



ENCRYPTION



Mark Schulman

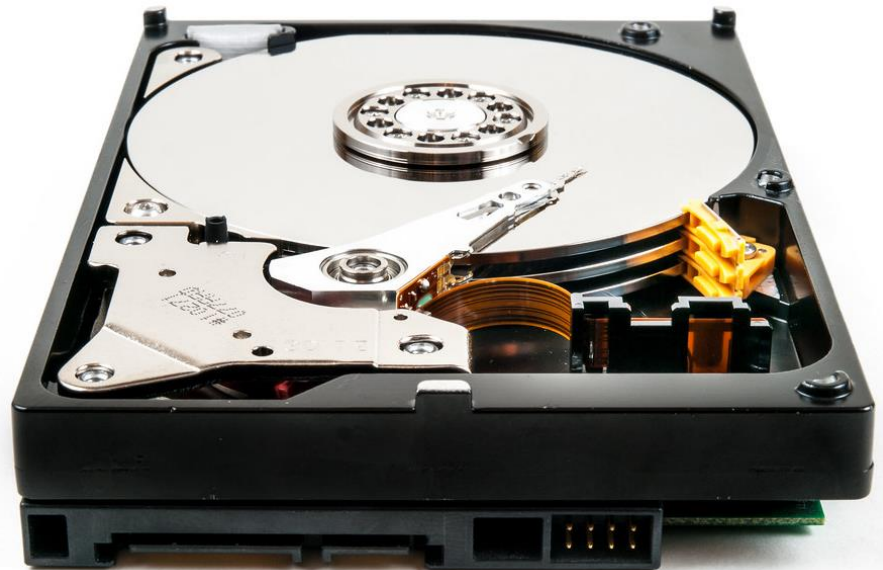
Your Presenter



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

Agenda

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



What is Encryption?

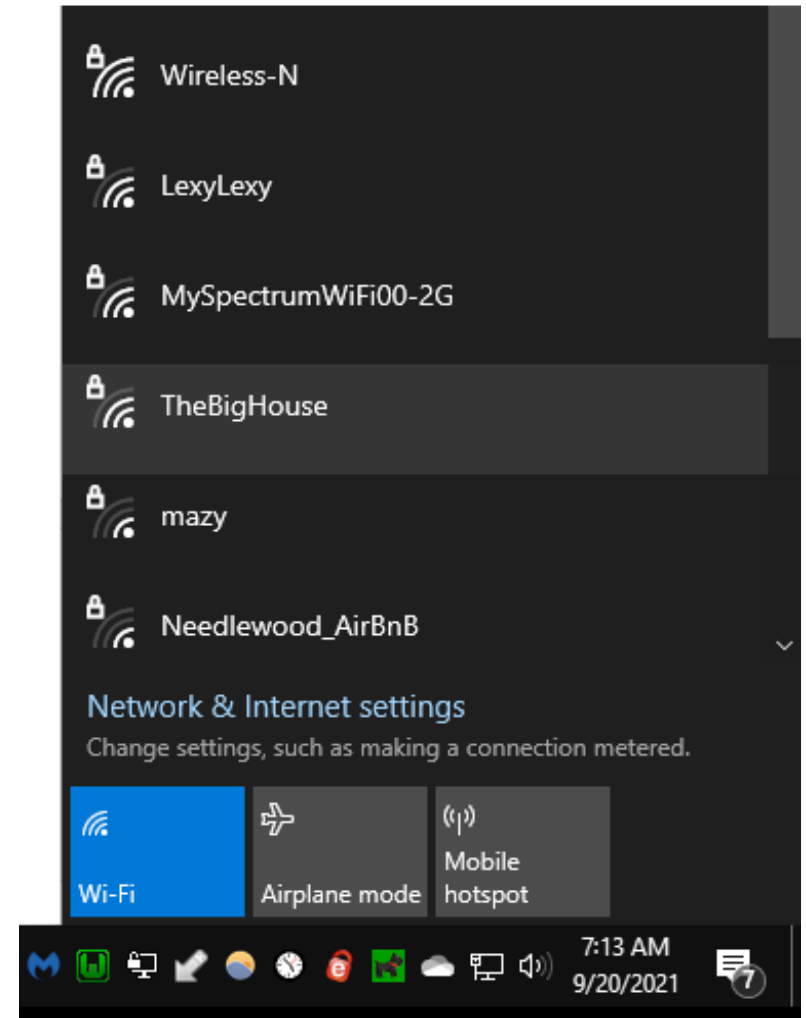
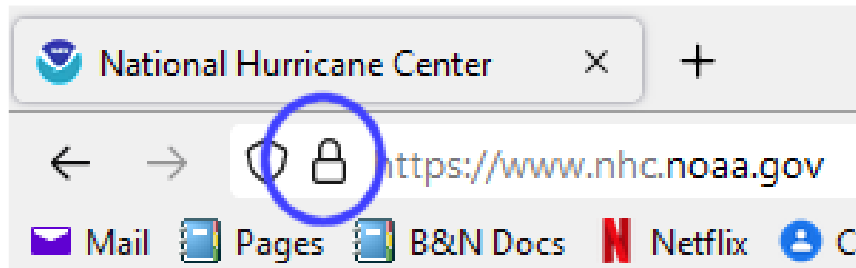


