

# Protecting your 📱 smartphones, 📺 tablets and 💻 computers from Spam and Malware, via Antivirus and other methods and 🔧 tools



Copyright © 2014-2023 by [Eric D. Piehl](#). This work is made available under terms of the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License <http://creativecommons.org/licenses/by-nc-sa/3.0/>."

While helping 🧑 family, friends and 🧑 colleagues on various projects, we have learned some things. In an attempt to keep these processes repeatable, *and keep myself organized*, I 📝 record and maintain some helps on this subject. Based on ideas from my own knowledge, [Network World](#) and [Kim Komando](#). I sent out precursors of this document to relatives four times in 2013 and early 2014. For date this file last updated, please see page footer. For information on 🌲 green or other </> programming subjects, please see a list of [this document's sister docs](#).

## Contents

Protecting your 📱 smartphones, 📺 tablets and 💻 computers from Spam and Malware, via Antivirus and other methods and 🔧 tools.....	1
1 Introduction .....	2
2 One-time: Shopping for your 📱 📺 communications platforms .....	3
2.1 One-time: Shopping for your 📱 smartphone.....	3
2.2 One-time: Shopping for your 💻 computer .....	3
3 One-time: Harden your 📱 📺 communications platforms.....	4
3.1 One-time: Harden your 📱 📞 phone life.....	4
3.2 One-time: Harden your iPhone 📱 smartphone or iPad 📺 tablet .....	5
3.3 One-time: Harden your Android 📱 smartphone, 📺 tablet or 💻 Chromebook.....	7
3.4 One-time: Harden your 💻 computer.....	13
3.5 One-time: Make your flash-drive/jumpdrive/thumbdrive/USB-drive/ USB-key/USB-stick more-usable .	20
3.6 One-time: Harden your web presence.....	21
3.7 One-time: Harden your voice-activated virtual assistants/voice butlers/smart speakers, TVs and toys!	22
3.8 One-time: Harden your Wi-Fi router, cable modem, and doorbell camera .....	23
3.9 One-time: Retiring/Donating/Disposing of a 📱 📺 computing device.....	24
4 Demonstrating protesting traveling in 🏠 heavily-policed authoritarian areas, or when targeted by adversaries	25
5 Emergency situations: 📺 search and rescue SAR, earthquake, flood, 🌪️ tornado, 🌀 hurricane .....	26
6 Emergency: Find or clean your 📱 📺 computing platforms.....	28
6.1 Emergency: Find or clean your iPhone 📱 smartphone or iPad 📺 tablet.....	28
6.2 Emergency: Find or clean Android smartphone or tablet, or Chromebook .....	29
6.3 Emergency: Find or clean your 💻 computer.....	31
6.3.1 Emergency: Fix up 📱's 💻 computer.....	36
6.4 Emergency: Change your 📧 email and other passwords.....	36
6.5 Emergency: Harden your Wi-Fi router, cable modem, and doorbellcam .....	37
7 Monthly/Quarterly: Harden your 📱 📺 computing platforms .....	39
7.1 Monthly: Harden your iPhone 📱 smartphone or iPad 📺 tablet.....	39
7.2 Monthly: Harden your Android 📱 smartphone, 📺 tablet or 💻 Chromebook.....	39
7.3 Monthly: Harden your 💻 computer .....	41
7.3.1 First steps.....	41
7.3.2 Backup your 💻 computer.....	42
7.3.3 More steps .....	44
7.4 Quarterly: Harden your 💻 computer.....	45
7.5 Quarterly: Harden your web presence.....	50
7.6 Quarterly: Correct your 📊 credit reports .....	51

7.7	Quarterly: Harden your Wi-Fi router, cable modem, and doorbell camera .....	51
7.8	Semiannually: Harden your ☎ phone life .....	51

**TODO:** Finish sections on configuring and updating your **Wi-Fi router, cable modem, doorbell camera, nannycam, or Tile or 🍏 Apple AirTag tracker device.**

**TODO:** For **Android** security, be sure to recommend apps [Whispercore](#) or [Lookout Mobile](#); and see [www.networkworld.com/news/2012/051412-android-259182.html](http://www.networkworld.com/news/2012/051412-android-259182.html).

**TODO:** Add steps from [www.windowsssecrets.com/top-story/start-the-new-year-with-a-clean-windows-pc](http://www.windowsssecrets.com/top-story/start-the-new-year-with-a-clean-windows-pc).

**TODO:** Add other cleanup steps, including Registry cleanup, from my other (but now very stale) *RunSafe stuff*.

**TODO:** Add [Blue Cyber Education Series for Small Businesses](#). And [SBA strengthenyour-cybersecurity](#).

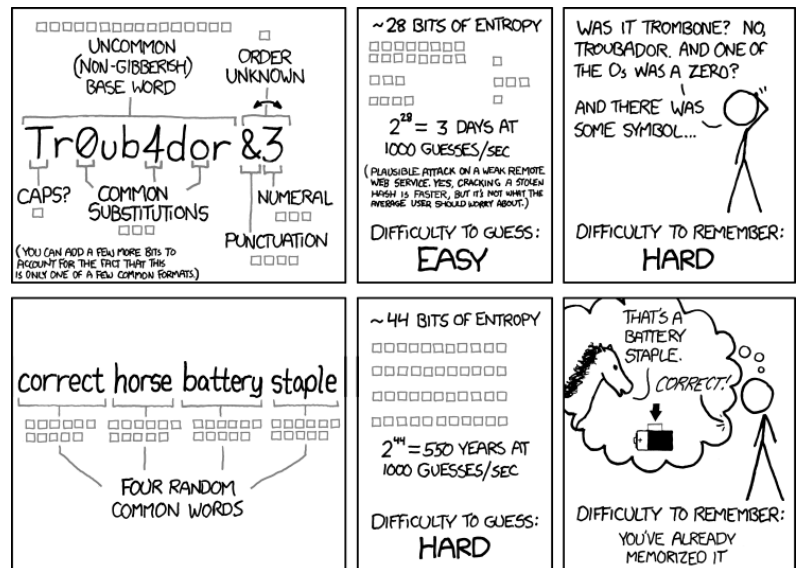
## 1 Introduction

*Like nuclear radiation, cyberwar doesn't make you bleed, but it destroys everything.*

*If you are not **paying** for the product, you **are** the product.* — R. David Edelman, as heard by EP on 2018-01-19.

Throughout your ☎ ☎ computer use, I ask you to use:

- ☐ Brian Krebs' [Three Rules for Staying Safe Online](#):
  - **If you didn't go looking for it, don't Install it!** This means, among other things:
    - **Don't let anything install** while you are just browsing the web or answering ☎ email.
    - If you see a **popup** Window you didn't expect, **Close** it with the **red X** in the corner (or **Alt+F4**), **not** any of its **Yes** or **No** or other buttons. The exceptions are **Flash** and **Java**, covered in a sec...
    - If you want it, go **Search** for it, at known good source, e.g., Search engine [DuckDuckGo](#). For example:
      - For **Flash**, see [below](#).
      - For **Java**, see [below](#).
    - If you are installing something, **uncheck** any checkboxes or radio buttons for offerings you don't need.
  - **If you Installed it, Update it.** Covered [below](#).
  - **If you no longer need it, Remove it.** Covered [below](#).
- ☐ **Strong, unique passwords, on every computer account:**
  - Yes, **unique**, i.e., **not shared** with other accounts. Sorry about that. Yes, you will have to maintain a **list**. There are electronic ways of doing this, e.g., LastPass, LogMeIn, Dashlane and KeePass. I don't, but keep mine in only three places, under my physical control. For details, call me.
  - OK, *if you can't handle unique passwords for every account:*
    - **reuse** passwords only for unimportant accounts (library, etc.),
    - use **unique** strong passwords for your ☎ email provider, bank, 401(k), IRA, etc.
  - Yes, passwords **strong** enough not to be guessed by *dictionary attacks*:
    - Hard to guess--not your mother's maiden name, SSN nor anything else that can be **looked up**.
    - **Longer is better.** [FBI recommends](#) [passphrases over password complexity](#). Pros are going to 64 characters, not 8. Even 12 or 16 ([FBI](#) and [NIST](#) recommend at least 15) letters is **stronger** (and easier to type) than 8-character combinations of lowercase, uppercase, numbers and symbols.
    - Increasingly popular are strings of [three unrelated words](#), such as [untidygreenideas](#) or [brilliancebronzeinputs](#).
    - Or perhaps in [camelCase](#), with numbers or symbols thrown in, like [94greenIdeas](#).
    - [Kim Komando's suggestions](#). [Nice password-checker](#). Google's [suggestions](#) and [Account Checkup](#) and [Security Checkup](#).



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

If you have a **new** ☎ smartphone, ☎ tablet, or

☎ computer, as soon as practical, please do the

[one-time harden your computing platforms](#) steps below. By "harden", I mean the process of securing a system, by reducing its *surface of vulnerability* (its *attack surface*), and making it more *resilient* to attack.

☒ If you have not yet upgraded your **Microsoft Windows 8.1** or **Windows 7** device to 🐧 **Linux** or **Windows 10** for free, please see my full instructions for 📱 [smartphone](#) or 📺 [tablet](#) or 💻 [computer](#).

☒ **Windows 11** is available, but I have not yet investigated. [App will tell you why you can't run Windows 11.](#)

Every **month** or so, please do the [monthly](#) steps below. Thank you for running a tight ship!

If **I** received **spam** that appears to be **from your** ✉ email address, I will ask you to do **all** the [emergency procedures](#) below. **Thank you!**

If **you** received **spam** that appears to be **from my** ✉ email address, I will clean my machine right away using the [emergency procedures](#) below. But to help me understand, and or find out if I am being spoofed, please tell me:

- Your spam appears to be from **which** of my email addresses?
- *Optional:* Can you send me the "**Internet Headers**" — a bunch of codes and stuff associated with the email — that doesn't come along if you Forward or Reply?

If you use 🍏 **Apple's email client** or Comcast Xfinity or Microsoft Outlook to do your email:

- Bring up the **offending email**.
- Get an email ready to go to me, perhaps by **Forwarding** the above. In the offending email:
  - If for email, you use 🍏 **Apple's email client**, do a **View** > **Message** > **Raw Source** > collect that stuff.
  - If for email, you use ✉ **Comcast Xfinity email client**, select the ☰ *hamburger* icon in upper-right corner > **View source** > collect that stuff.
  - If for email, you use ✉ **Microsoft Outlook**, do a **File** > **Properties** > bottom half under "**Internet Headers**" > click in it somewhere > **Ctrl-A** (Select All) **Ctrl-C** (Copy) > **Close**.
- Swap over to the email to me, and **Paste** it in somewhere. **Send** it to me!
  - I will probably analyze it as in <https://lifewire.com/how-to-find-email-server-ip-address-818402>.
- **Phone me** that you are sending it, so when I don't see it, I will check my two spamfilters. **Thank you!**
  - *Note for me:* If needed, analyze it after reviewing [How to Find An IP Address of An Email Sender](#).

## 2 One-time: Shopping for your 📱 📺 💻 communications platforms

### 2.1 One-time: Shopping for your 📱 *smartphone*

- See my recommendations on [very-low-cost mobile cellphone service](#).
- See recommendations of magazine *Consumers Reports* (free at your local library).
- After you buy your phone, [harden it as below](#). By "harden", I mean the process of securing a system, by reducing its *surface of vulnerability* (its *attack surface*), and making it more *resilient* to attack.
- After your new device is up and running well, [retire/donate/dispose of your old device as below](#).

### 2.2 One-time: Shopping for your 💻 *computer*

- List the **tasks** you intend to do on your 💻 computer (e.g., email, browse Internet, write documents/spreadsheets/presentations, do finances, family history/genealogy, write and build software).
- To that list, add a column for **apps/installed software** you need to run to **accomplish those tasks** (e.g., MS Office with Outlook, Quicken, Family Tree Maker, Beyond Compare and Eclipse).
- To that list, add a column for which **operating system** those apps/installed software need to run (e.g., 🍏 Apple macOS, 🐧 Linux, ☒ Microsoft Windows, and Chrome).
- If all your apps/installed software runs on one particular OS, put that OS on your list, along with probable:
  - size of harddrive,
  - amount of main memory,
  - form-factor you would like (e.g., full-sized desktop vs compact desktop vs all-in-one vs laptop vs 📺 tablet or 🖥 Surface),
  - display (e.g., 1366x768 vs **Full HD 1080p (1920x1080** at **16:9**), and
  - connectors.
- See recommendations of magazine *Consumers Reports* (free at your local library).
- After you buy it, [harden it as below](#). By "harden", I mean the process of securing a system, by reducing its *surface of vulnerability* (its *attack surface*), and making it more *resilient* to attack.
- After your new device is up and running well, [retire/donate/dispose of your old device as below](#).

### 3 One-time: Harden your 📠 📞 communications platforms

By "**harden**", I mean the process of securing a system, by reducing its *surface of vulnerability* (its *attack surface*), and making it more *resilient* to attack.

I used to have a good introduction here, but it has disappeared. Will try to find another one.

Until then, please follow the below ...

#### 3.1 One-time: Harden your 📞 📠 phone life

- ❑ Be aware of the [grandma scam](#).
  - Be ready with a test for **any caller claiming to represent a relative with an urgent need for money**., such as being arrested.
  - **Demand** to speak to your relative yourself. If they push back, it's a scam — hang up.
  - If it **sounds a bit like your relative**, ask them about something that cannot possibly be on social media, such as what they were sick with on their 8<sup>th</sup> birthday, or where they were when they stung by a bee. Any evasion means it's a scam — hang up.
  - Or just hang up, and call **your relative yourself** at the number you know is good. Probably about time you had a chat anyway.
- ❑ Be aware that the **IRS** does **NOT call you** when you owe them money or are being audited. I was able to ignore a series of 3 calls like this, because I knew that, under this condition, the IRS **sends you a letter**, and **never** calls.
- ❑ Likewise, ignore calls from car warrantee extensions.
- ❑ I consider all these attacks as variations on [spear-phishing](#).
- ❑ In fact, never answer the phone at all, unless your phone tells you someone in your Contacts list, such a "daughter Wilma cell", or "Dr Flintstone's office". If you have voicemail set up, they can leave you a message.
- ❑ *If you receive anything like the above:*
  - do **not** answer the 📞 📠 phone, but instead ...
  - **record** the phone number from your callerID;
  - **type it in** to:
    - your favorite Search Engine (such as [DuckDuckGo](#)), in format [AAA-EEE-NNNN](#) (e.g., <https://duckduckgo.com/?q=123-456-7890> or <https://google.com/search?q=123-456-7890>), or
    - <https://www.spokeo.com/reverse-phone-lookup>, or
    - <https://www.whitepages.com> > reverse phone, or
    - [www.whocallsme.com/Phone-Number.aspx/aaaaeenennn](http://www.whocallsme.com/Phone-Number.aspx/aaaaeenennn); and
  - analyze. Good luck!
- ❑ *If you get junk **robocalls** on your 📞 landline:*
  - Set up call-blocking call-blocker app [Nomorobo](#) (awesome!), free on most VoIP landlines (a landline provided digitally — perhaps from your cable TV provider).
  - Or, I hear, apps [Truecaller](#) or [RoboKiller](#).
  - [Other options](#)
- ❑ *If you get junk **robocalls** on your 📞 smartphone:*
  - Block all suspected spam calls, or send them directly to voicemail:
    - *If through Republic Wireless*, see [How to Block Robocalls/Spam Calls & Voicemails Using the Republic Wireless App](#).
    - *If through any other mobile company*, look into call-blocking call-blocker app [Hiya](#) or [others](#), or pay for [Nomorobo](#). Or perhaps, apps [Truecaller](#) or [RoboKiller](#), or [other choices](#).
  - *If using an Android, version 7.0 Nougat or above* (likely if your phone is from 2016 or later), block **individual numbers** via [How to Block Calls/Numbers on Phones with Android Nougat 7.0 or Higher](#).
- ❑ Sign up for [Smart911](#).

When you **get a new** 📠 📞 **electronic communications or computing device**, or when you first think about it, please do the following . . .

### 3.2 One-time: Harden your iPhone 📱 smartphone or iPad 📱 tablet

- ["Do These 12 Things First When You Get a New iPhone"](#) or iPad.
  - Activate your new 📱 smartphone or 📱 tablet in accordance with the instructions that came with it.
  - Set all relevant **ease-of-use settings**, including [gear] **Settings > Accessibility**:
    - > **Font size = Large** or whatever you need.
    - > **Display size = Large** or whatever you need.
    - > **Magnification** or **Color correction** or **Hearing aids** if you need those.
  - Set all relevant **emergency settings**, including [gear] **Settings**:
    - > **Display > Lock screen** > Notifications on lock screen = Show sensitive content only when unlocked.
    - > **Display > Lock screen > Add text on lock screen** = "Pls rtn to myName myPhone\*\*\*. Thank you!", where \*\*\* = your 📞 landline or sweetie's phone number, in form +1-aaa-eee-nnnn.
    - > **Security > Security update** if needed.
    - > **Security > Find My Device** = On.
    - > **Security > Screen Lock**.
    - > **Security > Pixel Imprint** > set up 2 fingerprints.
    - > **Security > Device admin apps** > allow **Lookout**, and **Find My Device**.
    - > **Security > Advanced > System update** > install any updates.
  - Set all relevant app marketplace **Google Play > ⋮ > [gear] Settings**:
    - > **App download preference = Over Wi-Fi only**.
    - > **Auto-update apps = Over Wi-Fi only**.
    - > **Auto-play videos = Auto-play videos over Wi-Fi only**.
    - > **App download = Over Wi-Fi only**.
  - If you have an **iPhone** 📱 smartphone or **iPad** 📱 tablet that does not yet have **antimalware** software, please install one of:
    - **Lookout** or
    - **Malwarebytes** (free is a terrific on-demand scan, but the prevention module costs \$),
    - [from somewhere other than China](#), Russia and associated countries.
  - I am familiar with **Lookout**; to install it:
    - launch app **App Store** >
    - 🔍 **Search** for "**Lookout**" >
    - select iPhone/iPad app "**Lookout - Backup, Security, Find Your iPhone, iPad or iPod touch**" "**Free**" from **Lookout Mobile Security** with icon of a **white-on-green shield** >
    - click button **Free** >
    - install free version.
    - Launch.
    - Sign in – with an email address and password.
    - **≡ Settings > Theft Protection** > top tab **Locate My Device**
      - > turn on **Location** (helped me greatly, at least once!),
      - > turn on **Scream** (helped me **immensely**, and M!);
      - and anything else you can.
- Consider **≡ Settings > Backup**.

**Lookout** will protect your device from **new threats**.

**Lookout** will periodically run scans to remove **existing threats**. Lately, once a day. If you wish to run another scan right now, launch app **Lookout** > tab **Security** > button **Scan Now**.

**Lookout** has a nice feature ("**Signal Flare**", I think) where, if your Android or iPad finds itself running out of battery, it finds out where it is and 📧 emails you its location (granular enough to see which building it is in, not where in that building). Cool!

**Lookout** tells you if there is a **software update** to your iPad, and if needed, how to get that update (connect iPad to Mac or PC > if iTunes does not auto-launch, launch it > when prompted to update the iPad software, click "[Download and Update](#)").

**Lookout** will automatically backup your **Contacts list** to the Cloud, from where you can download it at any time.

**Lookout Pro** will automatically backup your **photos** (¿videos?) to the Cloud, from where you can download it at any time. *If you take photos (¿videos?) at risk if your phone should get lost or confiscated by the authorities*, check out whether backups happen automatically, how often it happens, and if it includes videos, and if OK, **upgrade** to Lookout Pro for \$30/year and turn on photo backup.

