Tech Talks
Technology for Seniors

Glen Maxson

Living U

Fall 2020 – Session 3 of 3

www.seniortechadvisor.com (link to this presentation)

What we’ll cover in 3 weeks

1) ~~The Internet & The Web (September 10)~~
2) ~~Social Media (September 23)~~
3) Security & Privacy (November 18)

Who Am I?

Technology Trends
Center for Learning in Retirement
2020
Glen Maxson & Alan Freedman

Glen Maxson
glenmaxson@gmail.com, 267-866-7827
http://www.seniortechadvisor.com

LinkedIn profile

What we covered during the last 2 weeks

The Internet and the Web

- The Internet & The Web
  - The Internet, a massive network of networks, is an enabler for the World Wide Web (WWW) and Social Media
  - Information travels over the Internet via protocols*
  - The World Wide Web (the Web) is a way of accessing information over the medium of the Internet - the Web uses the HTTP protocol
  - The Web also utilizes browsers like Firefox or Chrome to access Web documents called Web pages (example)

*A Protocol is an agreed-upon format for transmitting data between two devices.
Protocols determine the following:

- error checking, data compression, how a sending device indicates it is finished sending a message, and how a receiving device indicates it has received a message

Social Media

Social Media - computer-mediated technologies that allow the creating and sharing of information, ideas, career interests and other forms of expression via virtual communities and networks. (source)

Common features:

1. social media are interactive Web 2.0 Internet-based applications
2. user-generated content such as text posts or comments, digital photos or videos, as well as data generated through all online interactions, are the lifeblood of social media
3. users create service-specific profiles for the website or app, that are designed and maintained by the social media organization
4. social media facilitates the development of online social networks by connecting a user's profile with those of other individuals or groups

What we’ll cover this week

Security and Privacy

Personal Digital Security

It’s about?

Protecting our ‘Computers’

our Passwords

our Online Accounts

our Data

our Credit & Debit Cards

our Cell Phones

ourselves From Telephone Attacks

our ‘Online Devices’ and other stuff

STATS (source)

- Identity Theft Resources Center (ITRC) had recorded 1,293 U.S. data breaches in 2017, exposing more than 174 million confidential records
- A single breach of data analytics company Alteryx exposed sensitive information for 123 million U.S. households (125.8 mil households in the U.S.)
- Dark Web database of 1.4 billion email addresses, usernames and passwords* discovered in 2017
- Cybercrime To Cost The World $10.5 Trillion Annually By 2025, up from $3 trillion USD in 2015
- Ransomware costs alone top $5 billion globally by end of 2017, and ransomware is growing at a yearly rate of 350%. Ransomware will claim a new victim every 5 seconds by 2021 and global ransomware damage costs will reach $20 billion by 2021 – 57x more than in 2015

For More Information

AARP Podcasts - The Perfect Scam

- You’ve Got More Mail, With Frank Abagnale
- Scammer Targets Victim of Equifax Data Breach
- A Hiker’s Trail of Lies
- Long-Distance Relationship is Actually a Romance Scam
- Scammers Persuade Grandfather to Send Ransom by Mail
- Scammers Set Up Fake Coronavirus Testing Site
- Recognizing the Red Flags in an Online Romance
- Etc…

What about using fingerprints instead?

Hacker: Fingerprints less secure than passwords on smartphones

What to Do?

* Hypocrite indicator

Keeping Your Computer Safe

- Apply OS and application updates as often as possible
- Run Anti-Virus software that updates automatically
- ***The Best Free Antivirus Protection for 2020***
  - *What about* **Microsoft Windows Defender Security Center**
- Run a MalWare software routinely
  - *Malwarebytes* free version
- And for extra protection, Ransomware Protection is now available*

  The Best Ransomware Protection for 2020
- Keep your PC free of unused applications and files*
- Repair infected systems immediately

What’s The Difference Between Antivirus and Anti-Malware, you might ask… (source)?

- Viruses are a specific type of malware (designed to replicate and spread), while malware is a broad term used to describe all sorts of unwanted or malicious code.
- Malware can include viruses, spyware, adware, nagware, trojans, worms, and more.
- Because viruses made headlines a few years ago, most security companies focused their marketing on them, which is why they're called "antivirus.“
- All antivirus programs in this collection offer real-time malware protection.

Passwords

Here are the top five passwords with the amount of accounts that used them:

1. Password: 123456 - 9.2million accounts
2. Password: 123456789 - 3.1million accounts
3. Password: qwerty - 1.6million accounts
4. Password: password - 1.3million accounts
5. Password: 111111 - 1.2million accounts

Password Best Practices

- Make passwords at least 10 characters in length*
- Include at least 1 upper case letter, 1 or 2 special characters, at least 4 numbers, and spaces (if allowed)
- Change at least once each year (twice/year is better)
- Don’t use the same password for all accounts
- If spaces are allowed, use them (demo)
- If 2-factor authentication is provided, use it (video)
- If your browser wants to save a password, don’t*
- Better to use a password manager like RoboForm

2-Factor Authentication

Online Accounts

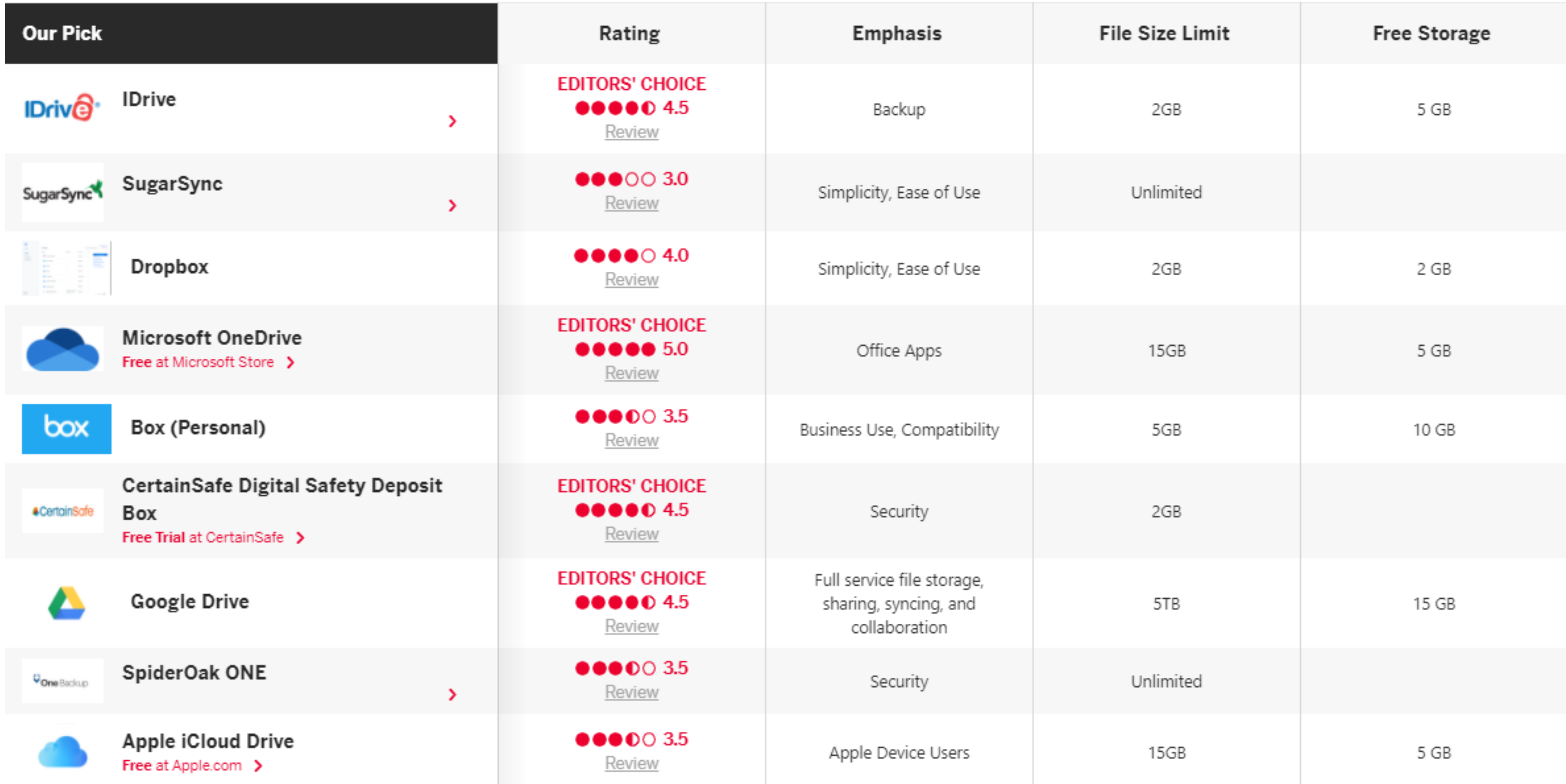
- Phishing attacks happen when someone tries to trick you into sharing personal information online
- E-mail addresses are public so anyone can contact you
- Scams try to trick you, disguised as legitimate businesses
- You don’t know for sure who is behind an e-mail, or who is trying to become your ‘Friend’ on Facebook
- Social network phishing is effective for criminals
- Security questions/answers are as important as passwords*
    - But do they have to be factual? Nope!
- If 2-factor authentication is available, use it
- Use a ‘secondary’ e-mail account for less critical online activity

Data (and the Cloud)

- Back up all important data locally and routinely
- In addition, create a secondary backup off-site (in the cloud?)
  - Carbonite just works…
- Encrypt sensitive data*

  The Best Encryption Software for 2020
- Data recovery may be possible for ‘deleted data’
- Don’t ever ‘donate’ used hard drives!
- Verify ‘public’ documents don’t include ‘private’ info

Cloud Storage & File Sharing Services (source)

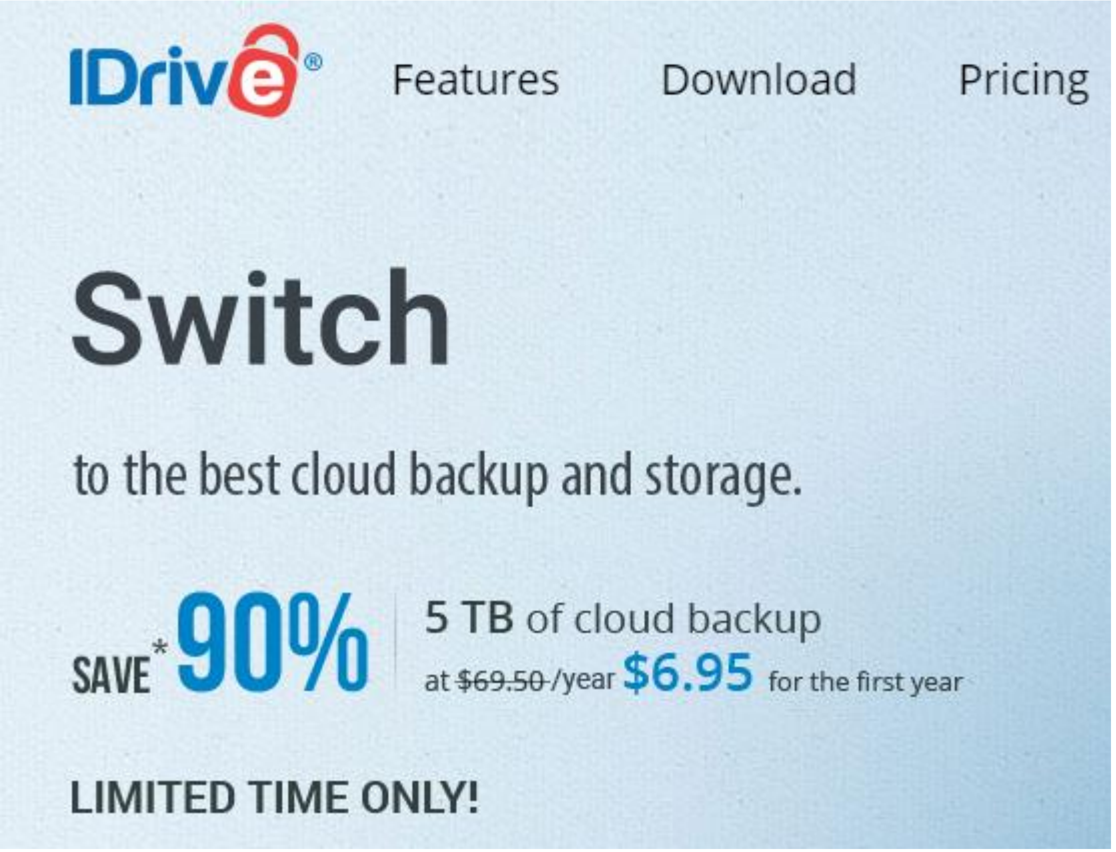


Our Pick	Rating	Emphasis	File Size Limit	Free Storage
IDrive ›	EDITORS' CHOICE ●●●●◐ 4.5 Review	Backup	2GB	5 GB
SugarSync ›	●●●○○ 3.0 Review	Simplicity, Ease of Use	Unlimited	
Dropbox	●●●●○ 4.0 Review	Simplicity, Ease of Use	2GB	2 GB
Microsoft OneDrive Free at Microsoft Store ›	EDITORS' CHOICE ●●●●● 5.0 Review	Office Apps	15GB	5 GB
Box (Personal)	●●●◐○ 3.5 Review	Business Use, Compatibility	5GB	10 GB
CertainSafe Digital Safety Deposit Box Free Trial at CertainSafe ›	EDITORS' CHOICE ●●●●◐ 4.5 Review	Security	2GB	
Google Drive	EDITORS' CHOICE ●●●●◐ 4.5 Review	Full service file storage, sharing, syncing, and collaboration	5TB	15 GB
SpiderOak ONE ›	●●●◐○ 3.5 Review	Security	Unlimited	
Apple iCloud Drive Free at Apple.com ›	●●●◐○ 3.5 Review	Apple Device Users	15GB	5 GB

