloud are vulnerable to hacking

You may not realize it, but you probably already have data stored in the cloud. If you use email (and who doesn't), listen to Spotify, do online banking, keep photos on Google, Amazon or iCloud, or use OneDrive or Dropbox, you are storing your stuff in the cloud. If you have multiple devices (phone, tablet, PC, laptop) that sync your data from device to device, that data is stored in the cloud. And while all of this is wonderfully convenient, it can also make your data vulnerable to bad actors.

After all, when your data is stored in the cloud, it isn't just sitting on your computer or device anymore. It's sitting on a server somewhere — one that you most likely don't have physical access to. Fortunately, a combination of common sense and clever security tools can keep your data safe.

## What you need to know

Generally, when people talk about "the cloud," they're either talking about cloud hosting or cloud computing. In either case, cloud technology allows multiple people to take advantage of a set of networked servers at a data center. In the past, if you wanted to host something at a data center, you had to spend a lot of money to rent a server — meaning it wasn't feasible for most people.

The cloud changes this by allowing a number of people to securely share a series of servers for numerous purposes – from storage to remotely completing basic tasks. Most applications that use the cloud tend to be automated, so the process is completely hands-off. In this scenario, you never really have to worry about your data — it's taken care of for you, automatically uploaded to the cloud server whenever you update it.

With an application based in the cloud, you can edit your files from any location. When you type a character into your web browser, it sends it to that cloud application provider's server, which actually modifies the file and saves the changes.

The cloud lets you access files from any compatible device and can decrease the risk of catastrophic hardware failure. If you edit documents using an installed word processor and store them on your hard drive, you're dependent on that drive. Even if you've made a backup, you'll have to reinstall the word processor to edit that file. With a file and application in the cloud, however, your data is stored on a server, along with the program. It's not invulnerable, but you're at much lower risk of something happening to it.

But it's important to note that the cloud also adds risks. When something is stored in the cloud, you don't have direct control over that file (or application). If someone manages to guess your password or finds a way to hack your account, all your data could be compromised. Large organizations are particularly vulnerable, as they often store large amounts of sensitive information using cloud-based services. If a malicious third party manages to find a security hole, hackers can make off with vast amounts of sensitive data, such as social security numbers, medical records, and credit card information Or they can steal your data and charge you a ransom if you want it back.

## Encrypt your data

Encrypted cloud storage provides an extra layer of security for your data. Even if a hacker gains access or a government court orders a cloud storage provider to disclose your personal information, they still won't be able to read it. Cloud encryption is the process of transforming data into an unreadable format (ciphertext) before it's stored or transmitted in a cloud environment. This ensures that sensitive information remains confidential and accessible only to authorized users with the decryption key.

Client-side encrypted cloud storage doesn't come standard with most SaaS business software such as Office 365 and Google Workspace. Many services encrypt data in motion — the information flowing between your computer and the

cloud service — which is a great start. However, this protection is usually based on SSL/TLS encryption, which is vulnerable to attacks. The other issue is that any data that is cached to a device that you use is not encrypted and could be stolen.

There are a lot of solutions out there that can help you encrypt your data. We like Cryptomator. It protects your data from end to end, it's relatively easy to use and it's FREE.

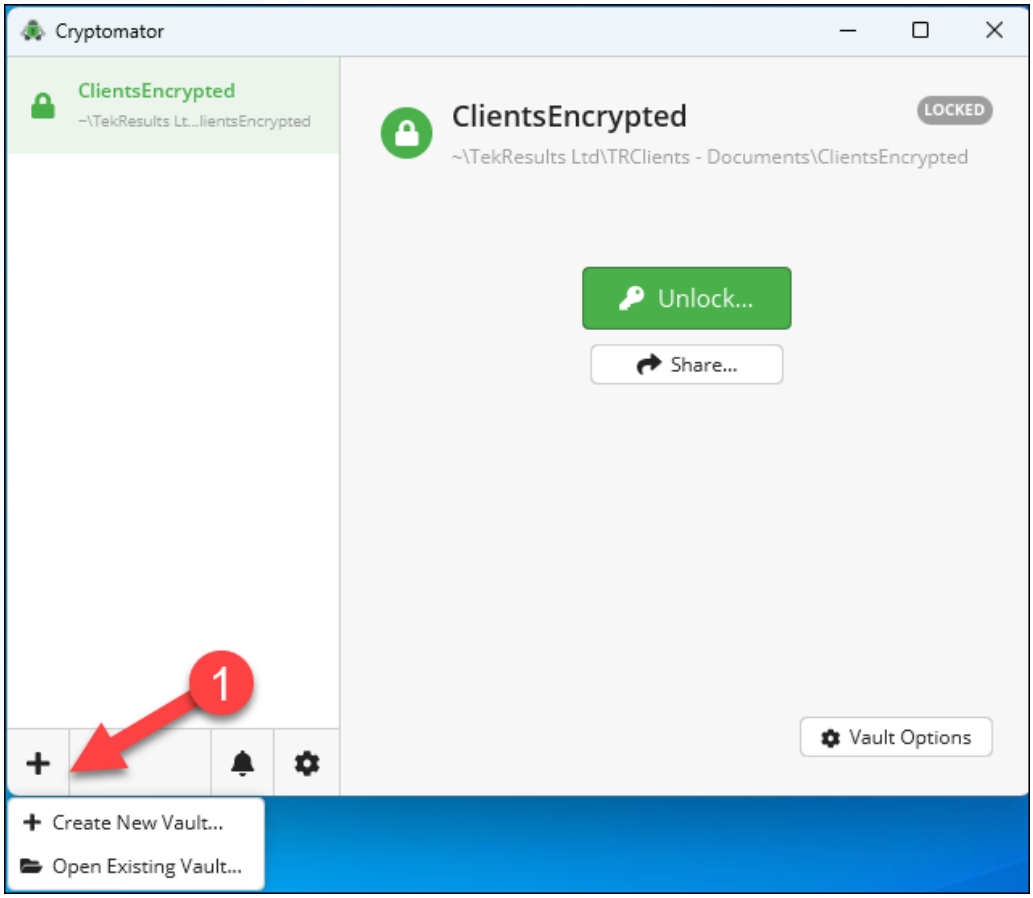
Cryptomator works with the cloud provider of your choice: Dropbox, OneDrive, Google Drive, just about any app that allows you to sync data between the cloud and your devices. The concept is simple.

