Listener question from Theresa: Hello! I enjoy your podcast so much. Thank you for doing it. I've passed various episodes along to family and friends and I feel like it's helped me understand new areas of technology. I have questions about doing a Windows backup. I know you're mostly Mac people but I'd like to ask anyway :) I've read articles about the latest Windows update breaking things. I'd like to backup my Windows 10 before I do the update. However, the various articles I've read give different information. For instance, how much space do I need on a hard drive or thumb drive? Should I use a different drive from the one on which I do file backups? Do I need other equipment? How long does it take? What are the risks of not doing one? I feel a bit of a time crunch since we can no longer indefinitely put off updates. Thank you so much!

Space: assume the same amount of disk space the original hard drive has. Don't use a flash drive, get an external sata drive*. Assume its going to take hours, again depending on how large the source drive is. I've had it take 6-28 hours. ALWAYS use a different drive than you use for file backups. No other equipment is necessary. The results on NOT having a restore media is the loss of the time involved in rebuilding your computer from scratch, having to reinstall all applications drivers settings and getting the data restore.

** SSD drives are faster, more expensive and tend to fail spectacularly all at once. SATA drives are cheaper and faster than flash drives and easier to pull data off even a drive that's starting to have bad spots.

Windows backing up before major update or after major work

You should have multiple backups in different formats on different media. That way you have multiple possible recoveries in case of media failure on the backup hard drive, software failure from your backup program, fire/disaster. One copy should be offsite and/or cloud based. Your backup strategy should also include a way to restore from an earlier version of a file or folders in case of a ransomeware attack. Eg. If the ransomware hits and the backup runs after the undetected attack, you need a way to get back to the uncorrupted version.

1) System restore: This allows you to drop back to an older "restore" if a driver malfunctions or you get hit by malware. This is often turned off by default on many machines. You can find this setting in the older control panel, or search for it with the start menu search. "Create restore point" usually finds it.
    i) This takes you to the "System properties" tab in control panel, in the "protection" section. Click on "configure restore settings" to say how much hard drive space to reserve (more space = more restore points saved). If it is "off" turn it on and make sure the space is not set to tiny amount (often I see it as zero). I like to have 10 gb or more, to make sure I have multiple restore points to choose from. Some reports are that each restore point takes about 600mb, but that varies.
    ii) Once you have upgraded operating systems, the old restore points are invalid.
2) Creating a system image – the time varies on size of the drive, I have had it take 5-24 hours. The size of the image is also dependent on the amount of data. I assume if I have a 750gb OS/Data drive, I need a drive with this much free space plus working space. I'd select a 1tb backup drive.

a) This creates a disk "snapshot" of what your entire drive(s) contain, including the operating system and all settings and data. You need a large external drive, with space at least the size of your existing hard drive (s). I allow for 1.5 times the size of my drive just to be safe.
b) There is one built into windows backup, but I've had problems creating one in many cases. And it's an all or nothing, you have to restore the entire image.
c) There are a couple of excellent reliable free ones I use. They hope you'll actually buy one of their other upgraded products, but I have created and restored from these images successfully with the free version. (I have paid to support them later after I made sure they worked). The usual protection is to create an image, then if something fails, you can wipe your drive and reload EVERYTHING from the image. They also come with the ability to go into the saved disk image and retrieve individual files and folders.
d) Easus ToDo free backup https://www.easeus.com/backup-software/tb-free.html I use this about once a month to create an image. You can store multiple images on a single drive, but for safety, I rotate among several drives in case of hard drive failure.
You can setup a schedule with additive backups, but for simplicity, I create a self-contained image when I want to.
e) Macrium Reflect https://www.macrium.com/reflectfree. I use this about twice a year to do an additional image to have multiple "brands" or types. It works just like ToDo, creates a file that is a disk image.

3) Windows attempts to give you a way to back out of an upgrade. Occasionally it works, but I have had too many instances of a partial update in progress that NOTHING could recover, not restore points, not "uninstall latest update" or "uninstall latest feature update" or even command line uninstalling the last update. The only thing to do was to backup the data and reinstall windows. And reinstall programs. And reinstall updates while making sure drivers were compatible and up to date.
If the client had a disk image created recently, then we could recover the image and reload the data from the just-backed up failed drive. Windows attempts to save the user profiles and data when you reinstall on top of a failed update, sometimes that works and sometimes we have to backup and actually remove partitions and reformat the drive..
4) total restore.
If all else fails, get the data off the drive (I use a windows recovery disk or a linux live cd to get in and copy all the folders) and get downloadable install (cd or flash drive) and reinstall windows. Then reinstall programs. Get data from the cloud if you can't get the most recent copy off the drive.