My favorites:

Google Drive – 15gb free,
then $1.99/mth for 100gb
Microsoft OneDrive – 5gb free,
then $1.99/ mth for 100gb
iCloud – 5gb free,
then $.99/ mth for 50gb
Dropbox – 2gb free,
then $9.99/ mth for 2tb
iDrive – 5gb free,
then $52.12/ yr for 5tb

IDrive offer – too good to refuse!



Switch

to the best cloud backup and storage.

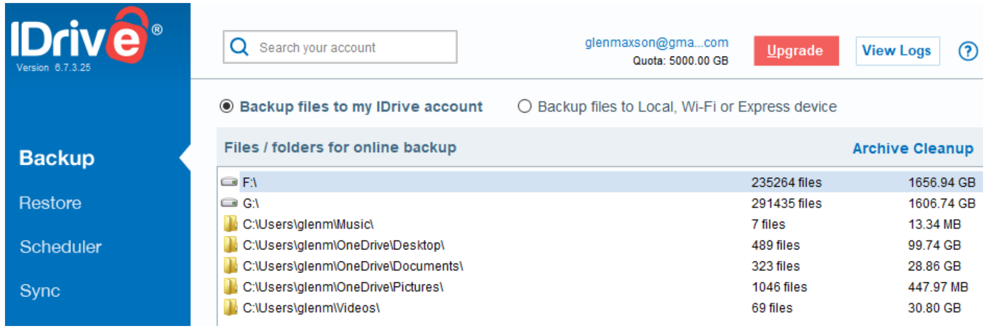
SAVE* 90%

5 TB of cloud backup

at ~~$69.50~~/year $6.95 for the first year

LIMITED TIME ONLY!

*The 90% offer is applicable for the first year only. 90% offer is valid only if you are currently using a paid competing cloud backup service. You need to provide proof of your existing paid service provider’s account. Competing services include Carbonite, Mozy, CrashPlan, Backblaze, SOS Online Backup, Dropbox and Google Backup and Sync.



Version 6.7.3.25

glenmaxson@gma...com
Quota: 5000.00 GB

● Backup files to my IDrive account ○ Backup files to Local, Wi-Fi or Express device

Files / folders for online backup

F:\	235264 files	1656.94 GB
G:\	291435 files	1606.74 GB
C:\Users\glenm\Music\	7 files	13.34 MB
C:\Users\glenm\OneDrive\Desktop\	489 files	99.74 GB
C:\Users\glenm\OneDrive\Documents\	323 files	28.86 GB
C:\Users\glenm\OneDrive\Pictures\	1046 files	447.97 MB
C:\Users\glenm\Videos\	69 files	30.80 GB

Credit & Debit Cards

- Monitor your credit report 3 times per year (for free)
- Opt-out of pre-approved credit offers*
- Use fraud alert* and credit freeze to eliminate ID theft
  - *Best Identity Theft Protection of 2019*
- Don’t fall for phishing attempts from fake financial institutions
- Consider a ‘virtual’ credit card for online purchases*

  When shopping use a randomly generated Virtual Account Number instead of your real account number. All purchases made with the temporary number will appear on your monthly statement with your other purchases and will include the Virtual Account Number that was used for each transaction.
- Protect your credit card(s) from skimmers*

  The all-in-one ATM skimmer: It stores card data using an integrated magnetic stripe reader, and it has a built-in hidden camera designed to record the PIN sequence after an unsuspecting customer slides his bank card into the compromised machine.

Cell Phones

- Enable the phone finding feature**
  - Find My Device (Android), Find iPhone (Apple)**
- Set a passcode (that you'll remember – 4 or 6 digits)*
- Update your phone's system software and apps when requested
- Enable cloud storage to back up your phone
  - Android –> Google Drive, Apple –> iCloud
- Use tougher passwords on your accounts
- Manage application 'permissions'***
- Install an anti-virus solution on your mobile device(s)
  - Android (AVG Free), iOS (Lookout)
- Disable Bluetooth when not in use*
- Be aware of 'meta-data' stored within each digital photo you take****
- Don't lose your phone!

**Find My ‘Device’

Android (*Find My Device*)

Open your device's Settings app ⚙ .
Tap Security & Location. (If you don't see "Security & Location,“tap Google, then Security.)
Tap Find My Device.
Turn on Remotely locate this device and Allow remote lock and erase.

Once set, here’s how to find your phone:
https://support.google.com/android/answer/6160491?hl=en

Apple (*Find My iPhone*)

Start at your Home screen.
Tap Settings > [your name] > iCloud. If you're using iOS 10.2 or earlier, go to Settings > iCloud.
Scroll to the bottom and tap Find My iPhone.
Slide to turn on Find My iPhone and Send Last Location.

Once set, here’s how to find your phone:
https://support.apple.com/en-us/HT201472

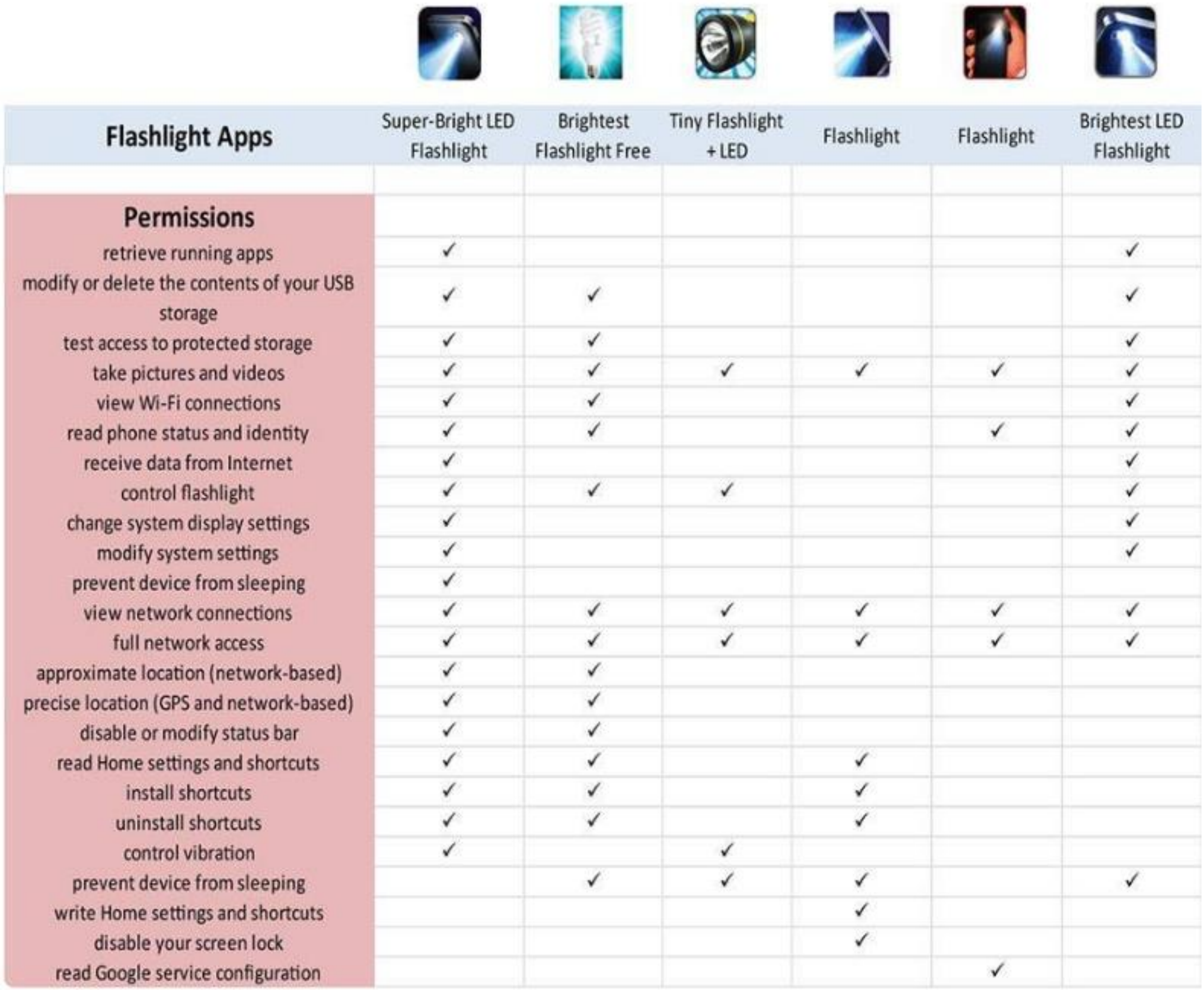
***Permissions

Android

Settings -> Apps -> click the gear icon -> App Permissions -> select category to deauthorize permission

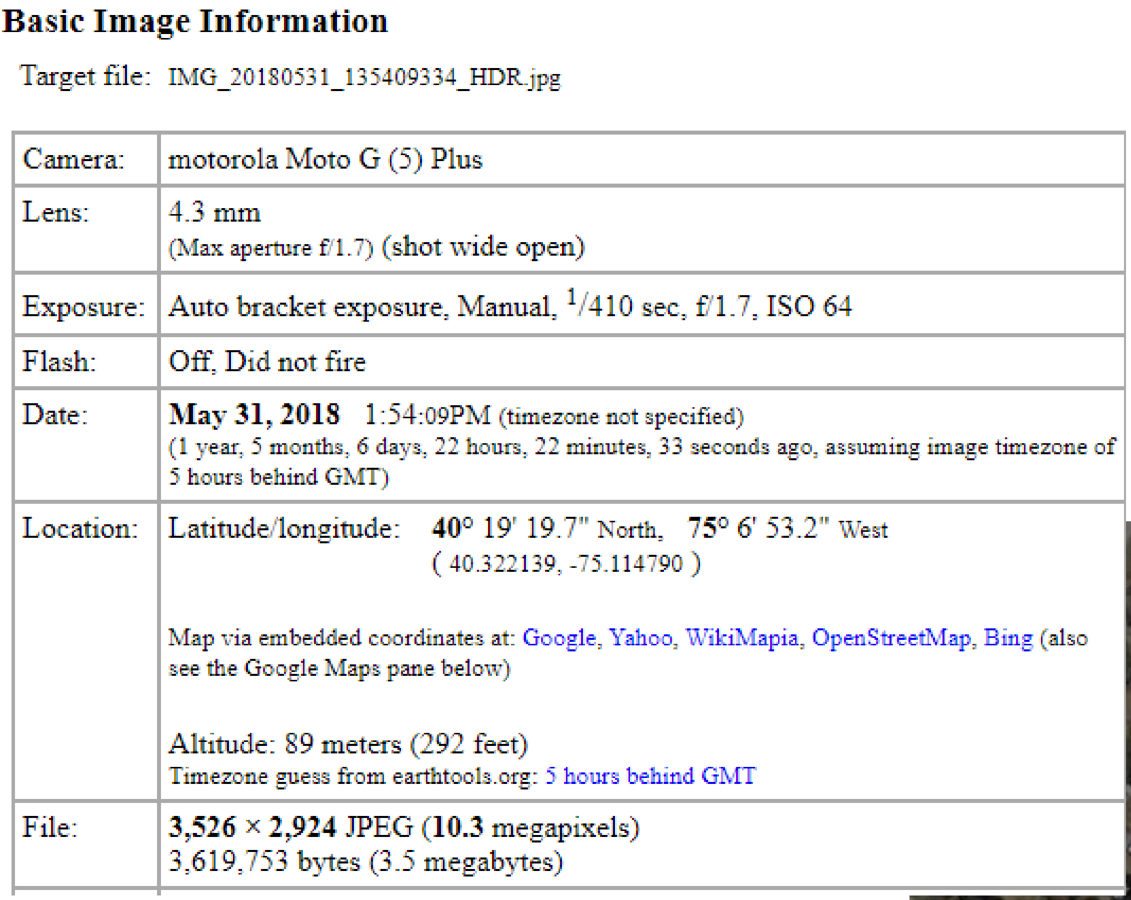
Apple

Settings -> [your name] -> iTunes & App Store -> Tap your Apple ID -> Tap View Apple ID -> Scroll to the App Permissions section -> Tap the service that you want to deauthorize access to