**Lookout** will (I imagine) occasionally ask you to **update** itself. Please tell it Yes.










- Ensure you have all your **old apps**, and they are **hooked up** and operating correctly. For example:
  - **Lookout** (above).
  - **Phone** and **Messaging**, including **Contacts**.
  - **Maps**.
  - Weather.
  - News.
  - Email..
  - Calendar
  - iCloud, including re-setting your Offline files.
  - Costco Pharmacy.
  - Tasks.
  - **Dropbox**, including re-setting your Offline files.
  - **Photos**.
  - ACLU [Mobile Justice app for your jurisdiction](#).
  - Local sheriff or police app, including signing up for local Groups relevant to you.
  - iNaturalist.
  - Wi-Fi Analyzer.
- Set all relevant **emergency settings** that didn't get done above, including:
  - [gear] **Settings > Security > Device admin apps** > allow **Lookout, Find My Device** and **ACLU Enable Lock Screen on Trigger**.
- Set all relevant **ease-of-use settings** that didn't get done above, including:
  - setting **volume-levels** and **ringtones** that you can actually hear. [How?](#)
- If needed, rebuild your **home screen**, by adding icons for:
  - Contact of your sweetie.
  - Your favorite [software for digital video virtual web-based meetings, conferences, gatherings or webinars](#).
  - YouTube.
  - Clock.
  - Your favorite websites (e.g., [ericpiehl.com](#) and [iCanSeeNature.com](#)).
- To help if your **iPhone** ☞ smartphone or **iPad** ☞ tablet is **lost** or **stolen**, please see "[Find My iPhone, iPad, iPod touch, or Mac](#)". Depending on details, you can ring it to locate its exact location, lock it or erase its data.
- Semi-permanently **mark** your ☞ smartphone or ☞ tablet with your **contact info**. Perhaps by:
  - **Write** your contact info on your device, with a Sharpie or other permanent marker.
  - **Tape** a business card to it, with tape coverage > 100%.
  - Make a business-card-like **label** yourself.
  - If above includes a ☞ 📞 phone number, verify that the above includes a phone number **other than** that of your device itself.
  - Do this in a way involving **bright colors**, to make it easier to **find in the couch**, or **see as it arcs into the trash**.
  - Consider making a second tag, hiding it somewhere within the device.
- Personalize your ☞ **smartphone** or ☞ **tablet name** by [renaming](#) it from its default to:
  - **your name** and **the year you bought it**, in [UpperCamelCase](#) format **FirstLast\_YYYY**, or



- permanently-available ☎ phone number, in format [AAA-XXX-NNNN](#).
- Please see 🍏 [Apple Device and Data Access when Personal Safety is at Risk](#) for 🍏 **Apple iPhone** ☎ **smartphones**; iPad ☎ **tablets**; Macintosh, iMac, iBook, and MacBook ☎ computers; and probably HomePod devices.
- If you need **physical protection** (I do!), get some **armor** (I do!):
  - I have seen an iPad with totally-awesome **armor**, which the owner identified as "Griffin Survivor". I believe he said it even had an optional cover for the Home button. Looks perfect for parents of even the most active or strong-willed kids. I found this at [www.griffintechology.com/survivor](http://www.griffintechology.com/survivor). They have other products, such as the Survivor Slim at [www.griffintechology.com](http://www.griffintechology.com) > *yourPlatform*.
  - I have seen a ☎ cellphone with a [Trident case](#). Seemed quite good. I didn't get that, but I really like [mine](#).
  - Order it in a **bright color**, to make it easier to **find in the couch**, or **see as it arcs into the trash**. [I did](#).
- Order ☎ ☎ smartphone/tablet **charger cables** for your car, briefcase, and travel bag.
  - And maybe an emergency battery-charger.
- [Consider charging via a surge suppressor](#) (I don't).
- If you do **not** use your ☎ ☎ smartphone/tablet's camera all the time, **put a piece of tape over the camera**. Cellophane tape is OK--it blurs stuff very well. Or use opaque electrical tape. If you are worried about adhesive preventing future use of the camera, put a little square of paper in the center of the tape, where the camera port will be.
- Examine [gear] **Settings** > **Privacy** > **Location Services**, and all other settings.
- If you aren't going to use **Bluetooth** on your device, turn it off. Same with Wi-Fi.
- [Disable ad id tracking, and why you should do it now](#).
- [Clear your browser's cache](#).
  - If you have browser Chrome, follow the few steps in <https://support.google.com/chrome/answer/2765944> > tab **iPhone & iPad**.
- If you commonly attach to **public Wi-Fi access points** (no password needed) in public spaces such as airports, hotels, libraries and Starbucks, consider installing a **VPN** (Why? [What does a VPN hide?](#)), such as [TunnelBear](#) or Avira Phantom VPN or [others](#).
  - As of 2018-03-29, there is 77% off a three-year subscription for up 6 devices (any combination of ☎ ☎ Android; 🍏 Apple ☎ iOS, ☎ iPadOS and ☎ macOS; and ☎☎ Microsoft Windows) at <https://nordvpn.com/Isaac>. As of 2019-05-20, there is 75% off a three-year subscription at <https://nordvpn.com/pilot>, and 1 month free with discount="pilot".
  - **NEW** As of 2022-07-10, Perun recommends [Private Internet Access](#), including a discount at <https://privateinternetaccess.com/Perun>. Four days later, [Artur Rehi](#), also.
  - Supertechies can use [WireGuard](#).
  - Or when I am going to be set up for more than a couple hours or days, I use a small router/Wi-Fi-repeater/-extender; at least I get started off encrypted (**TODO: Investigate this more**). And then my family's ☎ smartphones, ☎ tablets and ☎ computers all attach automatically.
- To help you **fall asleep**, consider turning on ☎ Microsoft Windows **night light** (search for it in [gear] Settings), or installing an app to not display blue light near bedtime. For a while on another platform, I used **f.lux** to good effect.


### 3.3 One-time: Harden your Android ☎ smartphone, ☎ tablet or ☎Chromebook

- If you [got a new ☎ smartphone from Republic Wireless](#):
  - Do what it says in the green booklet. Basically normal stuff, plus:
    - Connect to Wi-Fi.
    - Install app Republic Wireless.
    - Give it your Republic Wireless credentials.

- Activate your new  smartphone or  tablet in accordance with the instructions that came with it.
- **NEW** If in Android 10+, you want to see the **three navigation buttons Back, Home and Overview** at the bottom of the screen, like you did in previous versions of Android:
  - [gear] **Settings** > **System** > **Gestures** > **System Navigation** = **3-button navigation**, as in [show the 3 navigation buttons](#).
  - [The gesture method is superior, with a learning curve of 1-3 days](#).
- Set all relevant **ease-of-use settings**, including [gear] **Settings** > **Accessibility**:
  - > **Font size** = **Large** or whatever you need.
  - > **Display size** = **Large** or whatever you need.
  - > **Magnification** or **Color correction** or **Hearing aids** if you need those.
- Set all relevant **emergency settings**, including [gear] **Settings**:
  - > **Display** > **Lock screen** > Notifications on lock screen = Show sensitive content only when unlocked.
  - > **Display** > **Lock screen** > **Add text on lock screen** = "**Pls rtn to myName myPhone\*\*\*. Thank you!**", where **\*\*\*** = your  landline or sweetie's phone number, in form **+1-aaa-eee-nnnn**.
  - > **Security** > **Security update** if needed.
  - > **Security** > **Find My Device** = **On**.
  - > **Security** > **Screen Lock**.
  - > **Security** > **Pixel Imprint** > set up 2 fingerprints.
  - > **Security** > **Device admin apps** > allow **Lookout** and **Find My Device**.
  - > **Security** > **Advanced** > **System update** > install any updates.
- Set all relevant app marketplace **Google Play** >  > [gear] **Settings**:
  - > **App download preference** = **Over Wi-Fi only**.
  - > **Auto-update apps** = **Over Wi-Fi only**.
  - > **Auto-play videos** = **Auto-play videos over Wi-Fi only**.
  - > **App download** = **Over Wi-Fi only**.
- If you have an **Android**  smartphone or  tablet, or  Chromium OS **Chromebook** device, that does not yet have **antimalware** software, please install one of:
  - [Lookout](#),
  - [Malwarebytes](#) (free is a terrific on-demand scan, but the prevention module costs \$),
  - [Sophos Mobile Security for Android](#) or
  - [other options](#);
  - [from somewhere other than China](#), Russia and associated countries.
- I am familiar with **Lookout**. To install it:
  - launch app **Play Store** (icon may be on its own, may be in folder Google) >
  - **Q Search** for "**Lookout**" >
  - select Android app "**Lookout Security and Antivirus**" from **Lookout Mobile Security** with icon of a **white-on-green shield** >
  - click button **Free** >
  - install free version.
  - Launch.
  - Sign in – with an email address and password.
  -  **Settings** > **Theft Protection** > top tab **Locate My Device**
    - > turn on **Location** (helped me greatly, at least once!),
    - > turn on **Scream** (helped me **immensely**, and M!);
    - and anything else you can.
  - Consider  **Settings** > **Backup**.

**Lookout** will protect your device from **new threats**.

**Lookout** will periodically run scans to remove **existing threats**. Lately, once a day. If you wish to run another scan right now, launch app **Lookout** > tab **Security** > button **Scan Now**.

**Lookout** has a nice feature "**Scream**" that makes it make a loud noise. I used it once when my granddaughter dumped my  phone into a toybox while I was distracted for a second. A lifesaver! It also has a nice feature ("**Signal Flare**", I think) where, if your Android or iPad finds itself running out of battery, it finds



out where it is and 📧 emails you its location (granular enough to see which building it is in, not where in that building). Cool!

**Lookout** will automatically backup your **Contacts list** to the Cloud, from where you can download it at any time.

**Lookout Pro** will automatically backup your **photos** (¿videos?) to the Cloud, from where you can download it at any time. *If you take photos (¿videos?) at risk if your 📱 phone should get lost or confiscated by the authorities*, check out whether backups happen automatically, how often it happens, and if it includes videos, and if OK, **upgrade** to Lookout Pro for \$30/year and turn on photo backup.

**Lookout** will occasionally ask you to **update** itself. Lately, twice a year or so. Please tell it Yes.








- Ensure you have all your **old apps**, and they are **hooked up** and operating correctly. For example:
  - **Lookout** (above).
  - **Phone** and **Messaging**, including **Contacts**.
  - **Maps**.
  - Weather.
  - News.
  - Email (Gmail).
  - Calendar
  - Google Drive, including re-setting your Offline files.
  - Costco Pharmacy.
  - **Tasks**.
  - **Google Lens** (using your camera to find products, translate words, identify plants).
  - **Dropbox**, including re-setting your Offline files.
  - **Photos**.
  - ACLU [Mobile Justice app for your jurisdiction](#).
  - Local sheriff or police app, including signing up for local Groups relevant to you.
  - iNaturalist.
  - Wi-Fi Analyzer.
  - Google Developers.
- Set all relevant **emergency settings** that didn't get done above, including:
  - [gear] **Settings** > **Security** > **Device admin apps** > allow **Lookout**, **Find My Device** and ACLU **Enable Lock Screen on Trigger**.
- Set all relevant **ease-of-use settings** that didn't get done above, including:
  - setting **volume-levels** and **ringtones** that you can actually hear. **How?**
- If needed, rebuild your **home screen**, by adding icons for:
  - Contact of your sweetie.
  - [gear] Settings.
  - Calculator.
  - Your favorite [software for digital video virtual web-based meetings, conferences, gatherings or webinars](#).
  - YouTube.
  - Clock.
  - Your favorite websites (e.g., [ericpiehl.com](#) and [iCanSeeNature.com](#)).
  - Files.
  - NOAA Magnetic Field Calculator.
  - Google Lens.
- A **Motorola** phone I saw with Android 5.1 said it also has functions to **locate**, **lock** or **wipe** your 📱 phone, if you first use app **Moto** to activate device administrator, link to a Google account (you almost certainly did when you first got it), and later (when you need to locate, lock or wipe it?) log in to [www.motorola.com/support](http://www.motorola.com/support).
- To ensure your **Android** 📱 smartphone or 📱 tablet device does not suffer from the [Stagefright Flaw](#) of 2015-07-27, please:
  - launch app **Play Store** (icon may be on its own, may be in folder Google) >
  - **Q Search** for "[Stagefright Detector](#)" >s










- select Android app "[Stagefright Detector](#)" from **Lookout Mobile Security FREE** with white-on-green sad-face shield >
- [Install](#).
- When installed, [Open](#) it.
  - If it says, "**Everything is OK**", it is. *If you wish*, uninstall the app.
  - If it says your device is affected and the vulnerable behavior is enabled, please follow-up with "More info" or your local techie.
- To ensure your **Android** ☞ smartphone or ☞ tablet device does not suffer from the [Heartbleed Flaw](#) of 2014-04-09, please:
  - launch app **Play Store** (icon may be on its own, may be in folder Google) >
  - **Q Search** for "[Heartbleed](#)" >
  - select Android app "[Heartbleed Detector](#)" from **Lookout Mobile Security FREE** with white-on-green dripping-heart shield >
  - [Install](#).
  - When installed, [Open](#) it.
    - If it says, "**Everything is OK**", it is. *If you wish*, uninstall the app.
    - If it says your device is affected and the vulnerable behavior is enabled, please follow-up with "More info" or your local techie.
- Semi-permanently **mark** your ☞ smartphone or ☞ tablet with your **contact info**. Perhaps by:
  - **Write** your contact info on your device, with a Sharpie or other permanent marker.
  - **Tape** a business card to it, with tape coverage > 100%.
  - Make a business-card-like **label** yourself.
  - If a ☞ phone, verify that the above includes a phone number **other than** that of your device itself.
  - Do this in a way involving **bright colors**, to make it easier to **find in the couch**, or **see as it arcs into the trash**.
  - Consider making a second tag, hiding it somewhere within the device.
- Personalize your ☞ **smartphone** or ☞ **tablet name** by [renaming](#) it from its default to:
  - **your name** and **the year you bought it**, in [UpperCamelCase](#) format [FirstLast\\_YYYY](#), or
  - permanently-available ☞ ☎ phone number, in format [AAA-XXX-NNNN](#).
- *If you need **physical protection** (I do!),* get some **armor** (I do!):
  - I have seen an iPad with totally-awesome **armor**, which the owner identified as "Griffin Survivor". I believe he said it even had an optional cover for the Home button. Looks perfect for parents of even the most active or strong-willed kids. I found this at [www.griffintechology.com/survivor](http://www.griffintechology.com/survivor). They have other products, such as the Survivor Slim at [www.griffintechology.com](http://www.griffintechology.com) > *yourPlatform*.
  - I have seen a ☞ cellphone with a [Trident case](#). Seemed quite good. I didn't get that, but I really like [mine](#).
  - Order it in a **bright color**, to make it easier to **find in the couch**, or **see as it arcs into the trash**. [I did](#).
- Order ☞ ☞ tablet/smartphone **charger cables** for your car, briefcase, and travel bag.
  - And maybe an emergency battery-charger.
- [Consider charging via a surge suppressor](#) (I don't).
- *If you do **not** use your ☞ ☞ smartphone/tablet's camera all the time,* **put a piece of tape over the camera**. Cellophane tape is OK--it blurs stuff very well. Or use opaque electrical tape. If you are worried about adhesive preventing future use of the camera, put a little square of paper in the center of the tape, where the camera port will be.
- **Reduce data usage** by:
  - Apps > [gear] Settings > Data Usage > Cell data=ON > set Set cellular data limit-ON > move limits and warnings down to 500 MB and 350 MB or other appropriate levels > scroll down to App usage > for apps you don't need cell data (e.g., calendar, Dropbox, YouTube) tap and Restrict app background data=ON.
  - *If present*, Apps > [Republic Wireless](#) > [gear] Settings > Cell data settings > Cell data check "Enabled for all installed apps" > Back > top navigation bar to center "Cell Data" > in bottom-right of screen, tap app icons > turn off cell data for all apps you don't need it for, such as Bluetooth, calendar, clock, cloud print, contacts, Drive, Dropbox, gallery, Skype, YouTube, but leave on dialer, Lookout, Maps, rescue, etc.

- To reduce **battery duration** problems:
  - Launch Android app [gear] **Settings** >
    - **Battery** > select **each** app to see any settings that can reduce battery use.
    - **Battery** > ☰ hamburger icon in upper-right > **Battery saver** > Turn on automatically > at 15%.
    - **Location** > **Mode**=Battery saving.
- If you think your Facebook app requires too many permissions (it does), uninstall it, and replace it with [Tinfoil for Facebook](#). Saves a huge amount of space on your 📱 phone, too! So far, seems quite functional.
- If at home under Wi-Fi, update your apps via app **Play Store** > [gear] **Settings** ☰ hamburger icon in upper-left corner > **My apps & games** > **Updates** > for each app that needs an update whose existence and permissions you don't mind > **Update**.
- If at home under Wi-Fi, update your OS via [gear] **Settings** > **System Updates** > those three things.
- If you aren't going to use **Bluetooth** on your device, turn it off. Same with Wi-Fi.
- Examine [gear] **Settings** > [Google >] **Location**.
- Examine **Google Settings** > **Ads** > **Opt out of Ads Personalization**.
- [Disable ad id tracking, and why you should do it now](#).
- [Follow these Android tips](#). And [these Android security tips](#).
- [Clear your browser's cache](#).
  - If you have browser Chrome, follow the few steps in <https://support.google.com/chrome/answer/2765944> > tab **Android**.
- If you commonly attach to **public Wi-Fi access points** (no password needed) in public spaces such as airports, hotels, libraries and Starbucks, consider installing a **VPN** (Why? [What does a VPN hide?](#)), such as [TunnelBear](#) or Avira Phantom VPN or [others](#).
  - As of 2018-03-29, there is 77% off a three-year subscription for up 6 devices (any combination of 📱 Android; 🍏 Apple 📱 iOS, 📱 iPadOS and 🖥️ macOS; and 🖥️ Microsoft Windows) at <https://nordvpn.com/Isaac>. As of 2019-05-20, there is 75% off a three-year subscription at <https://nordvpn.com/pilot>, and 1 month free with discount="pilot".
  - Or when I am going to be set up for more than a couple hours or days, I use a small router/Wi-Fi-repeater/-extender; at least I get started off encrypted (**TODO: Investigate this more**). And then my family's 📱 smartphones, 📱 tablets and 🖥️ computers all attach automatically.
- To prevent Android from telling you "**Not enough space**":
  - Launch app [gear] **Settings** > **Storage** > if section **Available** space is under 500MB, select section **Cached data** > **OK**.
  - If still having trouble, launch app [gear] **Settings** > **Storage** > if **Available** space is under 500MB, select section **Apps** > tab ALL > for each app, select it:
    - If it has a button **Move to SD Card**, select that button.
  - If still having trouble, launch app **Chrome** > ☰ hamburger icon in upper-right > [gear] **Settings** > **Downloads** > set **Download location**=SD card.
  - If still having trouble, launch app [gear] **Settings** > **Storage** > in sections for **Pictures Audio Downloads Misc**, see if you can move them to your SD card.
    - For example, from app **Camera** > swipe left-to-right until [gear] **Settings** curve comes up > slide curve around until you see an icon that looks like an **SD card** > set **Storage location**=SD card.
  - If still having trouble, launch app [gear] **Settings** > **Storage** > if **Available** space is under 500MB, select section **Apps** > tab **ALL** > select app **Google Play services** > select button **Clear Cache** > Restart your machine.
  - If still having trouble, launch app [gear] **Settings** > **Storage** > if **Available** space is under 500MB, select section **Apps** > tab **ALL** > select app **Google Play services** > select button **Manage Space** > **Clear All Data** > Restart your machine.
- Optional, if you think you might lose physical control of your 📱 phone, [consider encrypting all data on it](#).

- To help you **fall asleep**, consider installing an app to not display blue light near bedtime. For a while on another platform, I used **f.lux** to good effect. [Info.](#) ~~[If you have or don't mind jailbreaking your Android device, download.](#)~~
- Until then, use app **Timeriffic**, set so night has Brightness=0%, and Notification=0%. I do. My wife no longer complains about my ~~phone notifying of appointments the next day, because it doesn't do that, during those hours.~~ Update: I use the features in Android 5.1 [gear] Settings > Sound & Notification > Interruptions > set Downtime "Days", "Start time", "End time" and "Interruptions allowed". And somewhere, to dim the screen to 35% or so. No removing blue and green yet, but not bad.

### 3.4 One-time: Harden your computer

-  If your computer runs **Microsoft Windows**, make it easier to use:
  - When you first power-up your new computer, make the **first user** (the **primary Administrative user**) have a username of a  permanently-available phone number, in format [AAA-XXX-NNNN](#).
    - Make this a local (non-Microsoft) account.
    - Logon to this account only for large-scale setup of your machine.
  - Create for yourself a **secondary personal username**, a local (non-Microsoft) account, via "Add someone else to this PC" > "I don't have this person's sign-in information" > "Add a user without a Microsoft account" > in [UpperCamelCase](#) format [FirstLast](#), with no spaces. After this startup stuff,  **Start** >  **Run** **"netplwiz"**.
    - Logon to this account for all day-to-day work.
    - If you do anything requiring Administrative rights, you will usually just be prompted to supply the Administrator's password. Only occasionally will you have to logon as the Administrator.
  - Personalize your  **computer name** by [renaming](#) it from its default to:
    - **Your name** and **the year you bought it**, in [UpperCamelCase](#) format [FirstLast\\_YYYY](#).
      - May be up to 15 characters: letters, numbers, hyphen "-" and underscore "\_"; cannot be only numbers.
  - While there, personalize the **name** of your **harddrive C:\** from [Windows](#) to something with **your name** and **location**, in [UpperCamelCase](#) format [FirstLastUSA](#), or a permanently-available  phone number, in format [AAA-XXX-NNNN](#).
  - To make things easy on yourself or buddies running  macOS or Unix, or running any platform and using [Unix or GNU utilities](#), I use (and highly-recommend) **usernames**, **filenames** and **foldernames** with **\*no\* spaces (blanks) " "**.
    - Instead use [camelCase](#) for metadata that relates to each other, perhaps separated by **underscores "\_"** or **hyphens "-"** to metadata that doesn't relate.
    - I try to put all metadata in the filename. For example, for photographs, I use format [date\\_WhoFromTopToBottomLeftToRight\\_Where\\_doingWhat\\_byWhom.ext](#), where:
      - **date** is in [ISO 8601](#) format, [yyyymmdd](#) (within the doc will be [yyyy-mm-dd](#)). The international standard, and it sorts correctly!
      - **Who** is in UpperCamelCase [FirstLast](#).
      - **Where** is in UpperCamelCase, perhaps [CityStateCountry](#) or [VillageCountyST](#).
      - **doingWhat** is in lowerCamelCase, perhaps [atZoo](#).
      - **byWhom** is probably sometimes their initials, perhaps [byEP](#).
      - **ext** is the file extension, perhaps [.png](#).
  - Tell **File Explorer/This PC** (formerly **Windows Explorer/My Computer**, and still called "Windows Explorer" *under-the-covers*) > ribbon tab **View** > check **Item check boxes** > check **File name extensions** > check **Hidden items** > Options > Change folder and search options > tab View > check boxes for options **Display...**, **Show...** and **Use...**, and uncheck options **Hide...**
  - In Windows 10, my **taskbar** color was **black**, making it hard for me to see. I changed that by something I found with my favorite Search Engine (such as [DuckDuckGo](#)) > [windows 10 taskbar color](#). Get used to doing this a lot to tweak Windows 10. Better, but I was not fully happy.
  - In Windows 10, my Windows' **Title Bar** color scheme was **medium gray** (windows without focus) and **light gray** (window with focus). What?!? To work efficiently, I need **more contrast** than this, with the window-with-focus's Title Bar set to a **hot color**. After living with a bad solution for a few months, I found . . .
  - The **best way** I found to do **both** these last two bullets is to right-click the empty desktop > [Personalize](#) > tab [Background](#) > set dropdown [Background](#) to [Slideshow](#) or [Picture](#) or [Solid Color](#) > [Browse](#) > if needed, set to [C:\Users\yourLogonName\Pictures\](#) or something > set [Change picture every 10 minutes](#) or whatever > tab [Colors](#) > [Automatically pick an accent color from your background](#) > set [Show color on Start, taskbar, action center](#) and > set [Show color on title bar](#).
  - In Windows 10, Windows **File Explorer/This PC** (formerly **Windows Explorer/My Computer**, and still called "Windows Explorer" *under-the-covers*) doesn't sort Folders on top. A pain--slows me down. To bring that back, <https://duckduckgo.com/?q=windows+10+sort+folders+top> or <https://google.com/search?q=windows+10+sort+folders+top> (get used to doing that) said to:
    - **View** > **Layout=Details** (OK, I run that way),
    - **View** > **Sort by=Date** (**NOT** Date Modified) (if **Date** is **not** there, **View** > **Sort by=Choose columns...** > check its checkbox > **OK**),
    - **View** > **Sort by=Descending**. Works. Weird.
  - More ideas at [How to make Windows 10 Look and Act more like Windows 7](#) (choose carefully).

