



ENCRYPTION



Mark Schulman

Your Presenter



- Mark Schulman
- IT professional for about 40 years
- No affiliation with any product

What is Encryption?

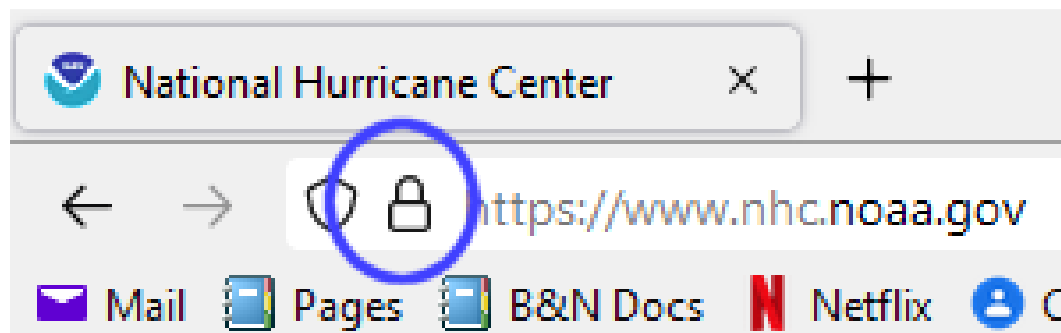
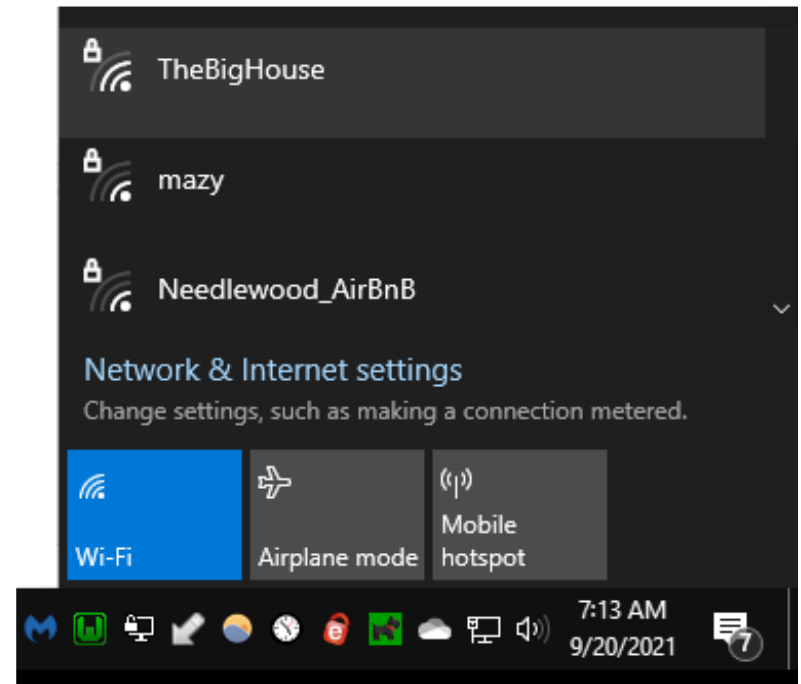


Scrambling information
so that it can't be read by
unauthorized people.



You Already Use Encryption

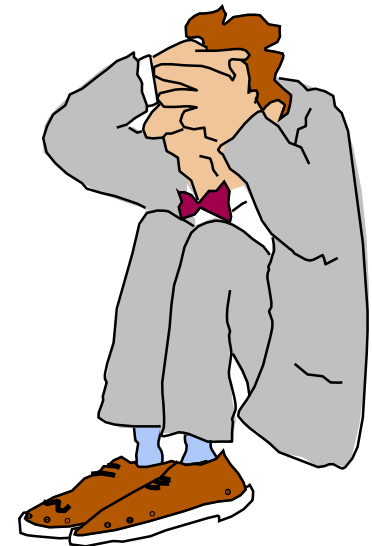
- Wifi
- https



Examples: Keeping Your Data Private

You have personal information that you want to keep private:

- You don't want your roommate snooping through your PC when you're not home
- Your flash drive has passwords for your social media accounts
- You want to email personal information to your tax accountant