Flashlight Apps	Super-Bright LED Flashlight	Brightest Flashlight Free	Tiny Flashlight + LED	Flashlight	Flashlight	Brightest LED Flashlight
Permissions						
retrieve running apps	✓					✓
modify or delete the contents of your USB storage	✓	✓				✓
test access to protected storage	✓	✓				✓
take pictures and videos	✓	✓	✓	✓	✓	✓
view Wi-Fi connections	✓	✓				✓
read phone status and identity	✓	✓			✓	✓
receive data from Internet	✓					✓
control flashlight	✓	✓	✓			✓
change system display settings	✓					✓
modify system settings	✓					✓
prevent device from sleeping	✓					
view network connections	✓	✓	✓	✓	✓	✓
full network access	✓	✓	✓	✓	✓	✓
approximate location (network-based)	✓	✓				
precise location (GPS and network-based)	✓	✓				
disable or modify status bar	✓	✓				
read Home settings and shortcuts	✓	✓		✓		
install shortcuts	✓	✓		✓		
uninstall shortcuts	✓	✓		✓		
control vibration	✓		✓			
prevent device from sleeping		✓	✓	✓		✓
write Home settings and shortcuts				✓		
disable your screen lock				✓		
read Google service configuration					✓	

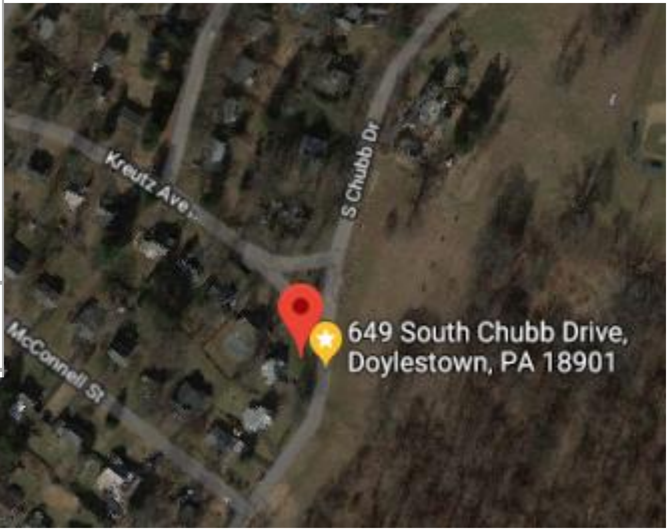
****Jeffrey's Image Metadata Viewer



Basic Image Information

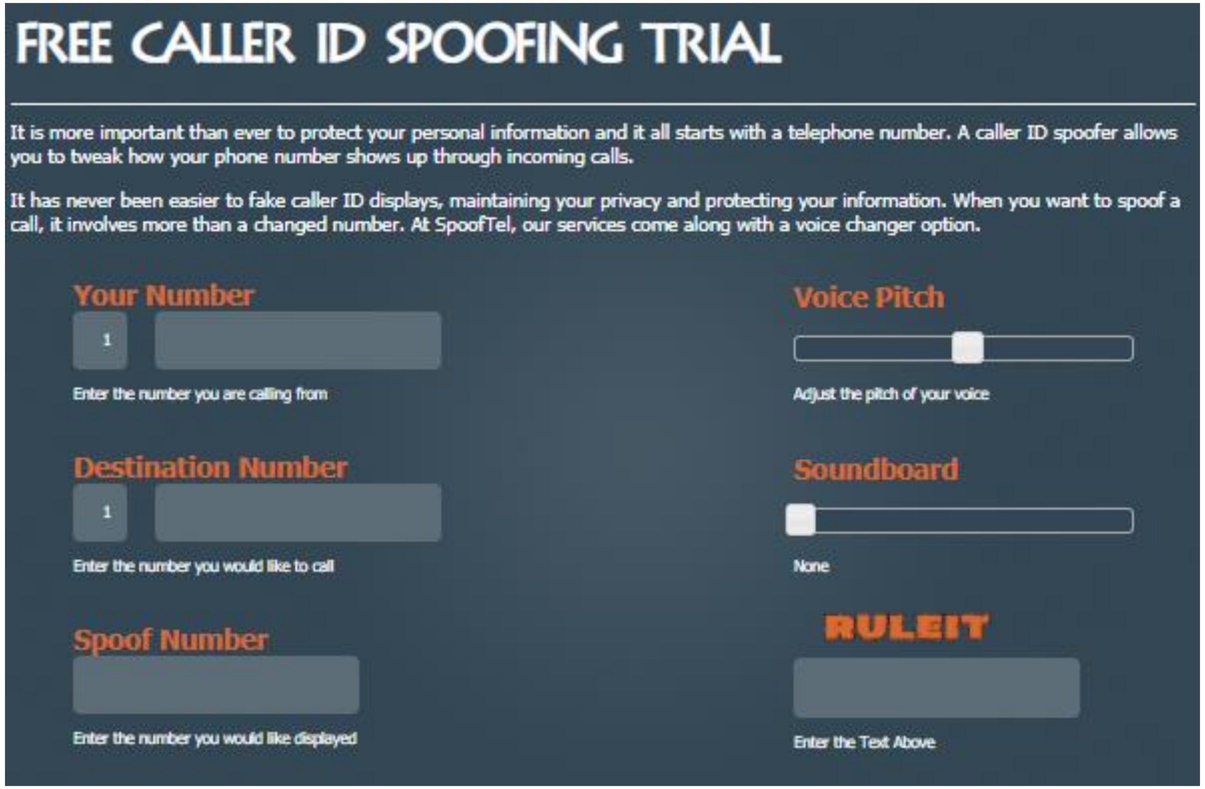
Target file: IMG_20180531_135409334_HDR.jpg

Camera:	motorola Moto G (5) Plus
Lens:	4.3 mm (Max aperture f/1.7) (shot wide open)
Exposure:	Auto bracket exposure, Manual, $^{1}/410$ sec, f/1.7, ISO 64
Flash:	Off, Did not fire
Date:	**May 31, 2018** 1:54:09PM (timezone not specified) (1 year, 5 months, 6 days, 22 hours, 22 minutes, 33 seconds ago, assuming image timezone of 5 hours behind GMT)
Location:	Latitude/longitude: **40°** 19' 19.7" North, **75°** 6' 53.2" West (40.322139, -75.114790) Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 89 meters (292 feet) Timezone guess from earthtools.org: 5 hours behind GMT
File:	**3,526** × **2,924** JPEG (**10.3** megapixels) 3,619,753 bytes (3.5 megabytes)



Telephone Attacks

- Caller ID can be manipulated
- Telephone surveys should be avoided – just hang up*
- Always question the authenticity of a caller – when in doubt, hang up and call back on a number you know
- Only allow remote access to your computer by someone you know AND trust!



FREE CALLER ID SPOOFING TRIAL

It is more important than ever to protect your personal information and it all starts with a telephone number. A caller ID spoofer allows you to tweak how your phone number shows up through incoming calls.

It has never been easier to fake caller ID displays, maintaining your privacy and protecting your information. When you want to spoof a call, it involves more than a changed number. At SpoofTel, our services come along with a voice changer option.

Your Number: 1

Enter the number you are calling from

Voice Pitch

Adjust the pitch of your voice

Destination Number: 1

Enter the number you would like to call

Soundboard: None

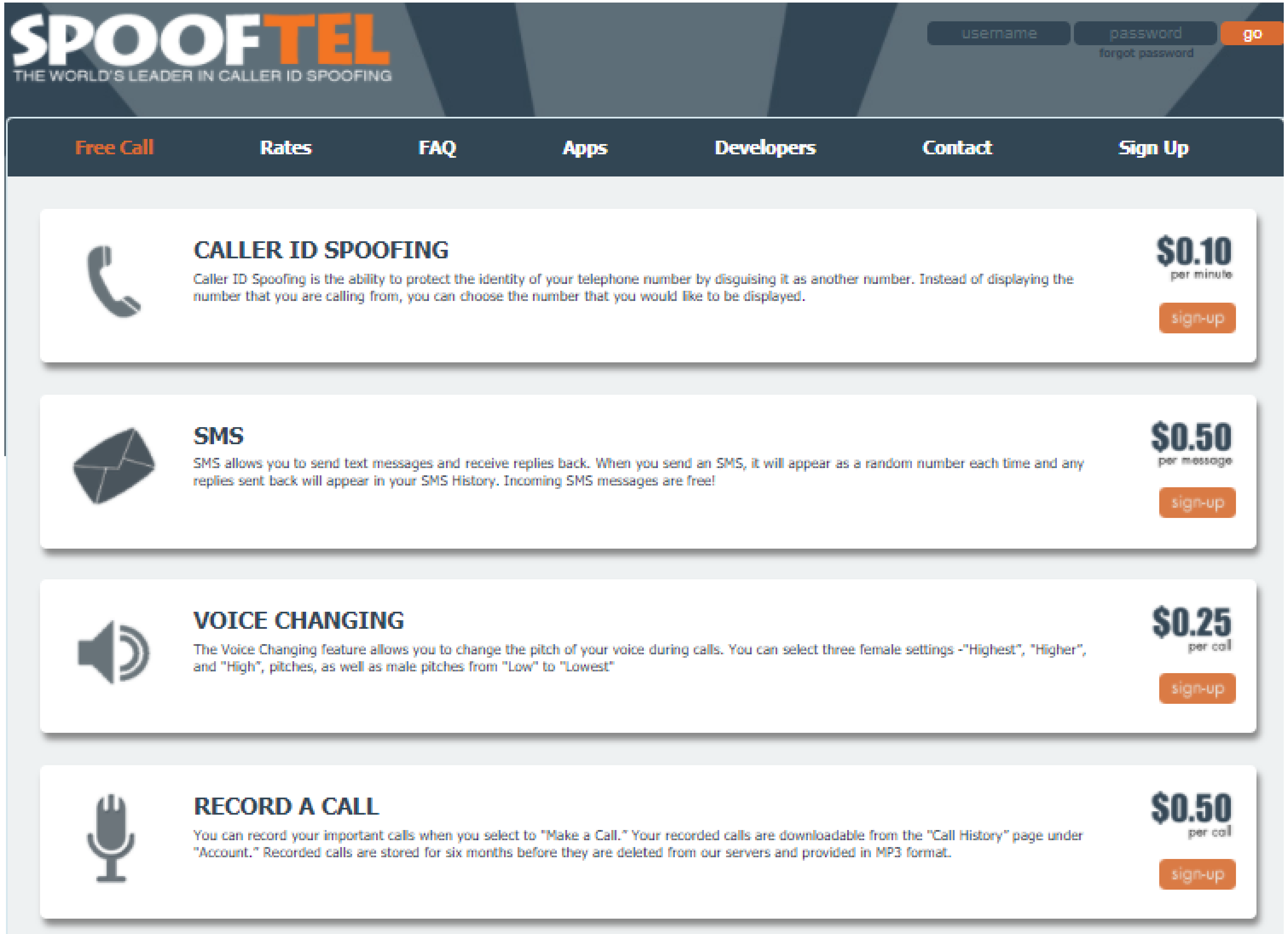
Spoof Number

Enter the number you would like displayed

RULEIT

Enter the Text Above

The World’s Leader in Caller ID Spoofing (source)



CALLER ID SPOOFING

Caller ID Spoofing is the ability to protect the identity of your telephone number by disguising it as another number. Instead of displaying the number that you are calling from, you can choose the number that you would like to be displayed.