- If you have a **new** Win10 machine, do **not** pay for any **pre-installed security suite**. You can safely **Uninstall** it. After you do, immediately **reboot**, bring up **Microsoft Defender Antivirus** (app **Windows Security**), and verify that it is **on**. Then Update and do a Full Scan, just for practice.
- If your  computer does not yet have **antimalware** software, **install** one, [from somewhere other than China](#), Russia and associated countries.  
I recommend these free-for-personal-use:
  -  For **Apple macOS** (Macintosh, iMac, iBook, and MacBook)  computers:
    - [Sophos AntiVirus for Mac Home Edition](#) (recommended by [UM](#) and [Cryptoparty Ann Arbor](#)), or
    - If you get your Internet via **Comcast**, you can get Norton Internet Security **free**:
      - Install under Comcast, from <https://internetsecurity.xfinity.com>.
      - Later, it will update itself from anywhere in the solar system with Internet access.
      - I mildly dis-recommend it.
    - I **dis-recommend Kaspersky** Anti-Virus or Kaspersky Internet Security due to (2015-2017-?) claims of close ties to Russian military and intelligence officials. I previously liked the company. I will keep my ears open for more developments.
    - [Current recommendations \(very good\) from the University of Michigan](#).
    - [Recommendations from Lifewire](#).
    - [Other recommendations from Lifewire](#).
  -  For **Linux**:
    - [Current recommendations \(very good\) from the University of Michigan](#).
    - [Other recommendations from Lifewire](#).
  -  For **Microsoft Windows 10**  computers:
    - **Microsoft Defender Antivirus** (app **Windows Security**). Already installed.
      - Verify that Microsoft Defender Antivirus (app Windows Security) is running, and updates itself. To do that:
        - Click  **Start** > type "**defender**" > wait for **Windows Security app** (formerly **Windows Defender desktop app**) to appear > launch it.
        - Look for:
          - **Virus & threat protection > Real-time protection=On,**
          - **Virus and spyware definitions=Up to date,** and
          - (assuming MWD installed more than a couple weeks ago) **Last-scan=sometime in the last week.**
        - If these are true, you are protected.
      - If Microsoft Defender Antivirus (app **Windows Security**) is **not** running, continue... Or I read that MWD is adequate for most users for most purposes; if you want better protection, install one of (after you do so, MWD will turn itself off)...
      - [Avast! Free Antivirus Essential](#) > Free Download (trying this now), or
      - [Avira AntiVir Personal](#), or
      - [F-Prot](#) (liked it a lot when I used some years ago when it had a free version), or
      - [Malwarebytes](#) (free is a terrific on-demand scan, but the prevention module costs \$), or
      - If you get your Internet via **Comcast**, you can get Norton Security software **free**:
        - Install under Comcast, from <https://internetsecurity.xfinity.com>.
        - Later, it will update itself from anywhere in the solar system with Internet access.
        - I mildly dis-recommend it.
      - I **dis-recommend Kaspersky** Anti-Virus or Kaspersky Internet Security due to (2015-2017-?) claims of close ties to Russian military and intelligence officials. I previously liked the company. I will keep my ears open for more developments.
      - [Current recommendations \(very good\) from the University of Michigan](#).
      - [Other recommendations from Lifewire](#).
  -  For **Microsoft Windows 8.1**:
    - **Microsoft Defender Antivirus** (app **Windows Security**). [Alleged to be already installed](#). Oops, when I checked a friend's machine, MWD was **not** installed--or maybe a subset. Please continue...
      - Verify that Microsoft Defender Antivirus (app Windows Security) is running, and updates itself. To do that:
        - Click  **Start** > type "**defender**" > wait for **Windows Security app** (formerly **Windows Defender desktop app**) to appear > launch it.
        - Look for:
          - **Virus & threat protection > Real-time protection=On,**
          - **Virus and spyware definitions=Up to date,** and
          - (assuming MWD installed more than a couple weeks ago) **Last-scan=sometime in the last week.**
        - If these are true, you are protected.



- If Microsoft Defender Antivirus (app Windows Security) is **not** running, continue... Or I read that MWD is adequate for most users for most purposes; if you want better protection, install one of (after you do so, MWD will turn itself off)...
- [Avast! Free Antivirus Essential](#) > Free Download (trying this now), or
- [Avira AntiVir Personal](#), or
- [F-Prot](#) (liked it a lot when I used some years ago when it had a free version), or
- [Malwarebytes](#) (free is a terrific on-demand scan, but the prevention module costs \$), or
- If you get your Internet via **Comcast**, you can get Norton Security software **free**:
  - Install under Comcast, from <https://internetsecurity.xfinity.com>.
  - Later, it will update itself from anywhere in the solar system with Internet access.
  - I mildly dis-recommend it.
- I **dis-recommend** **Kaspersky** Anti-Virus or Kaspersky Internet Security due to (2015-2017-?) claims of close ties to Russian military and intelligence officials. I previously liked the company. I will keep my ears open for more developments.
- [Current recommendations \(very good\) from the University of Michigan](#).
- [Other recommendations from Lifewire](#).
- ☐ For **Microsoft Windows 7, Vista or XP** (and 8.0 and any version other than Windows 10):
  - **Upgrade Windows now! Really!** Until you do, continue ...
  - [Microsoft Security Essentials MSE](#) **(TODO: get new link)** (recommended by [UM](#)) if free this week, or
    - If MSE is **not** running, continue... Or I read that MSE is adequate for most users for most purposes; if you want better protection, install one of (after you do so, MSE will turn itself off) ...
  - [Avast! Free Antivirus Essential](#) > Free Download (trying this now), or
  - [Avira AntiVir Personal](#), or
  - [F-Prot](#) (liked it a lot when I used some years ago when it had a free version), or
  - [Malwarebytes](#) (free is a terrific on-demand scan, but the prevention module costs \$), or
  - If you get your Internet via **Comcast**, you can get Norton Security software **free**:
    - Install under Comcast, from <https://internetsecurity.xfinity.com>.
    - Later, it will update itself from anywhere in the solar system with Internet access.
    - I mildly dis-recommend it.
  - I **dis-recommend** **Kaspersky** Anti-Virus or Kaspersky Internet Security due to (2015-2017-?) claims of close ties to Russian military and intelligence officials. I previously liked the company. I will keep my ears open for more developments.
  - [Current recommendations \(very good\) from the University of Michigan](#).
  - [Other recommendations from Lifewire](#).
- For **servers**:
  - [Current recommendations \(very good\) from the University of Michigan](#).
- For total expert needs, see [Communications Security Establishment CSE Assemblyline](#) and [Krebs on Security blog](#).
- Update your **antimalware/antivirus rules**.
- ☐ If running under **Microsoft Windows**, reboot (☐Start > 1/0 Power > Restart).
- If you have **vision issues** (you do, or you will):
  - Make your **display** display its contents larger.
    - ☐ Under Microsoft Windows, ☐Start > [gear] **Settings** > **Ease of Access** > left navigation bar **Display** > play with all those controls. I suggest:
      - Make everything brighter,
      - turn off **Show transparency in Windows**,
      - **Make everything bigger**,
      - **Make text bigger**,
      - turn off **Show animations in Windows**,
      - turn off **Show desktop background image**, and
      - other controls in these areas.
  - Make your **mouse pointer** easier to see.
    - **Enlarge** your mouse pointer **size**.
      - ☐ Under Microsoft Windows, (still in ☐Start > [gear] **Settings** > **Ease of Access**) > left navigation bar **Mouse pointer** > slide **Change pointer size** to the right, maybe **3–15**.
        - As of 2022, this size increase does **not** yet transmit over **Zoom Share Screen**.
      - ☐ Under Apple macOS, **Settings** > **Accessibility** > left navigation **Display** > top tab **Cursor** > check checkbox **Shake mouse pointer to location** > **Cursor size** to right 1 or 2 or 3 positions.





- Change your mouse pointer **color**.
  - **Win** Under Microsoft Windows, still at the above, try gold, red or **pink**!
- Make your mouse pointer **move faster**, **display mouse trails**, and **show its location**.
  - **Win** Under Microsoft Windows, **Win+Start** > type "**mouse**" > select **Change your mouse pointer or speed** > tab **Pointer Options** > check **Display pointer trails** and **Show location of pointer when I press the CTRL key**.
- Make your **display** easier to see.
  - **Win** Under Microsoft Windows, **Win+Start** > type "**contrast**" > select **Turn high contrast on or off** > set control **Turn on high contrast** to **On**.
- Make your **display colors** easier to see.
  - **Win** Under Microsoft Windows, **Win+Start** > type "**color filter**" [Enter] > set "Turn on color filters" = **Yes**, and probably check checkbox "Allow the shortcut key to toggle filter on and off" (**Win+Ctrl+C**).
    - If *colorblind*, also select radio button "Red-green", the other "Red-green" or "Blue-yellow".
    - If *have macular degeneration*, also select radio button "Grayscale" to get most active windows to show black-on-white (inactive windows show white-on-black). **TODO: find other way to get stronger black-on-white.**
- Tell **YouTube** to have captions:
  - Turned on for ALL YouTube videos: go to <https://youtube.com> > select your photo in upper-right (if needed, sign in to Google) > [gear] [gear] **Settings** > left navigation bar **Playback and performance** > section **Subtitles and Closed Captions** > check **Always show captions** and **Include auto-generated captions (when available)** > **Back** > **Back**.
  - So you can see the captions: in lower-right, select [gear] [gear] **Settings** > **Subtitles/CC** > **Options** > **Font color**="Black" (for me, "Green"), **Font size**=400% (for me, 150%), **Background color**="White", **Background opacity**=100% (for me, 0%), **Character edge style**="Outline", and **Window opacity**=0%.
- If you use Microsoft emailer **Outlook** or **Mail**, and **cannot** read "Plain Text" emails, and **can** read emails in font="Arial" size="14" black-on-white:
  - go into your email program >
    - ribbon "File" >
    - left navigation bar "Options" >
    - left navigation bar tab "Mail" >
    - section "Compose Messages" button "Stationary and Fonts ..." >
    - top tab "Personal Stationary ..." section "Composing and reading plain text message" button "Font ..." >
    - from something small
    - to Fonts="Arial" and Size="14" and Font color="Automatic" >
    - button "OK" >
    - button "OK" >
    - button "OK".
- If *paranoid*, turn on **Win+Start** > [gear] **Settings** (formerly **Control Panel**) > **Controlled Folder Access** > **On**.
  - Be prepared for, sometime in the following days and weeks, that an application may **fail to do its job properly**, while Windows Notify tells you it was **because Controlled Folder Access prevented it**. So far, this has happened to me with apps **Dropbox** and **Quicken**. When this happens, you need to:
    - come back here and **Allow an app through Controlled folder access** >
    - **+ Add an allowed app** >
    - the app that was just prevented.
    - Exit your app, reenter, and you should be fine (I am).
- If a *laptop*, semi-permanently **mark** your **laptop** computer with your **contact info**. Perhaps by:
  - **Write** your contact info on your device, with a Sharpie or other permanent marker.
  - **Tape** a business card to it, with tape coverage > 100%.
  - Make a business-card-like **label** yourself.
  - If a **phone**, verify that the above includes a phone number **other than** that of your device itself.
  - Consider making a second tag, hiding it somewhere within the device.
- Personalize your **laptop** **computer name** by **renaming** it from its default to:
  - **Your name** and **the year you bought it**, in **UpperCamelCase** format **FirstLast\_YYYY**.
  - May be up to 15 characters: letters, numbers, hyphen "-" and underscore "\_"; cannot be only numbers.

- Please see [🍏 Apple Device and Data Access when Personal Safety is at Risk](#) for [🍏 Apple iPhone](#) [📱 smartphones](#); [iPad](#) [📱 tablets](#); **Macintosh, iMac, iBook, and MacBook** [💻 computers](#); and probably HomePod devices.
- [Consider charging via a surge suppressor](#) (I don't).
- If you do **not** use your webcam camera all the time, **put a piece of tape over the camera**. Cellophane tape is OK--it blurs stuff very well. Or use opaque electrical tape. If you are worried about adhesive preventing future use of the camera, put a little square of paper in the center of the tape, where the camera port will be.
- If you commonly attach to **public Wi-Fi access points** (no password needed) in public spaces such as airports, hotels, libraries and Starbucks, consider installing a **VPN** (Why? [What does a VPN hide?](#)), such as [TunnelBear](#) or Avira Phantom VPN or [others](#).
  - As of 2018-03-29, there is 77% off a three-year subscription for up 6 devices (any combination of [📱 Android](#); [🍏 Apple](#) [📱 iOS](#), [📱 iPadOS](#) and [💻 macOS](#); and [💻📱 Microsoft Windows](#)) at <https://nordvpn.com/Isaac>. As of 2019-05-20, there is 75% off a three-year subscription at <https://nordvpn.com/pilot>, and 1 month free with discount="pilot".
  - Or when I am going to be set up for more than a couple hours or days, I use a small router/Wi-Fi-repeater/-extender; at least I get started off encrypted **(TODO: Investigate this more)**. And then my family's [📱 smartphones](#), [📱 tablets](#) and [💻 computers](#) all attach automatically.
- For **each** of your web browsers, consider:
  - [Test your browser against tracking](#).
  - [Secure access to your location](#).
  - To help ProPublica track displays of political ads, download their browser extension/add-on [Facebook Political Ad Collector](#) (scroll down to Download box).
  - To protect you against eavesdropping, tampering with or forging content in some websites you visit, install plug-in [HTTPS Everywhere](#) from the [EFF](#). I have used it for years, trouble-free for me.
  - Install plug-in [Privacy Badger](#) also from the EFF (good, but I have to tell it to exclude some websites), or
  - Install plug-in [www.ghostery.com](#) > set to block web tracking types [Advertising](#), [Analytics](#), [Beacons](#), [Privacy](#) and [Widgets](#). A cousin recommended this. I love it, too. I currently block everything, except for one Analytics that I use occasionally. So far, so good.
  - [Block ads on YouTube](#).
  - To have your web browser **forget** your **browsing history, cookies, cached files**, and **passwords** at the end of each session, whenever accessing important sites (bank, [✉ email](#), Facebook, etc.), get used to launching your web browser in mode **privacy/Incognito/InPrivate**.
  - Then once a month or so, [delete your browser's cookies](#) and [clear your browser's cache](#), and [on your iOS](#) [📱 iPhone](#) or [iPadOS](#) [📱 iPad](#).
  - If you have browser Chrome, follow the few steps in <https://support.google.com/chrome/answer/2765944> > tab **Computer**.
- If you aren't going to use **Bluetooth** on your device, turn it off. Same with Wi-Fi.
- There are many ways to **copy files** from an **old machine** to a **new machine**. Using a flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-sticks works fine, but may get a little confusing if you don't have the right tools on both machines. [Expert] [me] Assuming [💻 Microsoft Windows 10](#) throughout, my favorite way is to:
  - On each **secondary** computer (the computer(s) that will be a **passive** partner in the copying), set **File Explorer/This PC** (formerly **Windows Explorer/My Computer**, and still called "Windows Explorer" *under-the-covers*) > **C:\** > right-click entry **Users** > **Properties** > window **"User Properties"** > tab **Sharing** > button **Advanced Sharing** . . . > check checkbox **"Share this folder"** > button **Permissions** > Group=**Everyone** > Permissions for Everyone **"Full Control"** check **Allow**, **"Change"** check **Allow**, and **"Read"** check **Allow** > button **Apply** > button **OK** > button **Apply** > button **OK** > button **Close**.
  - On the **primary** computer (the computer from which you will **control** the copying), **log on** to the secondary computer(s) using that computer's logon credentials, and copy over needed files using my favorite tool described in the next paragraph. If you can't get on with UNC format, do a **This PC** (formerly **My Computer**) > ribbon tab **Computer** > group **Network** > **Map Network Drive** > **Map Network Drive** > *driveLetter* > **\\machineName\users** > check **Connect using different credentials** > **Finish** >

*credentials*. Then copy from the mapped drive.

If these instructions are a little obtuse for you, talk to someone who understands them.











- When you acquire a new **flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-stick**:
  - IF your drive came in format="**FAT32**",  
AND you want your drive to handle file sizes >4GB=**No**,  
THEN you can leave it just like this.
  - IF your drive came in format="**NTFS**",  
AND you want your drive for ☐ Microsoft Windows use=**Read-Write**  
AND 🍏 Apple macOS use=**Read-Only** or **not at all**,  
THEN you can leave it just like this.
  - IF your flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-stick came in format="**HFS+**",  
AND you want your drive for 🍏 Apple macOS use=**Read-Write**  
AND ☐ Microsoft Windows use=**not at all**,  
THEN you can leave it just like this.
  - IF you want your drive for use in the Honda Fit/Jazz Type 2 entertainment system,  
THEN reformat your drive to format="**FAT32**".
  - IF you are running 🍏 Apple macOS level lower than 10.6.6,  
THEN apply the "**exFAT patch**".
  - IF you are running ☐ Microsoft Windows release lower than 7,  
THEN apply the "**exFAT patch**".
  - IF you are running ☐ Microsoft Windows release lower than 10,  
THEN upgrade to a modern level of Windows with all due speed.
  - IF you want your drive for 🍏 Apple macOS use=**Read-Write**  
AND/OR ☐ Microsoft Windows use=**Read-Write**,  
AND/OR handle file sizes >4GB=**Yes**,  
THEN reformat your drive to format="**exFAT**" as in  
<https://support.wdc.com/knowledgebase/answer.aspx?ID=291> (creates folder "**MACOSX**").
- While you are at it, personalize the name of your **flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-stick** to:
  - something with **your name** and **location**, in format **FirstLastUSA**, or
  - a permanently-available ☎ phone number, in format **AAA-XXX-NNNN**.
- **Eric**, add to Excel:
  - Quick Access Toolbar commands **Insert Cells ...** and **Row Height ....**
  - Ribbon tabs **Developer** and **Add-Ins** Clear Excess Formats in #SWG.xlsm.
- [Speed up your boot by disabling the Windows 10 lock screen](#).
- If you think you might lose physical control of your ☑ computer, [consider encrypting some or all data on it](#).
- To help you **fall asleep**, consider turning on ☐ Microsoft Windows **night light** (search for it in [gear] Settings), or installing an app to not display blue light near bedtime. For a while, I used **f.lux**, to good effect. [Info](#). [Download for ☐ Microsoft Windows, 🍏 Apple Macintosh, and 🐧 Linux](#). After a year, I uninstalled it. Good, too.
- If you need **tools** or utilities to make your life easier, you might want to see my [tools document](#) and [Kim Komando's site](#) or [About's software tools](#) or [Lifewire's 10 Common Online Tasks That Everyone Should Automate](#).
- If you are going to ask me for support in the future, please [run](#) and have ready for me:
  - "**msinfo32**" > **Export** > **somewhereGood\myComputer\_MSINFO32.txt** > **Save**,
  - navigate **somewhereGood**, "**ipconfig /all**" > **myComputer\_IPCONFIG.txt** [Enter],
  - "**diskpart**", "**list volume**", "**exit**" and save the results in one of the files above, and
  - **Powershell** "(Get-WmiObject -query 'select \* from SoftwareLicensingService').OA3xOriginalProductKey" and save the results in one of the files above.
- If you have not yet upgraded your ☑ computer from ☐ **Microsoft Windows 8.1** or **Windows 7** (or 8.0, 7, Vista, XP or any version other than 10) to [🐧 Linux](#) or ☐ **Windows 10**:

- o [You must upgrade](#) to get future security patches. And your machine will run faster, and be more reliable. And I mostly like it. But there are some teething pains. But you can grow past those.
- o I recommend you do a [full backup](#) of your system. I have upgraded several machines from Windows 7 and 8, and I think one on Vista, and it has always gone very well, with no problems. But do a backup, just in case. You need a backup anyway.
- o The next time you have (A) your  computer **plugged in** and (B) **3 hours** for it to chug, and (C) **5 hours** to clean up from it, then . . .
- o Go to <https://zdnet.com/article/heres-how-you-can-still-get-a-free-windows-10-upgrade>. ~~[2019-04-18:— Was <https://microsoft.com/en-us/accessibility/windows10upgrade> > **Upgrade Now**.] [I recently read that Microsoft would turn this off 2018-01-01, but so far, it still seems active. —EP 2018-01-07.]~~
- o After W10 installs, and you **logon** for the first time, say **Personalize** and **Let me choose**, and **Deselect** almost all offerings MS chose for you. Very bad.
- o On my old Windows 7 machine, W10 kept using my **old username**, local, and same password. Great.
- o But on a new W8.1 machine, W10 insisted on setting me up with a **new username** that is also an  **email address**, that **Microsoft would control**, and keep a **copy of all my settings**? Why? I created some local usernames. **TODO: Take control of the Administrator user, too.**
- o After W10 installed, the connection to my home's **Wi-Fi** network disappeared. My attempts to fix it failed. After a half hour, it came back on its own. If this happens to you, reboot.
- o After W10 installed, **Chrome** was no longer my default web browser. I had to launch Chrome and tell **it** to be my default web browser. That worked.
- o After a while, Chrome turned all of its web content totally black--could not read a thing. My attempts to fix it failed. After a half hour, it came back on its own. If this happened to you, exit Chrome and re-launch, or reboot.
- o After W10 installed, my **taskbar** color was **black**, making it hard for me to see. I changed that by something I found with my favorite Search Engine (such as [DuckDuckGo](#)) > **windows 10 taskbar color**. Get used to doing this a lot to tweak Windows 10. Better, but I was not fully happy.
- o After W10 installed, my windows' **Title Bar** color scheme was **medium gray** (windows without focus) and **light gray** (window with focus). What?!? To work efficiently, I need **more contrast** than this, with the window-with-focus's Title Bar set to a **hot color**. After living with a bad solution for a few months, I found . . .
- o The **best way** I found to do **both** these last two bullets is to right-click the empty desktop > **Personalize** > tab **Background** > set dropdown **Background** to **Slideshow** or **Picture** or **Solid Color** > **Browse** > if needed, set to **C:\Users\yourLogonName\Pictures\** or something > set **Change picture every 10 minutes** or whatever > tab **Colors** > **Automatically pick an accent color from your background** > set **Show color on Start, taskbar, action center** and > set **Show color on title bar**.
- o After W10 installed, one of my **apps was broken**, and their website gave incomplete information on how to fix that. I figured out the real fix, and  emailed it to the app's vendor.
- o After W10 installed, my **Dropbox** icon no longer appeared in my *Notification Area* (will be *Action Center* in Win10X) (formerly *System Tray* — by the clock). After going to <https://dropbox.com> and logging in again, my Dropbox icon has returned.
- o After W10 installed, many of my **Start pins** were gone. I rebuilt them.
- o After W10 installed, Windows **File Explorer/This PC** (formerly **Windows Explorer/My Computer**, and still called "Windows Explorer" *under-the-covers*) stopped sorting Folders on top. A pain--slows me down. To bring that back, <https://duckduckgo.com/?q=windows+10+sort+folders+top> or <https://google.com/search?q=windows+10+sort+folders+top> (get used to doing that) said to:
  - **View** > **Layout=Details** (OK, I run that way),
  - **View** > **Sort by=Date** (**NOT** Date Modified) (if **Date** is **not** there, **View** > **Sort by=Choose columns...** > check its checkbox > **OK**),
  - **View** > **Sort by=Descending**. Works. Weird.
- o If you have a **new Win10 machine**, do **not** pay for any **pre-installed security suite**. You can safely **Uninstall** it. After you do, immediately **reboot**, bring up **Microsoft Defender Antivirus** (app **Windows Security**), and verify that it is **on**. Then Update and do a Full Scan, just for practice.
- o After W10 installed, **Microsoft Defender Antivirus** (app **Windows Security**) was installed. Seems to be OK, and adequate. Nothing in the *Notification Area* (will be *Action Center* in Win10X) (formerly *System Tray* — by the clock) until you click  **Start** > type "**defender**" > wait for **Windows Security app** (formerly **Windows Defender desktop app**) to appear > launch it. Its icon stays in the *notification area* (will be *Action Center* in Win10X) until you reboot, then it is gone. **TODO: Revisit--do I like the icon enough to Schedule a launch on logon?**