Scrambling information
so that it can't be read by
unauthorized people.



You Already Use Encryption

- https
- Wi-fi



Private Data

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



Single-File Encryption



Single-File Encryption

- Single file you want to encrypt
- Use when you want to encrypt a single file for yourself or someone else



Examples of Single-File Encryption

- Flash drive contains a list of lock combinations at work
- Email tax returns to your accountant

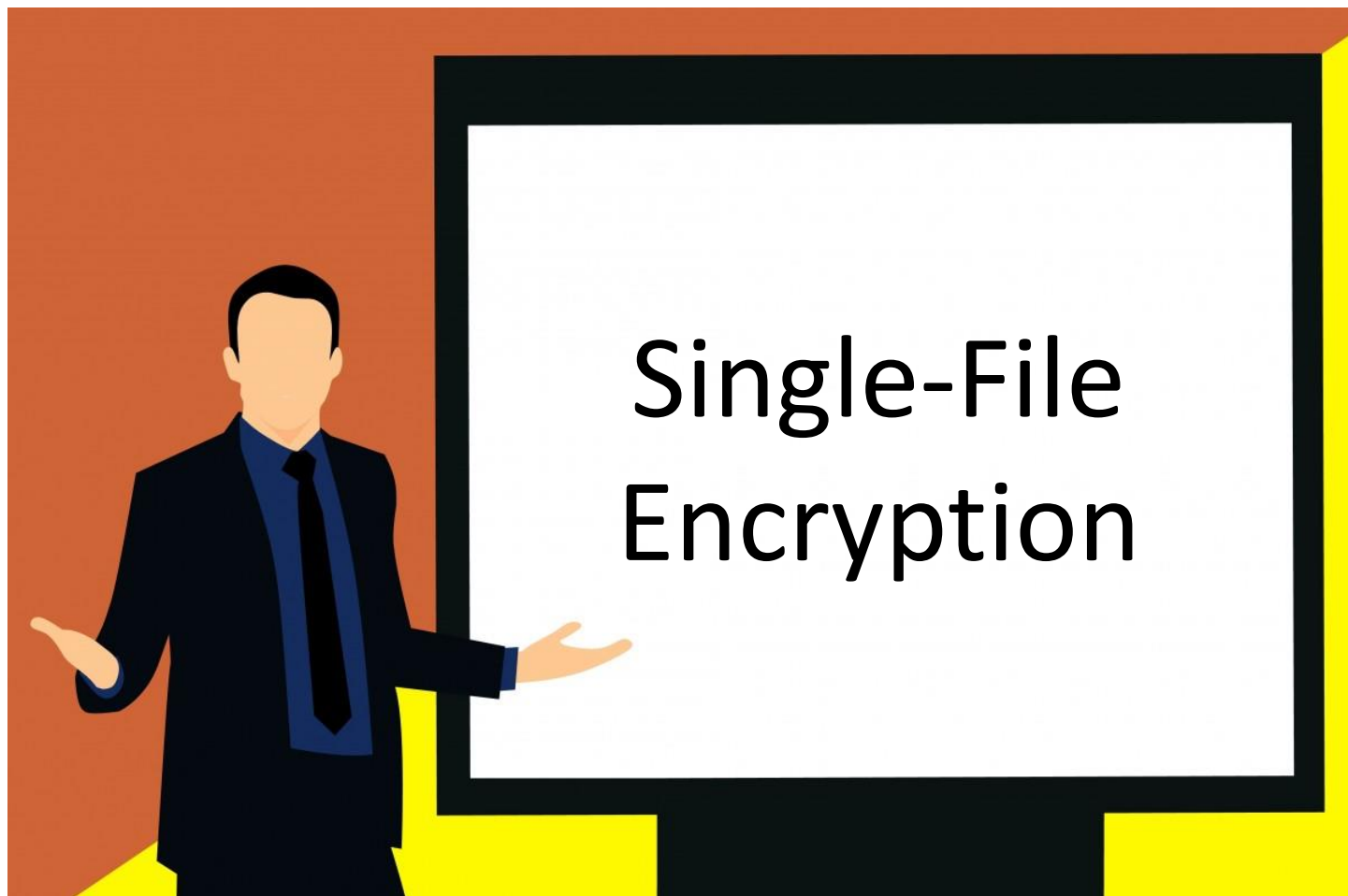


Single-File Encryption Options

- Microsoft Office (built-in)
- 7-Zip (free software)
- AESCrypt (free software)
- Many more ...






Demo



Single-File
Encryption

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

- Use a different type of communication to exchange passwords.

○ **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

Encrypted Container



Encrypted Container

- Enables you to easily store lots of encrypted files