$0.10 per minute

SMS

SMS allows you to send text messages and receive replies back. When you send an SMS, it will appear as a random number each time and any replies sent back will appear in your SMS History. Incoming SMS messages are free!

$0.50 per message

VOICE CHANGING

The Voice Changing feature allows you to change the pitch of your voice during calls. You can select three female settings -"Highest", "Higher", and "High", pitches, as well as male pitches from "Low" to "Lowest"

$0.25 per call

RECORD A CALL

You can record your important calls when you select to "Make a Call." Your recorded calls are downloadable from the "Call History" page under "Account." Recorded calls are stored for six months before they are deleted from our servers and provided in MP3 format.

$0.50 per call

Miscellaneous Stuff

- Surveillance cameras, copiers/printers, thermostats, home automation… are all network connected
  - If you can access your security cameras and other devices through the internet, so can everyone else
  - Change access username and password if possible
- Home Wireless
  - Use security built into your router and change the default admin user name and password*
- Public Wi-Fi
  - Be VERY cautious when using public networks or computers
  - <u>Never</u> use them to access sites/services that require you to enter accounts or passwords
  - Consider accessing public networks in ‘guest’ mode, or use your smartphone’s tethering service (if available)

From ‘How to Stay Safe on Public Wi-Fi Networks’

1. Turn Off Sharing

When you're at home, you may share files, printers, or even allow remote login from other computers on your network. When you're on a public network, you'll want to turn these things off.

2. Enable Your Firewall

Most OSes come with at least a basic firewall, and it's a simple step to keeping unwanted local users from poking at your computer.

3. Use HTTPS and SSL Whenever Possible

Regular web site connections over HTTP exchange lots of plain text over the wireless network you're connected to, and someone with the right skills and bad intent can easily ‘sniff’ that traffic.

4. Consider Using a Virtual Private Network (VPN)

These services let you route all your activity through a separate secure, private network, thus giving you the security of a private network even though you're on a public one.

5. Turn Wi-Fi Off When You Aren't Using It*

If you want to guarantee your security and you're not actively using the internet, simply turn off your Wi-Fi

Going Incognito

- Chrome, Firefox, Edge,Opera, IE (source)
- What happens in 'incognito' mode (aka privacy mode or private browsing)?
  - '**Incognito mode**' is a privacy feature in most mainstream web browsers to disable browsing history and the web cache. This allows a person to browse the Web without storing local data that could be retrieved at a later date. Privacy mode also disables the storage of data in cookies and Flash cookies. This privacy protection is only on the local computing device as it is still possible to identify frequented websites by associating the IP address at the web server.

Extensions to Help Maintain Your Privacy

- **AdBlock Plus** - content-filtering and ad blocking extension, available on Firefox, Firefox mobile, Chrome, IE, Edge, Opera, Safari, Yandex, and Android
- **Ghostery** - privacy and security-related browser extension and mobile browser app that enables its user to detect and control JavaScript "tags" and "trackers“, available for Firefox, Chrome, IE, Edge, Opera, Safari, iOS, Android, and Firefox for Android.
- **Disconnect.me** - browser extension that block trackers, enables private search
- **DuckDuckGo** – Internet search engine that emphasizes protecting searchers' privacy and avoiding the filter bubble of personalized search results – in 2016 The Tor Project made DuckDuckGo the default search engine for Tor Browser 6.0

Primary reference for this presentation:

Personal Digital Security: Protecting Yourself From Online Crime

2016 - Michael Bazzell

Other books by Michael Bazzell

Hiding from the Internet: Eliminating Personal Online Information - 3rd Edition

2016 - Michael Bazzell

Outsmarting Your Kids Online: A Safety Handbook for Overwhelmed Parents

2016 - Michael Bazzell & Amber Mac

Extreme Privacy: What It Takes to Disappear (2nd edition)

2019 - Michael Bazzell

Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information 7th Edition

2019 - Michael Bazzell

And Michael's website - https://inteltechniques.com/

Ransomware

What is Ransomware?

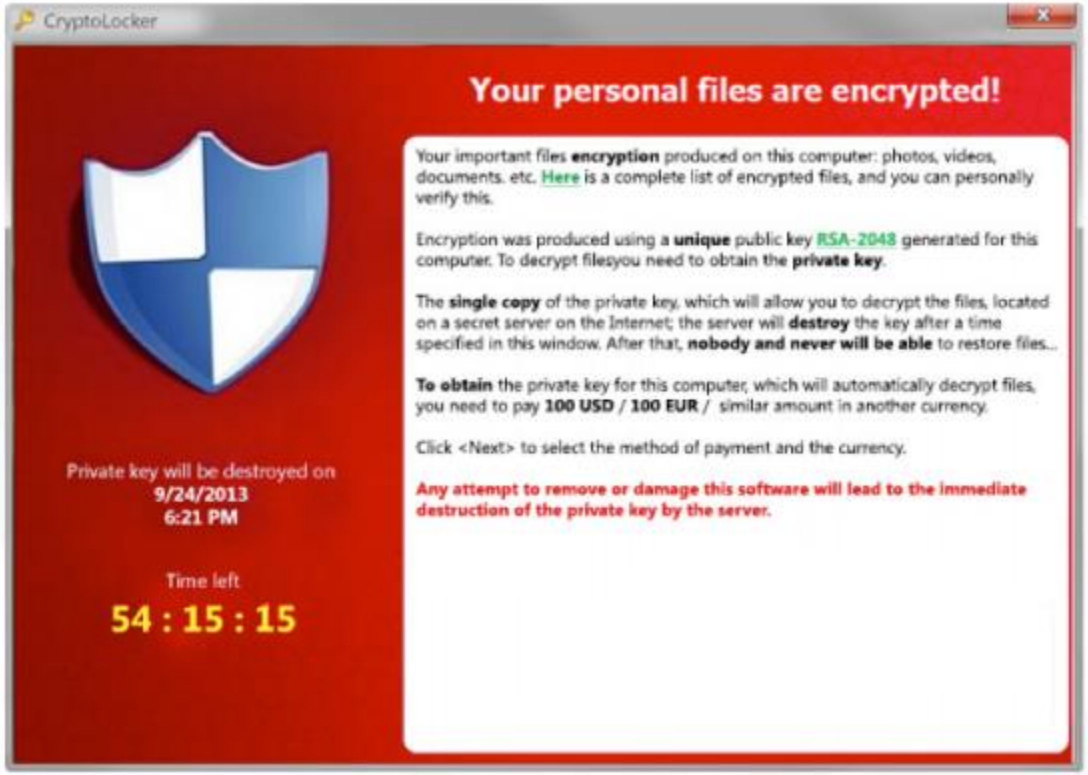
- Ransomware is a malicious piece of software that 'denies access to a device or files until a ransom has been paid'
- Ransomware can be 'delivered' via phishing emails, unpatched programs, compromised websites, online ads or free software downloads

What does Ransomware do?

- Ransomware will usually encrypt files on your computer, and on shared network drives
- Once files are encrypted, hackers will display a screen or web address explaining how to unlock your files
- Ransomware typically has a deadline for compliance (48-72 hours) and once passed the ransom will increase or will no longer be available
- Ransoms are usually paid with untraceable e-currency (cryptocurrency) like Bitcoin (BTC)
- Once payment is verified, encryption is removed and file decryption begins – hopefully…

Am I infected?

- Symptoms
  - Can’t open files – get errors such as ‘file corrupted’, ‘wrong extension’
  - Alarming message on your desktop telling you how to pay to unlock your files
  - Program warns you that there’s a countdown until the ransom increases or your files can no longer be decrypted
  - Windows opens to a ransomware program that can’t be closed
  - You have files with names like ‘HOW TO DECRYPT FILES.txt’ or DECRYPT_INSTRUCTIONS.html



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD** / **100 EUR** / similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

Infection Vectors (DON’T DO THIS!)

- Email (most common)
  - User receives an e-mail with an attachment or link to a software download
  - User install or opens the attachment without verifying the sender or the file/link’s ‘authenticity’

- ‘Drive-by-download’
  - User visits a website with an old browser or plug-in, or an unpatched 3rd party app
  - Hacker exploits a bug in the software that allows execution of malicious code

- Free software
  - Be really careful when downloading ‘free’ software! These downloads often contain malware and possibly ransomware (MineCraft mods example)

DO THIS!

- Don’t open attachments or click on links you’re not absolutely sure about
- Keep your operating system patched and applications up-to-date
- Be especially careful when downloading ‘free’ software
- Run both virus AND malware programs to catch and eliminate infections

You didn’t listen and you’re infected, now what?

1. Disconnect – get off the network, unplug connected devices, don’t erase anything!
2. Determine the scope – to what extent is your infrastructure compromised
   - Take inventory – shared drive and folders, network storage, external drives, USB drives, cloud-based storage (DropBox, Google Drive, OneDrive…)
   - What’s backed up and what’s not, what’s encrypted and what’s not
   - Check the ransomware file (probably in the registry) listing all the files it has encrypted
   - There are also tools available that will help list all the encrypted files
3. Determine the strain – what exactly are you dealing with?
   - Some strains have already been decrypted and you won’t have to pay anything
   - Cost can vary, as can the type of payment requested if not Bitcoin
4. Evaluate your response – what will your next action be?
   - Restore from recent backup (best case)
   - Decrypt using 3rd party decryptor (not likely)
   - Do nothing – lose your data and rebuild
   - Negotiate – pay the ransom

First response: Restore files from backup

What, you don’t have a backup? Why not? – moving on…

- Locate your possible backup sources
- Prepare for restoration – wipe and rebuild may be the safest approach
- Prevention – Anti-virus, anti-spam, anti-malware, backup software running – check!
  - But wait, there’s one more thing – that’s you, the ‘human firewall’

Second response: Try to decrypt (good luck with that)

- Determine the strain
- Locate an appropriate decryptor/unlocker
  - Be sure the decryptor you found is vetted from a reliable source
  - Consult the professionals before using these tools
- Success? – you lucked out!
- Failure? – so sorry. Time to restore from backup or pay the ransom…

Third response: Do nothing

No backup, don’t want to pay the ransom – time to rebuild

- Rid your computer of ransomware
  - Run multiple anti-virus scans if complete rebuild is not an option
- Option: Back up encrypted files – could get lucky if the decrypt keys become available
- Prevent future attacks (and why didn’t I think of this before)
  - Install and maintain effective anti-virus and anti-malware software
  - Configure regular backups and/or local backup device
  - Eliminate the ‘human factor’ through proper training and discipline

Fourth response: Negotiate and/or Pay the Ransom

You have no other option and your data is too important lose, so pay

- Question 1: If I pay, will the hackers decrypt my files? Most likely…
  - They want your money and will provide ‘excellent customer service’ to get it
  - However, they might lose access to your files before they can decrypt

But let’s assume the best and pay up – here’s how…

Paying your ransom

Locate your payment method instructions

- Instructions will be on the screen or in a file on the system – follow the instructions
    - How much to pay
    - Where to pay
    - Time left to pay (and what happens when the time expires)

Obtain Bitcoin

- Set up an account with a Bitcoin exchange (or get your Bitcoin faster through a broker)
- Buy a little more Bitcoin than required to compensate for price changes and transaction fees

Install a TOR browser (if necessary)

- Get the TOR browser only from here (https://www.torproject.org/)
- Install the browser and open it, then navigate to the site provided in the instructions

