Mac Security & Privacy Update

Main Line Macintosh User Group
May 12, 2018

Mike Inskeep
Gentle Computer Helpers
www.gentlehelpers.com
mike [at] gentlehelpers [dot] com
610-742-3927

New Developments

- No CrashPlan personal online backup
- macOS 10.13 released
- Apple discontinued Airport routers
- New DNS services available
- Malicious Chrome extensions
- Anti-malware tools
- Social media account vulnerabilities

Why Backup

- Protect against mechanical failure
- Revert updates or upgrades
- Recover from malware infection
- Restore damaged, lost items
- Restore previous version of item

Good Backup Characteristics

- Automatic, requiring little or no action
- Robust, reliable
- Not always connected
  (ransomware encrypts connected drives)
- Multiple targets, including off-site

Time Machine Backup

- Integrated into macOS
- Retains versioned copies of what is stored on the internal drive
- Supports multiple drives
- Connected USB or Thunderbolt drives

What's Changed?

- Previous recommendation:
  1. Connected portable USB 3.0 drive
  2. Online backup using CrashPlan
- CrashPlan personal plan discontinued
- Time Capsule discontinued

New Backup Recommendation

Two Alternatives:

- Rotate 2 external USB backup drives
- 1 USB drive + Backblaze online backup

Two External USB Drives

- Get two Toshiba portable drives
- Size: ~ 3 times storage used

  > About this Mac > Storage
- Set both up as Time Machine destinations
- Encrypt backups
- Swap ~ weekly
- Store one off-site if possible

Encrypting Backup Drives

- Using Finder in macOS 10.13 to encrypt a disk will convert it to APFS which is *incompatible* with Time Machine.
- Unplug the drive and plug it back in. It should offer you the option to encrypt it.
- If it doesn't, go Time Machine preference pane:
  1. > System Preferences > Time Machine
  2. [Select Disk] > (click disk) > [Remove Disk]
  3. (click disk) > [x] Encrypt > [Use Disk]

Why Buy Toshiba?

- Though inexpensive, many Seagate drives do not support encryption.
- WDC drives are less reliable.
- HGST drives are most reliable and most expensive.
- Toshiba drives are nearly as reliable and are more reasonably priced.

USB Drive + Backblaze

- Set up USB drive as an encrypted Time Machine backup destination.
- Subscribe to Backblaze to also backup over the Internet.

Backblaze

Personal Backup Plan

- $5/month. $50/year. $95/2 years.
- Versions of files stored up to 30 days.
- Unlimited storage, transfer speed.
- Will send USB drive with data and refund the cost if return in 30 days.
- Use a private encryption key.
- Enable 2 factor authentication.

USB Drive

- Use an encrypted Toshiba drive ~3 times the storage used.
- After macOS update or upgrade, disconnect the drive until you're confident that everything is working smoothly.
- If not, you can use it to restore to the previous version of macOS.

Backup Maintenance

- Regularly test restoring from your backups (weekly?)
- Run Disk Utility First Aid on backup volume from time to time (monthly?). This will take many hours.

Backup References

- For information about Time Machine:

  https://support.apple.com/en-us/HT201250

- For information about Backblaze:

  https://www.backblaze.com

✳ Thanks to Adam Rice for suggesting Blackblaze as an online alternative.

macOS 10.13 High Sierra

Supports Native Encryption so:

- Set Firmware Password
- Turn on FileVault full disk encryption

=> Especially on a laptop

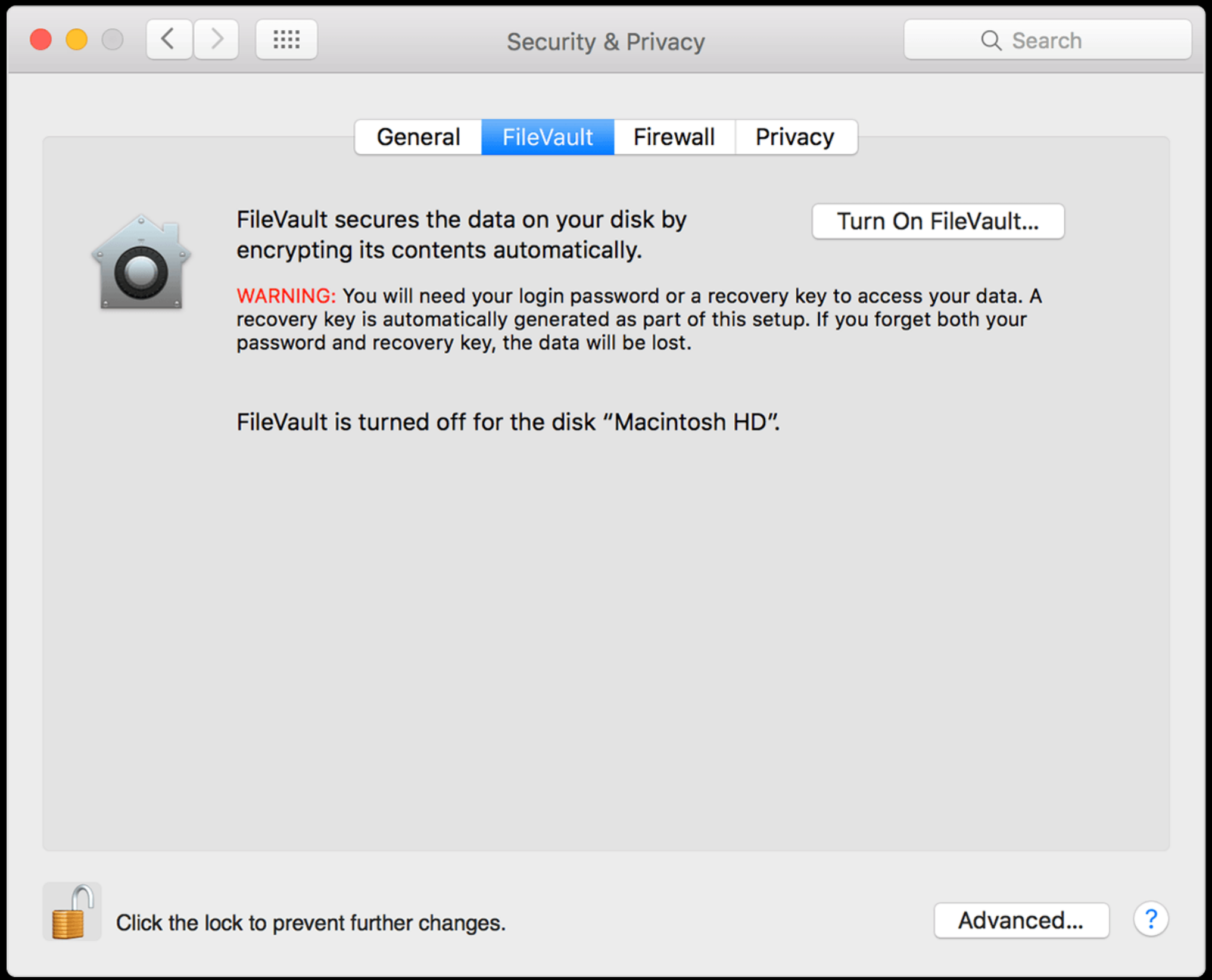
Set Firmware Password

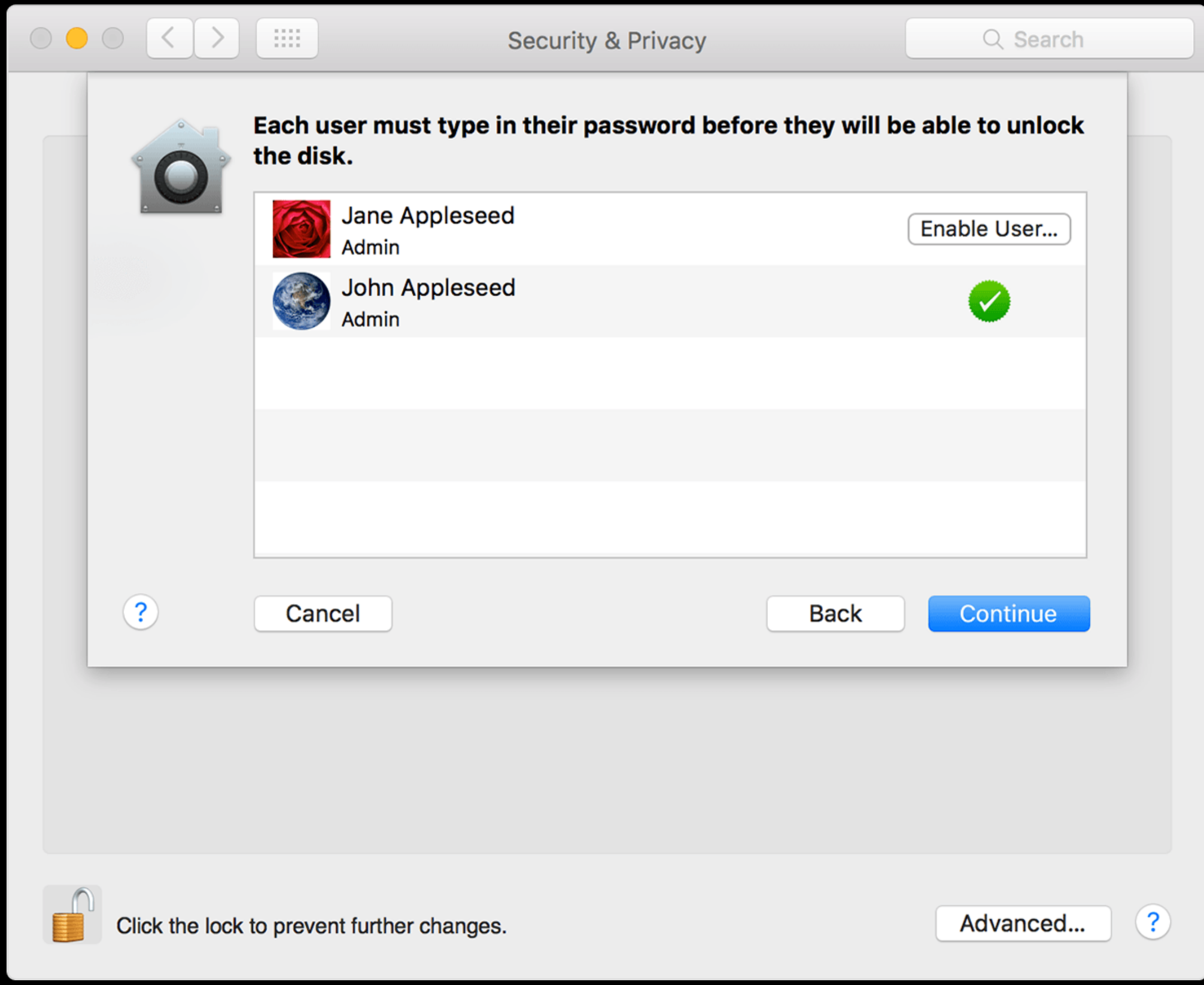
1. Restart, hold ⌘ R to enter Recovery
2. Utilities > Firmware Password Utility
3. [Turn on Firmware Password]
4. Enter password [Set Password]
5. Store the password in a safe place*
6. Test by restarting and holding ⌘ R

