ENCRYPTION

An International Association of Technology & Computer User Groups
Wednesday Workshop
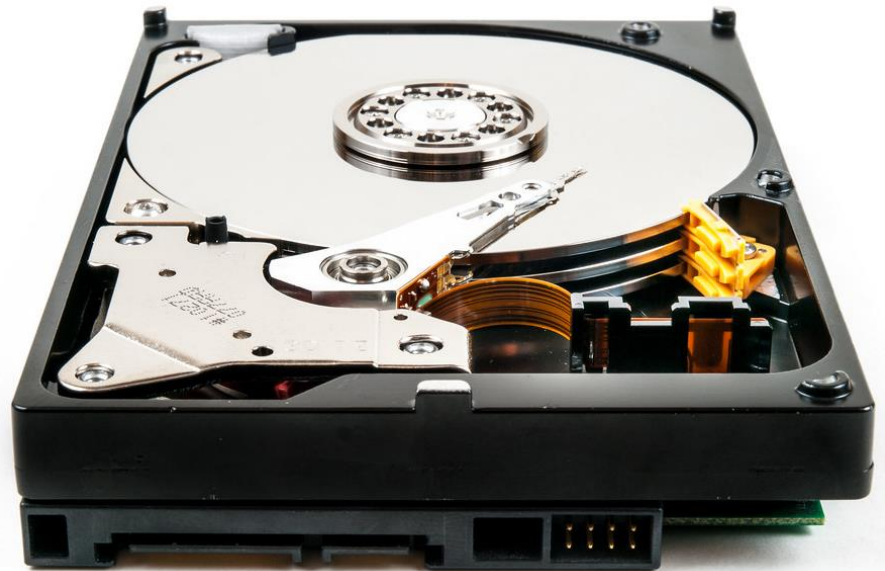
Mark Schulman

Your Presenter

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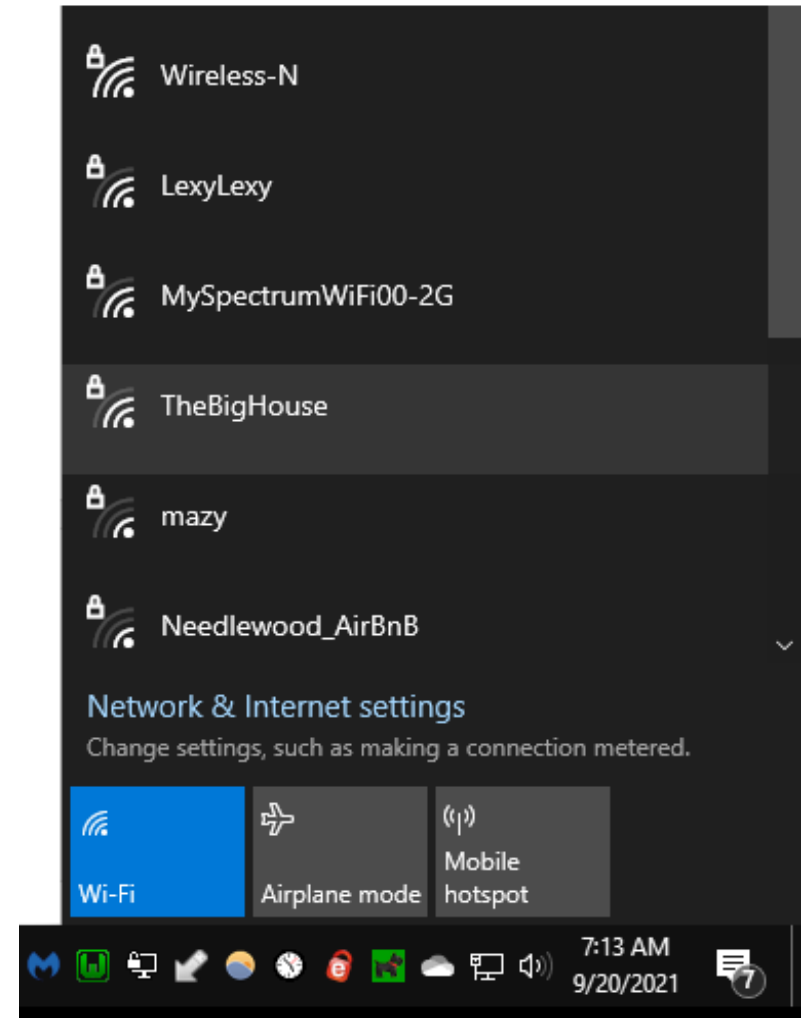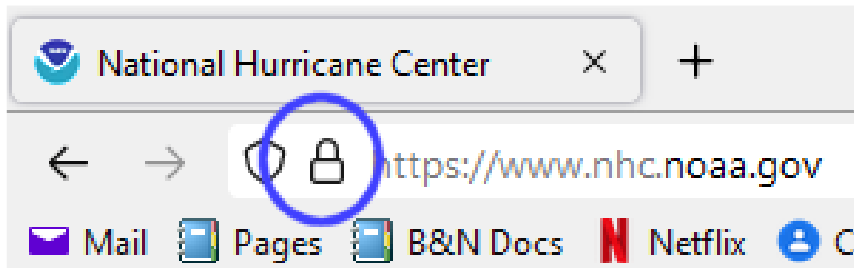- No affiliation with any product