- After W10 installed on one machine, **Norton Security Suite** was gone. After four hours, it popped up a box to **Install an updated version of your Norton product for Windows 10**. As far as I can tell, I don't need both Norton and Microsoft Defender Antivirus (app Windows Security), so I think I won't install this new Norton.
- After W10 installed on another machine, **Norton Security Suite** was there, but could not determine if it was licensed or not. Seemed to be active (MWD turned itself off, so it must have thought so, too), but that red checkmark was not giving me warm fuzzies, to eventually, I uninstalled Norton. After a **reboot**, **Windows Defender Antivirus** was running; good; I did an Update and Full Scan, to good effect.
- After W10 installed on another machine with **McAfee**, stayed on. Huh? Why the difference between these three machines? As far as I can tell, I don't need both McAfee and Microsoft Defender Antivirus (app Windows Security), so I **uninstalled** McAfee. After a **reboot**, **Windows Defender Antivirus** was running; good; I did an Update and Full Scan, to good effect.
- After W10 installed, Microsoft **OneDrive** was there. **TODO: Figure out what I think about that.**
- I told Microsoft "Many advantages, however (1) ~~you broke my FTP (still trying to fix that)~~, (2) the black Startbar and white Title Bars make it hard to work, (3) you unpinned many of my apps (as I needed one, I found and repinned them), (4) some confusion accepting the install, (5) Windows Defender Antivirus is good but I don't know whether to reinstall Norton, and (6) I don't know what to do with OneDrive (bloatware?), and (7) you chewed up some of my freespace (although the machine still runs faster). I will tell relatives to not install until I am there to fix things."


### 3.5 One-time: Make your flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-stick more-usable

- When you acquire a new **flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-stick**:
  - IF your drive came in format="**FAT32**",  
AND you want your drive to handle file sizes >4GB=**No**,  
THEN you can leave it just like this.
  - IF your drive came in format="**NTFS**",  
AND you want your drive for  Microsoft Windows use=**Read-Write**  
AND  Apple macOS use=**Read-Only** or **not at all**,  
THEN you can leave it just like this.
  - IF your flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-stick came in format="**HFS+**",  
AND you want your drive for  Apple macOS use=**Read-Write**  
AND  Microsoft Windows use=**not at all**,  
THEN you can leave it just like this.
  - IF you want your drive for use in the Honda Fit/Jazz Type 2 entertainment system,  
THEN reformat your drive to format="**FAT32**".
  - IF you are running  Apple macOS level lower than 10.6.6,  
THEN apply the "**exFAT patch**".
  - IF you are running  Microsoft Windows release lower than 7,  
THEN apply the "**exFAT patch**".
  - IF you are running  Microsoft Windows release lower than 10,  
THEN upgrade to a modern level of Windows with all due speed.
  - IF you want your drive for  Apple macOS use=**Read-Write**  
AND/OR  Microsoft Windows use=**Read-Write**,  
AND/OR handle file sizes >4GB=**Yes**,  
THEN reformat your drive to format="**exFAT**" as in  
<https://support.wdc.com/knowledgebase/answer.aspx?ID=291> (creates folder "**MACOSX**").
- While you are at it, personalize the name of your **flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-stick** to:
  - something with **your name** and **location**, in format **FirstLastUSA**, or
  - a permanently-available  phone number, in format **AAA-XXX-NNNN**.






### 3.6 One-time: Harden your web presence


To recover from the [Heartbleed Flaw](#) of 2014-04-09, if you haven't done so since this date, please:

- Change all your [passwords](#) at sites listed by [www.cnet.com/how-to/which-sites-have-patched-the-heartbleed-bug](http://www.cnet.com/how-to/which-sites-have-patched-the-heartbleed-bug) and/or [www.mashable.com/2014/04/09/heartbleed-bug-websites-affected/?cid=146326](http://www.mashable.com/2014/04/09/heartbleed-bug-websites-affected/?cid=146326):
  - "Vulnerability patched. Password change recommended": Do that.
  - "Awaiting response": Change your password.
  - "Was not vulnerable": I think you are OK (I trust CNET, mostly). If site is important to you, change your password.
  - "Not listed": Change your password.
- If you have  **Yahoo email**, change your password.


Regardless of the Heartbleed Flaw paragraph above:

- If you have  **Yahoo email**, please migrate to one of the other [free webmail providers](#), such as Google [Gmail.com](#) or Microsoft [Outlook.com/Live Mail \(formerly Hotmail\)](#). If you are scared of the USA, there are several in Europe. I make this recommendation after having helped **multiple family members** with Yahoo accounts recover from **three four separate hacks**.
- For many purposes, consider a [disposable email account](#).
- If your  email provider offers [two-factor authentication 2FA/2-step verification/multi-factor authentication MFA](#), use it. 2FA/2SV/MFA authenticate you by using two or more of these methods:
  - something-you-know (*knowledge*, such as a username and password),
  - something-you-have (*possession*, such as a SMS text account on a  cellphone), and
  - something-you-are (*inheritance*, such as fingerprints or eyeball imagery).[Google's](#) 2FA uses the first two methods, with the second method giving you a [one-time password OTP](#). Initially, it had some teething pains, but since 2014, has been great. Yahoo's even works great.

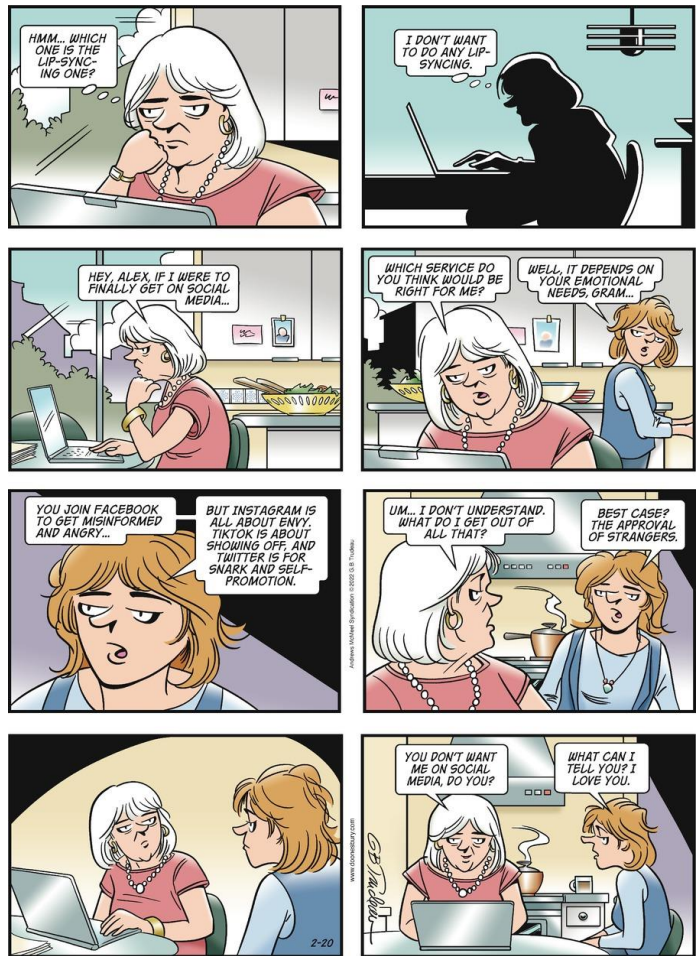
If you cannot/will not use a vendor's 2FA/2SV/MFA authentication, [look into app Authy](#).

2FA/2SV/MFA are not perfect — they do **not** protect against [man-in-the-middle MitM attacks](#), nor if your attacker has also gained access to your  phone's SMS account — , but they do reduce your attack surface.

For **any** provider that offers **two/multi-factor/step authentication/verification**, **use it!**

- Check if you have any accounts **compromised in announced data breaches**, at [Have I Been Pwned?](#) (HIBP) (built by an Aussie computer geek) > [your@email.address](#) and [usernames](#) > **pwned?**. And take appropriate action:
  - To get notified when **future** pwnage occurs and your account is compromised, [Have I Been Pwned?](#) > nav **Notify me** > [your@email.address](#).
  - If you have custom email addresses in form [you@yourDomain](#), you can get notified of pwnage of any of them via [Have I Been Pwned?](#) > nav **Domain search** > [yourDomain](#) > etc.
  - If you are considering a new password, [Have I Been Pwned?](#) > nav **Password** > [yourPassword](#) > **pwned?**.
  - [Helps on correcting your credit Reports](#).
- Use a **password manager**, such as:
  - KeePassXC, local, recommended to me.
  - LastPass.
  - 1Password.
  - Chrome extension passprotect.io.
  - On paper, while you keep physical security on that paper. And physical security on its backup.
- [The EFF says to change your Facebook settings to opt out of platform API sharing](#).
  - In a web browser, go to Facebook <https://facebook.com/settings?tab=applications> > section **Apps, Websites and Games** > button **Edit** > button **Turn Off**. And look around at other settings in the left navigation bar.
  - In the Facebook app, touch the three-line **Settings**  icon in upper-right corner > scroll **way** down to the last section **Settings & Privacy** > entry **Account Settings** > entry **Apps** > entry **Apps, Websites and Games** > (if it says **Turned On**) > press that entry > button **Turn Off**. And look around at other settings after pressing the **Back** button once and twice.

- [Remove from social media anything about drinking, drug use, other embarrassing information, kids' names, current location, vacation plans, home location, and full birthdate.](#)
- Review the **Privacy Settings** in your ✉ email provider, [Facebook](#), and web browsers. They occasionally change them.
- If you get creepy messages on your **Facebook** feed, please follow the procedures in [How to Safely Unfriend a Facebook Creeper](#).
- If you have a Google account (you might, even though you have no Gmail account), follow [Google's Privacy Checkup](#) and [Security Checkup](#).
- After Facebook disclosure of 2019-03-21, [change your Facebook and Instagram passwords](#). And those from other apps from Meta Platforms, Inc.
- Get used to using [check short URL](#) and [more short URL expanding for testing suspicious links without clicking on it](#).
- Follow Kim Komando's "[Google yourself to protect your reputation--online and off](#)".
- To have your web browser **forget** your **browsing history, cookies, cached files, and passwords** at the end of each session, whenever accessing important sites (bank, ✉ email, Facebook, etc.), get used to launching your web browser in mode **privacy/Incognito/InPrivate**.
- Then once a month or so, [delete your browser's cookies](#) and [clear your browser's cache](#), and [on your iOS 📱 iPhone](#) or [iPadOS 📱 iPad](#).
  - If you have browser Chrome, follow the steps in <https://support.google.com/chrome/answer/2765944> > tab **iPhone & iPad**.
- If you **host** any websites, patch them. Does this include Apache HTTP Server? Mine is turned off — isn't it? Gotta go find out how to check, and read [www.eff.org/search/site/heartbleed](http://www.eff.org/search/site/heartbleed) ...



### 3.7 One-time: Harden your voice-activated virtual assistants/voice butlers/smart speakers, TVs and toys!

- [Manufacturer warns customers not to discuss personal information in front of voice-activated devices.](#) Current examples:
  - virtual assistants (voice butlers) (smart speakers):
    - Amazon **Alexa** on Amazon **Echo** devices,
    - 🍏 Apple **Siri** on 🍏 Apple **iOS** and **iPadOS** (iPhone 📱 smartphones and iPad 📱 tablets), **macOS** (Macintosh, iMac, iBook, and MacBook 📱 computers), and **HomePod** devices,
    - Google **Assistant** on Google **Home** and other devices,
    - Microsoft **Cortana** on PC 📱 computers (and formerly, 📱 phones) running 🍷 Microsoft **Windows**,
    - Samsung **Bixby**,
  - smart **TVs** "[Your smart TV is spying on you. Here are step-by-step instructions to stop it.](#)",
  - voice-activated **toys**,
  - more devices soon?
- Please see 🍏 [Apple Device and Data Access when Personal Safety is at Risk](#) for 🍏 Apple iPhone 📱 smartphones; iPad 📱 tablets; Macintosh, iMac, iBook, and MacBook 📱 computers; and probably **HomePod** devices.





- Watch how your smart devices are watching you, with the [Princeton IOT Inspector](#).

### 3.8 One-time: Harden your Wi-Fi router, cable modem, and doorbell camera

- **If** your Wi-Fi router's **SSID (network name)** is personalized, (e.g., [HOME-XXXX](#) or [2Wire999](#) or [yourAddress](#) or [somethingAboutYou](#)), you can **skip** this step. *If the SSID is generic (the same as all others of its type) (e.g., [Guest](#) or [Linksys](#) or [xfinitywifi](#)), change it, using the router's administrative page:*
  - **Netgear** > [www.routerlogin.net](#) or [http://192.168.1.1](#) > "admin" "password" > tab **Advanced** > left navigation bar **Setup** > **Wireless Setup** > from "[NETGEAR99](#)" to something unique, such as your address or persona. Write it on the router or paperwork. --[idea 4](#)
  - **Others**
    - Get your router's **administrative URL** from [www.techspot.com/guides/287-default-router-ip-addresses](#); or [https://www.lifewire.com/how-to-enable-your-wireless-routers-built-in-firewall-2487668](#); or [Start](#) > [Run](#) > "[cmd](#)" [Enter] > "[ipconfig](#)" [Enter] > section "**Wireless LAN adapter Wi-Fi:**" > field "**Default Gateway**" > see something like "[10.0.0.1](#)". Write that down > prefixed with "[http://](#)" (e.g., "[http://10.0.0.1](#)").
    - Get your router's **administrative username and password** from [www.howtogeek.com/131338/how-to-access-your-router-if-you-forget-the-password](#) or [www.routerpasswords.com](#) (e.g., "[admin](#)" or blank, and "[admin](#)" or "[password](#)").
    - In a new browser window, **Enter** the administrative URL you found above (e.g., "[http://10.0.0.1](#)").
    - When it asks for a username and password, give it those you found above (e.g., "[admin](#)" or blank, and "[admin](#)" or "[password](#)").
    - Bop through the admin pages (Wireless sections) until you find how to change the **SSID (network name)** to something unique, such as your address or persona. --[idea 4](#)
  - Write your new **SSID (network name)** on the router or paperwork.
  - While you are at it, ensure your wireless is using great encryption, such as [WPA3](#) (if not available, use [WPA2-PSK AES](#)). --[idea 3](#)
  - While you are at it, ensure your wireless firewall is on, and set correctly. Mine from Comcast Xfinity is set to Typical Security (Medium). **TODO:** Read more about this at [https://www.lifewire.com/how-to-enable-your-wireless-routers-built-in-firewall-2487668](#).
  - **Apply.**
  - Tell **all** your networked devices (📱 smartphones, 📱 tablets, 💻 computers, etc.) to **connect to the new SSID**. And tell them to **forget about the old generic SSID** (this is actually the goal--you don't want your mobile devices to automatically connect to a *honeypot* machine). [Under 🖥 Windows 10](#). [Under 📱 Android](#).
- If you haven't [changed your Wi-Fi router's administrative password](#), do that, using the router's administrative page:
  - **Netgear** > log onto your router's administrative page as described in the previous paragraph > tab **Advanced** > left navigation bar **Administration** > **Set Password** > from "[password](#)" to your choice. Write it on the router or paperwork. --[idea 1](#)
  - **Others** > log onto your router's administrative page as described in the previous paragraph > bop through the admin pages until you find how to change your router's **administrative password** to your choice. Write it on the router or paperwork. --[idea 1](#)
- Follow [http://cnet.com/how-to/tips-to-stay-safe-on-public-wi-fi](#).
- Or [http://komando.com/tips/370327/your-router-needs-this-one-thing-manufacturers-dont-tell-you/all](#).
- [https://www.lifewire.com/wireless-router-security-features-you-should-turn-on-right-now-2487665](#).
- **More tips.** Some steps require a [Wi-Fi Analyzer](#), of which I love and use [this one](#).
  - If your networking is slow:
    - Use this **Wi-Fi Analyzer** to find a better channel number, and tell your router to use that. [https://duckduckgo.com/?q=my+router+change+channel](#).
    - [Change your computer's DNS Servers](#). **TODO:** Look into [OpenDNS](#).
- If you have **Comcast** and they provide a Wi-Fi network [xfinitywifi](#):
  - **TODO:** Write this. A start: [review your use of its SSID](#).

- See if your **cable modem** needs a **firmware update or configuration change**:
  - **TODO: Write this.**
- See if your **doorbell camera, nannycam, or Tile** or **Apple AirTag tracker device**, needs a **firmware update or configuration change**:
  - **TODO: Write this, including stalkerware.**

### 3.9 One-time: Retiring/Donating/Disposing of a computing device

- Please see [Apple Device and Data Access when Personal Safety is at Risk](#) for **Apple iPhone**  **smartphones**; **iPad**  **tablets**; **Macintosh, iMac, iBook, and MacBook**  **computers**; and probably **HomePod** devices.
- **TODO: Write something about wiping your personal information, including possible harddrive:**
  - Looks like [CCleaner](#) Free [except in 2021, is identified by Microsoft Defender Antivirus as a PUP Potentially-Unwanted Program, and may recently be crapware] now has > tab **Tools** > tab **Drive Wiper**.
  - <http://pcsupport.about.com/od/fixtheproblem/ht/wipe-hard-drive.htm> or
  - <https://www.lifewire.com/how-to-wipe-a-hard-drive-2624527> or
  - <https://www.lifewire.com/how-to-completely-erase-a-hard-drive-2626173> or
  - <http://zdnet.com/article/windows-10-tip-reset-your-pc-completely> or
  - <https://microsoft.com/en-us/software-download/windows10startfresh> or
  - <https://www.tomshardware.com/how-to/secure-erase-ssd-or-hard-drive>.
- If you want to **keep your old harddrive**, please do so. If you later need to get data off it, you can attach to it  another computer as a **non-bootable** drive, with a [USB-SATA harddrive adapter](#) or caddy.
- **TODO: Say who to donate it to, presumably** a local person/group who refurbishes equipment for low-income low-connected people, or a local electronic recycler. In West Michigan, donate small electronics and appliances to [Comprenew](#) (larger appliances to Republic Services).

## 4 Demonstrating protesting traveling in heavily-policed authoritarian areas, or when targeted by adversaries

- View [video How to Stop a Riot](#). For full effect, select the video link, then icons □ fullscreen, cc captions, ► Play, and □ ☒ Skip Ads.
- If traveling overseas, you may want to sign up with the US Department of State [Smart Traveler Enrollment Program STEP](#).
- Be professional in exercising your First Amendment rights. Your goals are reachable only by non-violent means: education, understanding, communication and sympathy.
- Follow the recommendations in <http://ericpiehl.com/#police>.
- **Have** a plan.
  - **Test like you fly; fly like you test.** — The way I learned it [writing aviation software](#).
  - **Train like you fight; fight like you train.** — The way I heard some of our users learned it.
  - **Plan your work; work the plan.** — The way I learned it in chainsaw safety training.
  - **Fail early, and pivot.** — The way I heard it in entrepreneur startup seminars.
- Be aware that anywhere the US President goes, your mobile devices probably will be [attached by an active cell-site simulator CSS, or tracked by a passive IMSI catcher](#) (e.g., [Stingray device](#)) ([mobile cellphone surveillance at protests](#)). And various other places in the USA and around the world.
- If you cannot afford to lose \* your ☒ phone \*\*, do not take it to a protest. Leave it behind!
  - \* = have taken/compromised.
  - \*\* = tablet/computer/data (flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-sticks).
- If you think your electronic devices may be taken or compromised, consider **leaving behind** your electronic devices (☒ smartphones, ☒ tablets and ☒ computers) and data (flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-sticks).  
However, if you need them:
  - [Disable location services, backup your data, run updates, enable 2FA, install Mobile Justice App.](#)
  - [Read "China Is Forcing Tourists to Install Text-Stealing Malware at its Border"](#).If you still need your electronic devices:
  - **Back up** all data, and keep your backups in a **secure location**.
  - **Sanitize** this data so you don't have anything you don't want disclosed.
  - Be prepared to, when you return from this travel/protest/demonstration, **wipe** all data back to factory-image **before** you connect to your home network or other assets.
  - Continue . . .
- Follow these [digital security tips for protesters from the EFF](#), including its nice instructions for installing and using app [Signal Private Messenger](#) (set **Disappearing Messages**), and the EFF's older [Occupy guide](#).
- Awesome list of [support to protestors and journalists](#), including EFF's guide on [attending protests in age of COVID-19](#).
- Consider doing some counter-surveillance, using a cheap Android ☒ phone and app **Haven**. [Anonymous email](#).
- Arrange for real **media** (preferably from large organizations with technical, legal and administrative support) to attend, record and report on your event.
- If you can't have real media attend, see if the ACLU has a [Mobile Justice app for your jurisdiction](#). Said to transmit video to the ACLU as soon as you Stop recording.
- [How to Record Phone Calls on your iPhone or Android](#).
- Form a **social media team**.
- Put a spare **sock** or light glove in your [pocket](#). If **teargassed**, I hear that your group needs someone to pick up the teargas canister and throw it back. It will be hot enough to badly burn you; a sock or something will provide adequate protection if you can complete your chuck within a second or two. Or kick it back.
- [PPE \(Personal Protective Equipment\)](#). For CN and CS tear gas, 3M 60926 may be effective.
- Have a **first aid** team standing to the rear, with training and equipment, including baby shampoo and LOTS of water (to help get pepper spray out of eyes), treatment for rubber bullet wounds [1% fatal], hypothermia if soaked with water, and whatever else you may run into.
- Form a **legal team** or **support team**? Snacks? Transport? Tracking who arrested, which agency, where taken?
- **Follow** your plan.
  - **Test like you fly; fly like you test.** (The way I learned it writing aviation software.)
  - **Train like you fight; fight like you train.** (The way I heard some of our users learned it.)
  - **Plan your work; work the plan.** (The way I learned it in chainsaw safety training.)
- Best wishes!