Welcome to the Darknet

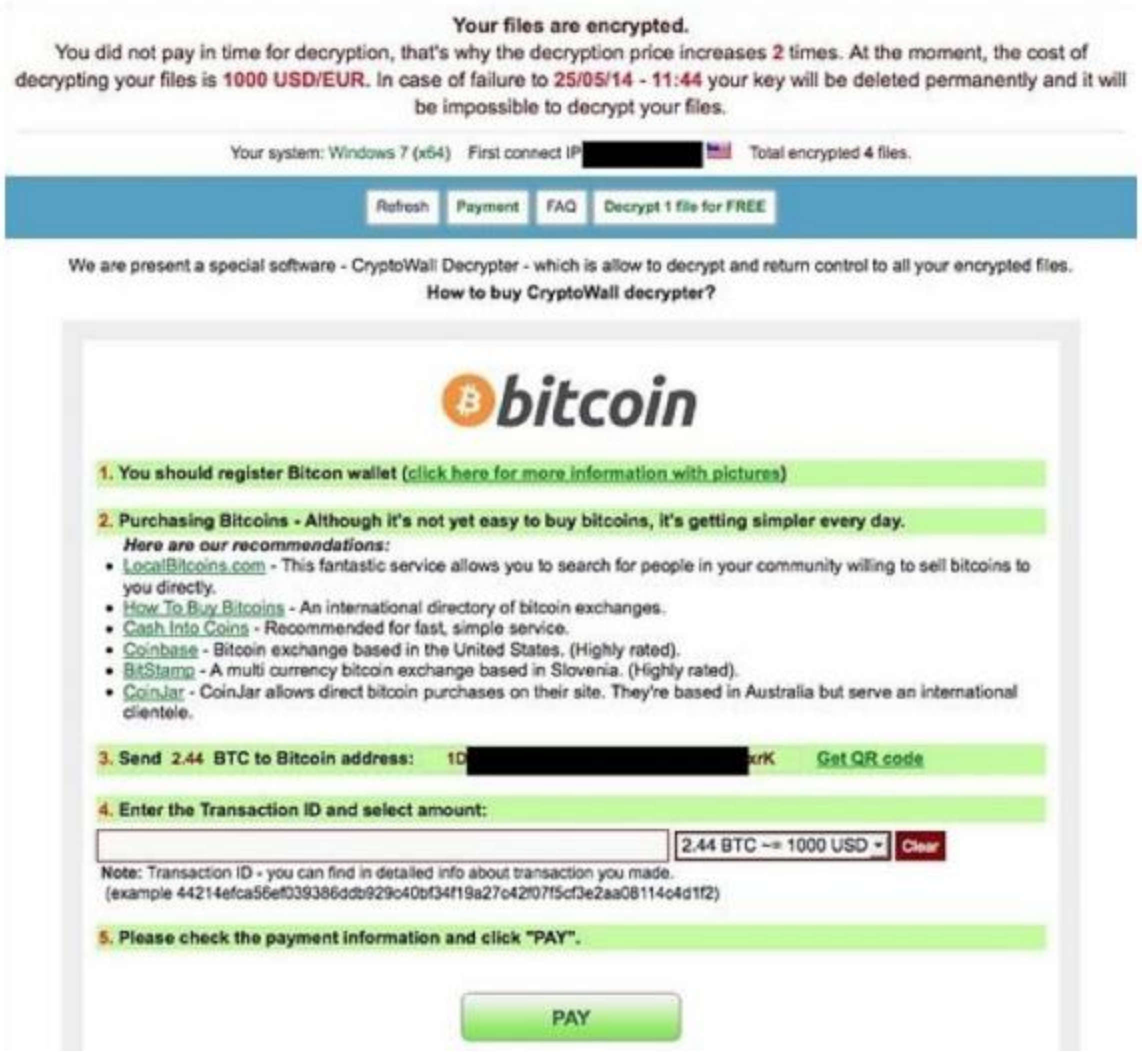
Paying your ransom (continued)

Pay the ransom

- Once you have your Bitcoin and TOR browser, navigate to the TOR address provided
- Get the hacker’s BTC wallet you’ll use to transfer BTC to
- Might also need the transaction ID or hash generated when the transfer is made
    - Once the transfer is made (20-40 minutes), then record the transfer hash
- Decrypt your files – once the transaction is processed you’ll receive a decrypt key
    - Make sure external drives, USB keys, etc. are connected and active
    - Shared folders and external drive paths need to be what they were at the time the encryption originally occurred

I Wish You Luck – You’re Going to Need It…

Sample CryptoWall payment screen:



Your files are encrypted.

You did not pay in time for decryption, that's why the decryption price increases **2** times. At the moment, the cost of decrypting your files is **1000 USD/EUR**. In case of failure to **25/05/14 - 11:44** your key will be deleted permanently and it will be impossible to decrypt your files.

Your system: Windows 7 (x64) First connect IP[redacted] Total encrypted **4** files.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You should register Bitcon wallet (click here for more information with pictures)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- LocalBitcoins.com - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Recommended for fast, simple service.
- Coinbase - Bitcoin exchange based in the United States. (Highly rated).
- BitStamp - A multi currency bitcoin exchange based in Slovenia. (Highly rated).
- CoinJar - CoinJar allows direct bitcoin purchases on their site. They're based in Australia but serve an international clientele.

3. Send 2.44 BTC to Bitcoin address: 1D[redacted]xrK Get QR code

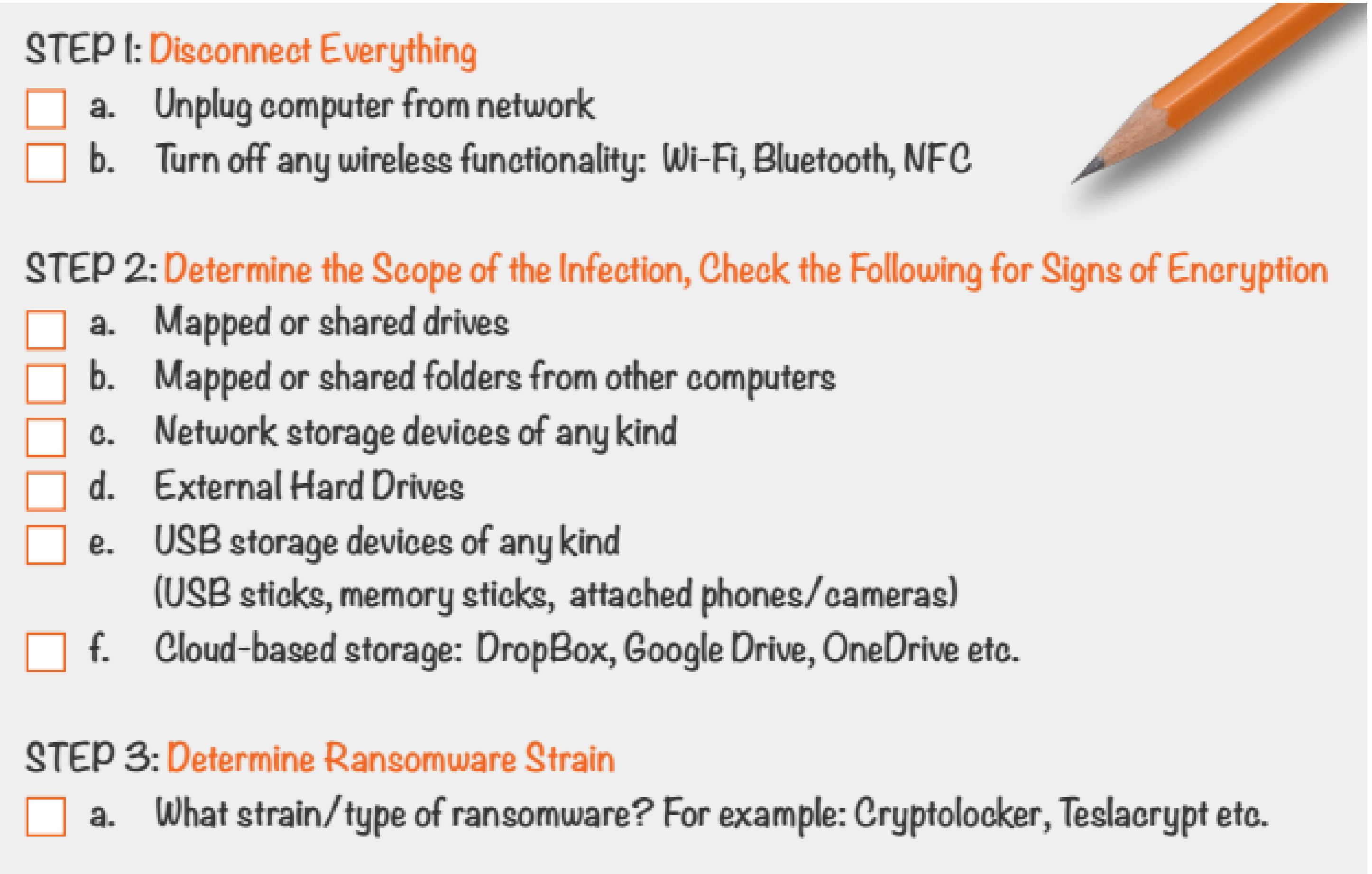
4. Enter the Transaction ID and select amount:

2.44 BTC ~= 1000 USD

Note: Transaction ID - you can find in detailed info about transaction you made. (example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

5. Please check the payment information and click "PAY".

Ransomware Attack Response Checklist (source)



STEP 1: Disconnect Everything

□ a. Unplug computer from network

□ b. Turn off any wireless functionality: Wi-Fi, Bluetooth, NFC

STEP 2: Determine the Scope of the Infection, Check the Following for Signs of Encryption

□ a. Mapped or shared drives

□ b. Mapped or shared folders from other computers

□ c. Network storage devices of any kind

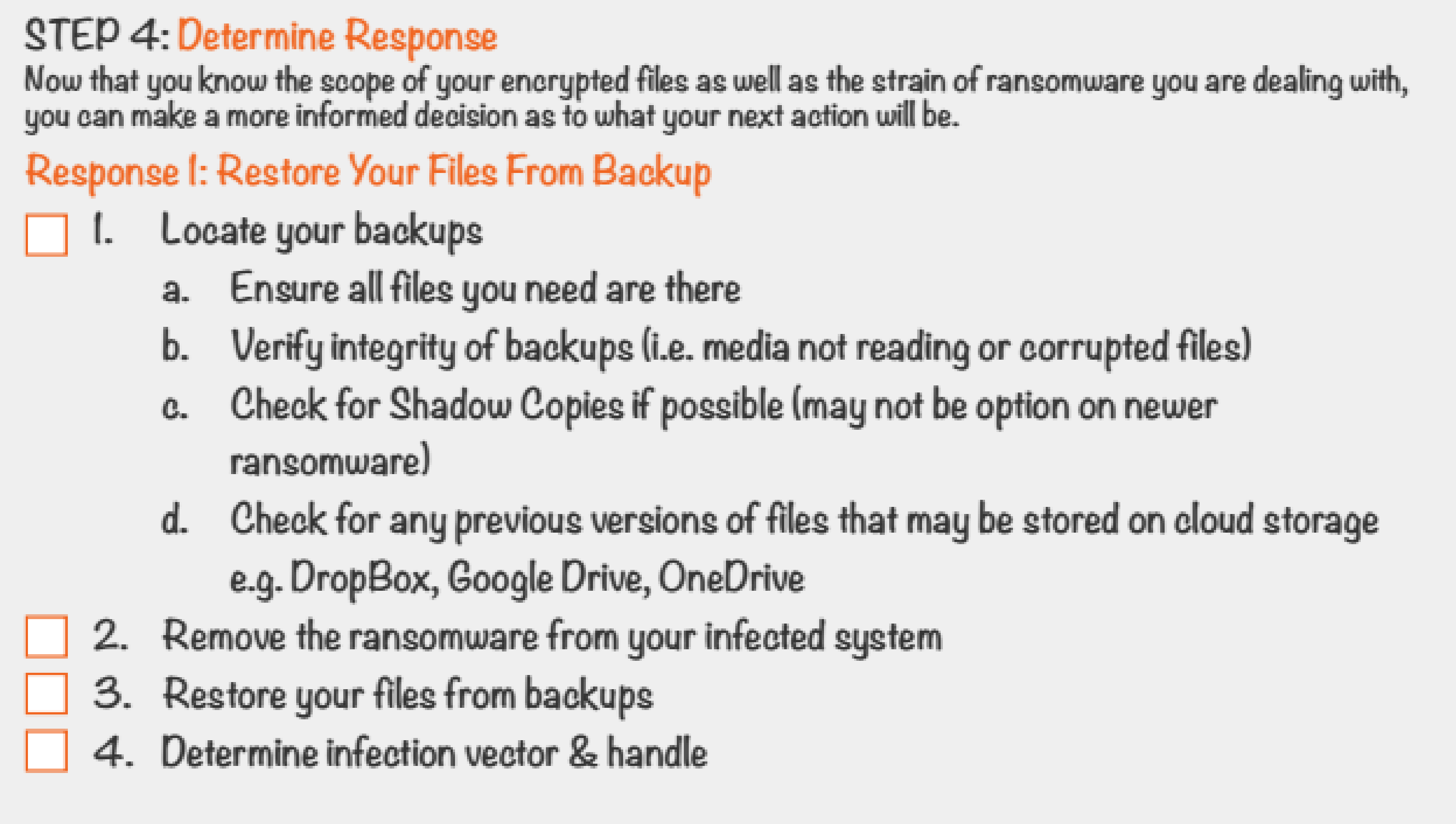
□ d. External Hard Drives

□ e. USB storage devices of any kind
(USB sticks, memory sticks, attached phones/cameras)

□ f. Cloud-based storage: DropBox, Google Drive, OneDrive etc.