Agenda

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

You Already Use Encryption

- https

- Wi-fi

What's the Problem?

- More and more data contained on portable devices
- Data shared over insecure methods (email, flash drives, CDs)

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

- Your laptop has client data that you're obligated to protect

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 plans

Single-File Encryption
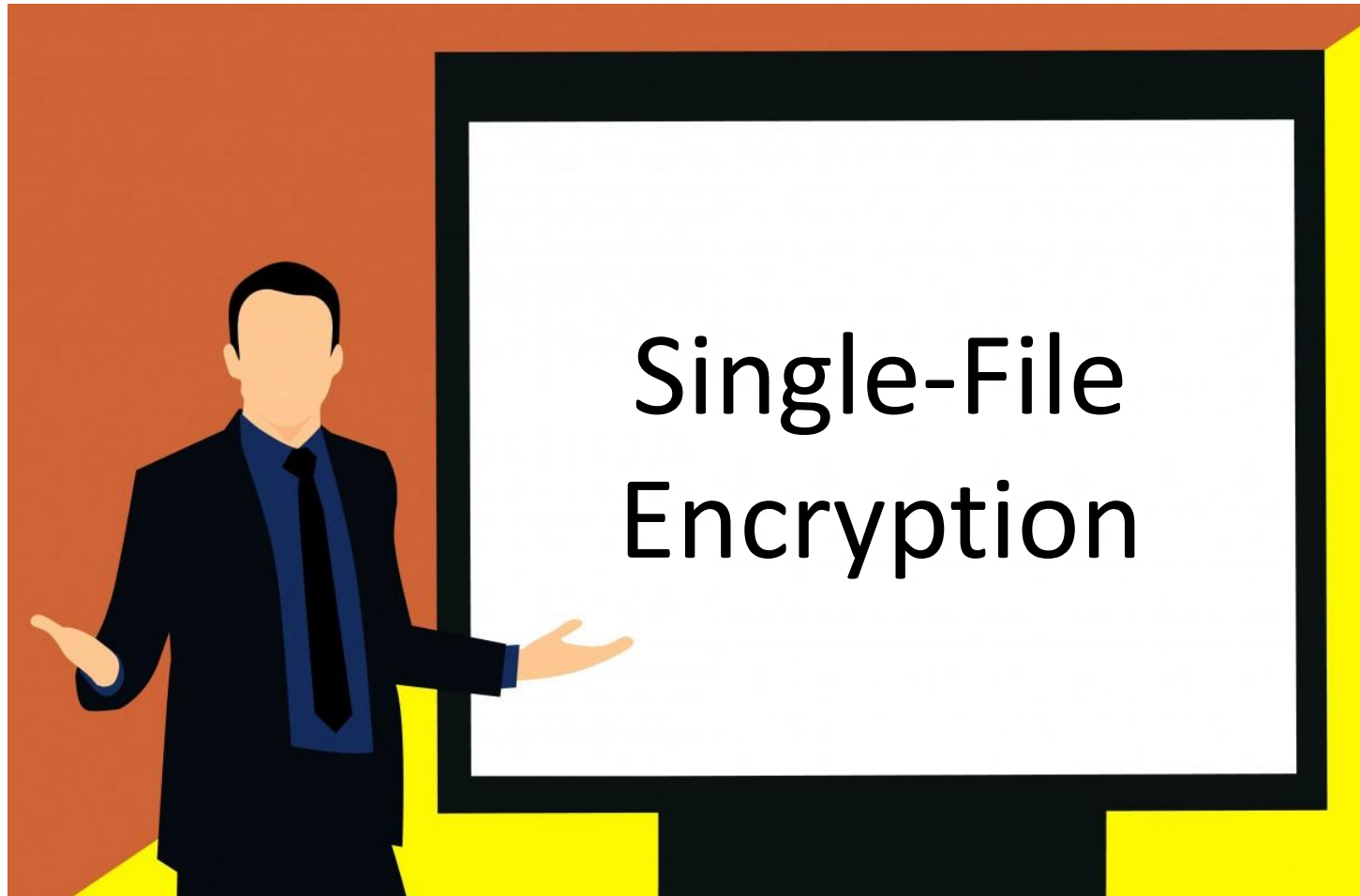
Single-File Encryption

