

Tech Talks

Security & Privacy

Glen Maxson

Center for Learning in Retirement

Spring 2020 – Session 5 of 6

Seniortechadvisor.com

What we'll cover in 6 weeks

- 1) ~~Computers & Operating Systems~~
- 2) ~~Applications & The Cloud~~
- 3) ~~The Internet & The Web~~
- 4) ~~Social Media~~
- 5) Security & Privacy
- 6) Entertainment & IoT

STATS ([source](#))

Record-Setting Year

1,579 breaches according to the [2017 Annual Data Breach Year-End Review](#). This correlates to a 44.7% uptick of breaches since 2016.

Depth of the Dark Web

A massive Dark Web [database of 1.4 billion email addresses, usernames and passwords](#) was discovered in 2017, the UK's Daily Express reported in December.

Cyber Crime Costs

Cyber crime is expected to cost the world [\\$6 trillion per year by 2021](#), up from \$3 trillion in 2015. To put that in perspective, profits will surpass those of the global illegal drug trade. Ransomware costs alone were predicted to [hit \\$11.5 billion by 2019](#).

What's My Information Worth?

Security expert Brian Krebs posted an article on [the market for stolen account credentials](#). The average for well-known e-commerce and banking sites is about \$15.

Cyber Security Spending

And the good guys profit from this as well. The global cyber-security industry was expected to reach [\\$93 billion for 2018](#), which accounts for all end-user spending.

AARP Resources

- AARP's weekly podcast [*The Perfect Scam*](#) profiles America's biggest scam stories. Hosted by [Julie Getz](#), and AARP Fraud Watch Network Ambassador [Frank Abagnale](#) (one of the world's most famous confidence men, inspiring the Steven Spielberg film *Catch Me if You Can*, he is now one of the world's most respected authorities on identity theft).
- Some podcast examples:
 - [Consumers Tricked into Buying Software in a Tech Support Scam](#)
 - [Debt Relief Agency Scams Homeowners](#)
 - [Grandparents Deceived by Scammers Demanding Cash](#)
 - [Widower Loses Life Savings in a Romance Scam](#)
 - [Robocalls Tricked Consumers into Buying Vacation Packages](#)
 - [Retiree Drains Her Bank Account in a Lottery Scam](#)
 - [You've Got Mail, With Frank Abagnale Part 1](#), and [Part 2](#)
 - And so much more...

'Tis the Season for

- Census Scams
- Tax Scams

The Census

- **Avoiding Fraud and Scams**

- The U.S. Census Bureau is committed to making the 2020 Census quick, easy, and safe for all participants. This [link](#) provides tips to help you stay safe.

- **Census Scams**

- April 1, 2020 is Census Day — Census scammers contact you by [phone](#), email, regular mail or home visit, or direct you to phony websites, seeking personal and financial information. Like other [government impostors](#), they adopt the mantle of officialdom in hopes of winning your trust.

- And a video (<https://www.youtube.com/watch?v=Gg202jSZgqw>)

Tax Time

- [Inside the IRS Phone Scam Bust](#)

- Every year Americans get fraudulent calls from con artists claiming to be from the IRS. We uncover how these call centers work.

- [Tax Scams/Consumer Alerts](#)

- Scammers use the regular mail, telephone, or email to set up individuals, businesses, payroll and tax professionals. The IRS **doesn't initiate** contact with taxpayers by email, text messages or social media channels to request personal or financial information. [How to know it's really the IRS calling or knocking on your door.](#)

- [3 Tax Scams to Watch Out For This Year](#)

1. Fake calls from the IRS
2. Fake tax preparers
3. Filing a fake tax return on your behalf

Scams Targeting Taxpayers

- Taxpayers should be on the lookout for new version of SSN scam
- Scams related to natural disasters
- Security Summit warns of new IRS impersonation email scam; reminds taxpayers the IRS does not send unsolicited emails
- IRS reminder: Tax scams continue year-round
- IRS warns of new phone scam using Taxpayer Advocate Service numbers
- IRS: Don't be victim to a 'ghost' tax return preparer
- IRS warns of "Tax Transcript" email scam; dangers to business networks
- IRS-Impersonation Telephone Scams

What to Do?