1. Cryptomator creates what it calls a vault in the folder where you store your cloud-synced data, OneDrive, DropBox, etc. When the vault is unlocked in Cryptomator, Cryptomator reveals a new drive mapping in File Explorer.
2. When that new drive is visible, you can just drag your documents into the drive (vault) where they will instantly be encrypted.
3. When you're finished adding files to the vault, you can lock it and the mapped drive disappears from File Explorer.
4. The data you put in the folder is synced to the cloud, but the data that's synced is encrypted, so even if someone intercepts the data on the way to the cloud, or compromises your cloud storage, they won't be able to read your data.

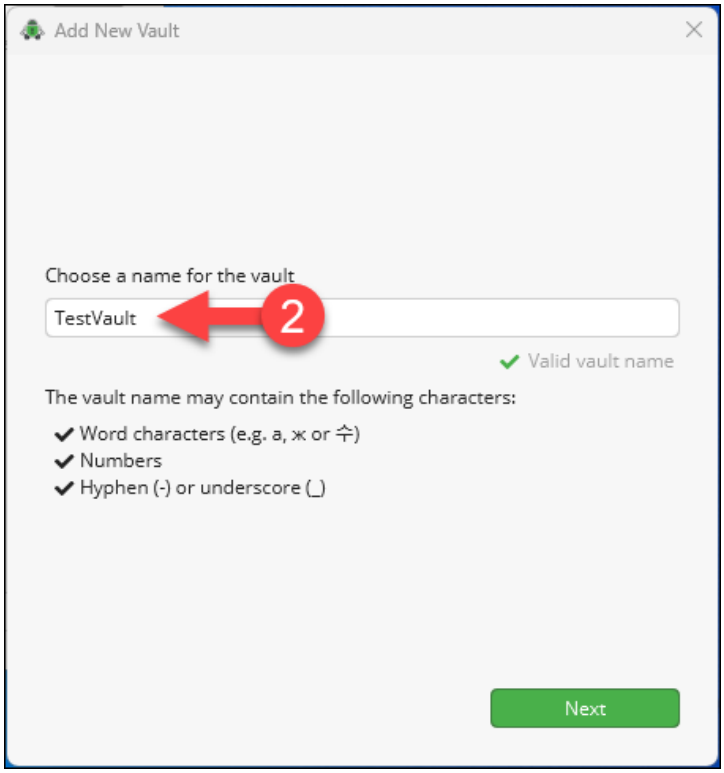
## Let's see how to set that up with pictures!

You can download Cryptomator here.

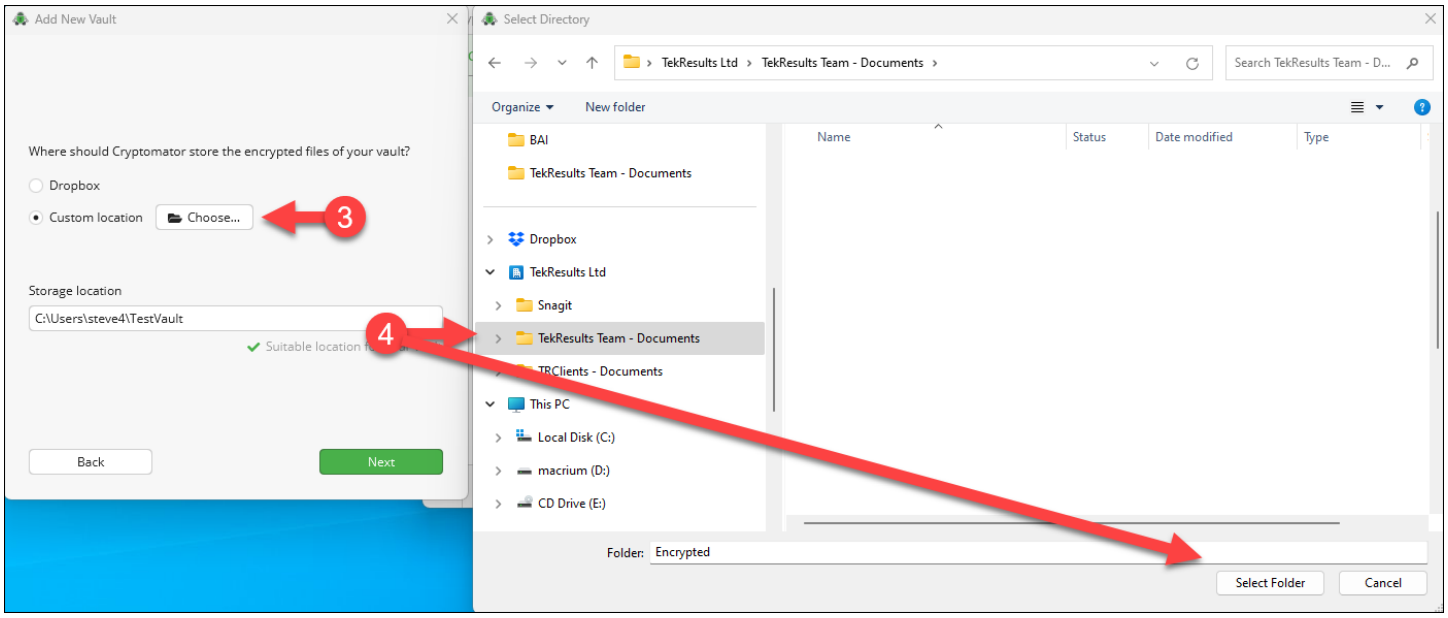
1. Open Cryptomator on your computer and click + to create a new vault.



