Project Upskill II

How to Protect the Data that is Stored on your Devices

Cathy Thorn

March 11, 2025

Previous presentations of Project Upskill II covered the following:

Awareness of what personal information is being collected over the Internet and how to reduce it

Basic Cybersecurity for Personal Computers and Mobile Devices

Identifying and Mitigating Cyber Threats to Your Assets

These presentations are posted on WVComputerClub.org

How to Help (Nothing is 100%!)
Protect the Data that is Stored on Your Devices From Threat Actors

Threat Actors are of 2 types – Malware and Ransomware

Malware is done by any person or software that gains access to your device or accounts to read, manipulate, or steal personal information or data

Ransomware is done by any person or software that denies you access to your device (DOS) or data and makes you pay money, gift cards, or cryptocurrency to restore your system or data.

So what can you do?

1. Backup, Full Backup, and/or Copy data to secure external media or vetted cloud service

2. Encrypt your computer, mobile device, hard drives, removable media – like a flash or USB drive

3. What do I do with old equipment?

So what can you do?

1. Copy data, Copy with Synchronization, and/or Full Backup using secure external media or vetted cloud service

Confusion!!

Copy, Data Copy with Synchronization or Full Backup

Backup can mean **FULL BACKUP**

Backup can mean **DATA COPY and Synchronization**

Backup can mean **Just a COPY**

People use the term Backup interchangeably among these 3
Sometimes it is not clear which is meant.
Always clarify!

Why would you Copy, Data Backup, or do a Full Backup?

1. You want to be able to completely restore your computer in case of a hardware failure
2. You started writing a book or Family History that you work on regularly
3. Family pictures and Genealogy records – Family Tree Maker
4. Financial or Legal records – Tax Returns & Wills
5. Powers of Attorney
6. A list of user names and passwords
7. Resumes or Career records
8. List of collections of any type (like a coin collection)
9. Whatever digital data that is important

What do I need to make a Copy, Data Copy with Synhronization, or Full Backup?

You need one or more of these.
Hardware and proper software or Cloud Services and vetted software

Flash Drive or Memory Stick

Cloud Service

External Hard Drive – can connect directly to your computer or Wi-Fi

Just a COPY

Copy makes a duplicate of any data - documents, pictures, videos, etc. – *WITHOUT* the software that was used to create it.

For example, if you create a copy of a Word Document, you will need the software (Like Libre Office or Microsoft Office) in order to open the Copy

DATA BACKUP and Synchronization

Data Backup term implies that your data will be synchronized using hardware and/or Cloud services, and software

Synchronization means causing a set of data or files to remain identical in more than one location.

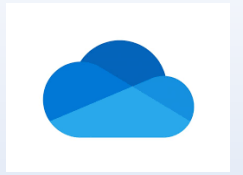
Many of the vendors have free versions or are reasonably priced, and depending on how much space you need, different pricing plans available.

Microsoft OneDrive – Data Backup and Synchronization Works across multiple devices

- Store files: Keep your files in one place, protected in the cloud
- Share files: Share documents and photos with others, and collaborate on files
- Access files: Get to your files from any device connected to the internet
- Sync files: Sync OneDrive to your computer so you can access your files even when you're offline
- Back up files: Keep your files, photos, and videos automatically backed up (COPIED)

Prices range from free to $20.00 per year to $100.00 per year.

Apple iCloud – Data Backup and Synchronization Works across Multiple Devices



iCloud is a service from Apple that stores data in the cloud and keeps it up to date across devices. It includes features like photo sharing, file backup, and password management.

- **iCloud Photos**: Access photos on all devices
- **iCloud Drive**: Store and access files in the cloud
- **iCloud Keychain**: Store and autofill passwords and credit card information
- **iCloud Backup**: Back up iPhones, iPads, and iPod touches
- **Family Sharing**: Share photos, collaborate on projects, and find shared content
- **Safari**: Sync open tabs, bookmarks, and Reading Lists across devices

Prices range from free to .$.99/month for 50 GB to $64.99/month for 12 TB

FULL BACKUP

FULL BACKUP

Encrypts and compresses the Operating System, applications, settings, configurations, **AND** all other data

FULL BACKUP

Requires a **Restore** to put everything back on a computer the way it was.