Just a Word of Warning

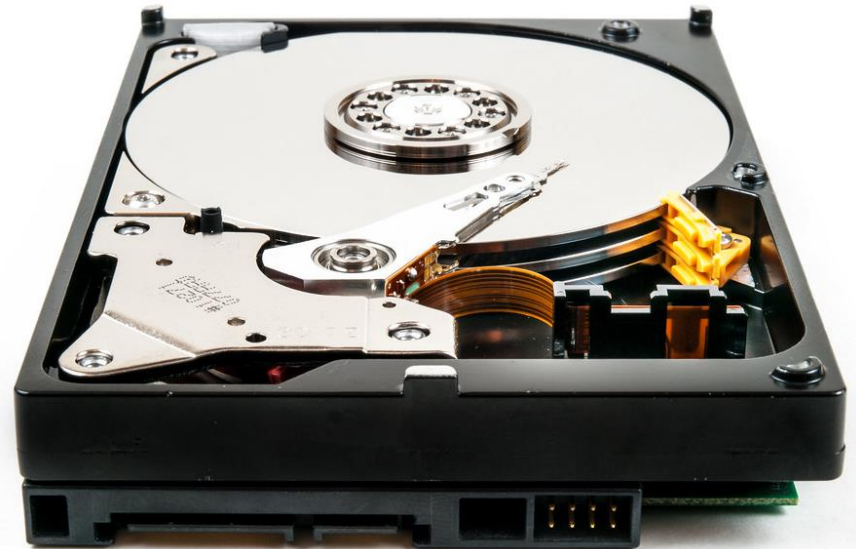
Q. How secure is your email?

A. *Not at all.*

Treat every email as if it would be published in the local newspaper.

Agenda

- Single-file encryption
- Encrypted containers
- Whole-disk encryption
- Phone encryption
- A little bit of other stuff



Single-File Encryption



Single-File Encryption

- Encrypt a single file
- Possible uses:
 - Email a file to your accountant
 - Store a list of your medications on your flash drive



Technique 1: Microsoft Office

- Microsoft Office has built-in encryption
- To encrypt:
 1. File
 2. Info
 3. Protect Document (or spreadsheet)
 4. Encrypt with Password



Demo



Technique 2: Other Types of Files

- Lots of free encryption software:
 - AESCrypt
 - 7-Zip
 - Many more ...



Demo



Caveat #1: Filenames

- Don't give away too much in the filename

Name	Date modified	Type
 ca.key	5/28/2019 7:42 PM	KEY File
 FBRN-PROD.ovpn	8/11/2020 10:38 AM	OpenVPN Config ...
 Job Search To-Do List.docx	9/18/2021 4:42 PM	Microsoft Word D...

Caveat #2: Password Exchange

- Don't send a password with the encrypted file!

○ **Mark Schulman** <marks@qcorp.com>

To Pete <pete@qcorp.com>

[Reply](#)

[Reply all](#)

[Forward](#)

[Delete](#)

[Add to Safe Senders](#)



1 attachment ▶

[View](#)

[Download](#)

Dear Pete,

The list of phone numbers is attached.

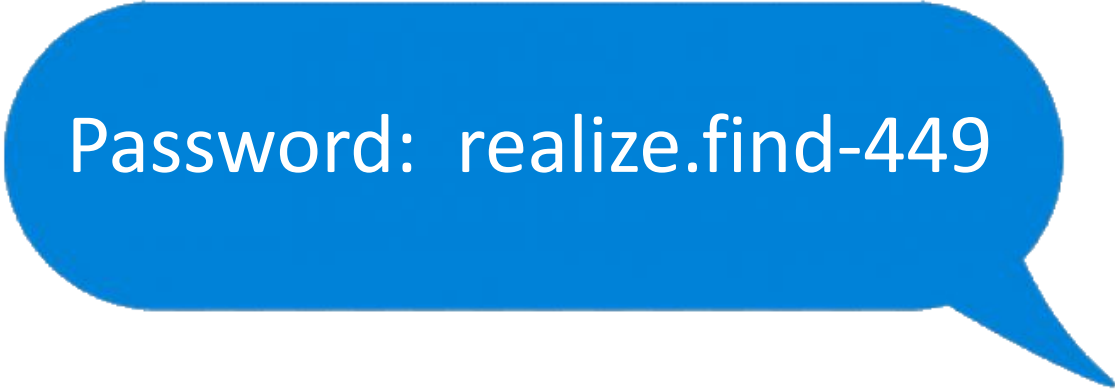
The file is encrypted. The password is "callmesoon!"

Thanks,

Mark

Caveat #2: Password Exchange

- Best way to send a password: Phone call
- 2nd-best: Text
- Absolute worst: Email



Password: realize.find-449

Encrypted Containers



Encrypted Container

- Enables you to create a virtual drive on which all your files are encrypted
- Possible uses:
 - Financial planner's client files on PC
 - Carry a large number of sensitive files on your flash drive



VeraCrypt

- Developed by French security company IDRIX
- Based on TrueCrypt
- Open source software
- Free
- Available for Windows, Mac, Linux