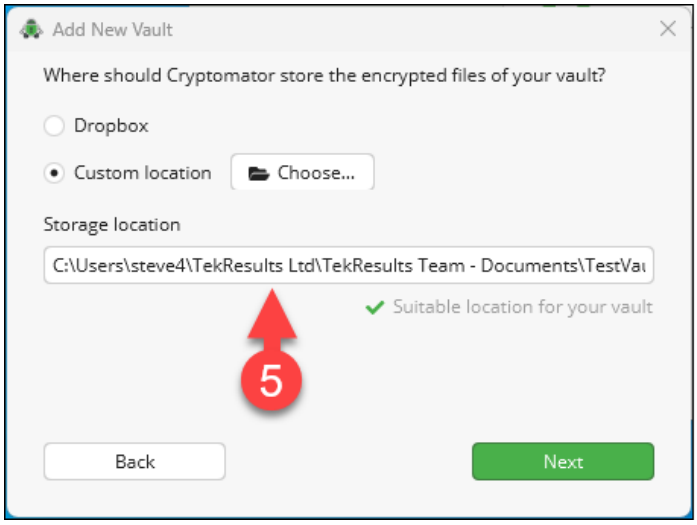
2. Type in a descriptive name for your vault. This can be anything you like. Click **Next**.

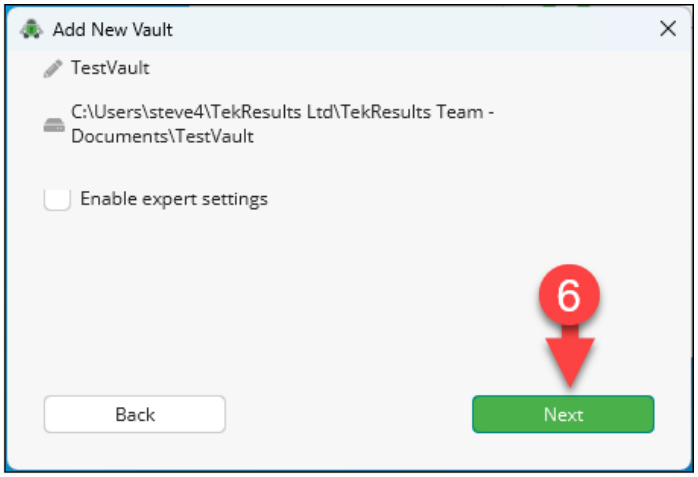



3. If you want to use Dropbox for your vault, just select **Dropbox** and click **Next**. In our scenario, we are going to use OneDrive, so we will have to tick **Custom location** and then click the **Choose** button to tell Cryptomator where we want to put the vault.
4. The app opens a File Explorer window. Navigate to your OneDrive folder and click the **Select Folder** button.