- Store a single encrypted file
  - Flash drive with 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 …

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

- Provides an encrypted virtual drive in which to store information
- Can be used with
  - flash drives
  - external drives
  - laptops, PCs

VeraCrypt

- Based on TrueCrypt
- Open source software
- Free
- Easy to use
- Works well on flash drives, external drives, computer hard drives
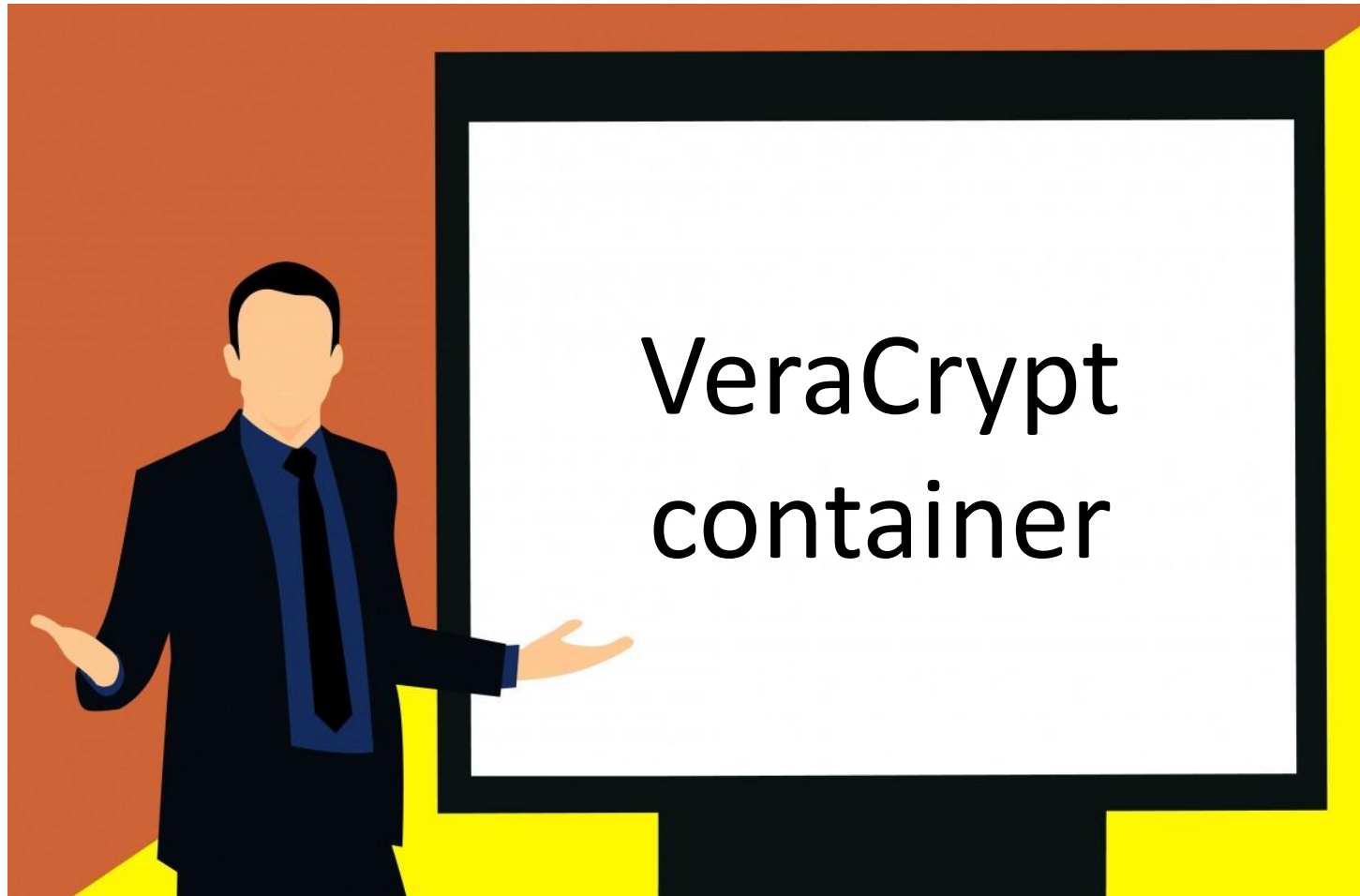- Available for Windows, Mac, Linux