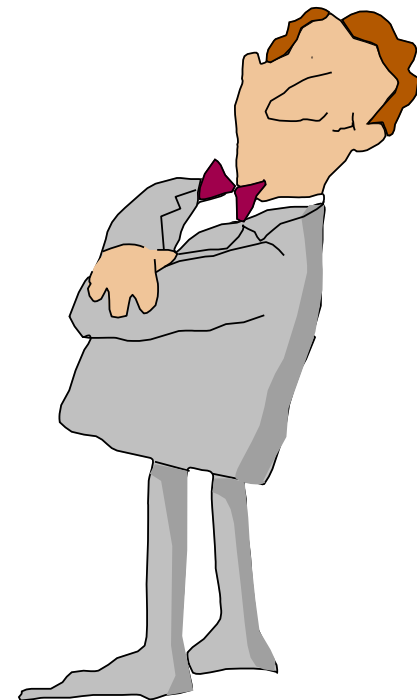
Encrypted Container

- Enables you to create a virtual drive on which all your files are encrypted
- Uses:
 - Area of your disk containing especially sensitive data
 - Flash drive that you're worried about losing



Creating a VeraCrypt Container

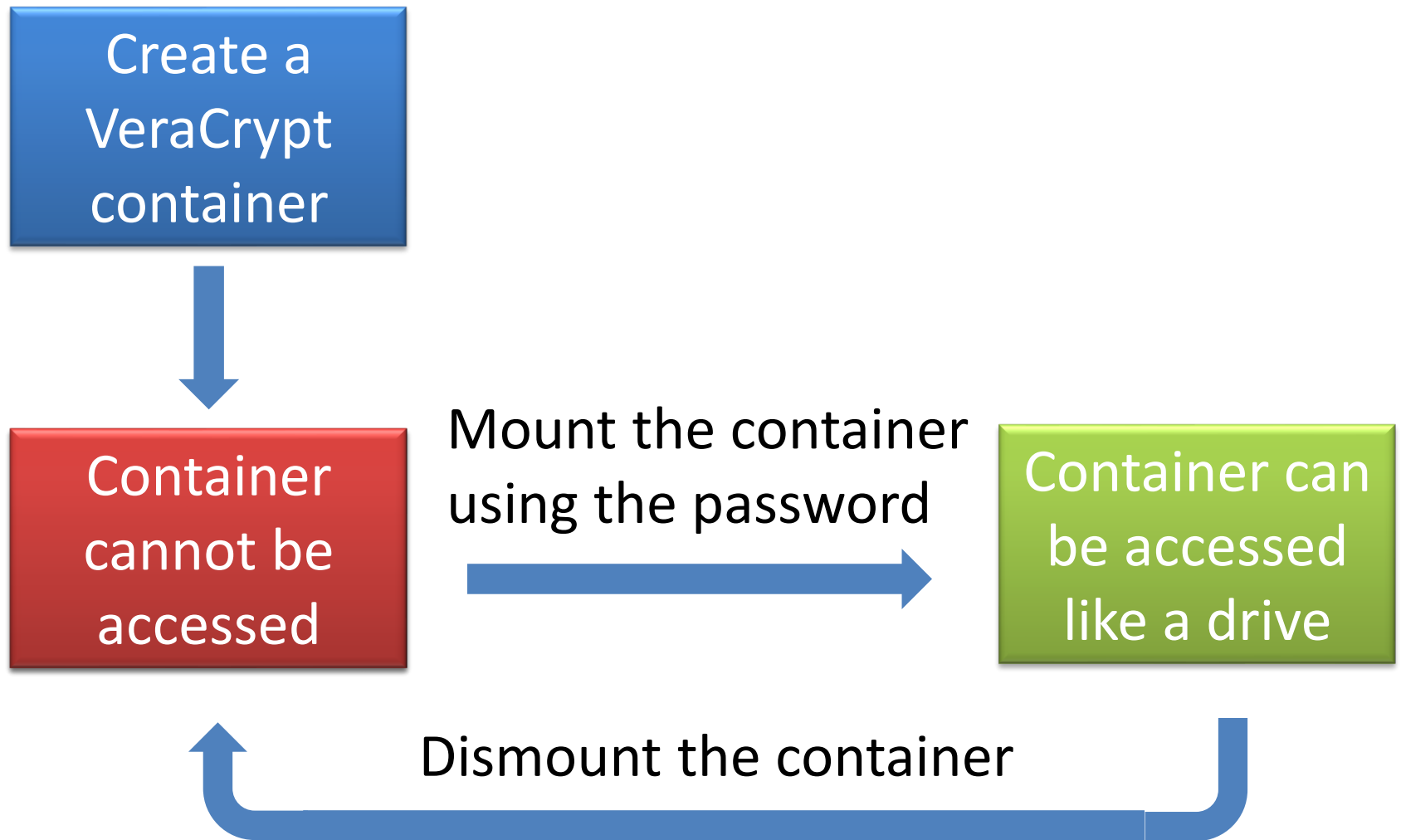
- Container is a file
- Create it wherever you want (hard drive, flash drive, external drive)
- Can be any size (can be very big)
- Encrypted based on a password