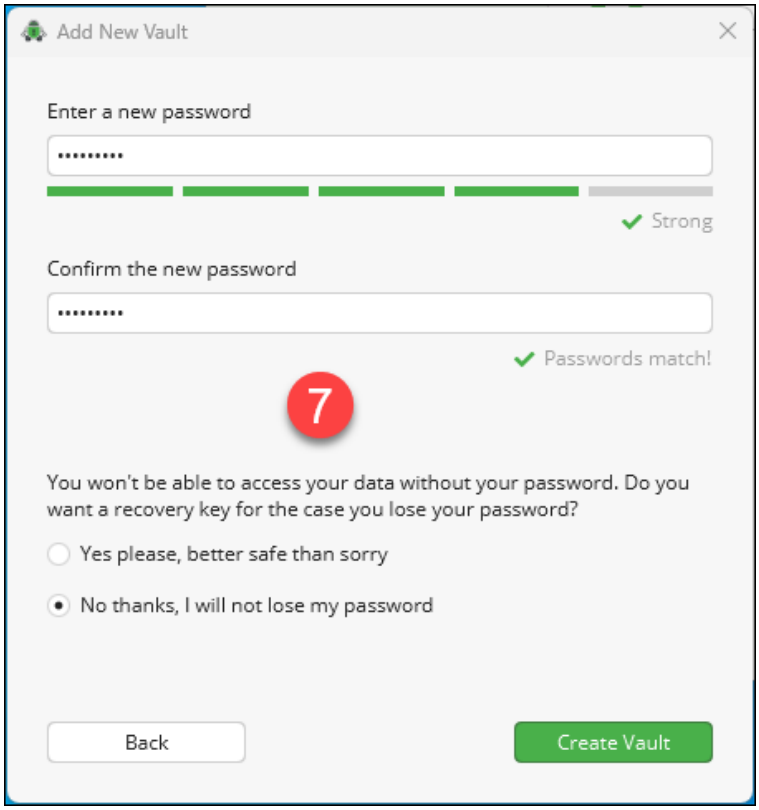


5. Back in the **Add New Vault** dialog, you will see the path to your OneDrive folder listed under **Storage location**. Click **Next**.
6. Accept the settings and click **Next**.

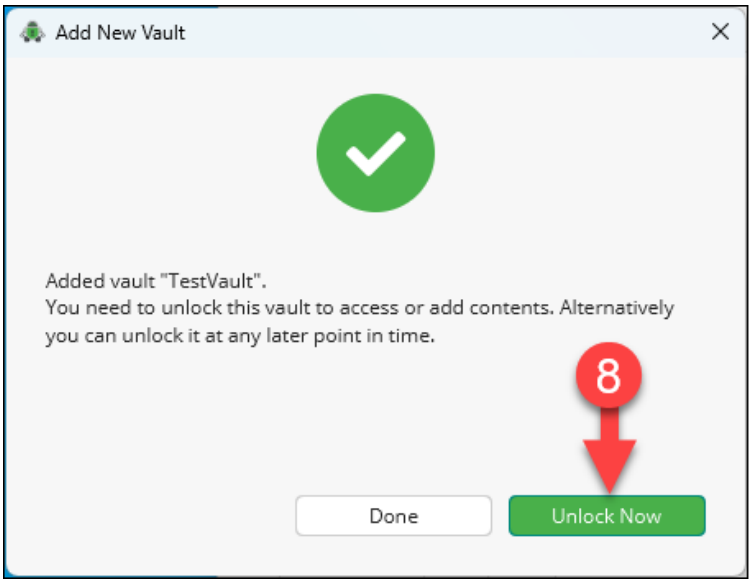


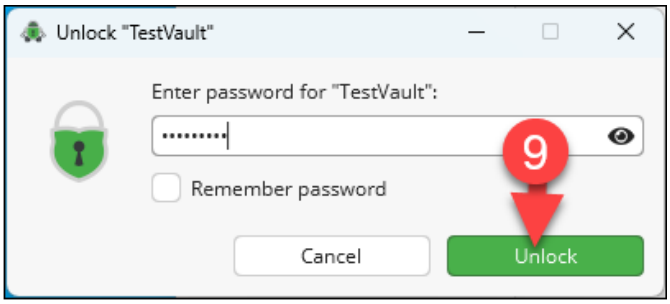




7. Enter a password for the new vault. Tick one of the two options about creating a recovery key and then click **Create Vault**.