How It Works

- You create a VeraCrypt container

- Contents of the container is encrypted with a password

- When you mount the volume, it becomes a virtual drive

Real-Life Use Case

- Medical records backups

VeraCrypt container

A Few More Cool VeraCrypt Features

- Traveler flash drive
- Key files
- Hidden containers

Proprietary Flash Drive Solutions

- Secure flash drives available

- Some don't allow secure and non-secure access simultaneously

- Some solutions 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

A Story

VeraCrypt

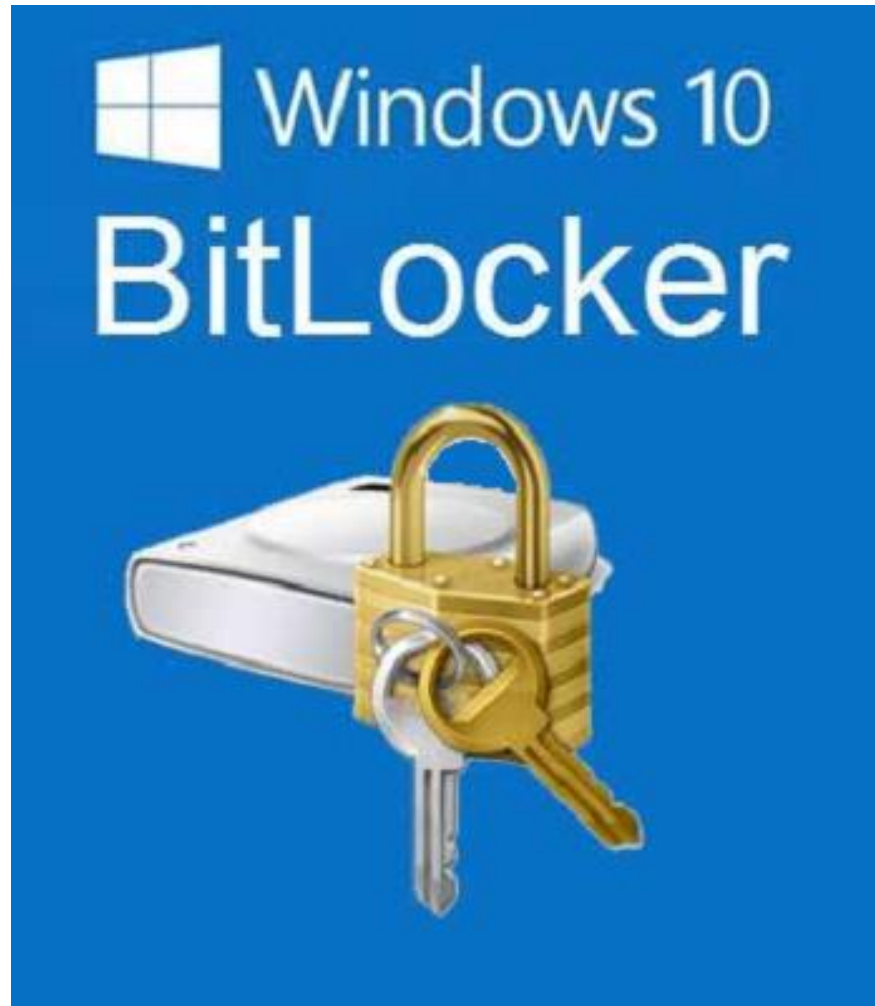- VeraCrypt can encrypt your entire hard drive

VeraCrypt Boot

How Safe Is It?