- Use: You have lots of files you want to be able to store encrypted on a flash drive or hard drive
- Creates an encrypted area
- Automatically encrypts and decrypts files as needed



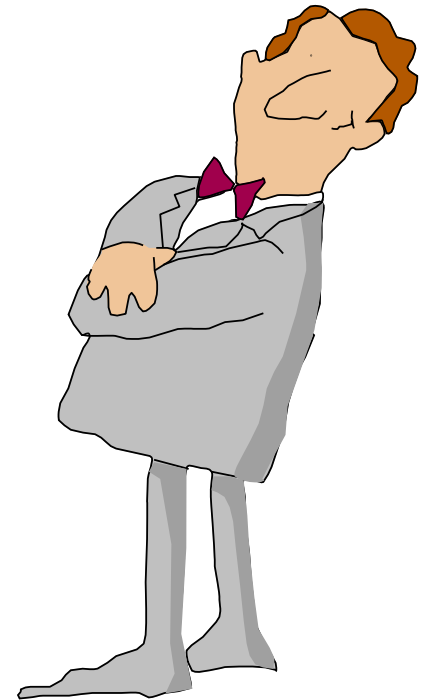
VeraCrypt

- Based on TrueCrypt
- Open source software
- Free
- Easy to use
- Available for Windows, Mac, Linux



How It Works

- Create a VeraCrypt container
- When you want to access the files in the container, you **mount** the container
- Once mounted, you access the files as if they were on a regular drive
- Encryption and decryption happen automatically



Demo



Real-Life Use Case

- Medical records backups



A Few More Cool VeraCrypt Features

- Traveler flash drive
- Key files
- Hidden containers



Proprietary Flash Drive Solutions

- Secure flash drives available
- Some devices lock the device with a password but don't encrypt it
- Beware trusting manufacturer apps that come free with the flash drive



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

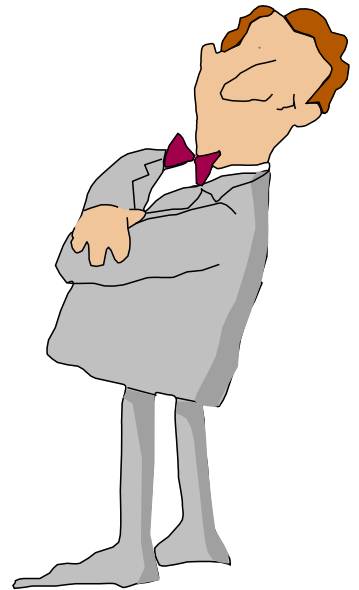
Password:



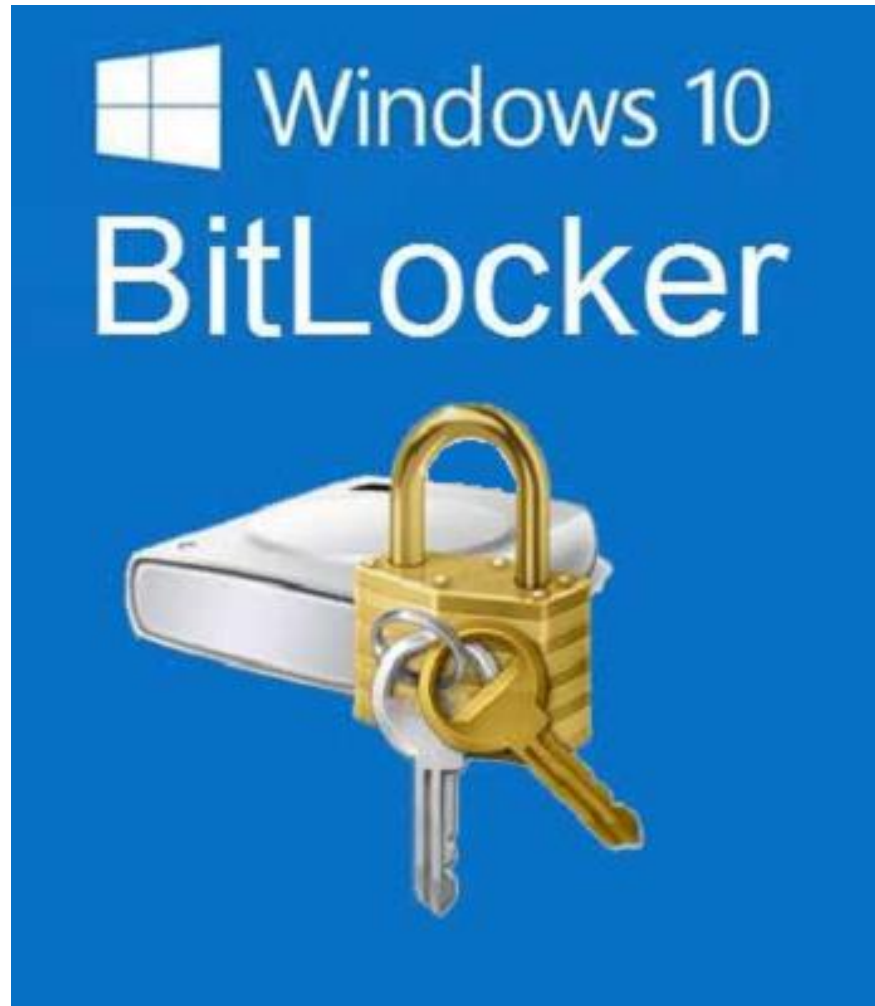
Inspiron

How Safe Is It?