## 5 Emergency situations: ☐ search and rescue SAR, earthquake, flood, ⚡ tornado, 🌀 hurricane

- ☐ Set up your 📱 mobile cell phone to play your **local alerts**.
  - Under Android, [gear] **Settings** > **Notifications** > **Advanced** > **Emergency alerts** > **Allow** > all.
- ☐ Assemble a **go-bag**, including:
  - **Personal Protective Equipment PPE**: sturdy shoes or boot, crew-length or taller socks, sturdy pants, long-sleeved-shirt, sturdy gloves, canvas hat or bike helmet, glasses or other eye-protection, folding saw or cutting device, etc.),
  - water, food,
  - medical supplies,
  - cash, id, phone numbers of anyone who could support you (even at a distance),
  - car-outlet/USB converter and charger cable, battery pack\*\*\*,
  - and more!
- ☐ A cousin in 🌀 hurricane country has a detailed pack list for each car, listing the various go-bags and go-boxes of living supplies for a week or more, family valuables (photos and such), etc.
  - And when authorities say to leave, they do! Early — before the freeways fill up. They take all the cars, which are filled with stuff, allowing them to stay away as long as needed.
- ☐ Fill up all cars with **gasoline**.
- ☐ **Stay healthy**, physically and mentally.
- ☐ \*\*\* = *Instead of a battery pack above, you could get an ..*  
**Emergency NOAA-alert weather-alarm radio**. It works! Nice product. I recommend it to many households.
  - *If you don't have one*, order something like <https://smile.amazon.com/dp/B07YCCJ7X4> (we did).
    - Takes **power** from a **built-in rechargeable battery**, **AAAs**, and a **hand-crank**.
    - **Radio** (of course): **NOAA weather**, **FM**, **AM** and **SW**. Not audiophile-quality, but is good enough to stay informed and feel connected.
    - Two **flashlights**: spotlight and reading. Nice. Although we have others.
    - A few other doodads. In a compact case. Ours is school-bus yellow, but the new red looks good.
  - To **configure for maximum effect**:
    - Plug radio into a **power source**, via its included micro-USB cable.
      - The micro-USB plug goes into the radio's right side, under the rubber cover, port "DC 5V".
        - [If an uber geek asks about micro-A vs. micro-B, get the micro-B.]
      - The USB-A plug goes into a laptop or housecurrent adapter with a USB-A port.
      - This will charge — and keep charged — its internal rechargeable battery.
      - We have our radio on a kitchen counter, on top of something else, out of the way. Sorta-centrally-located in our house, so we can hear it from anywhere — even while sleeping. Although, ...
      - *If your hearing is poor*, place in some central location, where the radio's left side's red flashing light will be highly-visible.
    - *With the micro-USB cable plugged into housecurrent*, set radio's **switch POWER** to **position "Li-Ion"** (its internal rechargeable battery).
    - Rotate radio's antenna pointing up, not necessarily extended.
    - Turn **knob VOLUME** up partway, so you can hear static on some bands.
      - In fact, this is a good time to play with **knob BAND** set to position **"FM"**, **"AM"** and **"SW"** (shortwave), using **knob TUNING** and various antenna directions and extension.
      - *When done playing*, ...
    - Turn **knob BAND** to position **"WB"** (weather band).
    - Try every position of **knob WEATHER BAND**. NOAA uses these 7 frequencies a bunch of weather transmitters splattered across the nation. If laid out in a hexagonal grid of the proper size, people should be able to receive 1, 2 or 3 stations, depending on where you live in that grid.
      - I looked it up — our state has 28 transmitters and 83 counties, or an average 3 counties/transmitter. More if their service areas overlap [they do].
      - For us, position "7" comes in very clear. After listening to it for a while, it said the transmitter is at a place about 16 km (10 miles) to our north.
        - Another setting is barely audible; I would guess that that transmitter would be to our southeast or southwest.
      - I could look up the correct position on [https://weather.gov/nwr/station\\_listing](https://weather.gov/nwr/station_listing).
        - But I think the pedestrian method above is more reliable.



- When done playing, ...
- Leave **knob WEATHER BAND** set to your **best local station**.
- When done listening to the radio, turn **knob VOLUME down so you can't hear it**, but **not** to position "OFF". [After rechargeable battery is fully-charged, you may be above to leave in position "OFF". But before I leave it this way, I want to test that it still alerts.]
- The radio's front should have **indicator lights**:
  - "1/0" (on/off) lit **green**, and
  - "CHARGING" lit **red** (this goes off in a couple hours, after its rechargeable battery is fully-charged).
- Go about your busy life.
- **When you:**
  - **hear a loud "WHOOOP WHOOOP WHOOOP" siren alert sound, and**
  - **see a red light flashing out the left side of the radio,**
  - **NOAA is alerting you.**
  - Walk over to the radio, and turn **knob VOLUME up** so you can hear details on your local emergency.
- A week or so after we configured the radio as above, we heard these alert siren at 11am sharp (High Noon if we weren't Sprung Forwards).
  - The alert siren **was loud enough** for me to notice from the other floor of our house, in a room with the door sorta-closed, playing a YouTube softly, while banging on my computer. Should be able to wake us.
    - But the alert siren was **not** too loud for Marty, sitting a couple meters away, on a Zoom meeting. She did have to explain it to her Zoom-mates.
    - The alert siren **lasted long enough** for me to hear it, and for my brain to deconstruct that it is an alarm of some sort, get up from my chair, leave the room, and start for the stairs. The alert siren stopped, so **not** long enough to be annoying. 15-30 seconds, maybe? Continuing, ...
    - **I walked over to the radio, and turned up the volume** so I could hear.
      - They read of a long list of stations and the counties they cover. Maybe 5-8 counties/transmitter, so I was correct above — the stations do overlap a lot, on their different frequencies.
      - The voice said **this was a test** for these areas. Then went back to normal weather info for our area. The whole process took 3 minutes.
  - Yea! I had been hoping NOAA would throw test-alerts periodically. So we would know we had the radio set up right. And it is! Nice peace-of-mind. Especially when a couple weeks later, we were alerted for major storms headed our way. About an hour in advance. Which we used to police the yard for items that might blow away, close the garage door, and plug in our phones.
- Bummer that the above process is only partly-documented in the directions.
- The radio's documentation says it can **recharge your mobile cellphone**, via the radio's right side, under the rubber cover, **port "USB CHARGING"**. And using your **mobile's charging cable**, having USB-A plug into the radio, and whatever plug goes into your cellphone (USB-C or Lightning, probably).
  - I have not yet tried this. But we have another charging stick or two.
- We currently have **not** put any **AAA batteries** into our radio. But:
  - We have lots of AAA batteries in our battery collection.
  - If alerted and then power fails, we would have lots of time to use the radio's two flashlights to go get some AAAs from our collection.
  - Backed up by our other electronics and flashlights. And the radio's windup generator, which does work. Although snuggling bed listening to the radio during a powerfailure is much easier if you don't have to sit up and wind the radio each minute.
  - Oh, as I write this at my computer with the radio unplugged, I see its indicator lights:
    - "1/0" (on/off) is **lit green**, (good, the radio is telling me our area's current weather), while
    - "CHARGING" is **not** lit **red**.
    - Thus, I am simulating a **power failure** right now, and **everything is working as it should**. OK, Saving this doc, and plugging our radio back into the wall, ready for our next extreme weather event.
- Sign up for a **Wilderness First Aid WFA** class. Nice long one. Covers much more than a couple-evening Red Cross class. Comes in handy. And helps make you the calmest person in an emergency.
- If part of a team that each needs to hear what other team members are doing, look into having your team install on their 📱 mobile cell phones communications app **Zello**. **Not** encrypted.
- If part of a team that does election monitoring and crisis response, look into [app Ushahidi](#).
- If part of a team that tracks search teams, which areas have been searched, etc., look into app **GPS Tracks**, and software **SARTopo**.
- [More emergency apps](#).
- See [section 4 "Demonstrating protesting traveling in 🇹🇿 heavily-policed authoritarian areas, or when targeted by adversaries"](#) above.

## 6 Emergency: Find or clean your 📱 📺 computing platforms

### 6.1 Emergency: Find or clean your iPhone 📱 smartphone or iPad 📺 tablet

- If your **iPhone** 📱 smartphone or **iPad** 📺 tablet is **lost** or **stolen**:
  - If you previously installed app "[Lookout](#)" [above](#), use [Lookout](#)'s features [Find My Device](#) > [Scream](#) or [Lock](#) or [Wipe](#).
  - If you did **not** previously install app "[Lookout](#)" [above](#), please see "[Find My iPhone, iPad, iPod touch, or Mac](#)". Depending on details, you can ring it to locate its exact location, lock it, or erase your personal data.
  - Or please see [🍏 Apple Device and Data Access when Personal Safety is at Risk](#) for [🍏 Apple iPhone 📱 smartphones; iPad 📺 tablets; Macintosh, iMac, iBook, and MacBook 📺 computers; and probably HomePod devices.](#)
- If you have an **iPhone** 📱 smartphone or **iPad** 📺 tablet that does not yet have **antimalware** software, please install one of:
  - [Lookout](#) or
  - [Malwarebytes](#) (free is a terrific on-demand scan, but the prevention module costs \$),
  - [from somewhere other than China](#), Russia and associated countries.
- I am familiar with **Lookout**; to install it:
  - launch app **App Store** >
  - **Q Search** for "[Lookout](#)" >
  - select iPhone/iPad app "[Lookout - Backup, Security, Find Your iPhone, iPad or iPod touch](#)" "[Free](#)" from **Lookout Mobile Security** with icon of a **white-on-green shield** >
  - click button [Free](#) >
  - install free version.
  - Launch.
  - Sign in – with an email address and password.
  - **≡ Settings > Theft Protection > top tab Locate My Device**
    - > turn on **Location** (helped me greatly, at least once!),
    - > turn on **Scream** (helped me **immensely**, and M!);
    - and anything else you can.
  - Consider **≡ Settings > Backup**.

**Lookout** will protect your device from **new threats**.

**Lookout** will periodically run scans to remove **existing threats**. Lately, once a day. Run a scan right now, by launching app [Lookout](#) > tab [Security](#) > button [Scan Now](#).

**Lookout** has a nice feature ("**Signal Flare**", I think) where, if your 📱 Android or iPad finds itself running out of battery, it finds out where it is and ✉ emails you its location (granular enough to see which building it is in, not where in that building). Cool!

**Lookout** tells you if there is a **software update** to your iPad, and if needed, how to get that update (connect iPad to Mac or PC > if iTunes does not auto-launch, launch it > when prompted to update the iPad software, click "[Download and Update](#)").

**Lookout** will automatically backup your **Contacts list** to the Cloud, from where you can download it at any time.

**Lookout Pro** will automatically backup your **photos** (¿videos?) to the Cloud, from where you can download it at any time. *If you take photos (¿videos?) at risk if your 📱 phone should get lost or confiscated by the authorities*, check out whether backups happen automatically, how often it happens, and if it includes videos, and if OK, **upgrade** to Lookout Pro for \$30/year and turn on photo backup.

**Lookout** will (I imagine) occasionally ask you to **update** itself. Please tell it Yes.

- If relevant, follow steps in [Domestic abuse paper from 🍏 Apple](#) in 2021.
- Ensure you have all your **old apps**, and they are **hooked up** and operating correctly. For example:

- **Lookout** (above).
  - **Phone** and **Messaging**, including **Contacts**.
  - **Maps**.
  - Weather.
  - News.
  - Email..
  - Calendar
  - **iCloud**, including re-setting your Offline files.
  - Costco Pharmacy.
  - **Tasks**.
  - **Dropbox**, including re-setting your Offline files.
  - **iPhoto**.
  - ACLU **Mobile Justice app** for your jurisdiction.
  - Local sheriff or police app, including signing up for local Groups relevant to you.
  - iNaturalist.
  - Wi-Fi Analyzer.
- Set all relevant **emergency settings** that didn't get done above, including:
- [gear] **Settings > Security > Device admin apps** > allow **Lookout**, **Find My Device** and **ACLU Enable Lock Screen on Trigger**.
- Set all relevant **ease-of-use settings** that didn't get done above, including:
- setting **volume-levels** and **ringtones** that you can actually hear. **How?**
- If needed, rebuild your **home screen**, by adding icons for:
- Contact of your sweetie.
  - Your favorite [software for digital video virtual web-based meetings, conferences, gatherings or webinars](#).
  - YouTube.
  - Clock.
  - Your favorite websites (e.g., [ericpiehl.com](http://ericpiehl.com) and [iCanSeeNature.com](http://iCanSeeNature.com)).
- [To take a screenshot on \[phone icon\] iOS or \[phone icon\] Android](#) (and probably [phone icon] iPadOS).
- On [laptop icon] **Windows**, do one of:
- **Win+Start** > type "**snip**" > wait > desktop app **Snipping Tool** > **New** > mouse drag rectangle you want > **Exit** > Save=**Yes** > to **.png** or **.tiff** format (lossless!), not **.jpg** (lossy!).
  - **Win+Shift+S** > choose a shape > drag your area > do something with your results in the Clipboard or Notification.
- [Disable ad id tracking, and why you should do it now](#).
- After you finish these Emergency steps, make a note to come back tomorrow, to continue with the [Monthly section](#) below.

## 6.2 Emergency: Find or clean Android smartphone or tablet, or Chromebook

- If your **Android** [phone icon] smartphone or [phone icon] tablet, or [laptop icon] Chromium OS **Chromebook** device is **lost** or **stolen**:
  - If you previously installed app "**Lookout**" [above](#), use **Lookout**'s features **Find My Device** > **Scream** or **Lock** or **Wipe**.
  - If you did **not** previously install app "**Lookout**" above, please see <https://myaccount.google.com/security> or "[How to use Google to find your lost Android phone](#)". Depending on details, you can locate its exact location, lock it, or erase your personal data.
- [What to do with Android in water](#).
- If you have an **Android** [phone icon] smartphone or [phone icon] tablet, or [laptop icon] Chromium OS **Chromebook** device that does not yet have **antimalware** software, please install one of:
  - **Lookout**,
  - **Malwarebytes** (free is a terrific on-demand scan, but the prevention module costs \$),
  - [Sophos Mobile Security for Android](#) or
  - [other options](#);

- [from somewhere other than China](#), Russia and associated countries.
- I am familiar with **Lookout**. To install it:
  - launch app **Play Store** (icon may be on its own, may be in folder Google) >
  - **Q Search** for "**Lookout**" >
  - select Android app "**Lookout Security and Antivirus**" from **Lookout Mobile Security** with icon of a **white-on-green shield** >
  - click button **Free** >
  - install free version.
  - Launch.
  - Sign in – with an email address and password.
  - **≡ Settings** > **Theft Protection** > top tab **Locate My Device**
    - > turn on **Location** (helped me greatly, at least once!),
    - > turn on **Scream** (helped me **immensely**, and M!);
    - and anything else you can.
  - Consider **≡ Settings** > **Backup**.

**Lookout** will protect your device from **new threats**.

**Lookout** will periodically run scans to remove **existing threats**. Lately, once a day. Run a scan right now, by launching app **Lookout** > tab **Security** > button **Scan Now**.

**Lookout** has a nice feature "**Scream**" that makes it make a loud noise. I used it once when my granddaughter dumped my ☞ phone into a toybox while I was distracted for a second. A lifesaver! It also has a nice feature ("**Signal Flare**", I think) where, if your ☞ Android or iPad finds itself running out of battery, it finds out where it is and ✉ emails you its location (granular enough to see which building it is in, not where in that building). Cool!

**Lookout** will automatically backup your **Contacts list** to the Cloud, from where you can download it at any time.

**Lookout Pro** will automatically backup your **photos** (¿videos?) to the Cloud, from where you can download it at any time. *If you take photos (¿videos?) at risk if your ☞ phone should get lost or confiscated by the authorities*, check out whether backups happen automatically, how often it happens, and if it includes videos, and if OK, **upgrade** to Lookout Pro for \$30/year and turn on photo backup.

**Lookout** will occasionally ask you to **update** itself. Lately, twice a year or so. Please tell it Yes.

- A **Motorola** ☞ phone I saw with Android 5.1 said it also has functions to **locate**, **lock** or **wipe** your ☞ phone, if you first use app **Moto** to activate device administrator, link to a Google account (you almost certainly did when you first got it), and later (when you need to locate, lock or wipe it?) log in to [www.motorola.com/support](http://www.motorola.com/support).
- To ensure your **Android** ☞ smartphone or ☞ tablet device does not suffer from the [Stagefright Flaw](#) of 2015-07-27, please:
  - launch app **Play Store** (icon may be on its own, may be in folder Google) >
  - **Q Search** for "**Stagefright Detector**" >
  - select Android app "**Stagefright Detector**" from **Lookout Mobile Security FREE** with white-on-green sad-face shield >
  - **Install**.
  - When installed, **Open** it.
    - If it says "**Everything is OK**", it is. *If you wish*, uninstall the app.
    - If it says your device is affected and the vulnerable behavior is enabled, please follow-up with "More info" or your local techie.
- To ensure your **Android** ☞ smartphone or ☞ tablet device does not suffer from the [Heartbleed Flaw](#) of 2014-04-09, please:
  - launch app Google **Play Store** >
  - **Q Search** for "**Heartbleed**" >

- select Android app "[Heartbleed Detector](#)" from **Lookout Mobile Security FREE** with white-on-green dripping-heart shield >
- [Install](#).
- When installed, [Open](#) it.
  - If it says "[Everything is OK](#)", it is. *If you wish*, uninstall the app.
  - If it says your device is affected and the vulnerable behavior is enabled, please follow-up with "More info" or your local techie.
- If you are having **battery duration** problems:
  - *If you use Republic Wireless*, [report your battery drain](#). Regardless of this ...
  - Launch Android app [gear] **Settings** >
    - **Battery** > select **each** app to see any settings that can reduce battery use.
    - **Battery** > ☰:hamburger icon in upper-right > **Battery saver** > Turn on automatically > at 15%.
    - **Location** > **Mode**=Battery saving.
- [To take a screenshot on](#) [📱 iOS or 📱 Android](#) (and probably [📱 iPadOS](#)).
- On [🖥 Windows](#), do one of:
  - [⌘Start](#) > type "[snip](#)" > wait > desktop app **Snipping Tool** > **New** > mouse drag rectangle you want > **Exit** > Save=**Yes** > to **.png** or **.tiff** format (lossless!), not **.jpg** (lossy!).
  - [⌘Win+Shift+S](#) > choose a shape > drag your area > do something with your results in the Clipboard or Notification.
- Examine [gear] **Settings** > [[Google](#) >] **Location**.
- Examine **Google Settings** > **Ads** > **Opt out of Ads Personalization**.
- [Disable ad id tracking, and why you should do it now](#).
- [Follow these Android tips](#). And [these Android security tips](#).
- [If you have to \(most of the early ones look OK\)](#).
- After you finish these Emergency steps, make a note to come back tomorrow, to continue with the [Monthly section](#) below.

## 6.3 Emergency: Find or clean your 🖥 computer

If you **lost** your 🖥 computer:

- 🍏 If **Apple macOS** (Macintosh, iMac, iBook, and MacBook 🖥 computers), please see "[Find My iPhone, iPad, iPod touch, or Mac](#)".
  - Or please see [🍏 Apple Device and Data Access when Personal Safety is at Risk](#) for 🍏 **Apple iPhone** 📱 **smartphones**; **iPad** 📱 **tablets**; Macintosh, iMac, iBook, and MacBook 🖥 computers; and probably HomePod devices.
- 🗑 If **Microsoft Windows** 🖥 computer: **TODO: write this.**

If your **harddrive** is **failing**, or your system is **badly compromised**, or you or your local geek are **scared**:

- If *laptop*, do a powerbutton long-press (at least 60 seconds). Unplug it. *If the battery is removable*, remove the battery.
- If *desktop*, pull the plug.
- Do **not** restore power your 🖥 computer again.
- Ask your local uber-geek for help; perhaps me, if you are close. Ask your geek to:
  - Remove your harddrive, and attach to it another computer as a **non-bootable** drive, perhaps with a [USB-SATA harddrive adapter](#) or caddy (docking station).
  - Look at the contents there, and clean or rebuild it, or copy your data to another drive.
- If *your computer is old*, buy a new one, reinstall your old software, and get your data from above.
- If *your computer is new*, find out from your geek above whether your harddrive can be cleaned. If No, buy a new harddrive, reinstall your old software, and get your data from above.
- When this happened to a close family member, s/he called me. I told him/her to do the above. Who did! I was impressed how fast everything was back up and running. Scary when you are in the middle of it; fine after recovery complete.
- [Harddrive testing programs](#).

If you **can't log on** to your computer or have a serious problem not as bad as above, ask your local geek for help; perhaps me, if you are close. If your local geek is me, I might look at:

- [I've Been Hacked! Now What?](#).
- [How to Hack Into Your Own Computer](#).
- [How To Fix a Computer That Won't Turn On](#).
- [How To Fix a Computer That Turns On But Displays Nothing](#).
- The notes I have somewhere on what I did in the past.