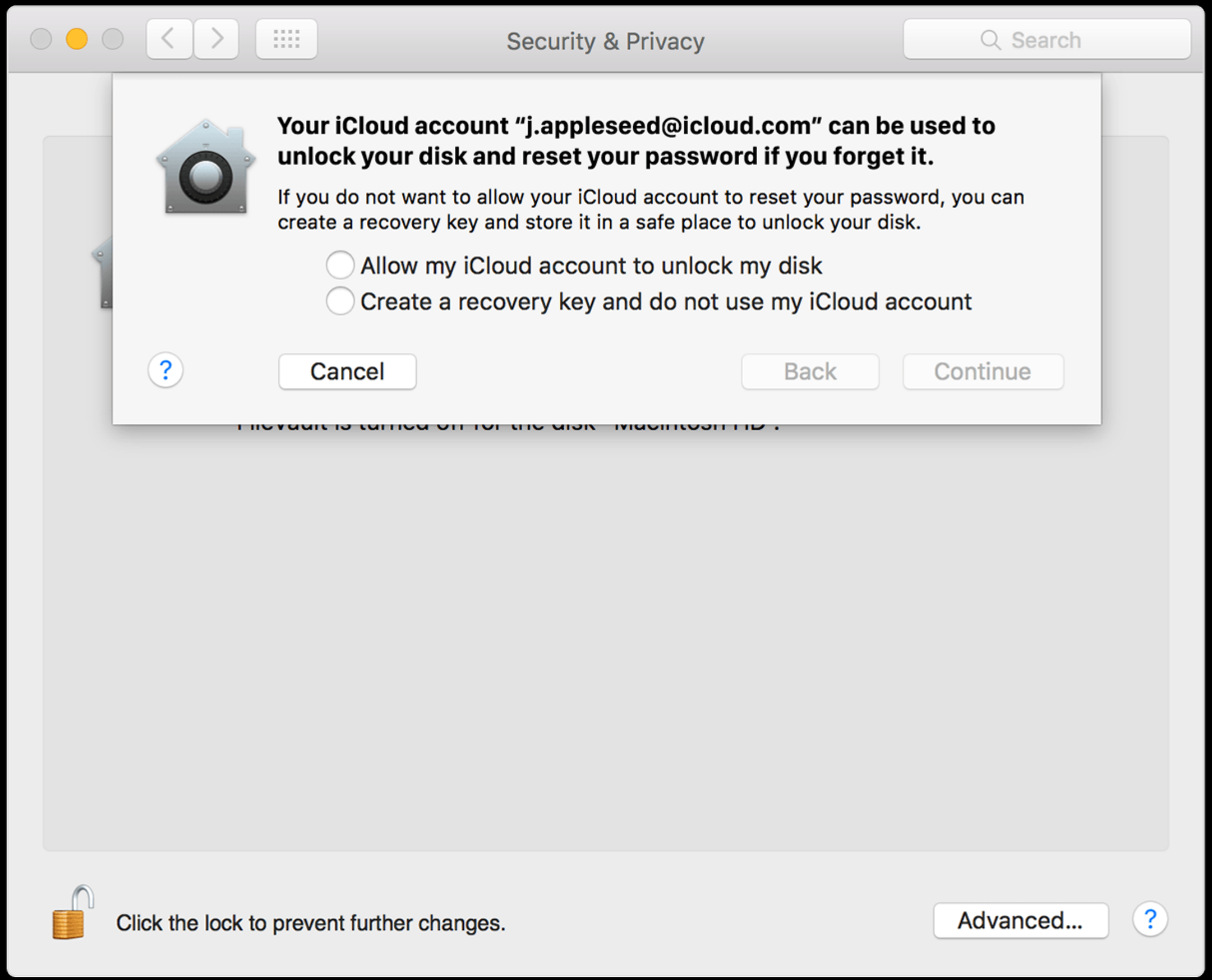
* Lose firmware password, and you may have to take your Mac to Apple Store

Turn on FileVault Encryption

1.  > System Preferences
2. Security & Privacy > FileVault tab
3. Click 
4. Enter administrator name, password
5. Click [Turn on FileVault]
6. If other user accounts, click [Enable User] to allow them to unlock the disk.
7. Choose to use iCloud account or create a local recovery key in case you forget the password


Security & Privacy
Search
General
FileVault
Firewall
Privacy
FileVault secures the data on your disk by encrypting its contents automatically.
Turn On FileVault...
WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.
FileVault is turned off for the disk "Macintosh HD".
Click the lock to prevent further changes.
Advanced...
?


Security & Privacy
Search
Each user must type in their password before they will be able to unlock the disk.
Jane Appleseed
Admin
Enable User...
John Appleseed
Admin
Cancel
Back
Continue
Click the lock to prevent further changes.
Advanced...


Security & Privacy
Search
Your iCloud account "j.appleseed@icloud.com" can be used to unlock your disk and reset your password if you forget it.
If you do not want to allow your iCloud account to reset your password, you can create a recovery key and store it in a safe place to unlock your disk.
Allow my iCloud account to unlock my disk
Create a recovery key and do not use my iCloud account
Cancel
Back
Continue
Click the lock to prevent further changes.
Advanced...