- With a good password, it's 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
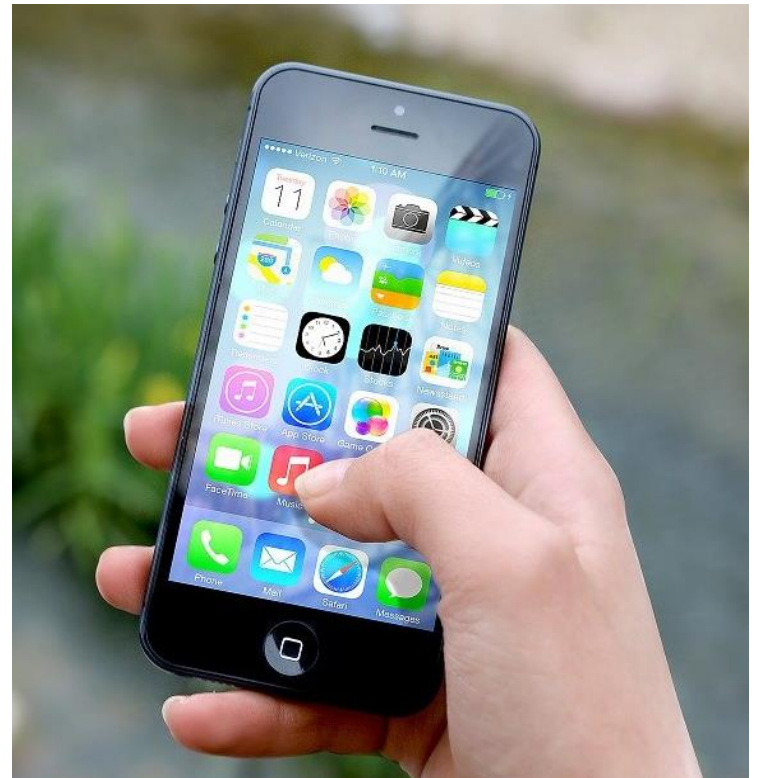
Phone Encryption