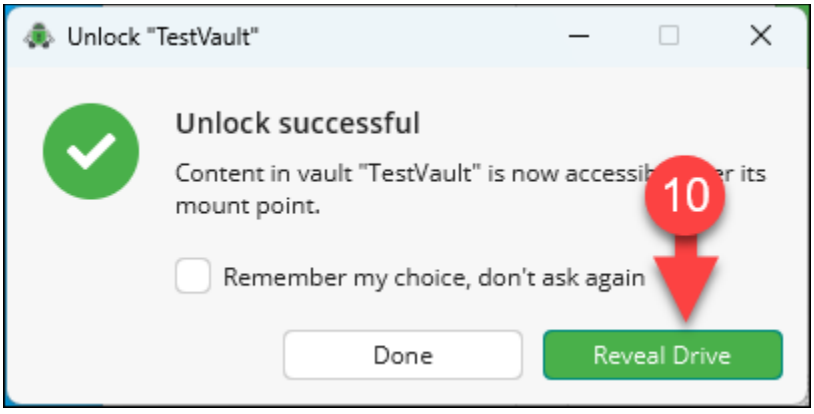


8. Now it’s time to see your new vault. Click **Unlock Now**.
9. Enter the password you created and click **Unlock**

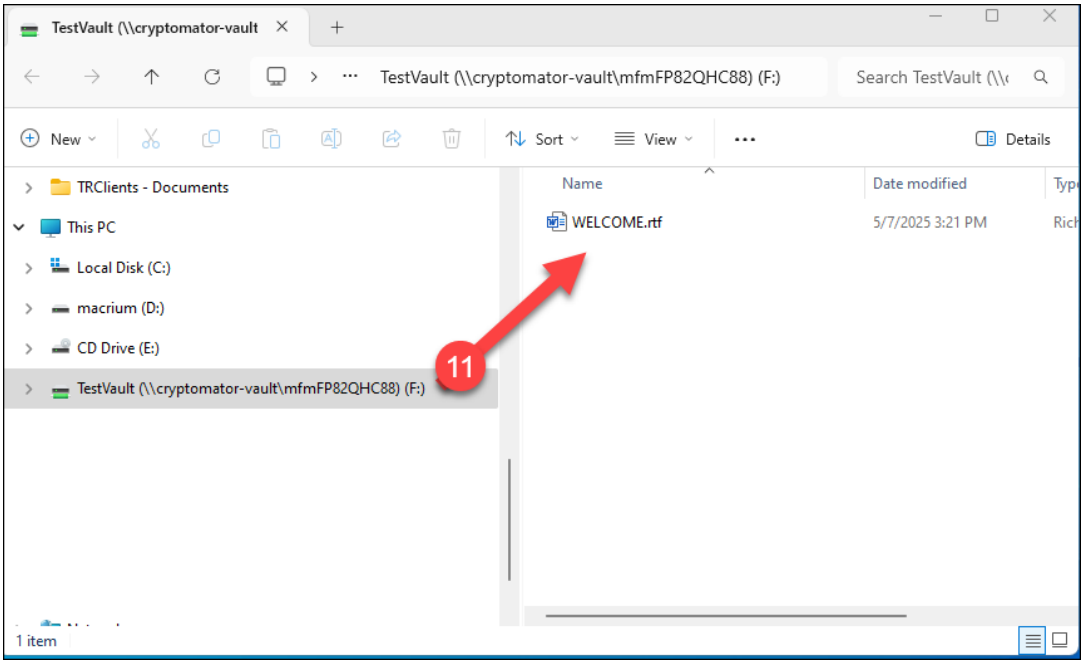


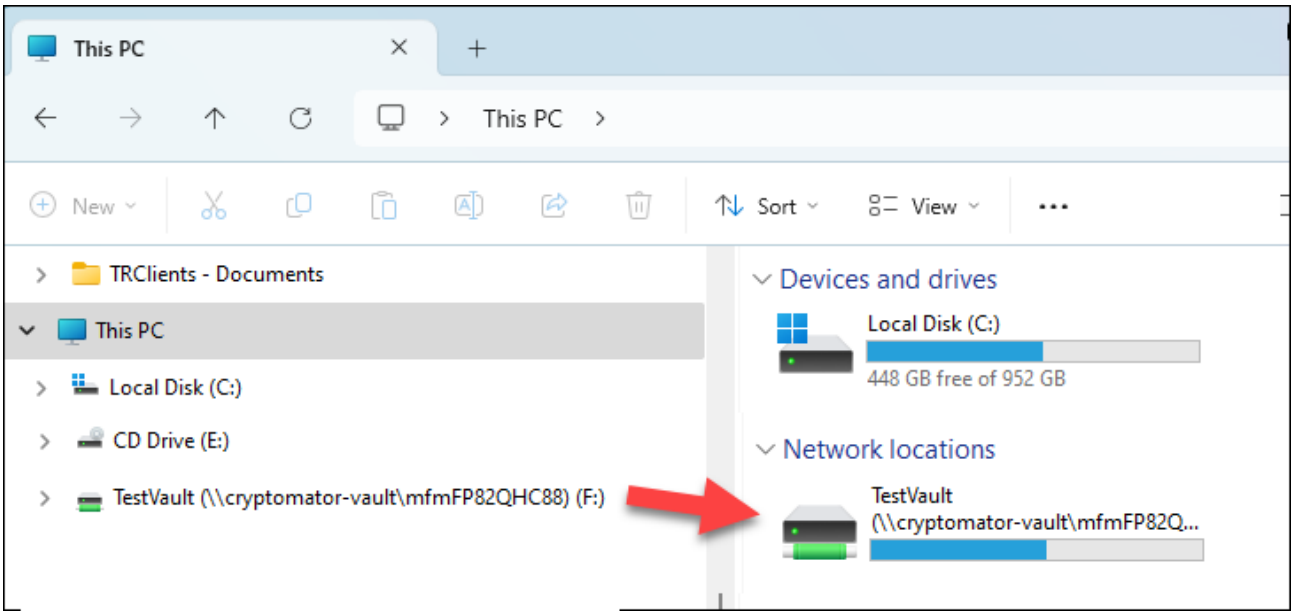

10. Click **Reveal Drive**.



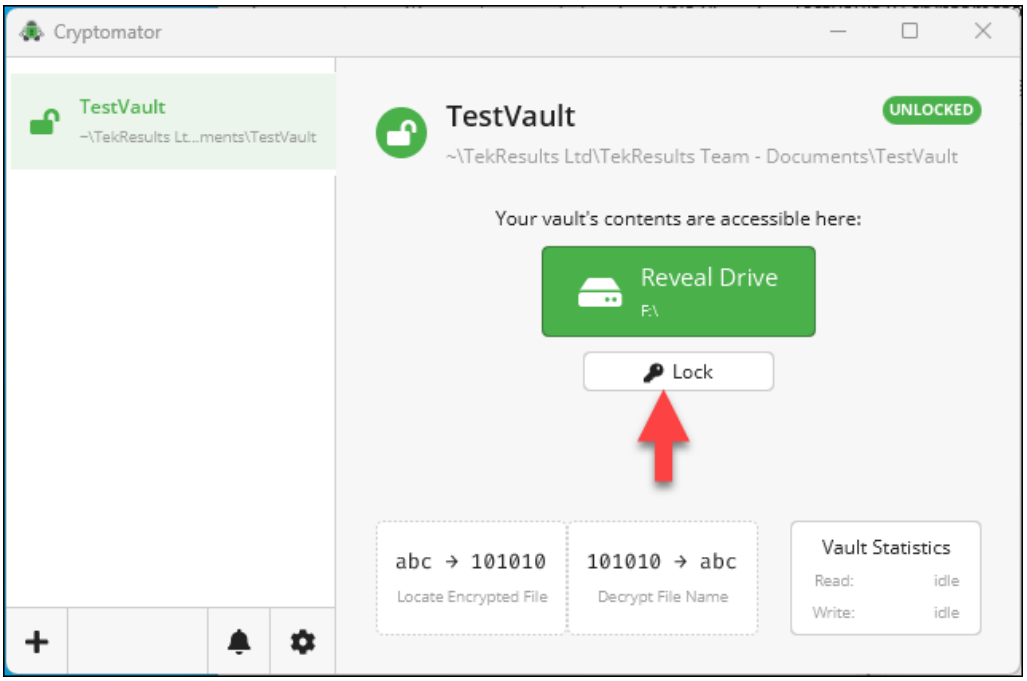
11. File Explorer opens with the vault open and ready for business.