* Hypocrite indicator

'Computers'

- 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
- Know what you're installing and don't allow 'tailgaters'
 - [*WinPatrol*](#) 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

- 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](#)

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
- 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!
- Consider ['cloud' storage solutions](#) – in addition to backup
- Verify 'public' documents don't include 'private' info

Cloud Storage & File Sharing Services ([source](#))

Product	IDrive	SugarSync	Dropbox	Microsoft OneDrive	Box (Personal)	CertainSafe Digital Safety Deposit Box	Google Drive	SpiderOak ONE	Apple iCloud Drive
Lowest Price	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT				SEE IT
Editors' Rating	●●●●● EDITORS' CHOICE	●●●○○	●●●○○	●●●●● EDITORS' CHOICE	●●●○○	●●●●● EDITORS' CHOICE	●●●●● EDITORS' CHOICE	●●●○○	●●●○○
Emphasis	Backup	Simplicity, Ease of Use	Compatibility	Office Apps	Business Use, Compatibility	Security	Collaboration	Security	Apple Device Users
File Size Limit	2GB	Unlimited	Unlimited	15GB	5GB	100GB	5TB	Unlimited	15GB
Free Storage	5 GB	None	2GB	5GB	10GB	None	15GB	None	5GB
Online Editing	—	—	✓	✓	✓	—	✓	—	✓
File Versioning	✓	✓	✓	✓	✓	✓	✓	✓	✓
Windows App	✓	✓	✓	✓	✓	—	✓	✓	✓
iOS App	✓	✓	✓	✓	✓	—	✓	✓	✓
Android App	✓	✓	✓	✓	—	—	✓	✓	—

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

Credit & Debit Cards

- Monitor your [credit report](#) 3 times per year (for free)
- [Opt-out](#) of pre-approved credit or insurance offers*
- Use fraud alert* and [credit freeze](#) to eliminate ID theft (and how to [unfreeze](#) your credit)
 - [Best identity theft protection: top services to keep your ID safe](#)
- 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) or touch ID
- 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 every 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					✓	

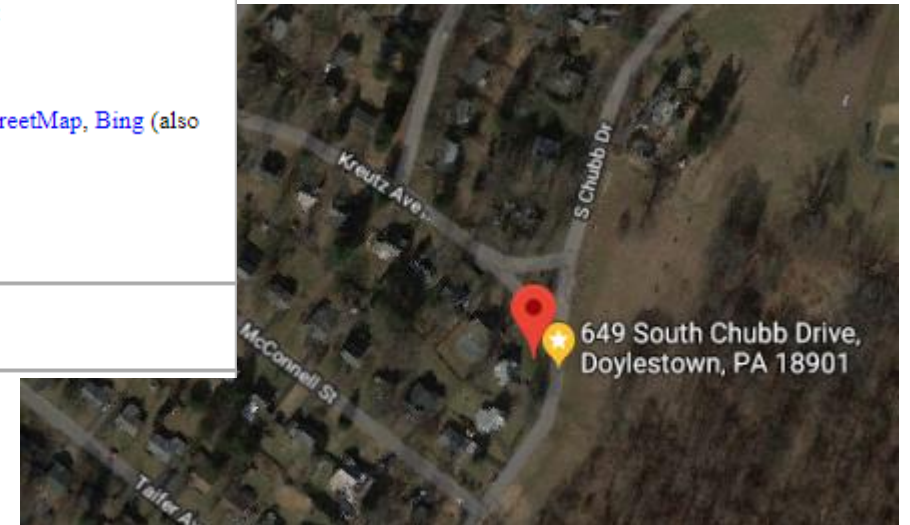
****Jeffrey's Image Metadata Viewer



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're familiar with, and trust!

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 available
- 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
 - **Never** 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)

[How to Stay Safe on Public Wi-Fi Networks](#)

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 in America](#)

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/>

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 ([demo](#))
- [**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

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



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.