- Modern phones include whole-phone encryption

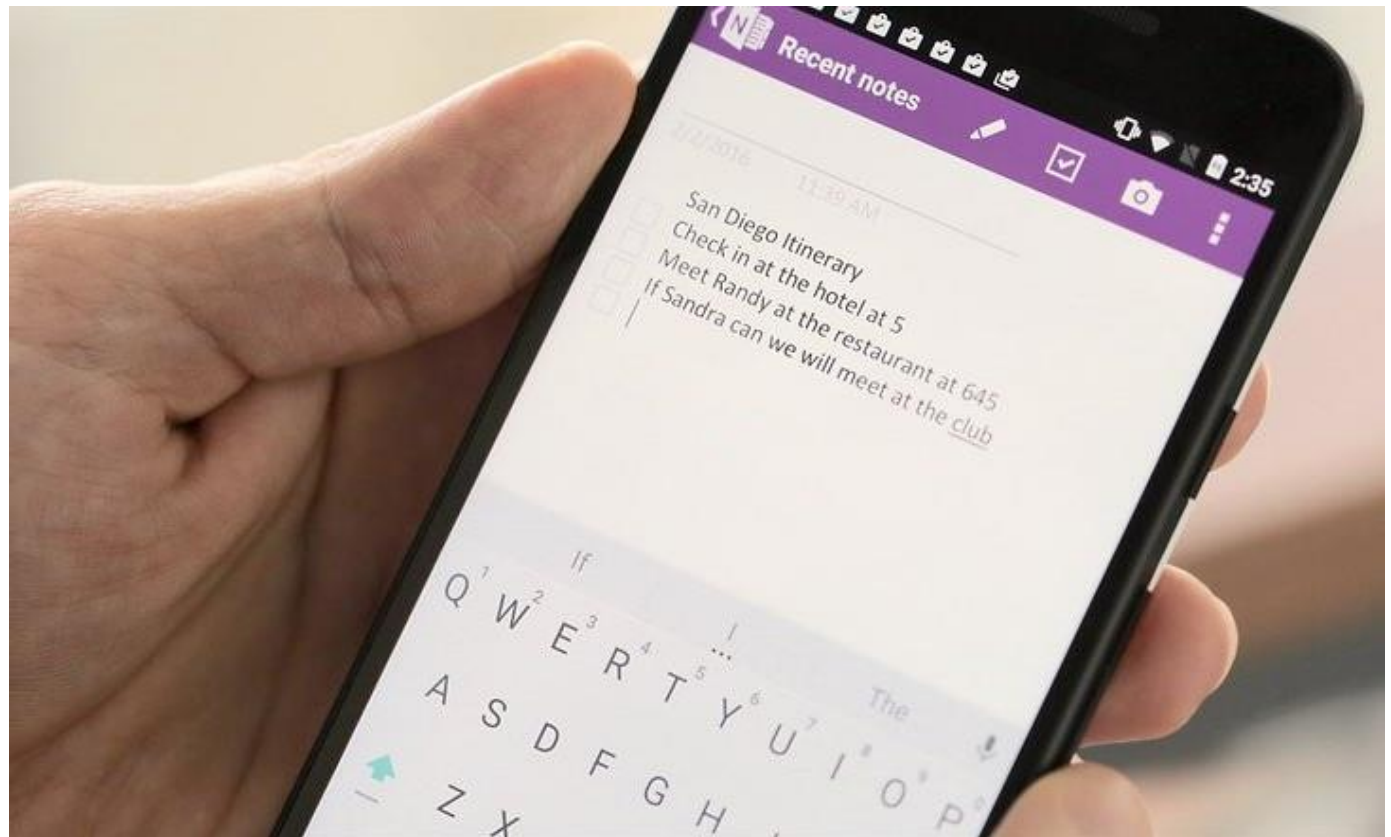- Encryption is only as good as your password
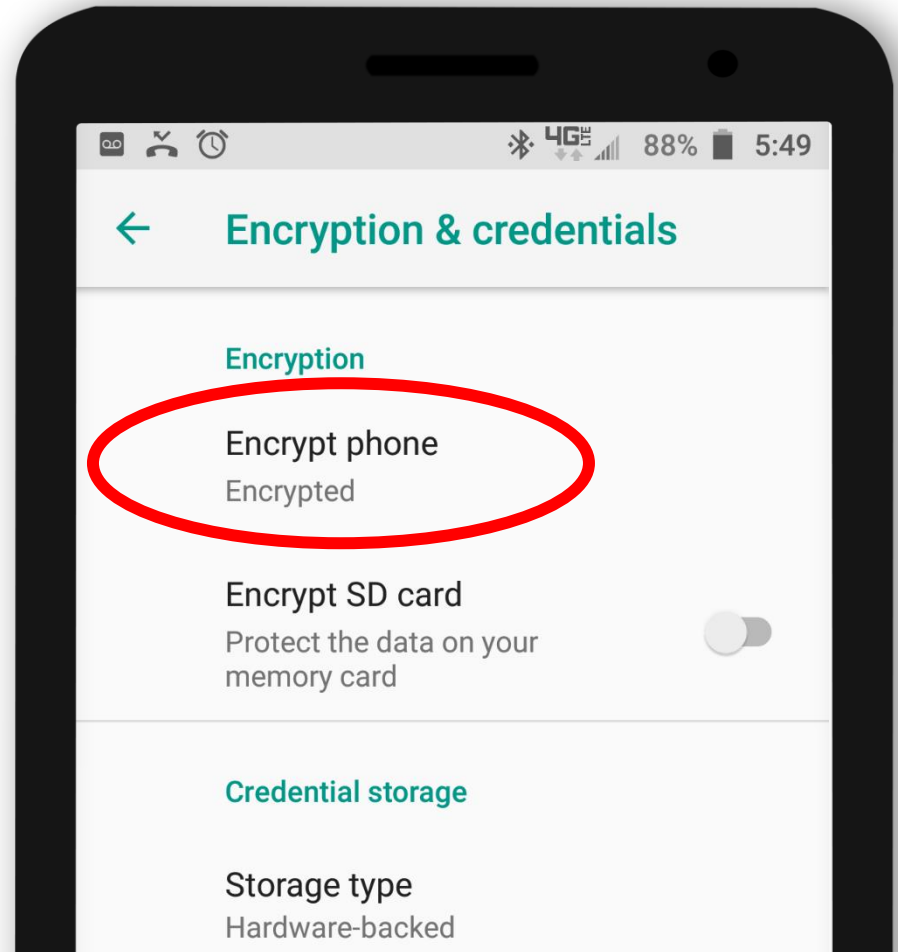
Encrypted Note App