Apple

Apple has a Full Backup Application called Time Machine

It is built into Apple computer products

External equipment or a cloud-based service is still required

In July of 2025 a course will be given on Time Machine.
Watch for Apple Newsletter or Renaissance Magazine

For more information on iPhone, iPad, and iTouch, navigate to **https://support.apple.com/en-us/108771**

Basic Strategy for Data 3-2-1-1

3 sets of data on 2 different media with 1copy offsite – Your computer, other local hardware, offsite hardware or the Cloud

So what's the second1??

The second 1 is for another copy that should be Write-Once-Read-Many (WORM) format or the data should be set to Read Only

This may seem excessive

Your choice!

Examples of Data Backup and Synchronization Software besides iCloud and OneDrive

Google Drive – part of the Google suite of products Does not offer Full Backup Service

Acronis

BackBlaze

EaseUs

iDrive

Macrium Reflect

Many of the companies who offer data backup also offer Full Back capabilities

Hardware and Software Needed for Backup or Copy

You need hardware or The Cloud to do Full Backups or synchronized Data Backup
Many of the types of hardware/software or the Cloud can be used for either

Educate Yourself on the free Full or Data Backup software vs. Licensed (paid for) software and on the hardware or The Cloud choices.

Hardware and Software Needed for Copy, Data Backup, or Full Backup

Several manufacturers make External Backup Drives

https://www.pcmag.com/lists/best-external-hard-drives

Some of the most popular are Samsung, Western Digital, SanDisk and Seagate.

Check the Internet for recommendations

Caution! Some of the comparison sites are sponsored

External Backup Drive Samsung

External Backup Drive Seagate

Hardware and Software Needed for Backup

How big an External Backup drive should I get?

Personal Recommendation is that you purchase the External Backup Drive or Cloud Service with as much room as possible that you can afford – 1-3 or more Terabytes
With Cloud Services, you can add on space as needed for a price

SSD vs HDD – Solid State Drive or Hard Disk Drive if one is not using a Cloud service