In File Explorer, you can get another view of the vault by clicking **This PC** in the left panel. Then, in the right panel you will see **TestVault.** You can simply open that folder/vault and drag stuff into it.




When you're finished adding to or working with the data in your vault, you can go back to the Cryptomator dialog box and click the **Lock** button. This causes the vault to disappear from File Explorer. Rest assured that, even if someone were to navigate to your OneDrive folder and find your TestVault, the files you put in there won't even be visible. In the meantime, the contents of *TestVault* are already syncing with the cloud, where they will continue to be encrypted. When you're ready to work with your vault again, open Cryptomator and click the **Unlock** button to reveal your vault in File Explorer.




# Upgrade to Windows 11 now

By now, most of our clients have heard the news that Windows 10 will reach the end of its supported life on October 14, 2025. And, along with our constant reminders, we've also routinely sent our clients a list of the computers they own that are not eligible for the Windows 11 upgrade (their hardware is not compatible), and we have highly recommended that they replace those noneligible computers with newer models. That's not what this article is about.

This article is about getting on with upgrading the computers you own that ARE eligible for the Windows 11 upgrade. Yes, it's true, many of our clients have computers that CAN run Windows 11 but are not doing so. There can be many reasons for this.

The most common reason is that it's inconvenient to upgrade multiple systems. The upgrade procedure is amazingly simple, but the 2 hours or more that it takes the upgrade to complete puts many people off.

Another reason is they don't know how to upgrade. Never fear, instructions are coming at the end of this article.

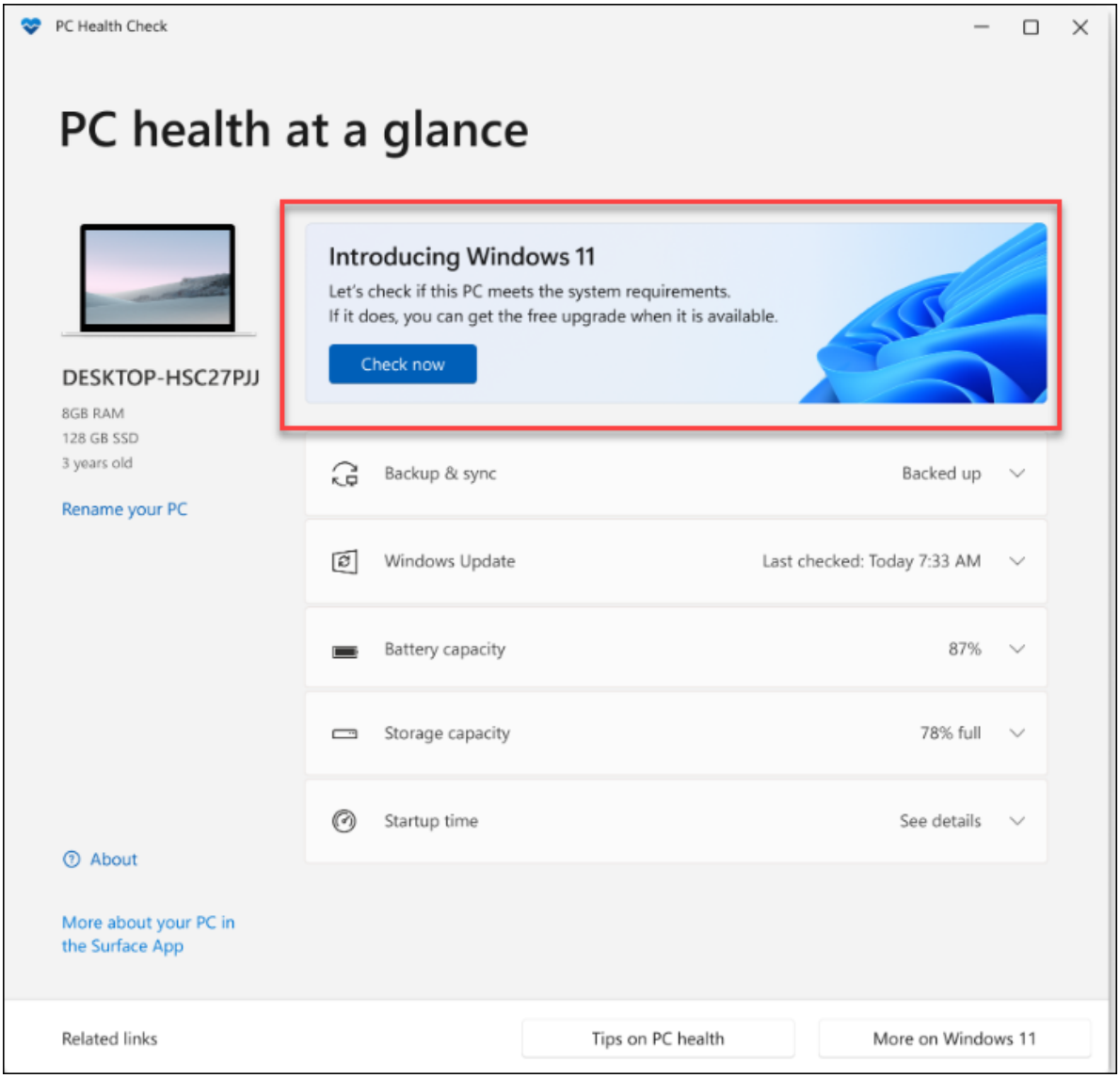
To us, the most important reason to put off upgrading is that the client may run business-specific software and due diligence needs to be done to make sure that the software will run on Windows 11. Typically, that just means a call to the software developer to ask them. You wouldn't want to upgrade your computers only to find that your accounting software won't run on 11.