- Endless encrypted note-taking apps

- At right: ColorNote
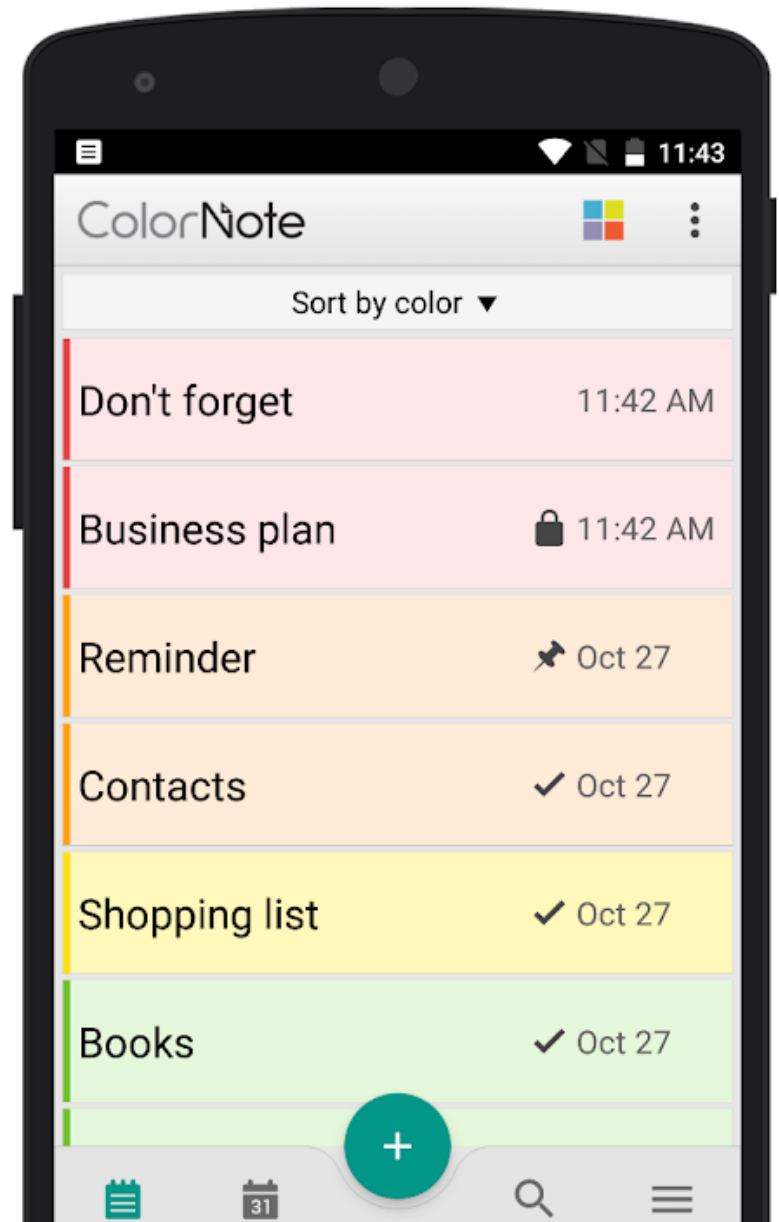
Microsoft OneNote

- Sophisticated note-taking and organization app that includes encryption

Where to Get It

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

All these apps are free

Encryption

Mark Schulman
Central Florida Computer Society

marks@schulmans.com