STEP 3: Determine Ransomware Strain

□ a. What strain/type of ransomware? For example: Cryptolocker, Teslacrypt etc.

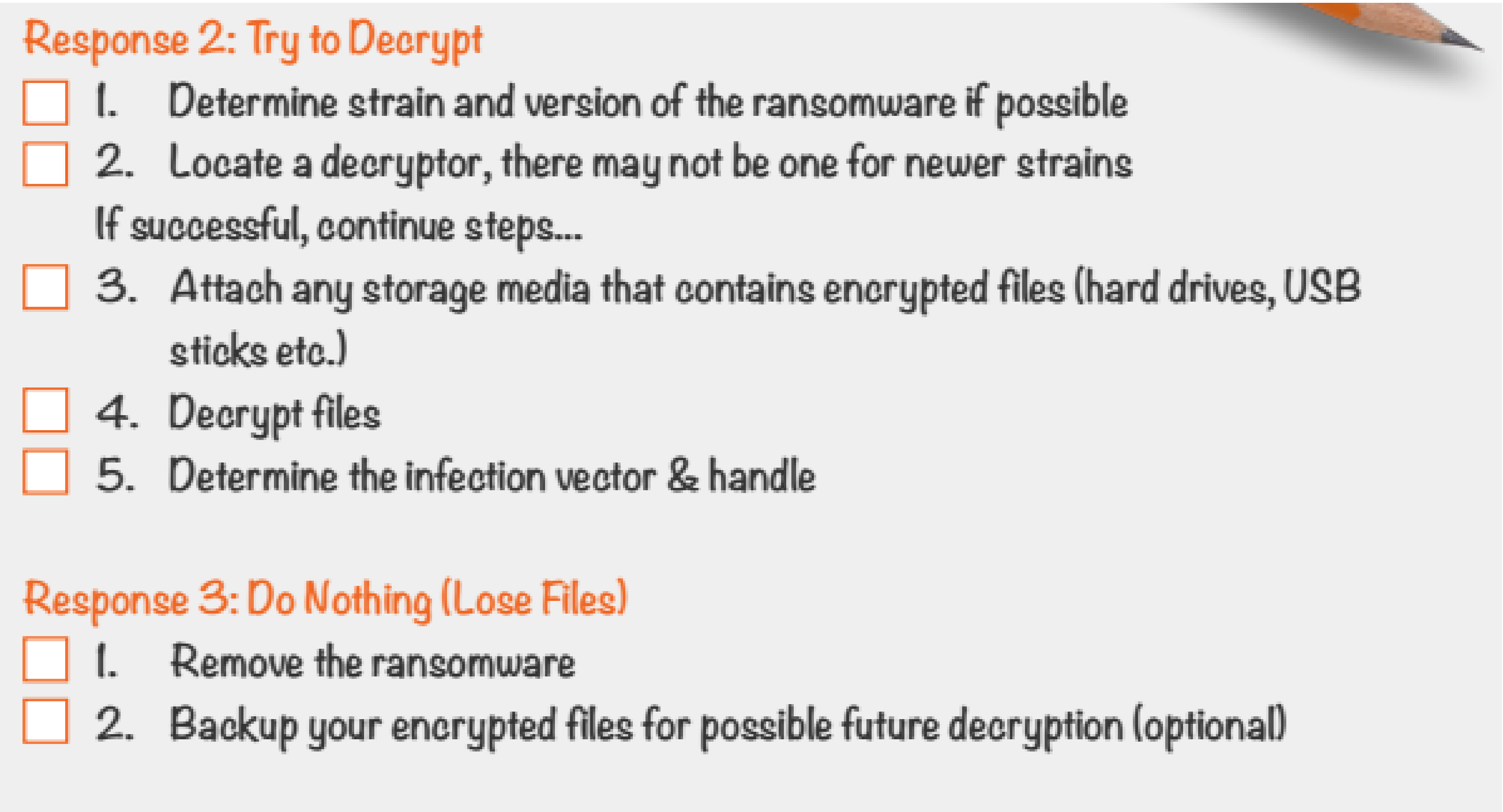


STEP 4: Determine Response

Now that you know the scope of your encrypted files as well as the strain of ransomware you are dealing with, you can make a more informed decision as to what your next action will be.

Response 1: Restore Your Files From Backup

- □ 1. Locate your backups
  - a. Ensure all files you need are there
  - b. Verify integrity of backups (i.e. media not reading or corrupted files)
  - c. Check for Shadow Copies if possible (may not be option on newer ransomware)
  - d. Check for any previous versions of files that may be stored on cloud storage e.g. DropBox, Google Drive, OneDrive
- □ 2. Remove the ransomware from your infected system
- □ 3. Restore your files from backups
- □ 4. Determine infection vector & handle



Response 2: Try to Decrypt

□ 1. Determine strain and version of the ransomware if possible

□ 2. Locate a decryptor, there may not be one for newer strains

If successful, continue steps...

□ 3. Attach any storage media that contains encrypted files (hard drives, USB sticks etc.)

□ 4. Decrypt files

□ 5. Determine the infection vector & handle

Response 3: Do Nothing (Lose Files)

□ 1. Remove the ransomware

□ 2. Backup your encrypted files for possible future decryption (optional)

Response 4: Negotiate and/or Pay the Ransom

□ 1. If possible, you may attempt to negotiate a lower ransom and/or longer payment period

□ 2. Determine acceptable payment methods for the strain of ransomware: Bitcoin, Cash Card etc.

□ 3. Obtain payment, likely Bitcoin:

   a. Locate an exchange you wish to purchase a Bitcoin through (time is of the essence)

   b. Set up account/wallet and purchase the Bitcoin

□ 4. Re-connect your encrypted computer to the internet

□ 5. Install the TOR browser (optional)

□ 6. Determine the Bitcoin payment address. This is either located in the ransomware screen or on a TOR site that has been set up for this specific ransom case

□ 7. Pay the ransom: Transfer the Bitcoin to the ransom wallet

□ 8. Ensure all devices that have encrypted files are connected to your computer

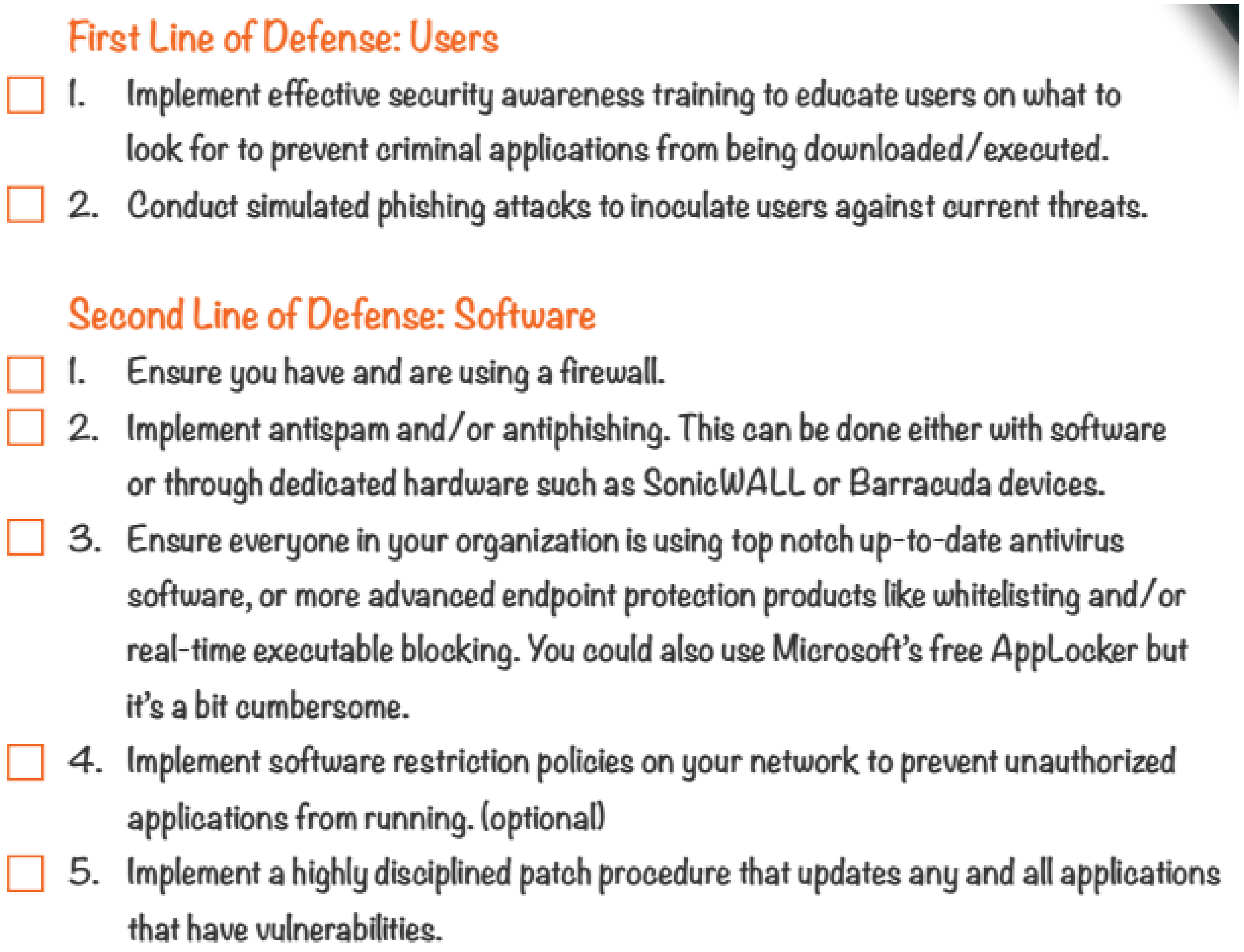
□ 9. File decryption should begin within 24 hours, but often within just a few hours

□ 10. Determine infection vector and handle

STEP 5: ProtectingYourselt in the Future

□ a. Implement Ransomware Prevention Checklist to prevent future attacks

Ransomware Prevention Checklist (source)



First Line of Defense: Users

- □ 1. Implement effective security awareness training to educate users on what to look for to prevent criminal applications from being downloaded/executed.
- □ 2. Conduct simulated phishing attacks to inoculate users against current threats.

Second Line of Defense: Software

- □ 1. Ensure you have and are using a firewall.
- □ 2. Implement antispam and/or antiphishing. This can be done either with software or through dedicated hardware such as SonicWALL or Barracuda devices.
- □ 3. Ensure everyone in your organization is using top notch up-to-date antivirus software, or more advanced endpoint protection products like whitelisting and/or real-time executable blocking. You could also use Microsoft's free AppLocker but it's a bit cumbersome.
- □ 4. Implement software restriction policies on your network to prevent unauthorized applications from running. (optional)
- □ 5. Implement a highly disciplined patch procedure that updates any and all applications that have vulnerabilities.

Third Line of Defense: Backups

□ 1. Implement a backup solution: Software based, hardware based, or both.

□ 2. Ensure all possible data you need to access or save is backed up, including mobile/USB storage.