Using a VeraCrypt Container

- When mounted, the container looks like a drive
- Must have the password to mount a container
- When not mounted, the container's contents is unreadable

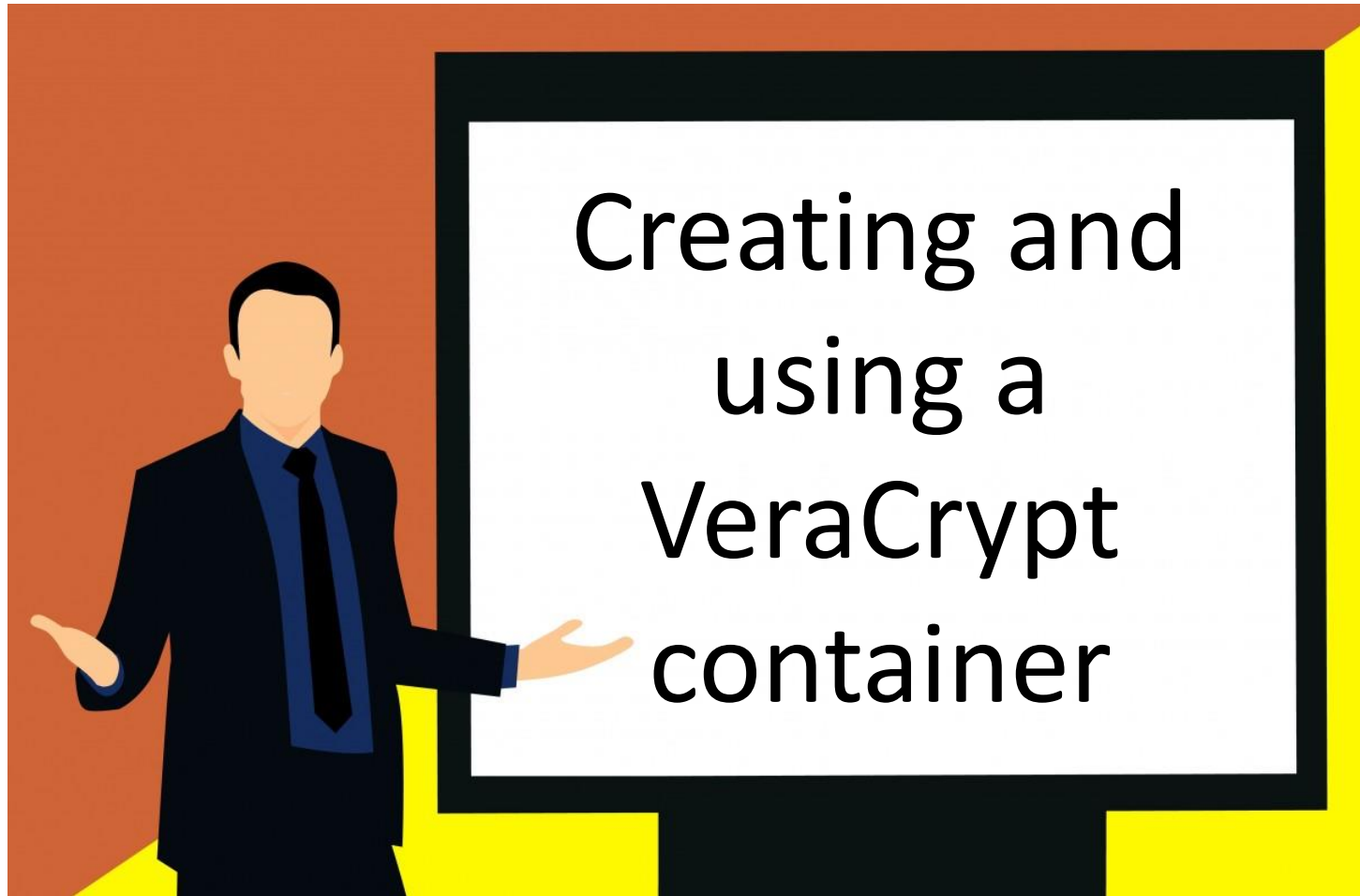
How It Works



Using a Container -- Summary

- Everything in the container is encrypted
- Encryption and decryption happens behind your back
- Also known as OTF (“on the fly”) encryption
- Data is only accessible when the container is mounted

Demo



Real-Life Use Case

- Medical records backups



Another Real-Life Case

- Travel flash drive
- Contains passport images, itinerary, password lists, and more



Keeping a Vault Inconspicuous

- A vault can have any extension you want.
- Modification date of the vault itself never changes.

Name	Date modified	Type	Size
 \$RECYCLE.BIN	2/1/2022 2:22 PM	File folder	
 System Volume Information	1/8/2024 9:34 AM	File folder	
 BackupV.mpg	10/28/2020 9:42 AM	Movie Clip	2,929,721,344 KB

What the Bad Guys Can't Tell

The bad guys can't tell ...