If you **can't fix your computer, and need help**, under ☐ Microsoft Windows:

- Find a good technically-proficient friend, that you trust a lot, to help.
- Have them click ☐ **Start** > type "**quick assist**" > wait for app **Quick Assist** to appear > launch it > button **Give assistance** > logon > and when they are set up and receive a 6-digit security code, give you the code that they got.
- Then you click ☐ **Start** > type "**quick assist**" > wait for app **Quick Assist** to appear > launch it > button **Get assistance** > type the 6-digit security code you got from your friend.
- They can now run your computer from their computer, and (perhaps) fix it.
- Let me know how this works out!

On **any** computer in your household suspected as being compromised:

- If your computer does not yet have **antimalware** software, **install** one, [from somewhere other than China](#), Russia and associated countries.
- I recommend these free-for-personal-use:
  - 🍏 For **Apple macOS** (Macintosh, iMac, iBook, and MacBook) ☐ computers:
    - [Sophos AntiVirus for Mac Home Edition](#) (recommended by [UM](#) and [Cryptoparty Ann Arbor](#)), or
    - If you get your Internet via **Comcast**, you can get Norton Internet Security **free**:
      - Install under Comcast, from <https://internetsecurity.xfinity.com>.
      - Later, it will update itself from anywhere in the solar system with Internet access.
      - I mildly dis-recommend it.
    - I **dis-recommend Kaspersky** Anti-Virus or Kaspersky Internet Security due to (2015-2017-?) claims of close ties to Russian military and intelligence officials. I previously liked the company. I will keep my ears open for more developments.
    - [Current recommendations \(very good\) from the University of Michigan](#).
    - [Recommendations from Lifewire](#).
    - [Other recommendations from Lifewire](#).
  - 🐧 For **Linux**:
    - [Current recommendations \(very good\) from the University of Michigan](#).
    - [Other recommendations from Lifewire](#).
  - ☐ For **Microsoft Windows 10**:
    - **Microsoft Defender Antivirus** (app **Windows Security**). Already installed.
      - Verify that Microsoft Defender Antivirus (app Windows Security) is running, and updates itself. To do that:
        - Click ☐ **Start** > type "**defender**" > wait for **Windows Security app** (formerly **Windows Defender desktop app**) to appear > launch it.
        - Look for:
          - **Virus & threat protection > Real-time protection=On,**
          - **Virus and spyware definitions=Up to date,** and
          - (assuming MWD installed more than a couple weeks ago) **Last-scan=sometime in the last week.**
        - If these are true, you are protected.
      - If Microsoft Defender Antivirus (app Windows Security) is **not** running, continue... Or I read that MWD is adequate for most users for most purposes; *if you want better protection*, install one of (after you do so, MWD will turn itself off)...
    - [Avast! Free Antivirus Essential](#) > Free Download (trying this now), or
    - [Avira AntiVir Personal](#), or
    - [E-Prot](#) (liked it a lot when I used some years ago when it had a free version), or
    - [Malwarebytes](#) (free is a terrific on-demand scan, but the prevention module costs \$), or
    - If you get your Internet via **Comcast**, you can get Norton Security software **free**:
      - Install under Comcast, from <https://internetsecurity.xfinity.com>.
      - Later, it will update itself from anywhere in the solar system with Internet access.



- I mildly dis-recommend it.
- I **dis-recommend Kaspersky** Anti-Virus or Kaspersky Internet Security due to (2015-2017-?) claims of close ties to Russian military and intelligence officials. I previously liked the company. I will keep my ears open for more developments.
- [Current recommendations \(very good\) from the University of Michigan.](#)
- [Other recommendations from Lifewire.](#)
- ☒ For **Microsoft Windows 8.1**:
  - **Microsoft Defender Antivirus** (app **Windows Security**). [Alleged to be already installed.](#) Oops, when I checked a friend's machine, MWD was **not** installed--or maybe a subset. Please continue...
    - Verify that Microsoft Defender Antivirus (app Windows Security) is running, and updates itself. To do that:
      - Click **Start** > type "**defender**" > wait for **Windows Security app** (formerly **Windows Defender desktop app**) to appear > launch it.
      - Look for:
        - **Virus & threat protection > Real-time protection=On,**
        - **Virus and spyware definitions=Up to date,** and
        - (assuming MWD installed more than a couple weeks ago) **Last-scan=sometime in the last week.**
      - If these are true, you are protected.
    - If Microsoft Defender Antivirus (app Windows Security) is **not** running, continue... Or I read that MWD is adequate for most users for most purposes; *if you want better protection*, install one of (after you do so, MWD will turn itself off)...
    - [Avast! Free Antivirus Essential](#) > Free Download (trying this now), or
    - [Avira AntiVir Personal](#), or
    - [F-Prot](#) (liked it a lot when I used some years ago when it had a free version), or
    - [Malwarebytes](#) (free is a terrific on-demand scan, but the prevention module costs \$), or
    - *If you get your Internet via Comcast*, you can get Norton Security software **free**:
      - Install under Comcast, from <https://internetsecurity.xfinity.com>.
      - Later, it will update itself from anywhere in the solar system with Internet access.
      - I mildly dis-recommend it.
    - I **dis-recommend Kaspersky** Anti-Virus or Kaspersky Internet Security due to (2015-2017-?) claims of close ties to Russian military and intelligence officials. I previously liked the company. I will keep my ears open for more developments.
    - [Current recommendations \(very good\) from the University of Michigan.](#)
    - [Other recommendations from Lifewire.](#)
  - ☒ For **Microsoft Windows 7, Vista or XP** (and 8.0 and any version other than Windows 10):
    - [Upgrade Windows now! Really!](#) Until you do, continue ...
    - [Microsoft Security Essentials MSE](#) **(TODO: get new link)** (recommended by [UM](#)) if free this week, or
      - If MSE is **not** running, continue... Or I read that MSE is adequate for most users for most purposes; *if you want better protection*, install one of (after you do so, MSE will turn itself off) ...
    - [Avast! Free Antivirus Essential](#) > Free Download (trying this now), or
    - [Avira AntiVir Personal](#), or
    - [F-Prot](#) (liked it a lot when I used some years ago when it had a free version), or
    - [Malwarebytes](#) (free is a terrific on-demand scan, but the prevention module costs \$), or
    - *If you get your Internet via Comcast*, you can get Norton Security software **free**:
      - Install under Comcast, from <https://internetsecurity.xfinity.com>.
      - Later, it will update itself from anywhere in the solar system with Internet access.
      - I mildly dis-recommend it.
    - I **dis-recommend Kaspersky** Anti-Virus or Kaspersky Internet Security due to (2015-2017-?) claims of close ties to Russian military and intelligence officials. I previously liked the company. I will keep my ears open for more developments.
    - [Current recommendations \(very good\) from the University of Michigan.](#)
    - [Other recommendations from Lifewire.](#)
  - For **servers**:
    - [Current recommendations \(very good\) from the University of Michigan.](#)
  - For total expert needs, see [Communications Security Establishment CSE Assemblyline](#) and [Krebs on Security blog](#).
- Update your **antimalware/antivirus rules**.
- **Reboot** (if under Windows, **Start** > **1/0 Power** > **Restart**).
- Run antimalware/antivirus **full-scan**.
- Update your **antimalware/antivirus rules**.
- Repeat these last five steps until **clean**.


- Install [Microsoft Security Scanner](#), and run it until clean. I used this and the below to get rid of some troublesome adware/potentially unwanted programs PUP.
- *If you don't use [Malwarebytes](#) antimalware*, install the **free** version, boot to **Safe Mode**, and **run it** until clean. I used this and the above to get rid of some troublesome adware/potentially unwanted programs PUP.
- *If you don't feel comfortable after the above*, I see there is (to install, follow the links, might be free):
  - Norton > Security > Run Scans > [Norton Power Eraser](#) utility. When I tried this when not in trouble, it complained about two apps. However, I have and like these apps, so I told NPE not to do anything. Bottom line, I have not yet found it useful.
  - [Norton Bootable Recovery Tool](#). I have not yet used this.
  - [If don't have Norton Security software at this time.](#)
- *If you use web browser **Chrome***, periodically use the [Chrome cleanup tool](#) ([discussion](#)).
- For your *other* web browsers (e.g., **Firefox, Edge, Chrome, Safari, Opera, Internet Explorer, Vivaldi or Brave**).
- *If paranoid*, turn on **Start** > [gear] **Settings** (formerly **Control Panel**) > **Controlled Folder Access** > **On**.
  - Be prepared for, sometime in the following days and weeks, that an application may **fail to do its job properly**, while Windows Notify tells you it was **because Controlled Folder Access prevented it**. So far, this has happened to me with apps **Dropbox** and **Quicken**. When this happens, you need to:
    - come back here and **Allow an app through Controlled folder access** >
    - **+ Add an allowed app** >
    - the app that was just prevented.
    - Exit your app, reenter, and you should be fine (I am).
- *If you are having any networking issues, and running* **Microsoft Windows 10**, run **Start** > **Network Status** > **Network Troubleshooter**.
- *If you are having any networking issues, run:*
  - **"ipconfig /all"**,
  - **"ipconfig /release"**,
  - **"ipconfig /renew"**,
  - **"ipconfig /all"**,
  - **"exit"**.
- And see [Ten Windows 10 network commands everyone should know](#).
- *If you are still having any networking issues, and running* **Microsoft Windows 10**, run **Start** > **Network Status** > **Network Reset** > **Reset**.
- You might be able to do some of the below, by **Start** > [gear] **Settings** > icon **Update & security** > left-tab **Recovery** > section **Advanced startup** > button **Restart now** > wait for reboot > **Troubleshoot** > **Advanced options** > **Startup Repair** > **Diagnosing your PC**.
- **Microsoft Windows 10 new file recovery app**.


*If I ever get the **Blue Screen of Death BSoD** or **other scary messages**:*

- Do a power-cycle: do a power-button long-press (at least 60 seconds).
- Bring up your computer into manufacturer diagnostics: press the **power-button** briefly, and start hitting key **Esc** (or **F2** or **F10**) repeatedly.
  - On a HP laptop, repeatedly hit **Esc**, and after the screen comes up, **F2** will take you to the diagnostics
  - Will come up in some diagnostics from the manufacturer, such as **HP system Extensive Test** or **HP PC Hardware Diagnostics UEFI**. Run some!
- Write down the results, or from inside the test software, or find their logs on your harddrive.
- While there, get other diagnostic files **\*.txt** and **\*.log** from:
  - [file:///%windir%\debug\WIA\](#).
  - [file:///%windir%\Logs\CBS\](#).
  - [file:///%windir%\Logs\DISM\](#).

- o <file:///C:/Windows/System32/logfiles/SRT/>
- o <file:///C:/Windows/>.
- o <file:///C:/SystemDrive/>.

Regardless of the **Blue Screen of Death BSoD** or **other scary messages**, continue ...

-  If your Microsoft Windows computer runs **slower** than it used to, and you don't need your computer for several hours (overnight or longer?), check for dodgy harddrive disk sectors--and fix them--by **running**:
  - o **Win+X** (or right-click of **Start** icon) > **Windows PowerShell (Admin)** or **Command Prompt (Admin)** > type "**chkdsk /F /R /X /B c:**" (no quotes) [Enter] > type "**Y**".
  - OR-
  - o **Start** > **File Explorer/This PC** > [formerly **Windows Explorer/My Computer**, and still called **Windows Explorer** under-the-covers] > **C:** > right-click **Properties** > tab **Tools** > area **Error checking** "**This option will check the drive for file system errors**" > button **Check [Now...]** > if you see checkboxes, check **both** > **Scan Drive** [or **Start** > **Schedule disk check**].
  - o **Finish what you are doing**, and only when your computer is **plugged in** and you **don't need it for several hours** (overnight or longer?), **Reboot** (**Start** > **1/0 Power** > **Restart**) and let her run!
  - o To see the results, **TODO: write this**. Apparently, redirect operators **>** or **>>** are not enough.
- If you are going to ask me for support, please **run** and have ready for me:
  - o "**msinfo32**" > **Export** > **somewhereGood\myComputer\_MSINFO32.txt** > **Save**,
  - o navigate **somewhereGood**, "**ipconfig /all**" > **myComputer\_IPCONFIG.txt** [Enter],
  - o "**diskpart**", "**list volume**", "**exit**", and save the results in one of the files above, and
  - o **Powershell** "(Get-WmiObject -query 'select \* from SoftwareLicensingService').OA3xOriginalProductKey" and save the results in one of the files above.
  - o A copy of <file:///C:/Windows/Logs/CBS/CBS.log>.
  - o Then when we get together, we will ...
- **Run** the various tools (free on Windows) in "**msconfig**" [Enter] tab **Tools**, including **mmc**.
- Run **Win+X** (or right-click of **Start** icon) > **Windows PowerShell (Admin)** or **Command Prompt (Admin)** > type "**sfc /VERIFONLY**" (no quotes) [Enter].
  - o If it shows anything bad, stay in the Admin command prompt, enter "**sfc /scannow**" [Enter]. It will take a while — a half-hour or so.
    - [This article says you may have to run it 3 times](#). In between, reboot, until it runs clean (fixes no errors).
- And:
  - o "**dism /Online /Cleanup-Image /CheckHealth**",
  - o "**dism /Online /Cleanup-Image /ScanHealth**",
  - o "**dism /Online /Cleanup-Image /RestoreHealth**",
  - o reboot, and
  - o run "**sfc /scannow**" a fourth time.
- If all this didn't correct everything, look for guidance on commands **chkdsk**, **sfc** and **dism** at <https://duckduckgo.com/?q=chkdsk+sfc+dism> or <https://google.com/search?q=chkdsk+sfc+dism>.
- Then have your local techie look at the output of your commands and their logs <file:///C:/Windows/Logs/CBS/CBS.log> and <file:///C:/Windows/Logs/DISM/dism.log>.
- Determine that you have your **computer** manufacturer's **Support Assistant** (if under Windows, **Start** > scroll down list of programs), or install it now.
  - o For example:
    - [HP Support Assistant](#), and
    - [HP PC Hardware Diagnostics](#).
  - o Run relevant of its/their:
    - **Updates** to any software or firmware,
    - **Operating System checks** (if any Fail, keep logs),
    - **System tests** (if any Fail, keep logs),
    - **Hardware tests** (if any Fail, keep logs),
    - **Diagnostic tests** (if any Fail, keep logs), and
    - **Optimizations**.

- Determine that you have your computer **chip** manufacture's *Support Assistant* (if under Windows, **Start** > scroll down list of programs), or install it now.
  - For example:
    - **Intel® Driver & Support Assistant DSA**.
    - **AMD** Catalyst Control Center.
  - Run relevant of its:
    - **Updates** to any software or firmware,
    - **System tests** (if any Fail, keep logs), and
    - **Diagnostic tests** (if any Fail, keep logs).
- [Remove the Fluff From Windows 10 With Windows Decrapifier & Debloater](#).
- If you have MS Outlook, [repair your MS Outlook .pst files](#) using command **scanpst**.
- If you **still** have problems with your PC, [reset your Windows PC to fix major problems](#), or <http://zdnet.com/article/windows-10-tip-reset-your-pc-completely> or <https://microsoft.com/en-us/software-download/windows10startfresh> or <https://lifewire.com/how-to-clean-install-windows-2624904>.
  - If **Microsoft Windows**  computer, may involve **Start** > [gear] **Settings** > icon **Update & security** > left-tab **Recovery** > section **Advanced startup** > button **Restart now** > wait for reboot > **Troubleshoot** > **Advanced options** > **Startup Repair** > **Diagnosing your PC**.
- To **reset to the factory image**, under Windows 10, **Start** > [gear] **Settings** > icon **Update & security** > left-tab **Recovery** > section **Recovery** > button **Get Started**. Worked great for a family member!
- [How to fix a computer that won't turn on](#).
- After you finish these Emergency steps, make a note to come back tomorrow, to continue with the [Monthly section](#) and [Quarterly section](#) below. Meanwhile, continue here with section ["6.4 Emergency: Change your !\[\]\(144980d038f2541d7b588a8a9132bd70\_img.jpg\) email and other passwords" ...](#)

### 6.3.1 Emergency: Fix up **M's** computer

To get **printer** to listen to you:

- Hover mouse over Windows Wi-Fi symbol; verify that your computer is connected to the same Wi-Fi network as your printer (in our house, "**NativePl\_\_\_\_\_**").
  - If not, connect to it.
- Power down other computers on this Wi-Fi network.
- Reboot printer.
- Reboot your computer.
- Move your computer closer to printer (be in same room).

To get computer to **show different content** on **second screen** versus the laptop screen:


- **Win+P** > **Extend**, or
- **Start** > type "**project**" > select **Project to a Second Screen** (System settings) > **Extend**, or
- **Start** > [gear] **Settings** > **System** > left navigation bar **Display** > scroll way down > set dropdown **Multiple displays** to value=**Extend these displays**.

To get back your Microsoft Office **ribbon bar**:

- Mouseclick, in the upper right corner, the little chevron "**v**".

## 6.4 Emergency: Change your email and other passwords

If I told you to harden your   computing platforms, no, you aren't done yet. Please continue:

- **Change** your  **email password** to something [unique \(not the same as any of your other passwords\)](#). Change to using your new email password on **all platforms** on which you use this email address!
- For many purposes, consider a [disposable email account](#).

- **Change** the answers to each of your backup-authentication questions — the *name of your first pet*, and whatever. Lie; don't use anything that can be looked up.
- If your ☒ email provider offers **two-factor authentication 2FA/2-step verification/multi-factor authentication MFA**, use it. 2FA/2SV/MFA authenticate you by using two or more of these methods:
  - something-you-**know** (*knowledge*, such as a username and password),
  - something-you-**have** (*possession*, such as a SMS text account on a ☒ cellphone), and
  - something-you-**are** (*inheritance*, such as fingerprints or eyeball imagery).
 Google's 2FA uses the first two methods, with the second method giving you a [one-time password OTP](#). Initially, it had some teething pains, but since 2014, has been great. Yahoo's even works great.
- If you cannot/will not use a vendor's 2FA/2SV/MFA authentication, **look into app Authy**.
- 2FA/2SV/MFA are not perfect — they do **not** protect against [man-in-the-middle MitM attacks](#), nor if your attacker has also gained access to your ☒ phone's SMS account — , but they do reduce your attack surface.
- For **any** provider that offers **two/multi-factor/step authentication/verification**, **use it!**
- Change any **other password** with the **same value** as your **old** ☒ **email password** (consider these compromised, too!), making the new password unique — right? Change on **all platforms** on which you use these passwords!
- Check if you have any accounts **compromised in announced data breaches**, at [Have I Been Pwned?](#) (HIBP) (built by an Aussie computer geek) > [your@email.address](#) and [usernames](#) > **pwned?**. And take appropriate action:
  - To get notified when **future** pwnage occurs and your account is compromised, [Have I Been Pwned?](#) > nav **Notify me** > [your@email.address](#).
  - If you have custom email addresses in form [you@yourDomain](#), you can get notified of pwnage of any of them via [Have I Been Pwned?](#) > nav **Domain search** > [yourDomain](#) > etc.
  - If you are considering a new password, [Have I Been Pwned?](#) > nav **Password** > [yourPassword](#) > **pwned?**.
  - [Helps on correcting your credit Reports](#).
- To recover from the [Heartbleed Flaw](#) of 2014-04-09, if you haven't done so since this date, please:
  - Change all your passwords at sites listed by [www.cnet.com/how-to/which-sites-have-patched-the-heartbleed-bug](#) and/or [www.mashable.com/2014/04/09/heartbleed-bug-websites-affected/?cid=146326](#):
    - "Vulnerability patched. Password change recommended": Do that.
    - "Awaiting response": Change your password.
    - "Was not vulnerable": I think you are OK (I trust CNET, mostly). If site is important to you, change your password.
    - *Not listed*: Change your password.
  - If you **host** any websites, patch them. Does this include Apache HTTP Server? Mine is turned off — isn't it? Gotta go find out how to check, and read [www.eff.org/search/site/heartbleed](#) ...
- OK, **relax** some:
  - If your machines were clean, but your ☒ **Yahoo email** was hacked, it must have been done on **Yahoo's servers**. You were cool.
  - Pour yourself a glass of wine. [Let me know how it went!](#)
  - Get a good night sleep, but come back tomorrow, to continue with the [Monthly section](#), to the end ...

## 6.5 Emergency: Harden your Wi-Fi router, cable modem, and doorbellcam

- If your Wi-Fi router's **SSID (network name)** is personalized, (e.g., [HOME-XXXX](#) or [2Wire999](#) or [yourAddress](#) or [somethingAboutYou](#)), you can **skip** this step. If the SSID is generic (the same as all others of its type) (e.g., [Guest](#) or [Linksys](#) or [xfinitywifi](#)), change it, using the router's administrative page:
  - **Netgear** > [www.routerlogin.net](#) or [http://192.168.1.1](#) > "admin" "password" > tab **Advanced** > left navigation bar **Setup** > **Wireless Setup** > from "[NETGEAR99](#)" to something unique, such as your address or persona. Write it on the router or paperwork. --[idea 4](#)
  - **Others**



- Get your router's **administrative URL** from [www.techspot.com/guides/287-default-router-ip-addresses](http://www.techspot.com/guides/287-default-router-ip-addresses); or <https://www.lifewire.com/how-to-enable-your-wireless-routers-built-in-firewall-2487668>; or **Start** > **Run** > "**cmd**" [Enter] > "**ipconfig**" [Enter] > section "**Wireless LAN adapter Wi-Fi:**" > field "**Default Gateway**" > see something like "**10.0.0.1**". Write that down > prefixed with "**http://**" (e.g., "**http://10.0.0.1**").
- Get your router's **administrative username and password** from [www.howtogeek.com/131338/how-to-access-your-router-if-you-forget-the-password](http://www.howtogeek.com/131338/how-to-access-your-router-if-you-forget-the-password) or [www.routerpasswords.com](http://www.routerpasswords.com) (e.g., "**admin**" or blank, and "**admin**" or "**password**").
- In a new browser window, **Enter** the administrative URL you found above (e.g., "**http://10.0.0.1**").
- When it asks for a username and password, give it those you found above (e.g., "**admin**" or blank, and "**admin**" or "**password**").
- Bop through the admin pages (Wireless sections) until you find how to change the **SSID (network name)** to something unique, such as your address or persona. --[idea 4](#)
- Write your new **SSID (network name)** on the router or paperwork.
- While you are at it, ensure your wireless is using great encryption, such as **WPA3** (if not available, use **WPA2-PSK AES**). --[idea 3](#)
- While you are at it, ensure your wireless firewall is on, and set correctly. Mine from Comcast Xfinity is set to Typical Security (Medium). **TODO:** Read more about this at <https://www.lifewire.com/how-to-enable-your-wireless-routers-built-in-firewall-2487668> and <https://www.lifewire.com/how-to-test-your-firewall-2487969>.
- **Apply.**
- Tell **all** your networked devices (📱 smartphones, 📱 tablets, 💻 computers, etc.) to **connect to the new SSID**. And tell them to **forget about the old generic SSID** (this is actually the goal--you don't want your mobile devices to automatically connect to a *honeypot* machine). [Under 📱 Windows 10](#).
- If you haven't [changed your Wi-Fi router's administrative password](#), do that using the router's administrative page:
  - **Netgear** > while still logged on to your router's administrative page above > tab **Advanced** > left navigation bar **Administration** > **Set Password** > from "**password**" to your choice. Write it on the router or paperwork.
  - **Others** > while still logged on to your router's administrative page above > bop through the admin pages until you find how to change your router's **administrative password** to your choice. Write it on the router or paperwork.
- If you have **Comcast** and they provide a Wi-Fi network [xfinitywifi](#):
  - **TODO:** Write this. A start: [review your use of its SSID](#).
- See if your **cable modem** needs a **firmware update or configuration change**:
  - **TODO:** Write this.
- See if your **doorbell camera, nannycam, or Tile** or 🍏 **Apple AirTag tracker device**, needs a **firmware update or configuration change**:
  - **TODO:** Write this, including stalkerware.
- Follow <http://cnet.com/how-to/tips-to-stay-safe-on-public-wi-fi>.
- Or <http://komando.com/tips/370327/your-router-needs-this-one-thing-manufacturers-dont-tell-you/all>.
- After you finish these Emergency steps, make a note to come back tomorrow, to continue with the [Monthly/Quarterly section](#) below.