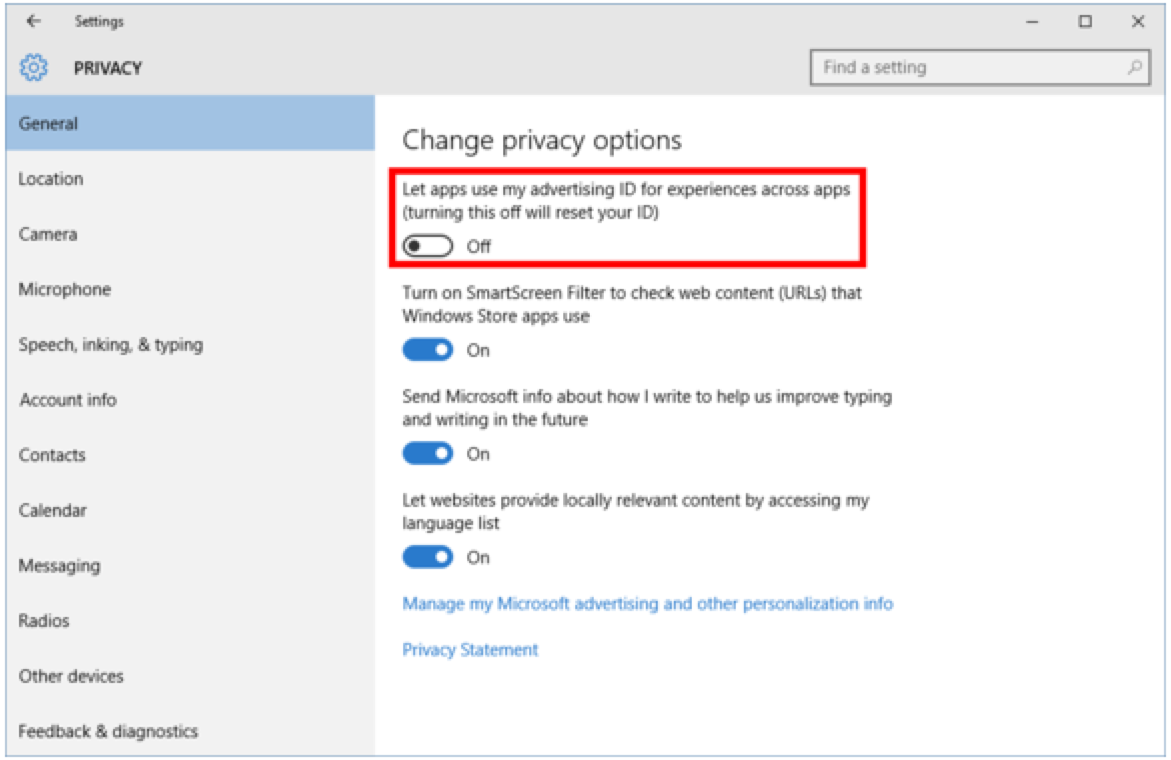
□ 3. Ensure your data is safe, redundant and easily accessible once backed up.

□ 4. Regularly test the recovery function of your backup/restore procedure. Test the data integrity of physical backups and ease-of-recovery for online/software based backups.

Microsoft (play video)

How to reclaim your privacy in Windows 10, piece by piece
Even when told not to, Windows 10 just can’t stop talking to Microsoft

What’s the problem?
Windows 10 is studded with data-tracking tidbits and hooks into Microsoft’s online services. Handing over all that data has some benefits, but not everyone is thrilled with the idea of an operating system constantly looking over their digital shoulder.



Change privacy options

Let apps use my advertising ID for experiences across apps (turning this off will reset your ID)

Off

Turn on SmartScreen Filter to check web content (URLs) that Windows Store apps use

On

Send Microsoft info about how I write to help us improve typing and writing in the future

On

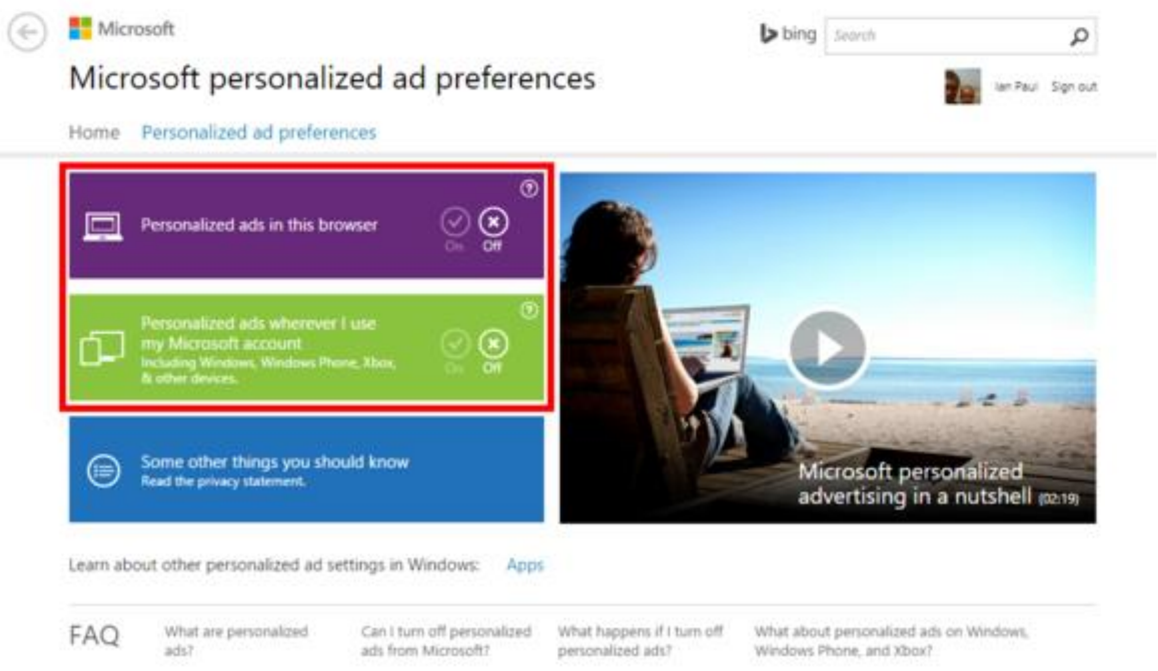
Let websites provide locally relevant content by accessing my language list

On

Manage my Microsoft advertising and other personalization info

Privacy Statement

Disable advertising integration - go to *Settings > Privacy > General* and slide the option that says ‘Let apps use my advertising ID for experience across apps (turning this off will reset your ID)’ to *Off*.



Microsoft

Microsoft personalized ad preferences

Home Personalized ad preferences

Personalized ads in this browser — On [✓ Off]

Personalized ads wherever I use my Microsoft account
Including Windows, Windows Phone, Xbox, & other devices. — On [✓ Off]

Some other things you should know
Read the privacy statement.

Microsoft personalized advertising in a nutshell (02:19)

Learn about other personalized ad settings in Windows: Apps

FAQ

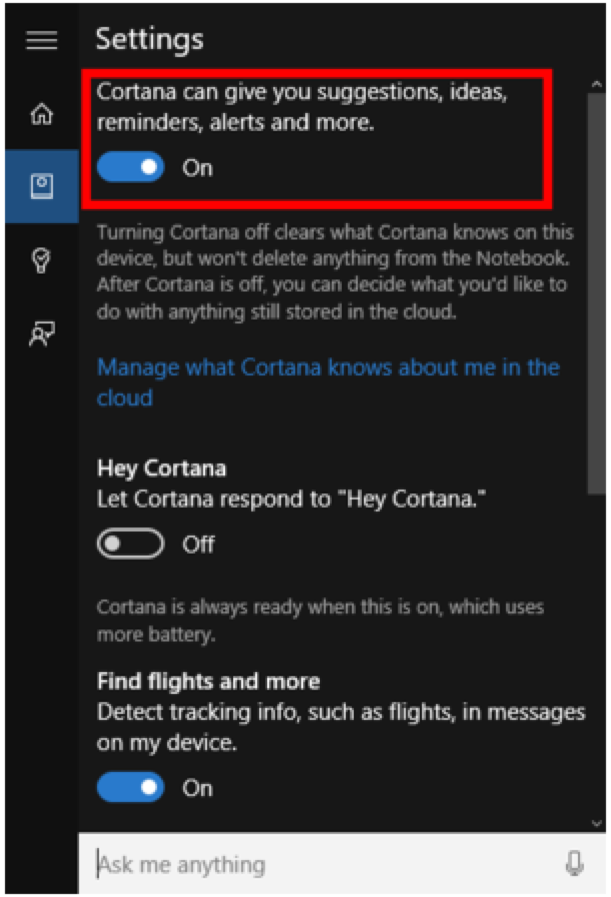
What are personalized ads?

Can I turn off personalized ads from Microsoft?

What happens if I turn off personalized ads?

What about personalized ads on Windows, Windows Phone, and Xbox?

Next, open your web browser and go to choice.microsoft.com/en-us/opt-out. There, select *Off* for “Personalized ads wherever I use my Microsoft account” and “Personalized ads in this browser.” note: you may need to turn your ad blocker off for this site before you’ll see the option



Settings

Cortana can give you suggestions, ideas, reminders, alerts and more.

On

Turning Cortana off clears what Cortana knows on this device, but won't delete anything from the Notebook. After Cortana is off, you can decide what you'd like to do with anything still stored in the cloud.

Manage what Cortana knows about me in the cloud

Hey Cortana

Let Cortana respond to "Hey Cortana."

Off

Cortana is always ready when this is on, which uses more battery.

Find flights and more

Detect tracking info, such as flights, in messages on my device.

On

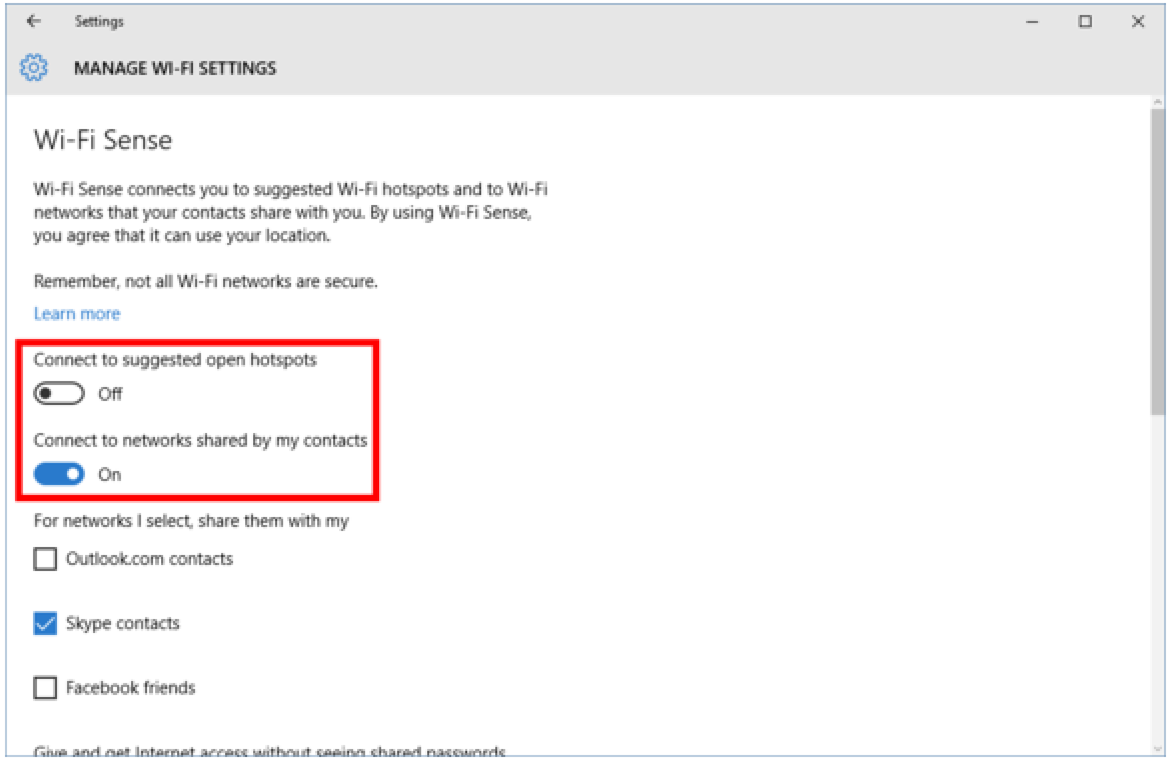
Ask me anything

Turn Cortana *Off* - click the Cortana icon in the taskbar, and then click the notebook icon on the left-hand side of the pop-up panel. Select *Settings* then slide the top option that says 'Cortana can give you suggestions, ideas, reminders, alerts, and more' to *Off*.

Once Cortana is gone, you'll see a new option that says 'Search online and include web results.' - this includes Bing results when you search for things on your PC. I'd disable this as well.

Next, return to the Settings app's privacy section. Open Settings and go to *Privacy > Speech, inking, and typing*. This setting allows Cortana to gather data about you to help it deliver services. Click the *Stop getting to know me* button to end that. This will delete collected data stored on your PC, and it also turns off dictation functionality.