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#)

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]crK [Get QR code](#)

4. Enter the Transaction ID and select amount:

[Clear](#)

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

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

[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 I: 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: Protecting Yourself 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

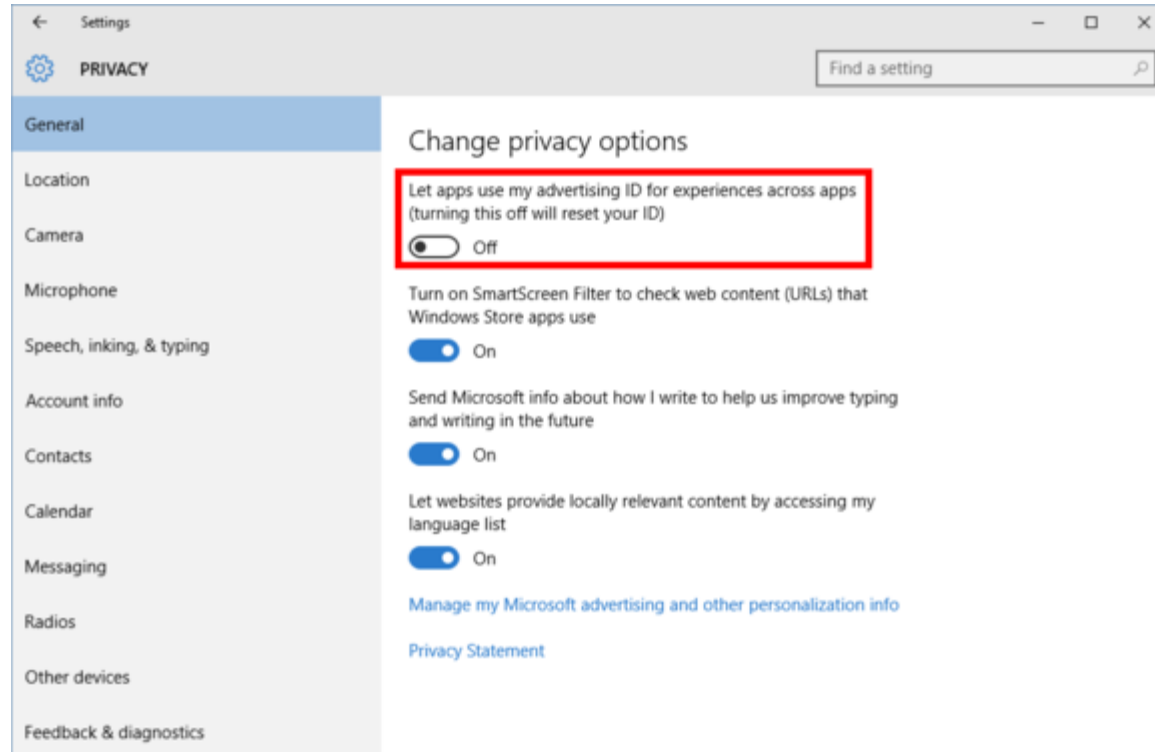
- 1. Implement a backup solution: Software based, hardware based, or both.
- 2. Ensure all possible data you need to access or save is backed up, including mobile/USB storage.
- 3. Ensure your data is safe, redundant and easily accessible once backed up.
- 4. Regularly test the recovery function of your 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.



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 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.

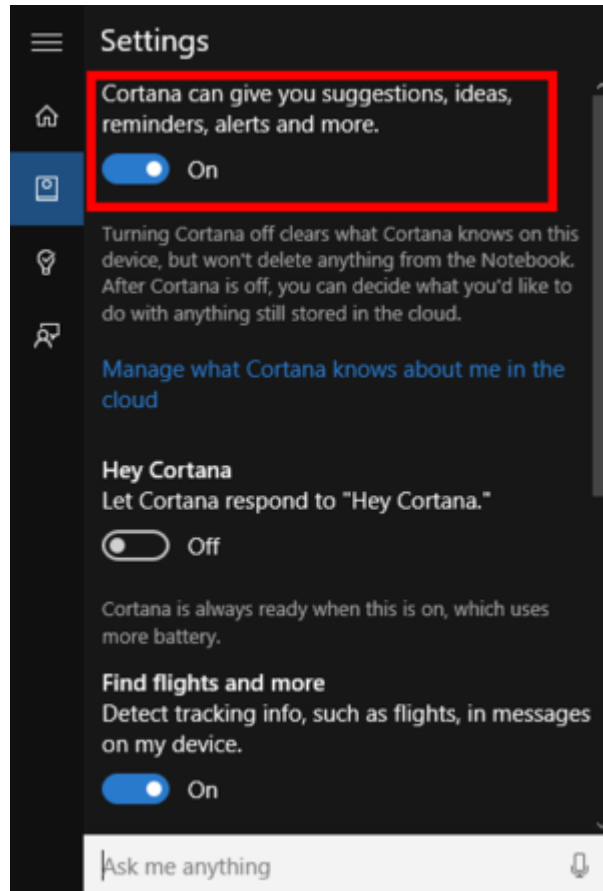
Microsoft personalized advertising in a nutshell (02:19)