## 7 Monthly/Quarterly: Harden your 📱 📺 computing platforms

By "harden", I mean the process of securing a system, by reducing its *surface of vulnerability* (its *attack surface*), and making it more *resilient* to attack.

This monthly section assumes that you previously followed the [one-time suggestions in section 3](#).

### 7.1 Monthly: Harden your iPhone 📱 smartphone or iPad 📺 tablet

- On your home screen, if App "[gear] **Settings**" has a number by it, click on it, and handle the message, including "Software Update".
- On your home screen, if App "**App Store**" has a number by it, click on it, and handle the message, including "Update".
- If in "[2.2 One-time: Harden your iPhone 📱 smartphone or iPad 📺 tablet](#)" above, you installed **Lookout** to **not** auto-update itself, it will (I imagine) ask you for an update:
  - Please do that.
  - If you wish to run a scan now, launch app **Lookout** > tab **Security** > button **Scan Now**.
- [Clear your browser's cache](#).
  - If you have browser Chrome, follow the few steps in <https://support.google.com/chrome/answer/2765944> > tab **iPhone & iPad**.
- If you get junk **robocalls** on your 📞 **landline**:
  - Set up call-blocking call-blocker app [Nomorobo](#) (awesome!), free on most VoIP landlines (a landline provided digitally — perhaps from your cable TV provider).
  - Or, I hear, apps [Truecaller](#) or [RoboKiller](#).
  - [Other options](#)
- If you get junk **robocalls** on your 📱 **smartphone**:
  - Block all suspected spam calls, or send them directly to voicemail:
    - If through Republic Wireless, see [How to Block Robocalls/Spam Calls & Voicemails Using the Republic Wireless App](#).
    - If through any other mobile company, look into call-blocking call-blocker app [Hiya](#) or [others](#), or pay for [Nomorobo](#). Or perhaps, apps [Truecaller](#) or [RoboKiller](#), or [other choices](#).
- Sign up for [Smart911](#).
- [Block ads on YouTube](#).
- Periodically, you might want to review section "[3.2 One-time: Harden your iPhone 📱 smartphone or iPad 📺 tablet](#)" above, in case I added any new items.

### 7.2 Monthly: Harden your Android 📱 smartphone, 📺 tablet or 📖 Chromebook

- If in "[2.3 One-time: Harden your Android 📱 smartphone or 📺 tablet or 📖 Chromium OS Chromebook device](#)" above, you installed **Lookout** to **not** auto-update itself, it will occasionally (~twice a year) ask you for an update:
  - Please do that.
  - If you wish to run a scan now, launch app **Lookout** > tab **Security** > button **Scan Now**.
- If at any time Android tells you "**Not enough space**":
  - See if app [gear] **Settings** > **Storage** > **Internal storage** > **Available** is at least **500MB** (needed to download anything new) or **1GB** (nice for speedy operation). If No, continue . . .
  - Launch app **Chrome** > ☰ hamburger icon in upper-right > [gear] **Settings** > **Downloads** > set **Download location=SD card**. **TOD0: Do I remove existing downloads from my computer via USB cable?**
  - App [gear] **Settings** > **Apps** > tab **ALL** > [gear] **Settings** ☰ hamburger icon in upper-right corner > **Sort by size** > for each of the top dozen or more apps, select the app, and if has a button "**Move to SD card**", select it.

- Currently, these apps seem to be **Facebook, Instagram, Translate, Wifi Analyzer, Wifi Connector Library, iNaturalist** and **GTasks**. Also check all other apps from Meta Platforms, Inc.
- App [gear] **Settings** > **Storage** > if sections for **Pictures Audio Downloads Misc** are more than a MB, see if you can move them to your SD card.
  - For example, from app **Camera** > swipe left-to-right until [gear] **Settings** curve comes up > slide curve around until you see an icon that looks like an **SD card** > set **Storage location=SD card**.
- App [gear] **Settings** > **Storage** > **Cached Data** > **Clear cached data?** = OK.
- See if app [gear] **Settings** > **Storage** > **Internal storage** > **Available** is now at least **500MB** (needed to download anything new) or **1GB** (nice for speedy operation). *If Yes, continue . . .*
- Go back to what you were doing > **Cancel** > retry what you were doing.
- If you have to, app [gear] **Settings** > **Apps** > tab **ALL** > [gear] **Settings** ≡ hamburger icon in upper-right corner > **Sort by size** > for each app you understand and do not use, select the app, and if has a button "**DISABLE**", select that. Currently, my Disabled apps are **charging-related noise suppression, Cloud Print, Google Pinyin Input, Google Play Movies & TV, Google Play Music, Google Text-to-speech Engine, Google+, Hangouts, Motorola Migrate, Photos** and **TalkBack**.
- Again, app [gear] **Settings** > **Storage** > **Cached Data** > **Clear cached data?** = OK (quickly leaks back in).
- Launch app **Chrome** > ≡ hamburger icon in upper-right > [gear] **Settings** > **Site Settings** > **Storage** > **Clear Site Storage....**
- See if app [gear] **Settings** > **Storage** > **Internal storage** > **Available** is now at least **500MB** (needed to download anything new) or **1GB** (nice for speedy operation). *If Yes, continue . . .*
- [How to Clear the Android System Cache on Motorola and Nexus Phones Running Android 8.0 or Below](#).
- Go back to what you were doing > **Cancel** > retry what you were doing.
- If you are having **battery duration** problems:
  - Launch Android app [gear] **Settings** >
    - **Battery** > select **each** app to see any settings that can reduce battery use.
    - **Battery** > ≡ hamburger icon in upper-right > **Battery saver** > Turn on automatically > at 15%.
    - **Location** > **Mode**=Battery saving.
- If you think your Facebook app requires too many permissions (it does), uninstall it, and replace it with [Tinfoil for Facebook](#). Saves a huge amount of space on your ☞ phone, too! So far, seems quite functional.
- *If at home under Wi-Fi*, update your apps via app **Play Store** > **Settings** ≡ hamburger icon in upper-left corner > **My apps & games** > **Updates** > for each app that needs an update whose existence and permissions you don't mind > **Update**.
- *If at home under Wi-Fi*, update your OS via [gear] **Settings** > **System Updates** > those three things.
- Ensure your Android does **not automatically attach to non-secure Wi-Fi networks**, run app [gear] **Settings** > **Wi-Fi** > three-dot **Settings** ≡ hamburger icon in upper-right corner > **Saved networks** >
  - For each Wi-Fi network SSID [still the default name from the router manufacturer](#) (e.g., **Guest** or **Linksys** or **xfinitywifi**), or that you no longer use, or that is not-encrypted, **delete** it with a **tap** > **Forget**.
  - If you want to reorder the remaining networks, apparently you need to install app **TBD**.
- [Clear your browser's cache](#).
  - *If you have browser Chrome*, follow the few steps in <https://support.google.com/chrome/answer/2765944> > tab **Android**.
- [If your Android ☞ smartphone or ☞ tablet is running slow](#).
- *If you get junk robocalls on your ☞ landline*:
  - Set up call-blocking call-blocker app [Nomorobo](#) (awesome!), free on most VoIP landlines (a landline provided digitally — perhaps from your cable TV provider).
  - Or, I hear, apps [Truecaller](#) or [RoboKiller](#).
  - [Other options](#)
- *If you get junk robocalls on your ☞ smartphone*:
  - Block all suspected spam calls, or send them directly to voicemail:

- If through Republic Wireless, see [How to Block Robocalls/Spam Calls & Voicemails Using the Republic Wireless App](#).
- If through any other mobile company, look into call-blocking call-blocker app [Hiya](#) or [others](#), or pay for [Nomorobo](#). Or perhaps, apps [Truecaller](#) or [RoboKiller](#), or [other choices](#).
- If using an Android, version 7.0 Nougat or above (likely if your phone is from 2016 or later), block **individual numbers** via [How to Block Calls/Numbers on Phones with Android Nougat 7.0 or Higher](#).
- Sign up for [Smart911](#).
- [Block ads on YouTube](#).
- Periodically, you might want to review section ["3.3 One-time: Harden your Android ☞ smartphone or ☞ tablet or ☞ Chromium OS Chromebook device" above](#), in case I added any new items.

## 7.3 Monthly: Harden your ☞ computer

Please do the following **once a month** or so. ☞ Microsoft Windows might run some of these tasks periodically in the background. But some of you have Windows' [gear] **Settings** (formerly **Control Panel**) > **1/0 Power Settings** set so tightly, that Windows *never* gets a chance to run them. So you **have** to run them yourself.

A good time to do this would be shortly after **Microsoft Patch Tuesday** (the second Tuesday of the month). Easier to remember is to do it after you pay your **rent, mortgage** or ☞ **phone bill**. **When** you do it periodically is not as important as that you **do it** periodically (Nike: *Just do it!*):

### 7.3.1 First steps

- If since the last time you rebooted (under ☞ Microsoft Windows, ☞ **Start** > **1/0 Power** > **Restart** or **Shutdown**), you may have **installed, uninstalled** or **updated** any software, or have had your machine up for more than a half hour or so, **reboot now** (☞ **Start** > **Restart**).
- ☞ [One-time] If running under **Microsoft Windows 8.0** (if not sure, please check <http://windows.microsoft.com/en-us/windows/which-operating-system>, or ☞ **Start** > **Run** > **winver**, or ☞ **Start** > **Run** > **msinfo32**):
  - Please follow <http://windows.microsoft.com/en-us/windows-8/update-from-windows-8-tutorial>.
- ☞ If running under **Microsoft Windows**, it should be auto-updating. In case it isn't, also do it manually, via ☞ **Start** > [gear] **Settings** > **Update & Security** > "**Check for updates**". When it finishes scanning:
  - If you see *required updates on top that are not installing now because you are actively using the machine*, it is OK to install them now. If you don't, Microsoft will probably will install them in the next few hours.
    - If there are ~~**Important**~~ updates listed, select them.
      - If not, and there are ~~**Recommended**~~ updates, click ~~**Recommended**~~ and select them.
    - > ~~**OK**~~ > ~~**Install updates**~~.
  - If you see link **View optional updates**, select it.
    - If there is a dropdown **Driver Updates**, drop it.
      - Consider installing these, especially if you are having any *new* problems in your computer.
        - For example, if you are *having audio problems*, install any optional drivers regarding audio, such as from Realtek (an audio software vendor), and probably any system firmware drivers.
      - [Expert] Regarding **Optional** updates, you may wish to **not** install these, until I or another expert is around. Most are good — better function for your display or mouse or other hardware. But I see no reason to install Bing Desktop and Bing Bar, nor to put on Remote Desktop stuff I am not going to let anyone use. And I have **twice** had to *back off* an update — one on my wife's machine, an update to some nice HP-proprietary software that caused the **Blue Screen of Death BSoD** until I could back it off (that was I nice trick — I felt proud after that), and one update to my own computer that caused my screen to go totally **wacky, barely usable until** I could back it off. Probably best to install when you have reinforcements.
      - On the other hand, installing **Optional** updates has **fixed real-life problems** for a buddy (1 problem) and a close family member (2 problems). So use your judgement!
    - While that runs, you can continue doing ordinary tasks, e.g., send ☞ email, webpages, and stream videos.
    - If it asks you to **reboot**, please do so after you finish whatever you are doing.

- When it comes back up, run **Windows Update again**. Yes, again — not all updates can go on at the same time — some updates are prerequisites of other updates. If **Windows Update** lists any **Important** or **Recommended** updates, please install them.
- If the above didn't work, see <https://www.lifewire.com/latest-windows-service-packs-updates-2624595>.
- 🍏 If running an **Apple macOS** (Macintosh, iMac, iBook, and MacBook) 🖥 computer, update your **macOS** by selecting icon 🍏 **Apple** at the top left of your screen > **About this Mac** > button **Software Update...** > check checkbox **Automatically keep my Mac up to date** > button **Advanced...** > check all checkboxes > button **OK**.
  - If you get "**An update is available for your Mac**", apply it.
  - If needed, button "**Restart Now**".
  - If you get the [Spinning Pinwheel of Death SPOD](#).
- Update your **antimalware/antivirus rules**. It should be auto-updating, but in case it isn't, do it manually.
  - Usually in your *Notification Area* (will be *Action Center* in Win10X) (formerly *System Tray* — by the clock), there is an icon — right-click it > "**Update**" or something.
  - Verify that you are up-to-date.
- [Clear your browser's cache](#).
  - If you have browser **Chrome**, follow <https://support.google.com/chrome/answer/2765944> > tab **Computer**.

### 7.3.2 Backup your 🖥 computer

- **Backup** your 🖥 computer! (If I told you to do anything, please defer this step until the end.)
  - This uses the principle of **LOCKSS Lots of Copies Keep Stuff Safe**. At least two copies (e.g., your computer and your backup drive). Preferably, three. Preferably, one copy off-site. [5 Way to Back up Your Data](#).
  - For your **most important** data (e.g., 📞 **phone numbers** and such you might want to have on paper while traveling), consider printing it out!
  - If you are a **lightweight user** or have a **lightweight machine**, keep all your files in **the Cloud**, in Facebook, ✉ email via webpage, **Dropbox** (Basic plan FREE) (I love this, and use all the time!), **Box**, **Microsoft OneDrive**, 🍏 **Apple iCloud**, **Google Drive** ([review](#)), **pCloud**; secure **milDrive**, **sync.com**, **SpiderOak ONE** (\$); or other [file hosting](#), [file synchronization](#), or [online backup](#) services. Except **milDrive** and **SpiderOak**, these are free for the first few GB. Except **milDrive** and **SpiderOak**, these were designed for sharing files with others, but you can share files with yourself, too! If you are scared to do this, call me. **TODO: look into whether [SyncBackFree](#) is a good way to manage this.**
    - If you have 🍏 **Apple** devices, you probably already have access to **iCloud**.
    - If you have a ✉ **Gmail** email account, you already have access to **Google Drive** ([review](#)) and **Docs, Sheets and Slides** through your email account.
    - If you have an ✉ **Outlook.com/Live Mail** (formerly **Hotmail**) email account, you already have access to **Microsoft OneDrive** and **Office Online** through your email account.
  - If you have lots of files on your 🖥 computer (docs, photos, music, video, family history, et al add up fast!), I recommend you buy an **external harddrive** (or a very large flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-stick). \$80 might be about right. As of 2015-April that will get you a very nice compact don't-power-from-wall USB drive that holds 2 TB. More TB is better. Compact is good. Power-from-wall will be a hassle. If confused, see me.
    - When you acquire a new **flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-stick**:
      - IF your drive came in format="**FAT32**",  
AND you want your drive to handle file sizes >4GB=**No**,  
THEN you can leave it just like this.
      - IF your drive came in format="**NTFS**",  
AND you want your drive for 🖥 Microsoft Windows use=**Read-Write**  
AND 🍏 Apple macOS use=**Read-Only** or **not at all**,  
THEN you can leave it just like this.
      - IF your flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-stick came in format="**HFS+**",  
AND you want your drive for 🍏 Apple macOS use=**Read-Write**  
AND 🖥 Microsoft Windows use=**not at all**,  
THEN you can leave it just like this.
      - IF you want your drive for use in the Honda Fit/Jazz Type 2 entertainment system,  
THEN reformat your drive to format="**FAT32**".



- 🍏 IF you are running Apple macOS level lower than 10.6.6, THEN apply the "[exFAT patch](#)".
- IF you are running 🇺🇸 Microsoft Windows release before 7, THEN apply the "[exFAT patch](#)".
- IF you are running 🇺🇸 Microsoft Windows release before 10, THEN upgrade to a modern level of Windows with all due speed.
- IF you want your drive for 🍏 Apple macOS use=**Read-Write** AND/OR 🇺🇸 Microsoft Windows use=**Read-Write**, AND/OR handle file sizes >4GB=**Yes**, THEN reformat your drive to format="[exFAT](#)" as in <https://support.wdc.com/knowledgebase/answer.aspx?ID=291> (creates folder "[\\_\\_MACOSX](#)").
- While you are at it, personalize the name of your **backup drive** to:
  - something with **your name** and **location**, in format [FirstLastUSA](#), or
  - a permanently-available 🇺🇸 phone number, in format [AAA-XXX-NNNN](#).
- **TODO:** Add here how to back up **Facebook data** (and other apps from Meta Platforms, Inc.). [Save videos from Facebook](#).
- There are **two** main types of backups:
  - The contents of your **entire** harddrive, right now. Such as with:
    - [Clonezilla](#), to a USB harddrive. Said to be a good way to make sure you can get your harddrive back to this state, exactly. **TODO: Try this.**
    - Proprietary software, to a tapedrive or other medium. I have used this many times, to very good effect. Don't have a current method to do this.
  - Your **critical userdata**. Whatever *critical* means. Might be splattered all over, or hiding. Presumably, you would have another method to reinstall your operating system and necessary software (e.g., MS Office, Quicken, photo software), before you then get your critical userdata back from here. This is the option mostly discussed below. Nicest is to have: a full backup first, then incrementals (whatever changed since the previous full backup), preferably where at restore time, you can pick any particular version of any particular file, as in Time Machine.
- 🍏 For **Apple macOS** (Macintosh, iMac, iBook, and MacBook) 🇺🇸 computers, please see "[Mac Basics: Time Machine backs up your Mac](#)" and [http://reviews.cnet.com/8301-13727\\_7-57407390-263/how-to-set-up-time-machine-on-your-mac/](http://reviews.cnet.com/8301-13727_7-57407390-263/how-to-set-up-time-machine-on-your-mac/).
- 🇺🇸 For **Microsoft Windows**:
  - Please see "[If we show you how to back up your PC for free, will you finally do it?](#)".
  - If you have a large backup drive (look at the box) compared to the number of size of files on your harddrive (look at [File Explorer/This PC](#) [formerly [Windows Explorer/My Computer](#), and still called [Windows Explorer under-the-covers](#)] icon for the C: drive), it is OK to use Microsoft backup, via [Start](#) > [gear] [Settings](#) (formerly [Control Panel](#)) > [Backup and Restore](#), to that external harddrive. I find MS Backup:
    - Probably backs up everything I want. **TODO: Verify.**
    - Wasteful on space--a large drive I bought to backup 🇺🇸 two computers, only does mine.
  - Probably more sure/easier to understand is [Karen's Power Tools replicator-backup utility](#) (although it takes some setup from you). **TODO: Try this.**
  - **TODO: Investigate Windows command [robocopy point 14](#).**
  - I use a utility different from all the above.
  - If you need to be *thrifter*, it might be OK to use the software that came with your external harddrive: some are OK; some do **NOT** back up all the files I need; and most only keep **one copy** of each file, and I want versioning for my many files that change a lot.
  - If you use **PhotoShop Elements PSE**, manually copy your **PSE catalogs** from "[C:\ProgramData\Adobe\\\*\Catalogs](#)" to your [My Documents](#) or [%USERPROFILE%\Documents\Backup\AdobeCatalogs\\_yyyymmdd\](#) folder that **is** backed up. This should take care of all [\\*.prel](#) [\\*.psess](#) [\\*.ps\\*](#) [\\*.psd](#) [\\*.pse](#) [\\*.pspImage](#) files.
  - If you use **Microsoft Outlook**, and have not yet moved your [.pst](#) files to your [My Documents](#) or other folder that **is** backed up, copy them to [%USERPROFILE%\Documents\Backup\MSOutlook\\_yyyymmdd\](#).
  - What I really want is Time Machine (in the 🍏 **Apple Macintosh** bullet above) or Intelligent Backup (what I used to have years ago). [Why can't I have these, on my machine now?](#)
  - **TODO:** see above article's link to [SyncBackFree](#) (looks very promising).