And finally, click 'Go to Bing and manage personal info for all your devices.' Here you can scrub any data that Microsoft has collected about you. Go to the bottom of the page and click *Clear.*



Settings

MANAGE WI-FI SETTINGS

Wi-Fi Sense

Wi-Fi Sense connects you to suggested Wi-Fi hotspots and to Wi-Fi networks that your contacts share with you. By using Wi-Fi Sense, you agree that it can use your location.

Remember, not all Wi-Fi networks are secure.

Learn more

Connect to suggested open hotspots

Off

Connect to networks shared by my contacts

On

For networks I select, share them with my

□ Outlook.com contacts

☑ Skype contacts

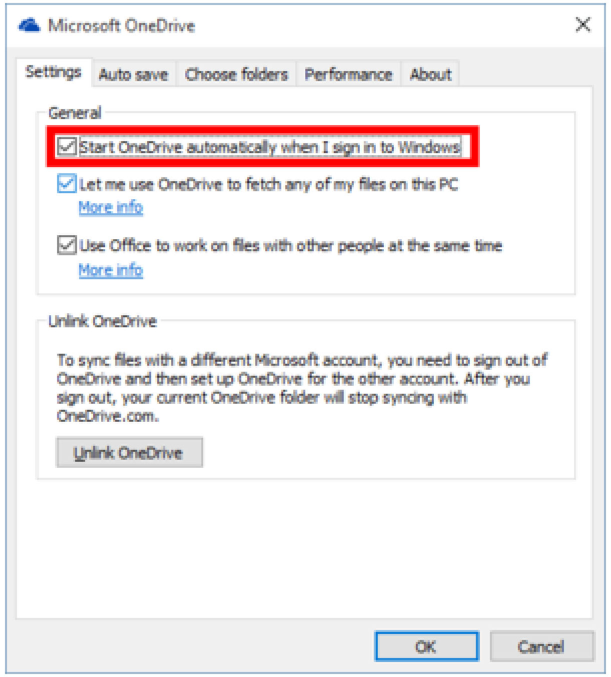
□ Facebook friends

Give and get Internet access without seeing shared passwords

Wi-Fi Sense is turned on by default. It lets you share access to password-protected Wi-Fi routers. The idea is that friends or family don't have to ask for your password. Instead, anyone that uses a Windows 10 device *and* is a 'digital friend' is automatically logged in.

To make sure Wi-Fi Sense is off, go to *Settings > Network & Internet > Wi-Fi > Manage Wi-Fi Settings*. Then slide the two options that say 'Connect to suggested open hotspots' and 'Connect to networks shared by my contacts' to *Off.*

I also recommend controlling how files and updates are delivered to your PC. Go to *Settings > Update & Security > Windows Update > Advanced options > Choose how updates are delivered*. By default, 'Updates from more than one place' is enabled and set to both local sources and other PCs on the Internet. You can distribute updates only to PCs on your local network, or shut off the P2P updates entirely and stick to using Microsoft's servers alone. I would shut off everything by moving the slider on this screen to *Off.* If you want to share with PCs on your local network, leave the slider in the On position and select the radio button that says 'PCs on my local network.'



General

☑ Start OneDrive automatically when I sign in to Windows

☑ Let me use OneDrive to fetch any of my files on this PC
More info

☑ Use Office to work on files with other people at the same time
More info

Unlink OneDrive

To sync files with a different Microsoft account, you need to sign out of OneDrive and then set up OneDrive for the other account. After you sign out, your current OneDrive folder will stop syncing with OneDrive.com.

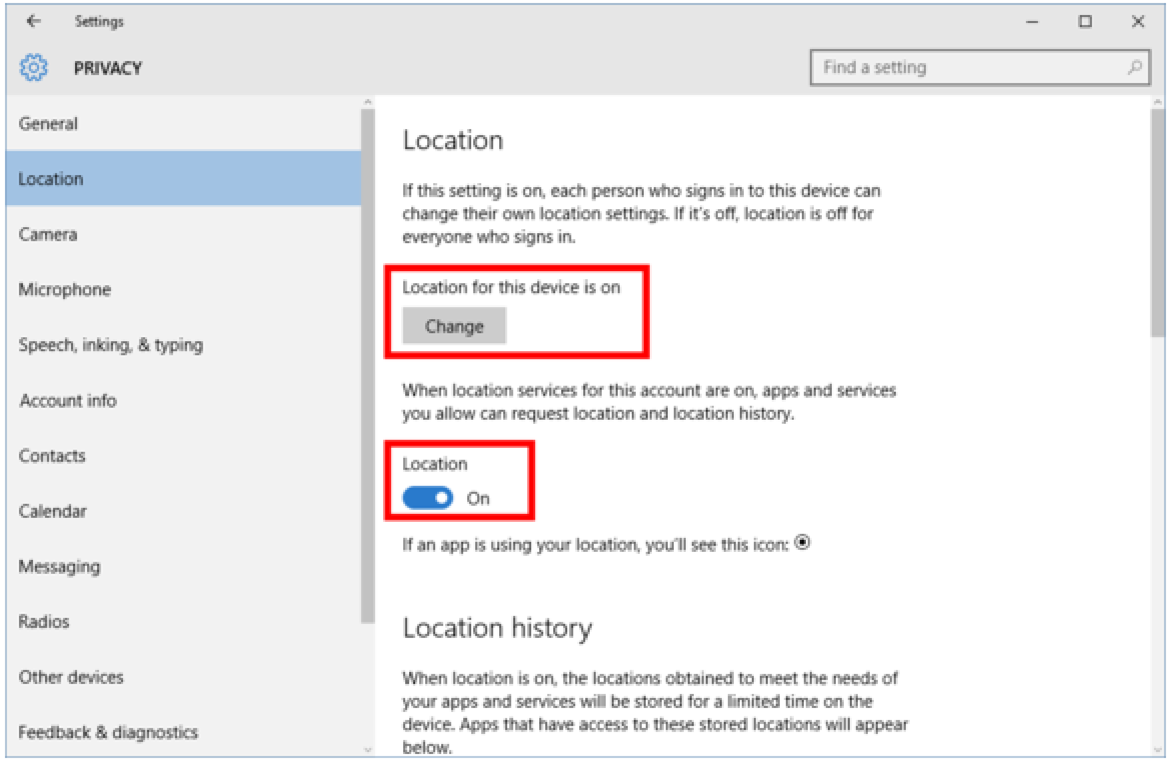
Unlink OneDrive

If you’re not interested in storing files in Microsoft’s OverDrive cloud server, you can turn it off so it stops bugging you to configure it. Click the upward-facing arrow in the system tray on the right-hand side of the taskbar. Then right-click the OneDrive icon and select *Settings.*

In the new window that opens, uncheck 'Start OneDrive automatically when I sign in to Windows.' You can also uncheck the other two boxes if they’re selected as well: 'Let me use OneDrive to fetch any of my files on this PC,' and 'Use Office to work on files with other people at the same time.’

Now it’s time to dive into all those other privacy options in the Settings app by going to *Settings > Privacy*.

This is the heart of Windows 10’s privacy controls. Under *Privacy > General*, you’ll want to turn off 'Send Microsoft info about how I write to help us improve typing and writing in the future.' You may also want to shut off 'Let websites provide locally relevant content by accessing my language list.'



Location

If this setting is on, each person who signs in to this device can change their own location settings. If it's off, location is off for everyone who signs in.

Location for this device is on

When location services for this account are on, apps and services you allow can request location and location history.

Location: On

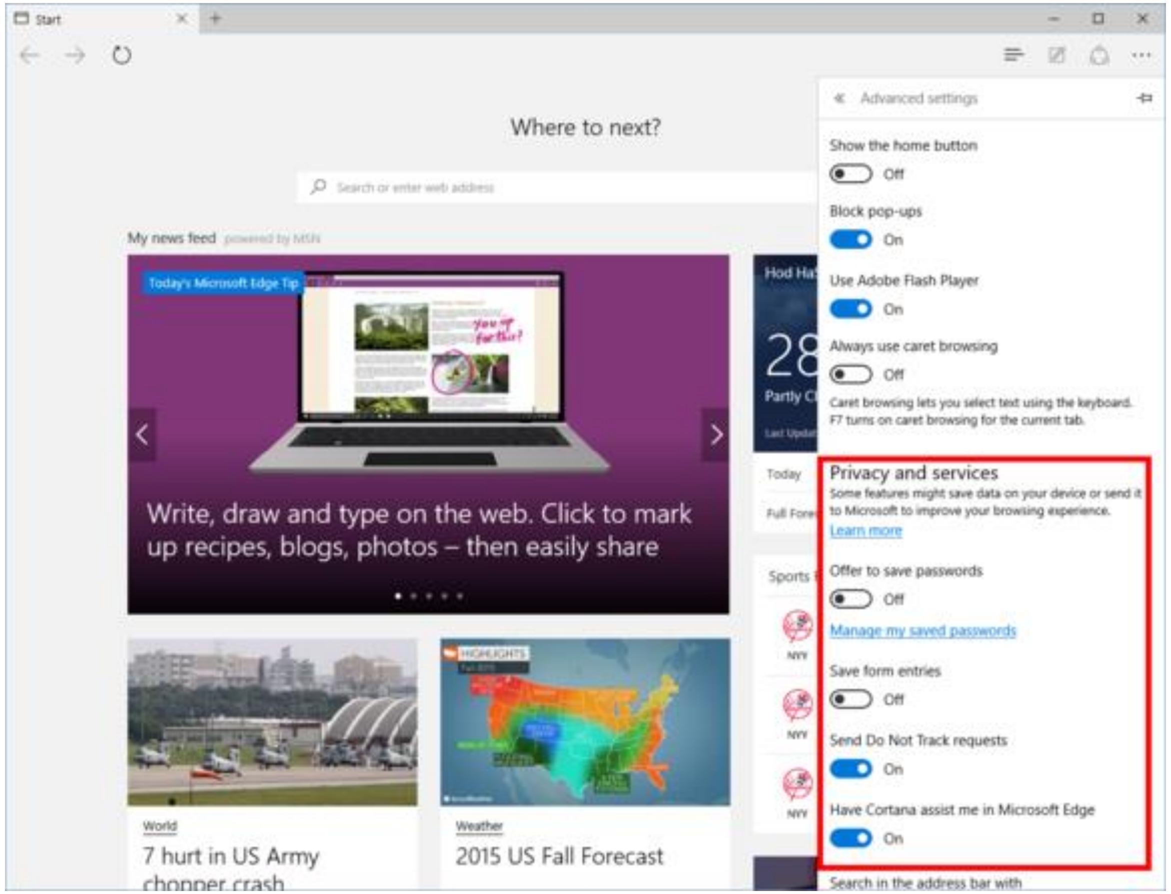
If an app is using your location, you'll see this icon: ⦿

Location history

When location is on, the locations obtained to meet the needs of your apps and services will be stored for a limited time on the device. Apps that have access to these stored locations will appear below.

The Location section lets you control whether apps can use your location to deliver services like weather forecasts or local news. Location can be set both on a per-device or per-user basis. To turn off location for the whole PC, click the *Change* button. To turn it off for only the logged-in user, turn the Location slider to *Off.* You can also control location settings on a per-app basis by scrolling down to 'Choose apps that can use your location.'

The rest of the privacy settings follow a similar format, but choose carefully so you don’t disable services you really need.


Start
Where to next?
Search or enter web address
My news feed powered by MSN
Today's Microsoft Edge Tip
Write, draw and type on the web. Click to mark up recipes, blogs, photos – then easily share
World
7 hurt in US Army chopper crash
Weather
2015 US Fall Forecast
HIGHLIGHTS
Hod Ha
28
Partly Cl
Today
Full Fore
Sports
NYY
NYY
NYY

Advanced settings

Show the home button
Off

Block pop-ups
On

Use Adobe Flash Player
On

Always use caret browsing
Off

Caret browsing lets you select text using the keyboard. F7 turns on caret browsing for the current tab.

Privacy and services

Some features might save data on your device or send it to Microsoft to improve your browsing experience.
Learn more

Offer to save passwords
Off

Manage my saved passwords

Save form entries
Off

Send Do Not Track requests
On

Have Cortana assist me in Microsoft Edge
On

Search in the address bar with

If you use Microsoft's new browser (which I don't), you may want to disable some features—like Cortana integration and typing prediction—to avoid sending data back to Microsoft.

Open Edge and click on the menu icon in the far right corner (three horizontal dots). Go to *Settings > View Advanced Settings*. Here you have the option to turn off Adobe Flash—stop those Flash cookies!—and under 'Privacy and services' you can switch off a number of other settings (next page)…