External Backup Drive Seagate

Always find out which type of drive is in the equipment

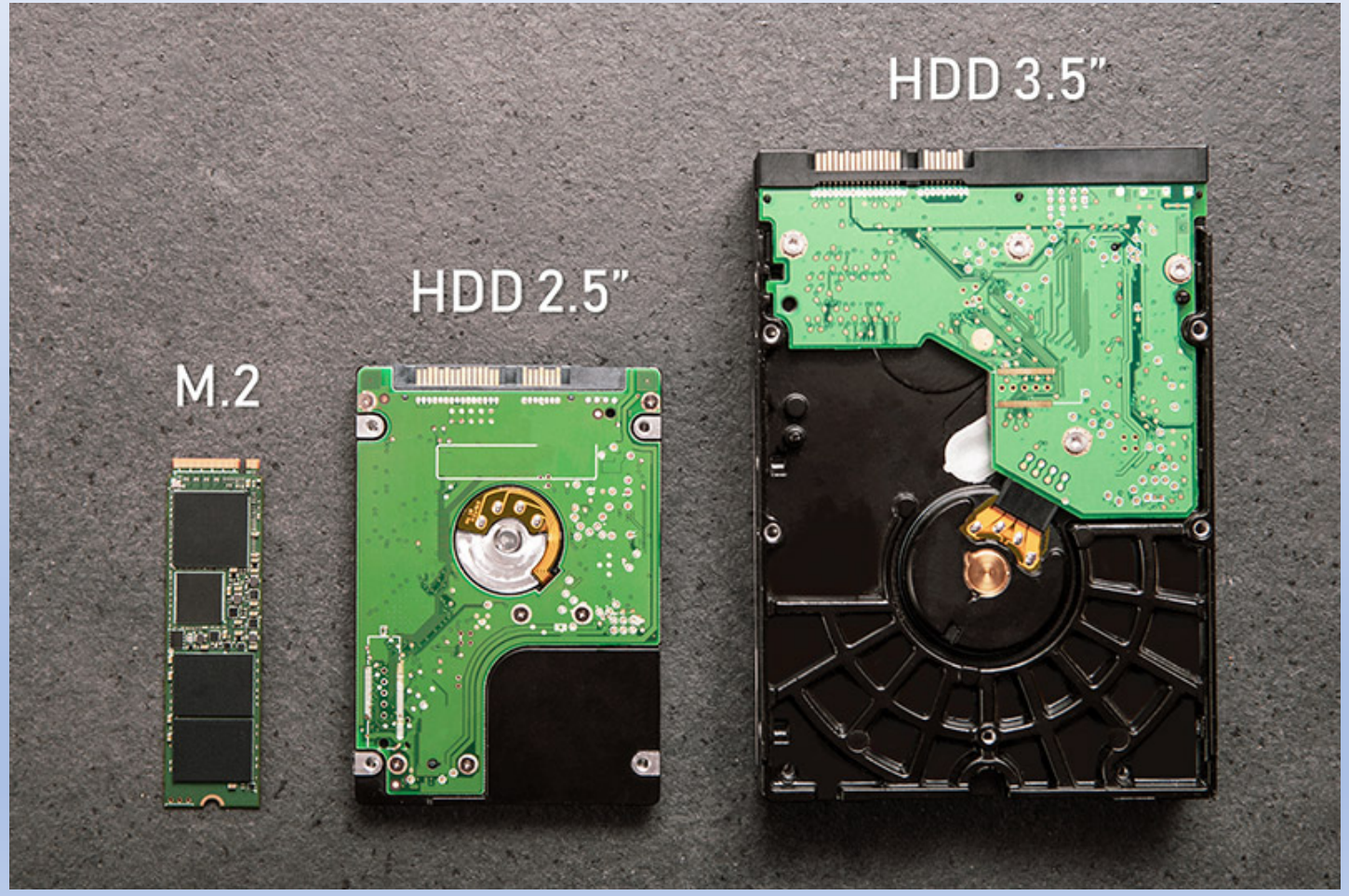
Solid State Drives are smaller, faster, but more expensive (getting cheaper)

But Hard Disk Drives are still fine

Be Aware – If either type of drive fails, some data may be recoverable

https://www.backblaze.com/blog/how-reliable-are-ssds/

Solid State Drive vs. Hard Disk Drive



Easy to see the differences in SSD and HDD – the M.2 is an SSD

What about Flash Drives (Memory Sticks)? Can they be used for Full Backup and Recovery?

The answer is Yes, depending on the size you need

There are flash drives larger than 1 Terabyte available, but be careful!

The USB port in your device must be able to support the larger flash drive.

Do not purchase one of these higher capacity flash drives unless it is a major manufacturer like Samsung, Western Digital, Seagate + others.

Do Your Homework!!

Educate Yourself on the free Backup software vs. Licensed (paid for) software and on the Hardware or Cloud choices that support Flash Drives

Some More Points

Microsoft's Win10 and Win 11 have a "backup" feature which copies apps, data, settings, and configurations called Backup Tool.

Type backup in the Type here to search field on the Task Bar

If you choose to use Microsoft's OneDrive or Backup Tool,

It is ESSENTIAL to take a Tutorial!

Go to Microsoft.com.

Search for tutorials for a list.

Questions?

So what can you do?

2. Encrypt your computer, mobile device, hard drives, removable media – like a backup external drive or a flash or USB drive

What is encryption anyway?

Encryption is based on an algorithm – a mathematical way to convert data into an unreadable format unless one has the key to unlock the algorithm code

National Security Agency recommends Advanced Encryption Standard (AES)

3 Versions AES 128
AES 192
AES 256
ALL ARE SECURE

Usually one would want to use AES 256, the most secure

Older equipment may need to use AES 128 or 192 avoiding slowing the system

The numbers refer to the encryption key length – the longer the more secure

To Encrypt may seem a daunting task

Some Encryption Software Examples you may already have

Bitlocker – built-in encryption software for Win 10 and Win 11

Caution: Win 10 version is not as complete or robust and has some technical issues

Uses AES-128 or XTS-AES 128-bit Works with Win 10 PRO but some manual installation may be required

FileVault – built in encryption software for Mac OS Uses AES XTS which is a "tweakable" version of AES256

Works with Panther 10.3 since 2003 and forward

FileVault 2 has been available starting with OS X Lion since 2007

Possible Disadvantages of Bitlocker and FileVault

Not Open Source – What does that mean?