For More Information

- Set Firmware Password

  https://support.apple.com/en-us/HT204455

- Turn on FileVault full disk encryption

  https://support.apple.com/en-us/HT204837

Install Your Own Router

- Apple discontinued Airport Wi-Fi routers
- Search for online reviews
- Want automatic firmware updates
- Wired connections faster
- Good customer support

Wi-Fi Router Options

- Check out:
  - Eero (easy set up, small units, fast performance, best customer service, but expensive)
  - Netgear Orbi (largest coverage, fastest, big units, 4 ethernet ports, USB, so-so support)
  - Google WiFi (easy set up, slower, cheap, linked to Google account)

Change Gateway Set Up

- Change login user name, password
- Disable remote administration
- Automatically update firmware

For instructions, see my May 2017 “Secure Your Mac” presentation.

New Public DNS Options

- Cloudflare DNS
- Quad9

What is DNS?

- The domain name system matches domains (e.g. www.apple.com) with their numerical IP address (17.142.160.59)
- When you type in a domain, the request is transmitted from server to server until it reaches the authoritative endpoint for the domain

Problems

- Queries are sent in the clear so intermediaries can see where traffic going (but not its content)
- Responses can be “poisoned” - replaced with ones supplied by attacker (https largely prevents)
- Many domains host malicious webpages

Advantages

- Validity: using DNSSEC they block attempts to provide fake answers to DNS queries
- Improve privacy: using “query name minimization”, only minimal info is shared with intermediate servers
- Encrypted: using DNS-over-TLS (DoT) or DNS-over-HTTPS (DoH) to prevent sniffing (eavesdropping)

Advantages of Quad9

- Non-profit organization founded by IBM, Packet Clearing House and the Global Cyber Alliance
- Provides free services to minimize exposure and risk
- Aggregated info shared with partners to alert them to, help them mitigate risks
- DNS blocklist: blocks millions of identified malicious addresses

Configure Your Mac's DNS

1. > System Preferences
2. Network > Advanced > DNS tab
3. Click [+] under DNS Servers. Enter DNS server IP address 9.9.9.9
4. Repeat for: 149.112.112.112
5. Click [OK] then [Apply]

Use DoT with Quad9

- If you're adventurous, try enabling DNS-over-TLS with the Quad9 DNS service:

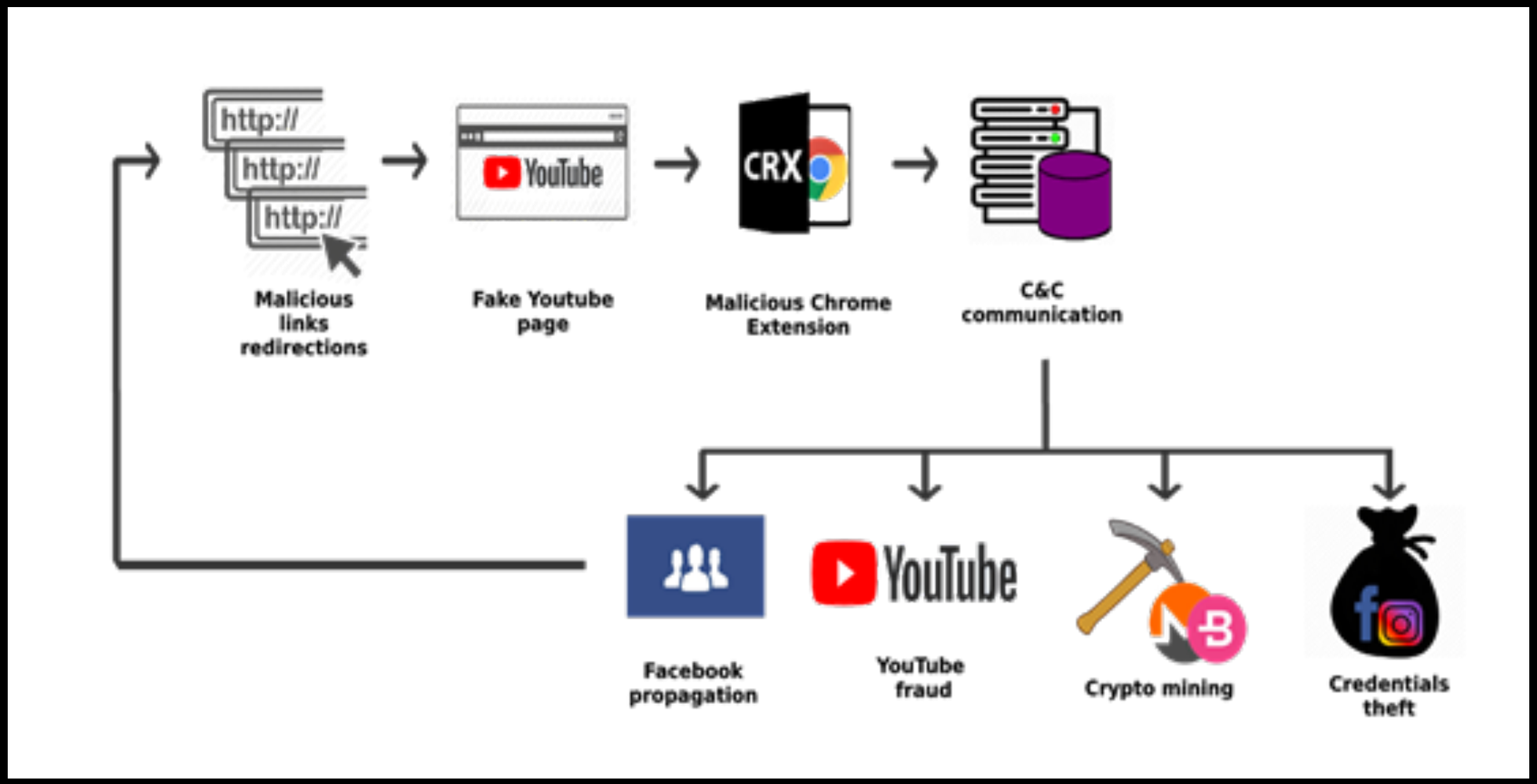
https://medium.com/nlnetlabs/privacy-using-dns-over-tls-with-the-new-quad9-dns-service-1ff2d2b687c5

For More Info on DNS Services

- "Cloudflare and Quad9 Aim to Improve DNS" by Glenn Fleishman, published April 20, 2018 in Tibits:

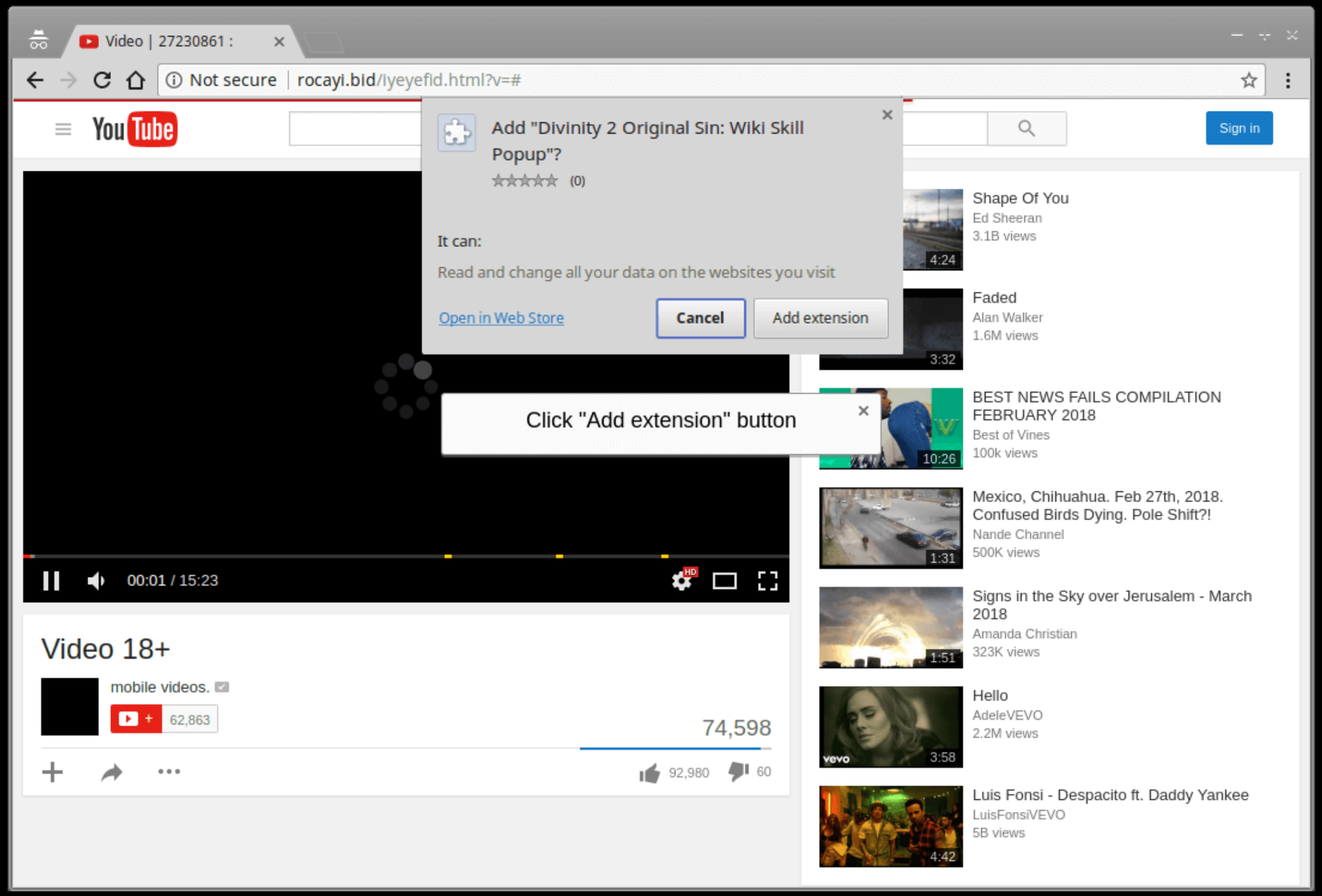
  https://tidbits.com/2018/04/20/cloudflare-and-quad9-aim-to-improve-dns

Nigelthorn Malware



Source: https://blog.radware.com/security/2018/05/nigelthorn-malware-abuses-chrome-extensions/

Fake YouTube Page



Source: https://blog.radware.com/security/2018/05/nigelthorn-malware-abuses-chrome-extensions/

How to Protect Yourself?

- Use a Mac or iOS device
- Don’t use Facebook Messenger
- Use Quad9 DNS service
- Don’t allow webpages to install browser extensions

For More Information

- "Nigelthorn Malware Abuses Chrome Extensions to Cryptomine and Steal Data" by Aldi Raff and Yuval Shapira published in the Radware Blog May 10, 2018:

https://blog.radware.com/security/2018/05/nigelthorn-malware-abuses-chrome-extensions/

Malware Techniques

- Checked against VirusTotal, then "packed" (using e.g. UPX)
- Encrypted using integrated key
- Signed with stolen Apple developer certificate
- Access OAuth (Google's authentication system) bypassing 2FA

Anti-Virus Failure

- Traditional AV can’t detect new malware
- Invasive: hooks into browser, even OS
- Large attack surface
- 6/2017 Google’s Project Zero found 25 high-severity bugs in Symantec/Norton (others found in Kaspersky, McAfee, Eset, Comodo, Trend Micro, etc)

Objective-See Security Tools

Do Not Disturb

alerts you if someone opens your laptop

KnockKnock

identifies applications which are executed when your computer restarts, you log in, or you launch a browser and compares against malicious applications catalogued at Virus Total

Objective-See Security Tools

BlockBlock (beta)

monitors for new persistently installed applications, allowing you to block them

RansomWhere?

monitors for file encryption, allowing you to generically stop ransomware

OverSight

alerts you when your Mac's mic or webcam is accessed or activated

Objective-See Security Tools

- Get more information, download them, and contribute, if you wish, at:

https://objective-see.com/

Malwarebytes

- Malwarebytes for Mac (free)
  - scans for viruses, spyware, malware infections
  - premium version has roots deep in macOS so makes you more vulnerable if it is compromised

https://www.malwarebytes.com/mac/