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

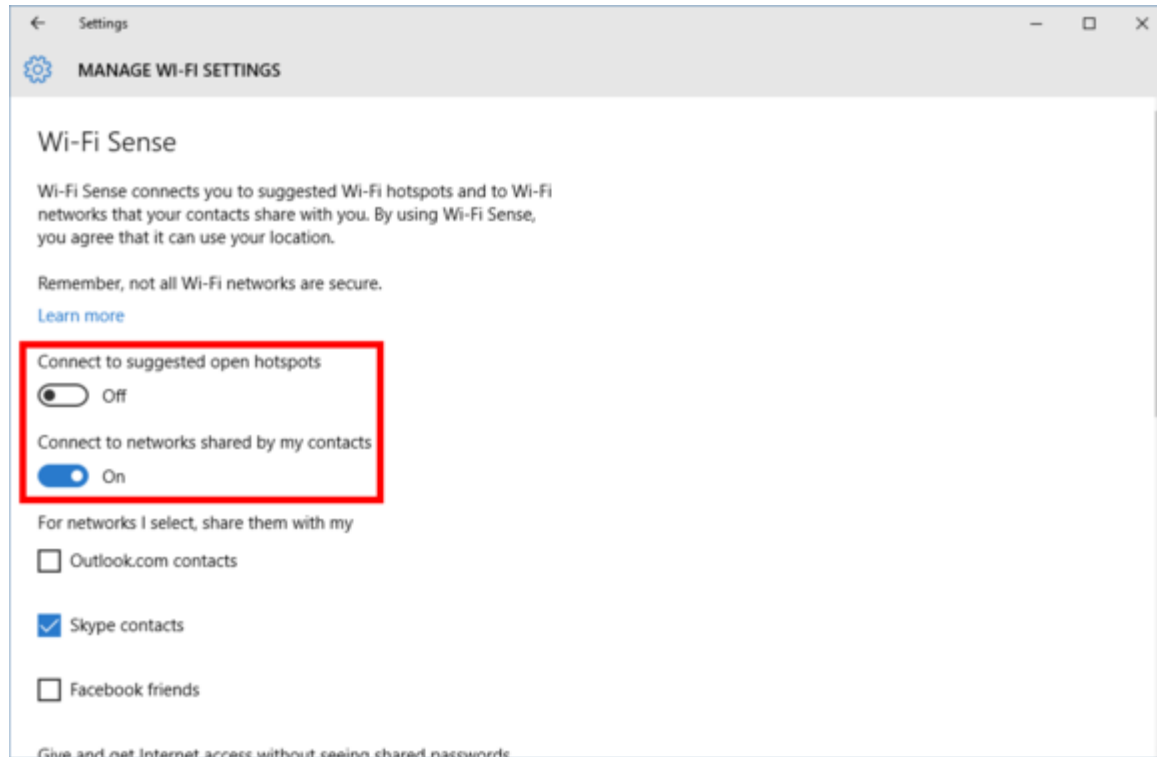


Turn Cortana *Off* - click the Cortana icon in the taskbar, and then click the notebook icon on the left-hand side of the pop-up panel. Select *Settings* then slide the top option that says 'Cortana can give you suggestions, ideas, reminders, alerts, and more' to *Off*.

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.