- that a particular file is or is not a VeraCrypt container
- when a container was last accessed
- what's in a container
- how much of a container is used

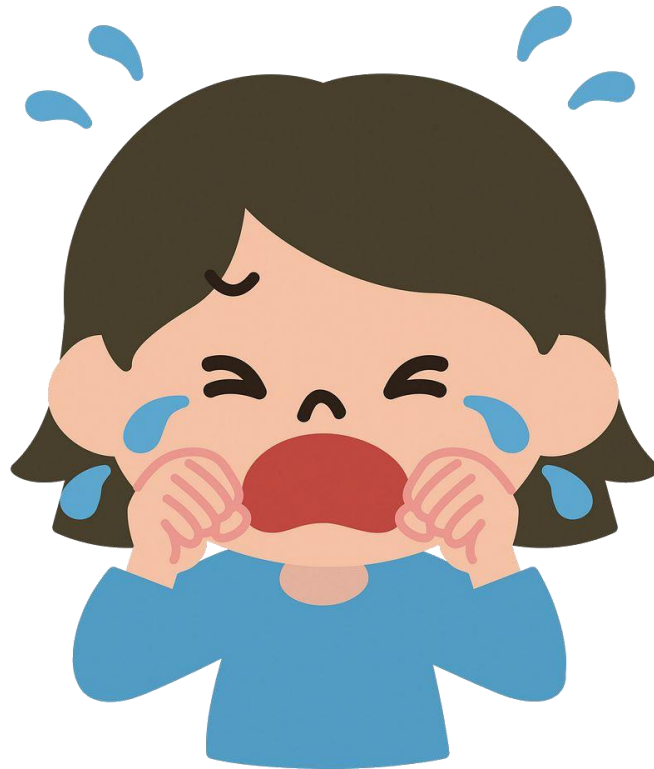
A Few More Cool VeraCrypt Features

- Traveler flash drive
- Key files
- Hidden containers



Lost Password

- If you lose your password



Whole-Drive Encryption



Whole-Drive Encryption

- Encrypts the entire contents of your hard drive
- Use: Prevent anyone from accessing your PC or laptop without a password



A Story



VeraCrypt

- VeraCrypt can encrypt your entire hard drive



VeraCrypt Boot

Password:



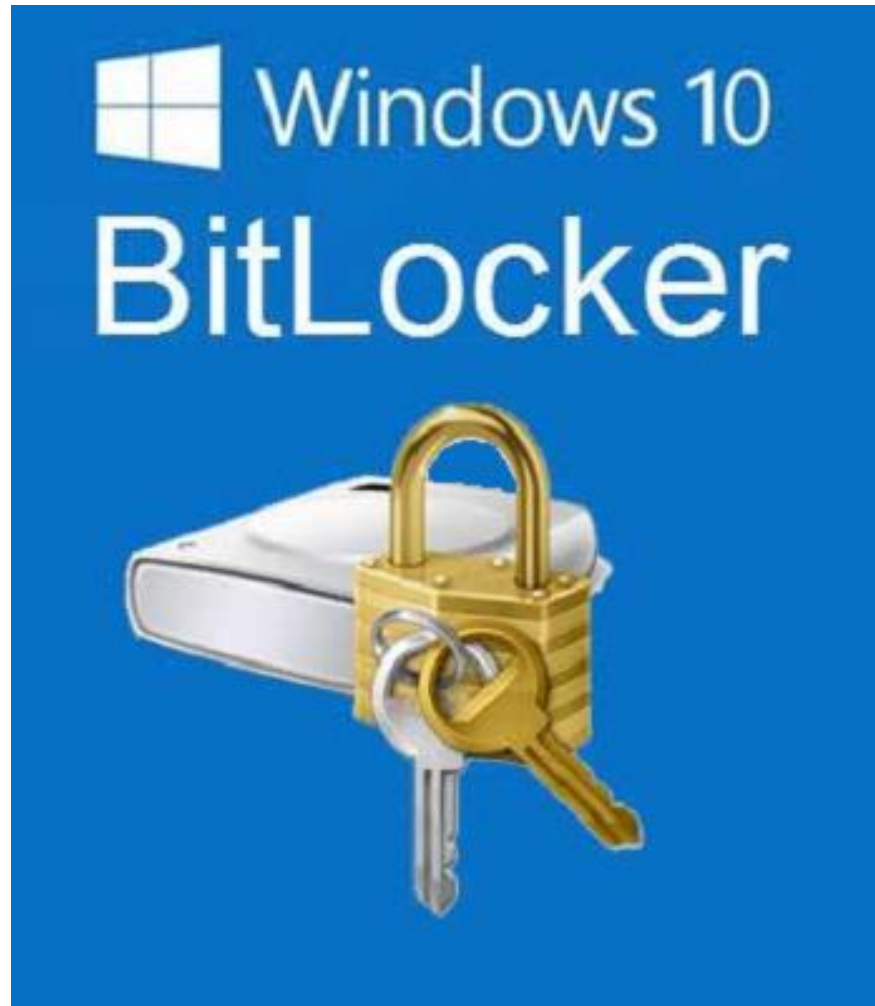
Inspiron

How Safe Is It?