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



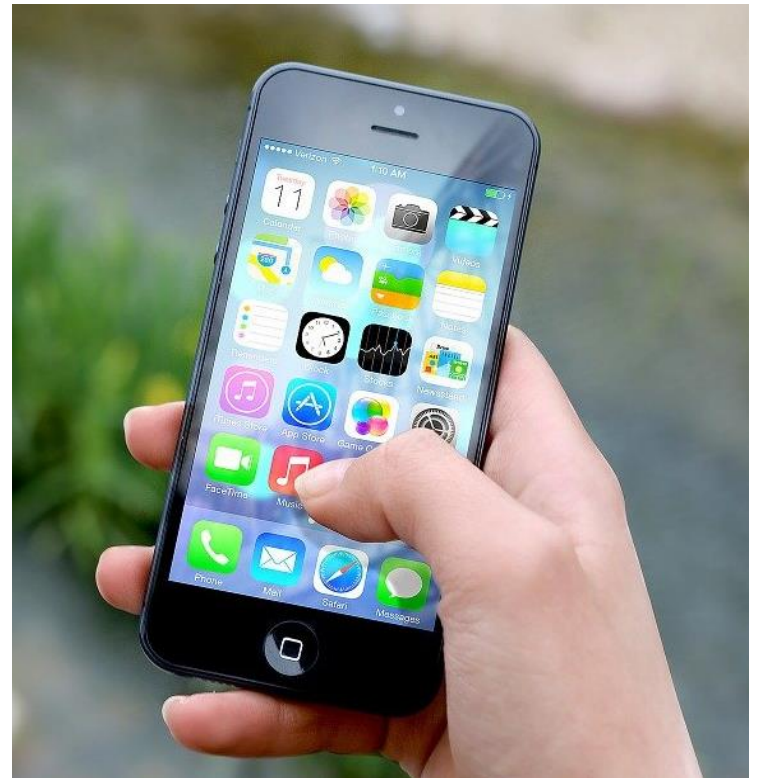
Microsoft's Solution



VeraCrypt vs. BitLocker

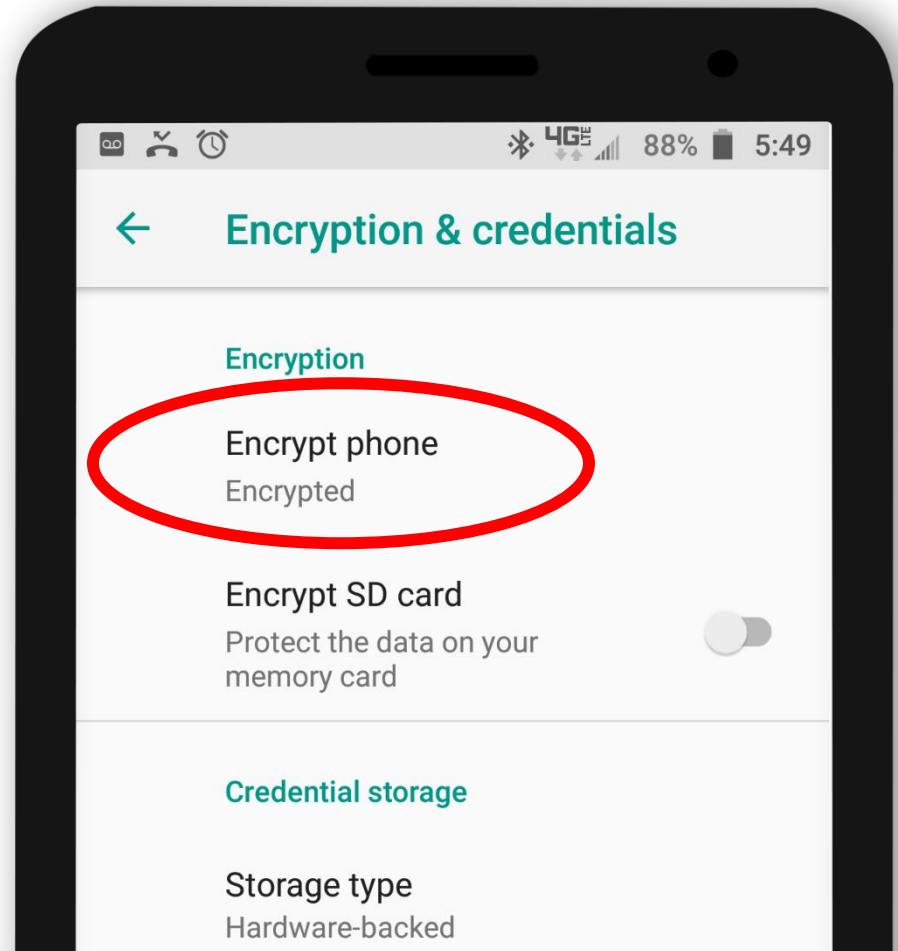
	VeraCrypt	BitLocker
Written by	IDRIX, TrueCrypt	Microsoft
Available for	Windows (any version), Mac, Linux	Windows Pro or Enterprise
Preinstalled	No	Yes
Transparency	Open source	Proprietary
Management	No corporate features	Can be managed by Active Directory