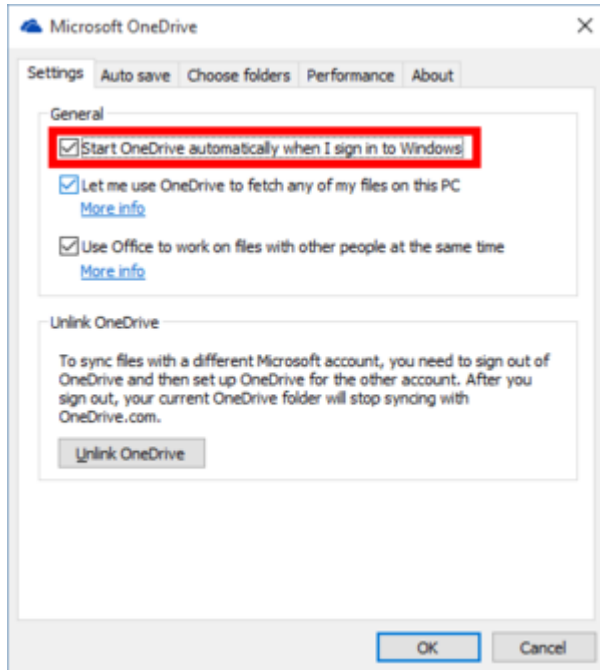
And finally, click 'Go to Bing and manage personal info for all your devices.' Here you can scrub any data that Microsoft has collected about you. Go to the bottom of the page and click *Clear*.



[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.'

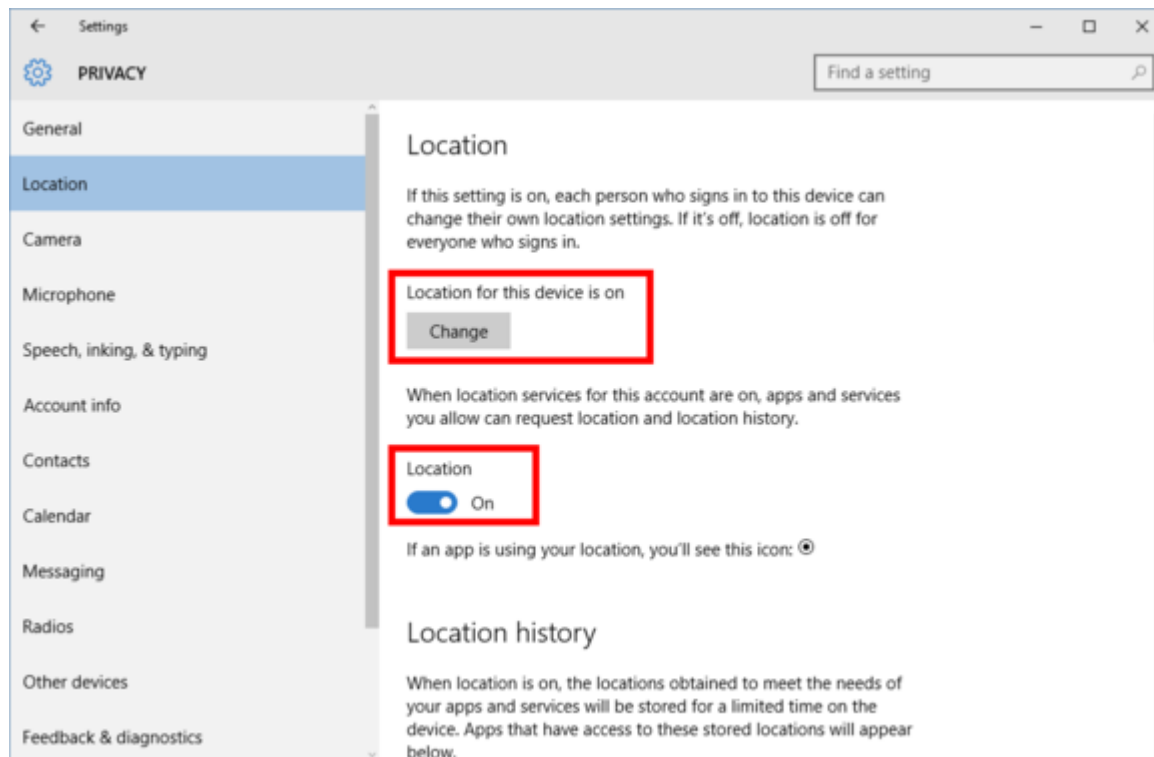


If you're not interested in storing files in Microsoft's OverDrive cloud server, you can turn it off so it stops bugging you to configure it. Click the upward-facing arrow in the system tray on the right-hand side of the taskbar. Then right-click the OneDrive icon and select *Settings*.