## How do I know if my Windows 10 computer is eligible for the upgrade?

If you are a regular PM client with TekResults, we can tell you. By now, you've probably already received the list of your eligible computers, which we sent you by email. Missed the email? No problem, just ask us. If you are not a regular PM client, do this:

On your computer, go to Start > Settings > Windows Update. Typically, if your computer is eligible for the upgrade, there will be a **Download and install** button for Windows 11.

And finally, if you are unsure about your system's eligibility, download, install and run Microsoft's PC Health Check app.
In the PC Health Check app, under the **Introducing Windows 11** banner, click the **Check now** button.
After a quick check of your system, the app will tell you if your computer is eligible for the upgrade.

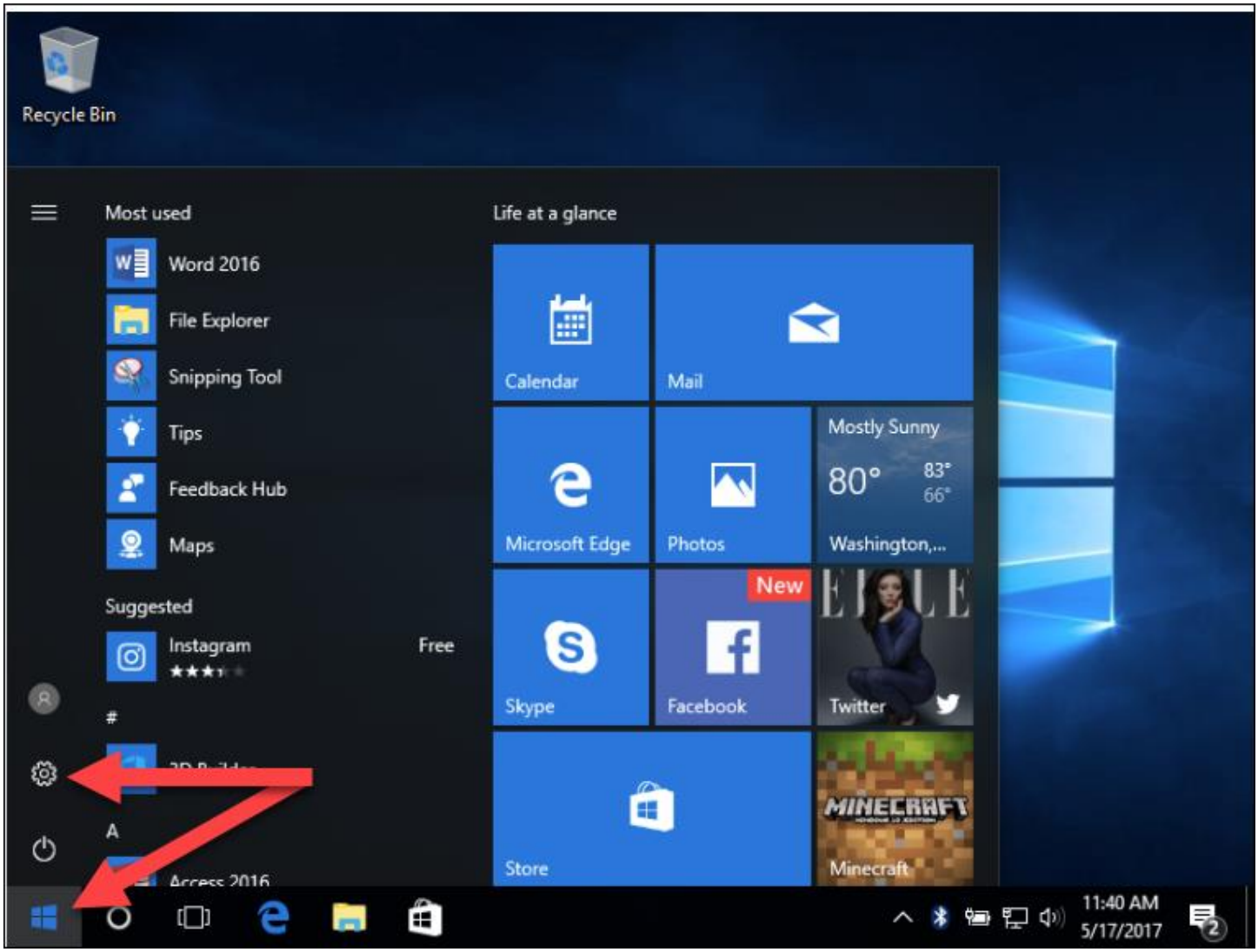



## How to do the upgrade

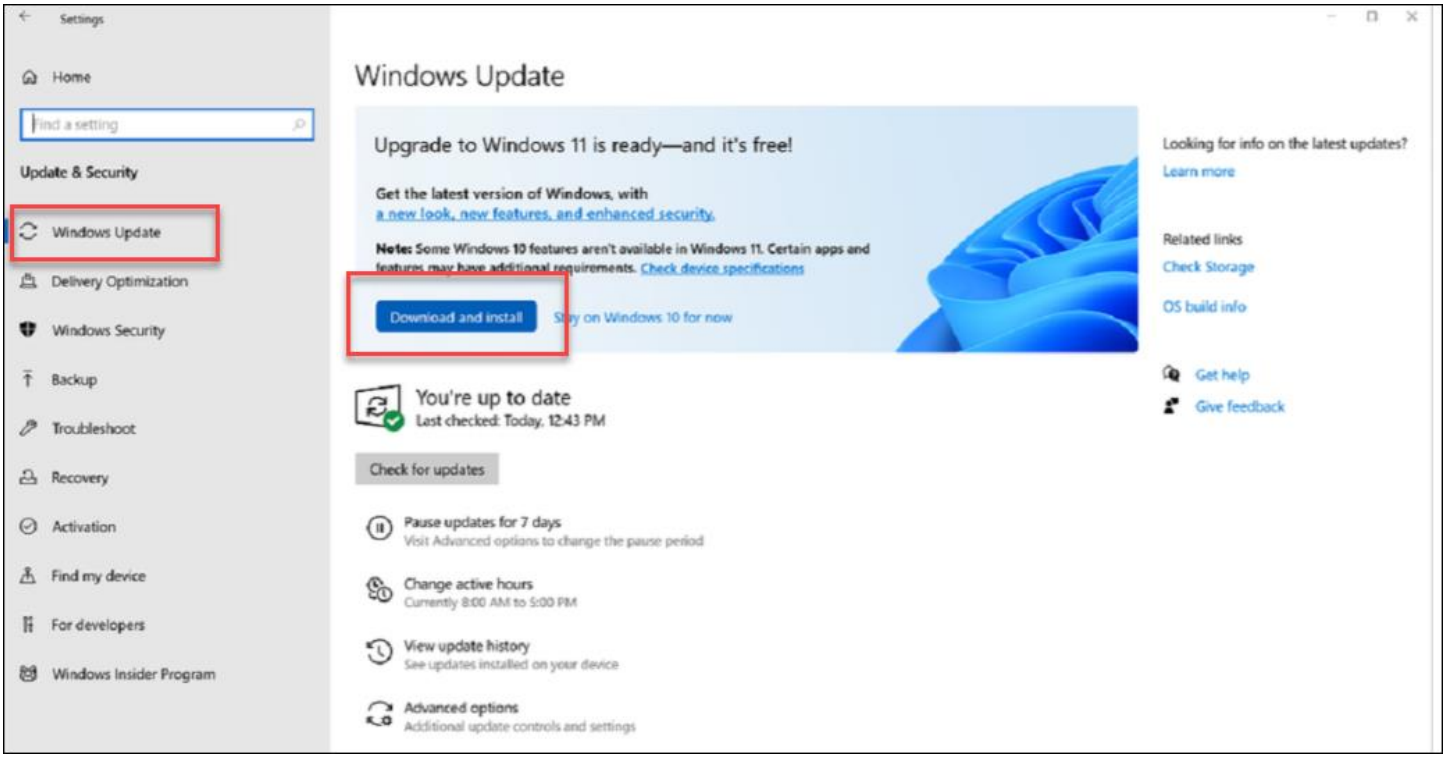
Ok, so you know your computer is eligible for Windows 11, you've done the due diligence to make sure all your software will run on Windows 11 and you're ready to go. We recommend you schedule the upgrade at the end of a workday. You can start the upgrade and let it run overnight. We recommend doing this one computer at a time. No sense in having multiple computers with issues when you come in the next day… yes, it can happen. Sometimes the upgrade fails, and you have to call us to fix the problem. Don't worry, we're here for you!

So HOW do you do the upgrade. That's the easy part.

1. Click **Start** and then in the menu that appears, click the **Settings** cog.




2. In the left panel, click **Windows Update**.
3. In the right panel, look for a section that offers to upgrade to Windows 11 and then click **Download and install**. Note, Microsoft changes the appearance of this menu all the time, so your menu may not match the screenshot below.




4. The download itself may take some time, and if you're doing this at the end of the day, don't be in a hurry to leave. It's a good idea to at least wait till the download completes and the installation starts. Once the installation starts, there may be some questions you have to answer at the beginning of the install.

As we mentioned, sometimes the upgrade runs into issues and fails to install. We can help if that happens. Please give us a call. How do you know if the upgrade was successful? The best clue is the position of the taskbar. Windows 11 places the taskbar in the center of the monitor. Windows 10 aligns it to the left of the screen.
Once you have upgraded you have a week to go back to Windows 10 if you find there are problems.

We can provide assistance if necessary.