Phones



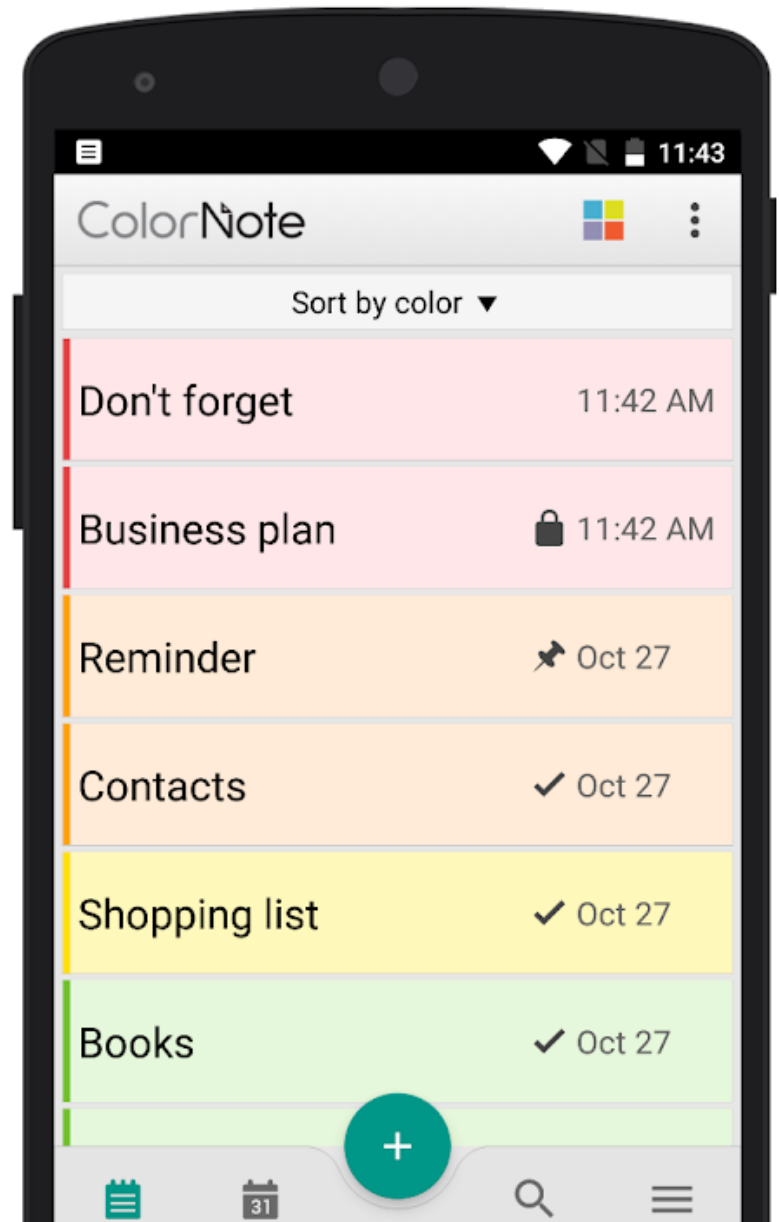
Phone Encryption

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



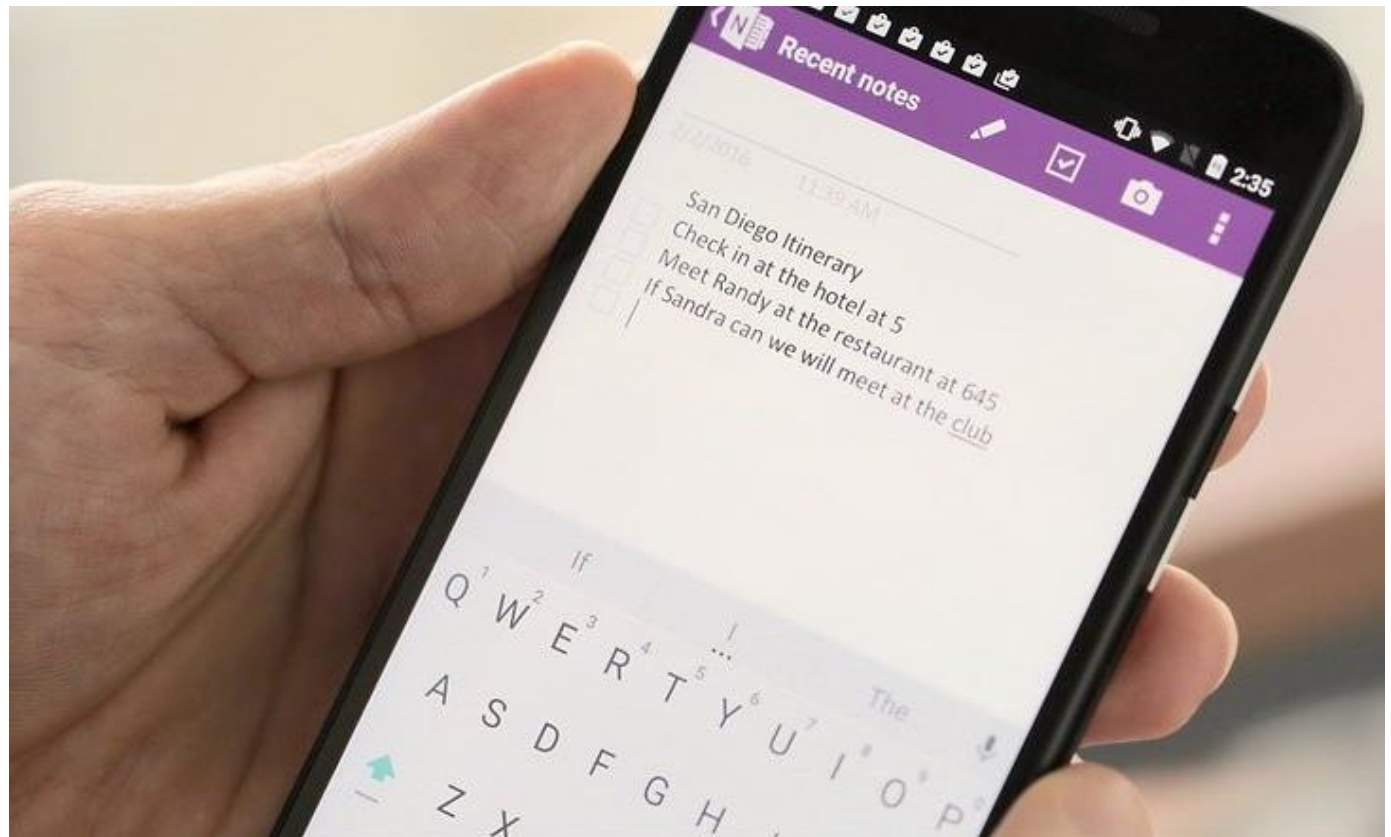
Encrypted Note App

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



Microsoft OneNote

- Sophisticated note-taking and organization app that includes encryption



Where to Get It

AESCrypt	https://www.aescrypt.com
ColorNote	https://www.colornote.com
OneNote	https://www.onenote.com
VeraCrypt	https://veracrypt.fr

All these apps are free

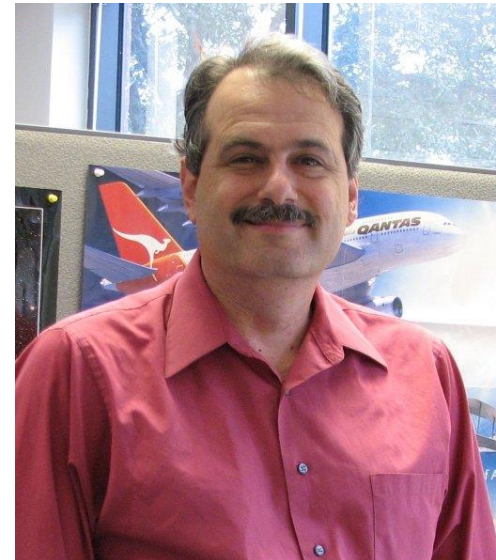
Questions?

Encryption

Mark Schulman

Central Florida Computer Society

marks@schulmans.com



An International
Association of Technology
& Computer User Groups

Spare Slides



Class of Problem #1

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



Class of Problem #2

Keeping secrets is life or death:

- You're a covert freedom fighter in Tibet, and your flash drive has a detailed list of all your operatives
- You work for the government and your laptop contains military secrets



What's the Problem?

- Large amounts of private data on our devices
- More and more data on portable devices
- Data shared over insecure methods (email, flash drives, CDs)