- Uncrackable by any known technology
- Use a good password
- Don't lose your password!
- Back it up like anything else



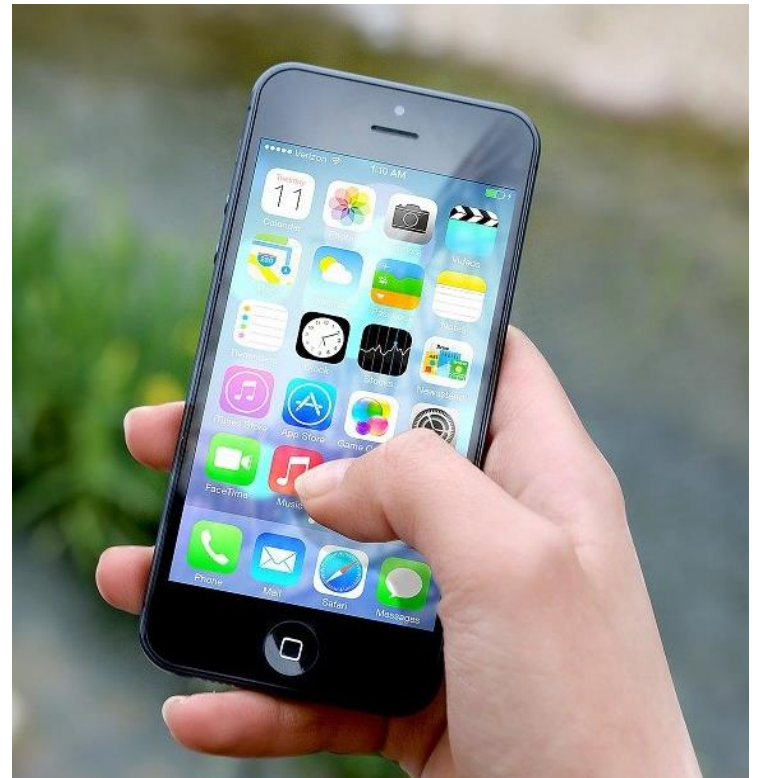
Microsoft's Solution



VeraCrypt vs. BitLocker

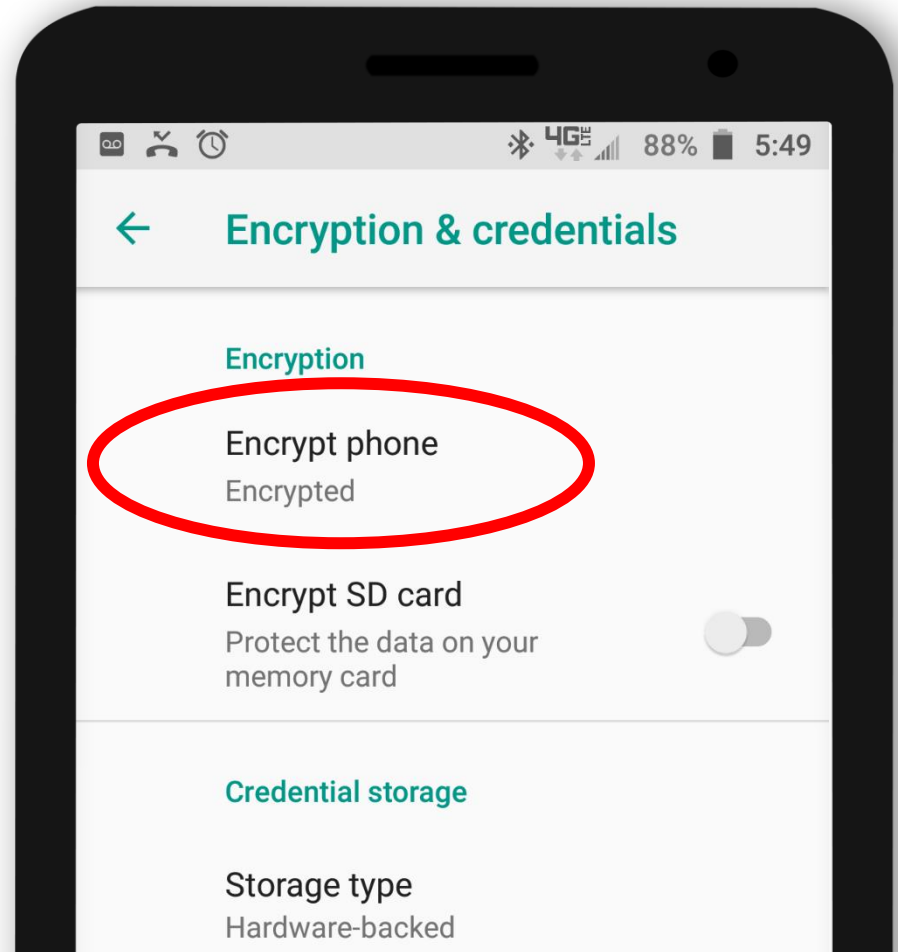
	VeraCrypt	BitLocker
Written by	IDRIX, TrueCrypt	Microsoft
Available for	Windows (any version), Mac, Linux	Windows Pro or Enterprise
Preinstalled	No	Yes
Transparency	Open source	Proprietary
Management	No corporate features	Can be managed by Active Directory