The program code for the software is not available to the public. Expert programmers cannot examine and find bugs in the software or improvements to alert Apple

When possible choose applications that are Open Source code

Neither is granular. That is, they cannot be used to encrypt a folder or file. They can encrypt only systems.

Other Encryption Software

VeraCrypt **a free, open-source program that encrypts files, partitions, and storage devices**. It can be used to protect personal files, company data, and entire drives. **Although it gets high marks, it has greater depth and ore functionality and may not be for the typical user**

AxCrypt **a file encryption program that protects your data with strong encryption.** You can use it to secure files, manage passwords, and back up your data.

It is not open source

Cryptomator **a free, open-source application that encrypts files stored in the cloud or on a NAS**. It's available for Windows, macOS, Linux, Android, and iOS. Appears to be more user-friendly and simpler.

Advantage of the Other Encryption Software

During my research, these three came up on every comparison web site I visited

These three all allow individual folders and files to be encrypted which FileVault and Bitlocker do not

Why would you want to encrypt just some files an folders? Encryption of an entire system MAY create performance issues especially on older equipment

CAUTION!!

Once you have your encryption key – assigned to you at the time you encrypt – put a copy of this key in a home safe or Safe Deposit Box.

Make sure the Executor of your estate knows where to find the key and how to get it from either or both of these places.

So what can you do?

3. What do I do with old equipment?

Reimage your computer – Wipe it Clean

Writes 0s and 1s across an entire drive

Many software packages provide a method to wipe more than once

Choose software that is NTIS compliant

If you know the drive you are wiping is an HDD and not an SSD, the software using the older DoD standard may be used

Several Software Products are available

1. **For Home use Open source may not be important to you**
2. **Software that does not work across most devices may not be important to you if you are a PC user**

Jetico Best Crypt

This software is primarily designed for **data encryption** but also offers **disk wiping** capabilities as part of its suite of tools. When it comes to disk wiping, Jetico's disk wipe software focuses on ensuring that deleted data is irrecoverable

NTIS Compliant
Not Open Source
Works across most devices

Several Software Products are available

Specific to Apple

MacOS Built-in Disk Utility

- **Features**: macOS has a built-in disk wiping tool through Disk Utility. You can securely erase disks or volumes with the "Erase" function, and for more secure wiping, you can choose to erase free space or use multiple-pass erase methods.
- **Supported Devices**: MacBooks, iMacs, external drives
- **Free Version Available**: Yes (built into macOS)
- **How to Use**: Open Disk Utility, select the disk, and choose the "Erase" option. For a more secure erase, you can select "Security Options" and adjust the level of erasure.
- **Website**: Apple Support - Disk Utility

Several Software Products are available

Blancco

Offers certified data erasure solutions for enterprises, ensuring compliance with various data privacy standards.

NTIS Compliant
Not Open Source
Works across most devices

DBAN

A free and open-source tool for wiping hard drives. It is widely used for personal use and small businesses.

Non NTIS Compliant
Open Source
Does NOT work across most devices

Several Software Products are available

KillDisk

Provides disk-wiping solutions for individuals and organizations, with both free and paid versions. Offers support for a wide range of drives.

NTIS Compliant
Not Open Source
Does NOT work across most devices

Macrium Reflect

A popular disk imaging and backup software for Windows that provides users with powerful tools to create backups and restore systems in the event of data loss or system failure.

NOT CLEAR on NTIS Compliance
NOT Open Source
Does NOT work across most devices including Apple

Several Software Products are available

Ccleaner Drive Wiper

Wipes either just the free space on a drive or the entire drive, depending on the user's needs, with different levels of overwrite security to choose from depending on how thoroughly they want to erase data.

NOT NTIS Compliance
NOT Open Source
Does NOT work across most devices including Apple

CAUTION! Drive Wiper can harm SSDs

Questions?