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.'

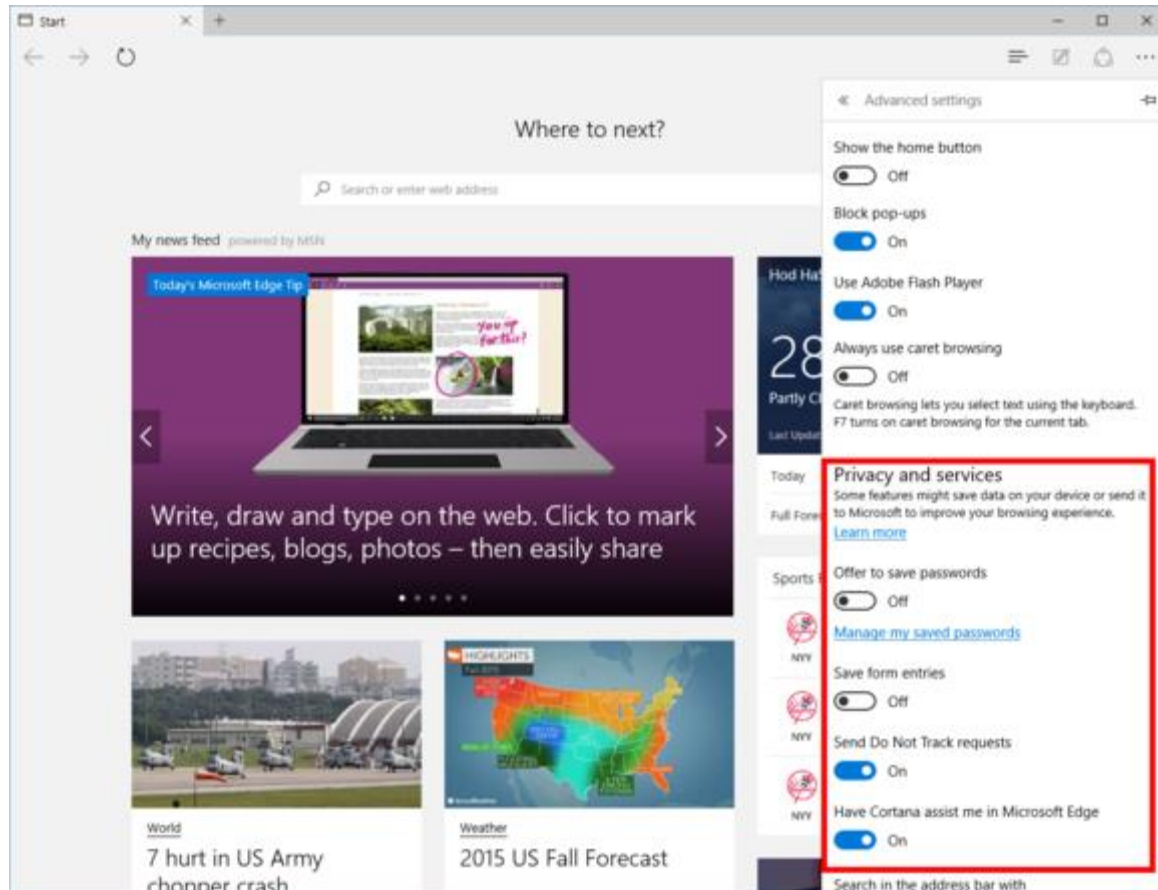
Now it's time to dive into all those other privacy options in the Settings app by going to *Settings > Privacy*.

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.'



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.



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)...