Phones



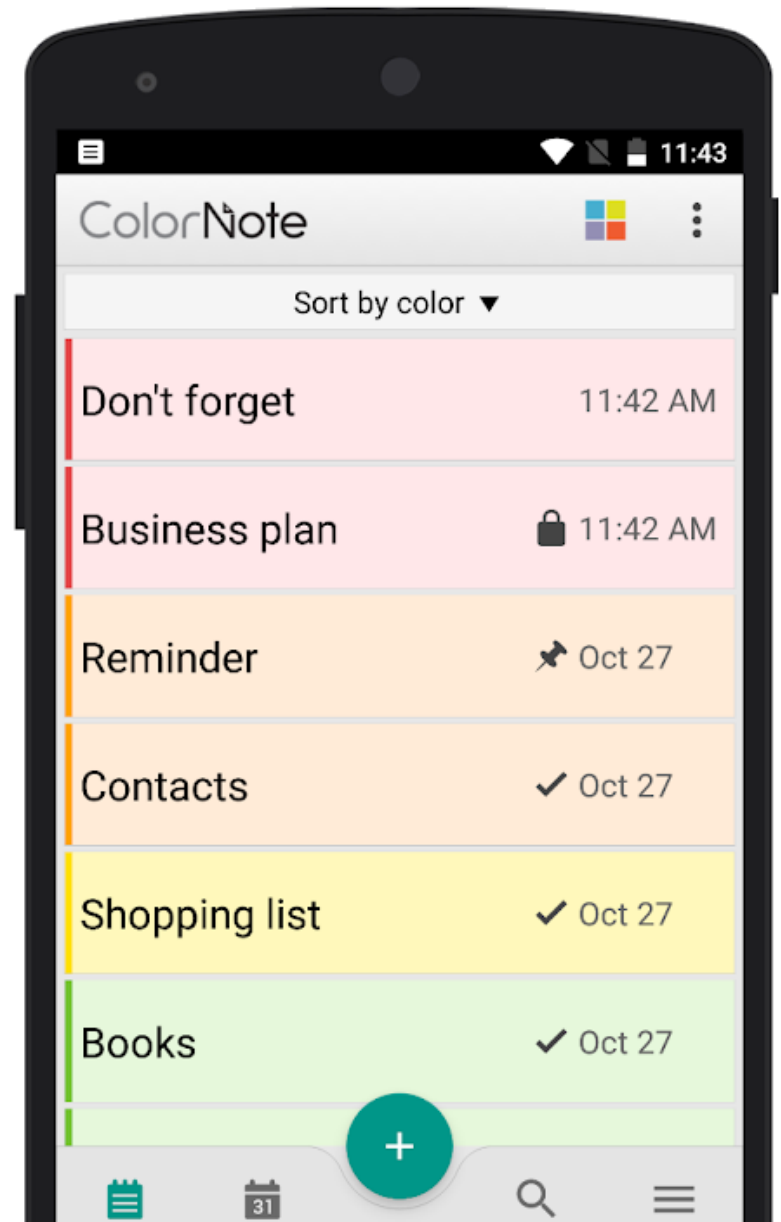
Phone Encryption

- Modern phones include whole-phone encryption
- Encryption is only as good as your password



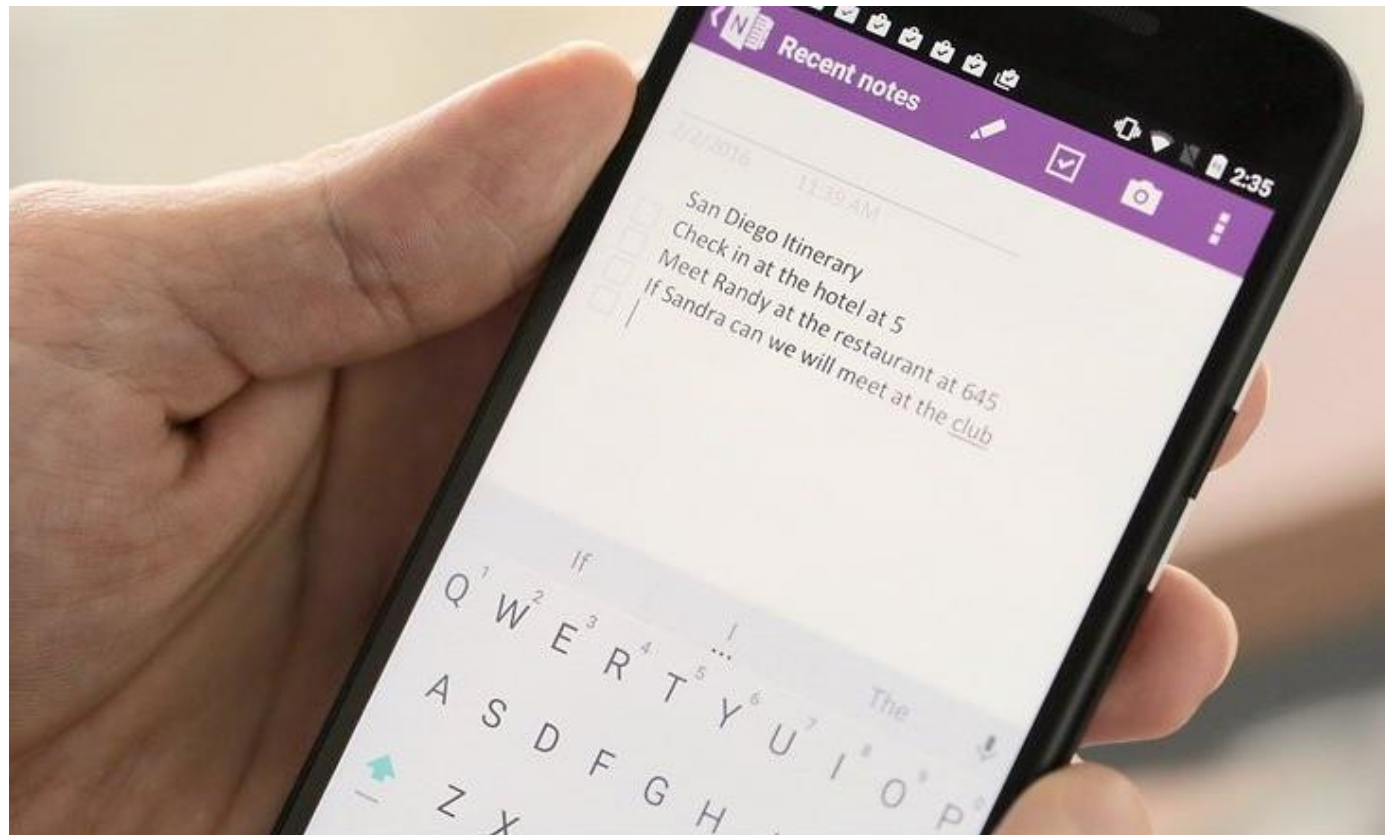
Encrypted Note App

- Endless encrypted note-taking apps
- At right: ColorNote



Microsoft OneNote

- Sophisticated note-taking and organization app that includes encryption



Using Good Passwords



PASSWORD COMMANDMENTS

- 1. use a password manager*
- 2. Different password everywhere*
- 3. use a password generator*

Password Generator

- All password managers have one built in
- Some free password generators:

BitWarden

<https://bitwarden.com/password-generator>

Dashlane

<https://dashlane.com/features/password-generator>

Mark

<https://whatsthisthen.com/passwords>

Where to Get It

AESCrypt	https://www.aescrypt.com
ColorNote	https://www.colornote.com
OneNote	https://www.onenote.com
VeraCrypt	https://veracrypt.fr
7-Zip	https://www.7-zip.org

All these apps are free

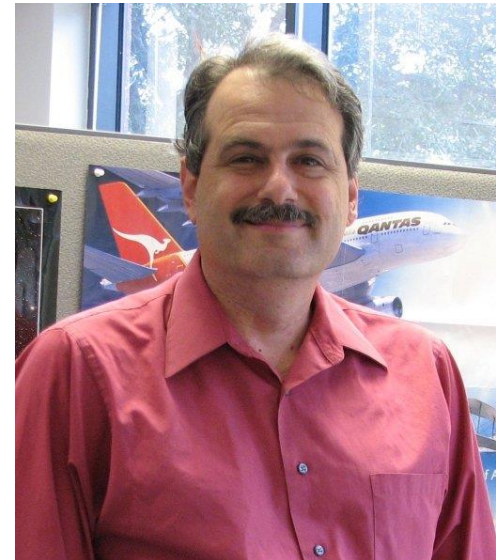
Questions?

Encryption

Mark Schulman

Central Florida Computer Society

marks@schulmans.com



An International
Association of Technology
& Computer User Groups