- To back up your machine, while doing all you can to [protect against cryptoviral extortion ransomware](#) (e.g., [CryptoLocker](#)) from wrecking your backup drive as well:
  - Verify that your antivirus is up-to-date, has run recently, and ran clean.
  - *[Expert] [me]* Turn **off** your Internet connection (optional) (if you are paranoid: required) (me: I try to, unless rushed for time), to increase chance your backup is secure if you get infected by malware or ransomware.
  - *[Expert] [me]* To prevent Norton from quarantining some of my tools, set **Norton** > *[gear]* **Settings** > **Removable media scan=OFF**.
  - **Connect** your backup drive.
  - Do the **backup** as above.
  - **Disconnect** your backup drive. (Now, if you get infected and notice it before your next backup, this backup is safe.)
  - *[Expert] [me]* If four bullets up, you told **Norton** > *[gear]* **Settings** > **Removable media scan=OFF**, set it back **=ON**.
  - *[Expert] [me]* If six bullets up, you turned it off, turn **on** your Internet connection.
- Even if you backup to an **external harddrive** (up five open-bullets), you can supplement that by also backing up your most important files at **Dropbox** (Basic plan FREE) (I love this, and use all the time!), **Box**, **Microsoft OneDrive**, **Apple iCloud**, **Google Drive** ([review](#)), **pCloud**; secure **milDrive**, **sync.com** (up six open-bullets), or **SpiderOak ONE** (\$); or other [file hosting](#), [file synchronization](#), or [online backup](#) services. **TOD0:** look into whether [SyncBackFree](#) is good for this.
  - If you have **Apple** devices, you probably already have access to **iCloud**.
  - If you have a **Gmail** email account, you already have access to **Google Drive** ([review](#)) and **Docs**, **Sheets** and **Slides** through your email account.
  - If you have an **Outlook.com/Live Mail** (formerly **Hotmail**) email account, you already have access to **Microsoft OneDrive** and **Office Online** through your email account.
- If your house catches on **fire**, be sure to grab at least **one** of your **computer** or backup drive!
  - Or keep your backup drive in a fireproof safe, bolted to a wall.
  - Or store your backup drive in the house of a trusted family member or friend!
- **TOD0:** See if there is anything else I need to copy from [tools.pdf](#) and [the other doc](#).

### 7.3.3 More steps

- Ensure your **computer** does **not automatically attach to non-secure Wi-Fi networks**.
  - **Under Microsoft Windows 10:**
    - **Run** **Win+X** (or right-click of **Start** icon) > **Windows PowerShell (Admin)** or **Command Prompt (Admin)** > type "**netsh wlan show profiles**" (no quotes).
    - For each Wi-Fi network SSID [still the default name from the router manufacturer](#) (such as "**Guest**" or "**Linksys**"), or that you no longer use, **delete** it with something like:
 

```
netsh wlan delete profile name="Guest"
```
    - For each **public** or **not-encrypted** Wi-Fi network to which you sometimes connect, **move it to the bottom of the list** with something like:
 

```
netsh wlan set profileorder name="xfinitywifi" interface="Wi-Fi" priority=13
```
    - For your **preferred home private encrypted** Wi-Fi network to which you connect a lot, **move it to the top of the list** with something like:
 

```
netsh wlan set profileorder name="myNetwork" interface="Wi-Fi" priority=1
```
    - Verify that the list appears as you intended, by repeating:
 

```
netsh wlan show profiles
```
  - **Under Apple macOS** (Macintosh, iMac, iBook, and MacBook **computer**s):
    - Open **Spotlight** by pressing Command key **⌘-spacebar**.
    - Type "**network**" [Enter].
    - Look for a **System Preference** called **Network** and double-click it.
    - Click on button **Advanced**.
    - For each Wi-Fi network SSID [still the default name from the router manufacturer](#) (such as "**Guest**" or "**Linksys**"), or that you no longer use, **delete** it by clicking its name in the list, and then button **-**.
    - For each **public** or **not-encrypted** Wi-Fi network to which you sometimes connect, **drag it to the bottom of the list**.
    - Drag your **preferred home private encrypted** Wi-Fi network to the top of the list.
    - If **iCloud Keychain** is active, click **Remove**.
    - Click **OK**.

- Click **Apply**. If you use *iCloud Keychain*, all connected devices will get these changes, too.

- **TODO:** Add stuff about the **Outlook** Detect and Repair utility that is NOT via > have MS Outlook installation CD available > MS Outlook > Help > Detect and Repair > Start > wait for run > exit Outlook.
- Periodically, you might want to review section "[3.5 One-time: Harden your !\[\]\(6302aad5aed157b291fddf37b4870784\_img.jpg\) computer](#)" above, in case I added any new items. And continue ...

## 7.4 Quarterly: Harden your computer

If I told you to do anything, please continue this section **until the end**...

If your  computer has been **slow** or **dodgy** lately, please continue **until the end**...

If you are a **relative** or **close friend**, and I clean your machine once a year, you can [skip this section](#).

If I do **not** clean your machine once a year, some months, [skip this section](#); other months, continue on...

- If a website fails to launch video or audio "[Get ADOBE FLASH PLAYER](#)" in web browser **Chrome** or **Internet Explorer**, try the site in browser **Firefox**, **Edge**, **Safari**, **Opera**, **Vivaldi** or **Brave**.
- Check **Adobe Flash** (previously Shockwave Flash) (used by some fancy graphics) via either (A)  **Start** >  **Settings** (formerly **Control Panel**) > **Flash** > tab **Updates** > button **Check Now**; or (B) <http://helpx.adobe.com/flash-player.html> > "**Check Now**"; (this might work better under Microsoft **Edge** or **Internet Explorer** than under **Chrome**):
  - **TODO:** look into:
    - <https://www.hos.com/Flash-help-Windows.6.23.2017.pdf>
    - <https://www.hos.com/Flash-help-Chrome.6.23.2017.pdf>
    - <https://www.hos.com/Flash-help-Firefox.6.23.2017.pdf>
    - <https://www.hos.com/Flash-help-Safari.7.01.2017.pdf>
    - <https://www.hos.com/Flash-help-InternetExplorer.7.22.2017.pdf>
  - If needed, **Update**.
  - If during the install, you see a **checkbox** checked, **consider unchecking** it!
  - launch it, and into its URL field, Paste "<http://helpx.adobe.com/flash-player.html>" > **Enter** > "**Check Now**" > etc., as described above.
  - While doing this, keep in mind that [below](#) you will want:
    - **Adobe Flash Player 23.0.0.207/Shockwave Flash 23.0 r0 Disabled**.
  - For your other web browsers (e.g., **Firefox**, **Edge**, **Chrome**, **Safari**, **Opera**, **Internet Explorer**, **Vivaldi** or **Brave**).
- Launch **Adobe Reader**, and ask it **Help** > "**Check for Updates...**".
  - If during the install, you see a **checkbox** checked, **consider unchecking** it!
- Launch **iTunes**, and ask it to **Help** > "**Check for Updates**".
  - If during the install, you see a **checkbox** checked, **consider unchecking** it!
- Review all settings within  **Start** >  **Settings** > **Privacy**, including all entries in the left navigation bar.
- If low on storage space, Launch  **Start** >  **Settings** > **Storage** > turn on **Storage sense** or click **Change how we free up space**, including perhaps button **Clean now**.
- [Delete cookies from all sites you don't recognize and like](#). **TODO:** including some of them (not all) (**Chrome**). And [clear your browser's cache](#). And [on your iOS !\[\]\(4a20c858524295d2b586b58826d34eb7\_img.jpg\) iPhone](#) or [iPadOS !\[\]\(cdbbc2244079ed4c75056c9432abc2fd\_img.jpg\) iPad](#).
  - If you have browser **Chrome**, follow the few steps in <https://support.google.com/chrome/answer/2765944> > tab **Computer**.
- Remove **QuickTime**.
  -  If running under Microsoft Windows, use  **Start** >  **Settings** (or **System Settings**) (formerly **Control Panel**) > **Apps** > tab **Apps and features** [optional > **Programs and Features**] > **QuickTime** > press or right-click > **Uninstall** > Yes, you are sure > wait. When done, verify that **QuickTime** is no longer listed. At your next convenience, **reboot** (under Windows,  **Start** > **1/0 Power** > **Restart** or **Shutdown**).

- Scroll through **all your programs** (in **Microsoft Windows**, listed in **Start** > **All Programs**), and for anything interesting, launch them and see if they need updating. After every two or three, **reboot** (under Windows, **Start** > **1/0 Power** > **Restart** or **Shutdown**).
- Consistent with principles [at top](#), **remove** any programs you **no longer need**.
  - If running under Microsoft Windows, use **Start** > [gear] **Settings** (or **System Settings**) (formerly **Control Panel**) > **Apps** > tab **Apps and features** [optional > **Programs and Features**] > **for each** program you no longer need > press or right-click > **Uninstall** > Yes, you are sure > wait for it to finish. After every two or three apps, **reboot** (**Start** > **1/0 Power** > **Restart** or **Shutdown**).
- If you use web browser **Chrome**, periodically:
  - [Some of these ideas are from [Chrome cleanup tool \(discussion\)](#), but are improved below.]
  - Launch Chrome > upper-right icon : kebab > **Settings** > left navigation **Advanced** > **Reset and clean up** or **Reset Settings** > (or new tab <chrome://settings/reset>):
    - **Clean up computer** > button **Find**.
      - If you're asked to remove unwanted software, click **Remove**. You may be asked to reboot your computer.
      - If in trouble, consider **Restore settings to their original defaults** > button **Reset settings**.
  - Launch Chrome > upper-right icon : kebab > **Settings** > left navigation **Extensions** > (or new tab <chrome:extensions>) > **for each Chrome App** > **Remove** or turn Off, unless you totally recognize that Extension as being from a reliable vendor AND that you actually use that Extension.
  - Launch Chrome > upper-right icon : kebab > **Settings** > left navigation **Search Engine** > (or new tab <chrome://settings/search>) > **Manage search engines** > **for each** search engine > : kebab Remove from List unless you know it is legitimate, or is one of:

Keyword	Query URL
duckduckgo.com	<a href="https://duckduckgo.com/?q=%s">https://duckduckgo.com/?q=%s</a>
bing.com	<a href="https://www.bing.com/search?q=%s&amp;PC=U316&amp;FORM=">https://www.bing.com/search?q=%s&amp;PC=U316&amp;FORM=</a>
ecosia.com	<a href="https://www.ecosia.org/search?q=%s&amp;addon=opensearch">https://www.ecosia.org/search?q=%s&amp;addon=opensearch</a>
google.com	<a href="https://www.google.com/search/q=&amp;s">https://www.google.com/search/q=&amp;s</a>
google.com	{google:baseURL}search?q=%s&{google:RLZ}{google:originalQueryForSuggestion}{google:assistedQueryStats}{google:searchFieldtrialParameter}{google:iOSSearchLanguage}{google:prefetchSource}{google:searchClient}{google:sourceId}{google:contextualSearchVersion}ie={inputEncoding}
yahoo.com	<a href="https://search.yahoo.com/search{google:pathWildcard}?ei={inputEncoding}&amp;fr=crmas&amp;p=%slook">https://search.yahoo.com/search{google:pathWildcard}?ei={inputEncoding}&amp;fr=crmas&amp;p=%slook</a>

- Remove toolbars.
- Set home page to something reasonable.
- Go through settings ...
- **chrome:plugins**
  - ~~Uncheck all checkboxes **Always allowed**. I find I don't need any of them.~~
  - ~~Disable any plugins you don't use:~~
    - ~~Adobe AAM Detect, **Disable**.~~
    - ~~Adobe Reader, **Disable**. I use **Chrome PDF Viewer** instead...~~
    - ~~Chrome PDF Viewer, **Enable**.~~
    - ~~Chrome Remote Desktop Viewer, **Disable**.~~
    - ~~Google Earth, your choice. I use it.~~
    - ~~Google Update, **Enable**.~~
    - ~~iTunes App Detector, **Disable**. Don't need it.~~
    - ~~Microsoft Office, **Disable**.~~
    - ~~yourAntivirusProvider Identity Safe, **Enable**.~~
    - ~~yourAntivirusProvider Vulnerability Protection, **Enable**.~~
    - ~~QuickTime, **Disable**. Then **remove it**.~~
    - ~~Shockwave Flash 12.0 r0, it should not be here: update Flash [as above](#), reboot, and if it is not gone, please call me.~~
    - ~~Shockwave Flash 14.0 r0, update Flash [as above](#).~~
    - ~~Shockwave Flash 15.0 r0, update Flash [as above](#).~~

- ~~Shockwave Flash 16.0 r0~~, update Flash ~~as above~~.
- ~~Shockwave Flash 17.0 r0~~, update Flash ~~as above~~.
- ~~Adobe Flash Player/Shockwave Flash 18.0 r0~~, update Flash ~~as above~~.
- ~~Adobe Flash Player 23.0.0.207/Shockwave Flash 23.0 r0~~, **Disable**, unless you find this breaks one of your needed websites.
  - I have to set mine to **Enable**, because [FrogWatch](#) requires it. Or I toggle it, keeping it Enabled only when I need it.
- ~~Silverlight~~, your choice. I Enable, as it is needed on one or two websites I visit regularly.
  - As of 2014-10-22, it seems that Chrome has disabled Silverlight. Run Silverlight pages in IE.
- ~~VLC Detector~~, **Disable**.
- ~~VLC Web Plugin~~, **Disable**.
- ~~Widevine Content Decryption Module~~, **Enable**. I looked it up once. I forgot why it is OK.
- ~~Windows Activation Technologies~~, **Disable**.
- ~~Windows Live Photo Gallery~~, **Disable**.
- ~~WPI Detector~~, **Disable**.
- [chrome:settings/content](#)
- [chrome:settings/passwords](#)
- [chrome:about](#)

- ☐ If you use web browser **Internet Explorer**, periodically look through **Tools > Manage add-ons**:
  - In tab **Toolbars and Extensions**, **Disable** each entry other than [yourAntivirusProvider Identity Protection](#) and [yourAntivirusProvider Vulnerability Protection](#).
  - Other tabs, look at them and set as you wish.
  - Then stop using this obsolete vulnerable browser.

□ For your *other* web browser (e.g., **Firefox, Edge, Safari, Opera, Internet Explorer, Vivaldi or Brave**).


- I think the **Java** programming language and runtime are great. But old versions, including **1.6**, have **big security holes**.

If your employer has **not** made you install a special Java app, and you are **not** a `</>` computer programmer working in Java, you **do not need Java**, and **should remove it**.

- See what Java you have, via [www.java.com/verify](#) (if your primary web browser **Chrome** or **Edge** won't run this, Paste into **Firefox, Safari, Opera, Vivaldi or Brave**), or set [\[gear\] Settings](#) (formerly **Control Panel**) > **Java** > tab **Security** > check **Enable Java content in the browser** > **Apply** > **"Agree and Continue"** > and maybe **"Run"**.
  - If you do **not** have Java, great! Go to next paragraph.
  - If you have Java but don't need it, **Uninstall** it.
    - ☐ If running under Microsoft Windows, use **Start** > [\[gear\] Settings](#) (or **System Settings**) (formerly **Control Panel**) > **Apps** > tab **Apps and features** [optional > **Programs and Features**] > **for each** instance of **Java n Update nn** or **Java SE Development Kit n Update nn (nn-bit)** or **J2SE** or **Java 2** or **Java SE** or **Java Runtime Environment** > press or right-click > **Uninstall** > Yes, you are sure > wait for it to finish. After every two or three apps, reboot (**Start** > **1/0 Power** > **Restart** or **Shutdown**).
  - If you have Java and it is out of date, **Update** it.
    - If during the Install/Update, you see a **checkbox** checked, **uncheck** it!
    - Afterword, set [\[gear\] Settings](#) (formerly **Control Panel**) > **Java** > tab **Update** > check **Check for Updates Automatically** > button **Advanced...** > set **Weekly** or **Monthly** > OK > **Apply**; and tab **Update** > check **Suppress sponsor offers when installing or updating Java** > **Apply** > OK.
- Check for **old Java** via [www.java.com/en/download/uninstallapplet.jsp](#) (if your primary web browser **Chrome** or **Edge** won't run this, Paste into **Firefox, Safari, Opera, Vivaldi or Brave**), or set [\[gear\] Settings](#) (formerly **Control Panel**) > **Java** > tab **Security** > check **Enable Java content in the browser** > **Apply** > **"I Agree to the Terms and Want to Continue"** > and maybe **"Run"**.
  - If this finds any out-of-date versions, **remove** them. If this then breaks any apps your employer made you install, bug your employer to update that app!
  - Helps at [www.java.com/en/download/faq/remove\\_olderversions.xml](#).



- You can now probably turn off what you set above, via [gear] **Settings** (formerly **Control Panel**) > **Java** > tab **Security** > uncheck **Enable Java content in the browser** > **Apply**. If this then breaks any apps your employer made you install, please set this back.
  - [Expert] Only if necessary, uninstall Java via instructions at [www.java.com/en/download/help/uninstall\\_java.xml](http://www.java.com/en/download/help/uninstall_java.xml).
  - ☞ [Expert] If running under Microsoft Windows, use ☞ **Start** > [gear] **Settings** (or **System Settings**) (formerly **Control Panel**) > **Apps** > tab **Apps and features** [optional > **Programs and Features**] > **for each** program you no longer need > press or right-click > **Uninstall** > Yes, you are sure > wait for it to finish. After every two or three apps, **reboot** (☞ **Start** > **1/0 Power** > **Restart** or **Shutdown**).
- ☞ If your Microsoft Windows computer or web browser runs **slower** than it used to, or if you have **any reason** to suspect malware:
- Run a **full-scan** on your existing antimalware/antivirus program, until clean.
  - [One-off] If you don't use [Malwarebytes](#) antimalware, install the **free** version, boot to **Safe Mode**, and **run it** until clean.
  - [One-off] Install [Microsoft Security Scanner](#), and run it until clean.
  - [One-off] Instead of the above, you could experiment with (if don't have Norton Security software at this time) Norton > Security > Run Scans > [Norton Power Eraser](#) utility, and the [Norton Bootable Recovery Tool](#). I have not used these.
- ☞ If your Microsoft Windows computer runs **slower** than it used to, whack or delay unnecessary programs that **start themselves automatically**, using:
- [Easy] If you have **Norton Security software** (free with Comcast) > **Tuneup** > **Startup Manager**; or
  - [Easy] If running Microsoft Windows 10, **Task Manager** tab **Startup** (works fine, easier than below); or
  - [Moderate] If running Microsoft Windows 7, **msconfig** tab **Startup** (works fine, easier than below; Windows 10 has nice link to where they moved it: **Task Manager** tab **Startup**); or
  - [Moderate] [services.msc](#); or
  - [Don't remember] [Winternals Autoruns](#); or
  - [Moderate] find all your **Startup** folders, and move bad entries to new sister folder **StartupNOT**, and
  - [Expert] Registry entries [HKEY\\_CURRENT\\_USER\Software\Microsoft\Windows\CurrentVersion\Run](#) and [HKEY\\_LOCAL\\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run](#) (delete the bad entries) (works great).
- ☞ If your Microsoft Windows computer runs **slower** than it used to, run **CCleaner** Free [except in 2021, is identified by Microsoft Defender Antivirus as a PUP Potentially-Unwanted Program, and may recently be **crapware**] > tab **Cleaner** > unselect all "**Windows Explorer**" checkboxes except **Thumbnail Cache** > **Run Cleaner**; or
- Windows **Disk Cleanup** via **This PC** (formerly **My Computer**, and still called that *under-the-covers*) > **C:** > right ribbon tab **Manage** > **Cleanup**.
- While that runs, you can continue doing ordinary tasks, e.g., send ☞ email, webpages, and stream videos.
  - When ready, change its selections if you wish, and click **OK**, and let it run.
  - If your **system drive** freespace is less than **15%** of the total space, move, compress or delete unneeded files. **CCleaner** Free [except in 2021, is identified by Microsoft Defender Antivirus as a PUP Potentially-Unwanted Program, and may recently be **crapware**] > tab **Tools** > **Duplicate Finder** seems to be adequate at cleaning up from projects that you completed quickly, but left files splattered all over. It does this by finding, showing, and optionally deleting these files. But I like [Auslogics duplicate file finder](#) a little better. But to keep out bloatware, during the install:
    - select radio button "**Custom install (advanced)**", and
    - uncheck **every checkbox**.
- ☞ If your Microsoft Windows computer runs **slower** than it used to, **defragment** your harddrive, probably via **This PC** (formerly **My Computer**) > your Windows system drive, usually **C:** > right ribbon tab **Manage** > **Optimize** > **Optimize** (previously **Defragment Now . . .**).
- If Windows **Optimize Drives** (previously **Disk Defragmenter**) came up, run it on each of your harddrives.
    - Don't run it on your flash-drive/jumpdrive/thumbdrive/USB-drive/USB-key/USB-sticks (it wears out the Flash memory).
    - While that runs, you can continue doing **lightweight tasks**, e.g., browse some webpages or stream videos. I suggest not using MS Outlook or other heavy-duty apps while that runs.

- If you get a Warning box [Disk Defragmenter was scheduled using another program](#), click [Cancel](#), and run using **Norton** or whatever software took over scheduling.
  - If you think Norton is too risk-averse at running Defrag (it is), get [Auslogics Disk Defrag Free](#). If you want a defrag now, it does that — works great. I like and trust their free utilities (I have not yet felt the need to use their paid utilities, although they keep asking). But to keep out bloatware, during the install:
    - **select** radio button "**Custom install (advanced)**", and
    - **uncheck every checkbox**.
-  If your Microsoft Windows computer runs **slower** than it used to, and you don't need your computer for several hours (overnight or longer?), check for dodgy harddrive disk sectors--and fix them--by [running](#):
  - **Win+X** (or right-click of **Start** icon) > [Windows PowerShell \(Admin\)](#) or [Command Prompt \(Admin\)](#) > type "[chkdsk /F /R /X /B c:](#)" (no quotes) [Enter] > type "[Y](#)".  
-OR-
  - **Start** > [File Explorer/This PC](#) > [formerly [Windows Explorer/My Computer](#)] > [C:](#) > right-click [Properties](#) > tab [Tools](#) > area [Error checking](#) "[This option will check the drive for file system errors](#)" > button [Check \[Now...\]](#) > if you see checkboxes, check **both** > [Scan Drive](#) [or **Start** > [Schedule disk check](#)].
  - **Finish what you are doing**, and only when your computer is **plugged in** and you **don't need it for several hours** (overnight or longer?), **Reboot** (**Start** > [1/0 Power](#) > [Restart](#)) and let her run!
  - To see the results, **TODD**: write this. Apparently, redirect operators [>](#) or [>>](#) are not enough.
- If you are going to ask me for support, please [run](#) and have ready for me:
  - "[msinfo32](#)" > **Export** > [somewhereGood\myComputer\\_MSINFO32.txt](#) > **Save**,
  - navigate [somewhereGood](#), "[ipconfig /all](#)" > [myComputer\\_IPCONFIG.txt](#)" [Enter],
  - "[diskpart](#)", "[list volume](#)", "[exit](#)", and save the results in one of the files above, and
  - **Powershell** "(Get-WmiObject -query 'select \* from SoftwareLicensingService').OA3xOriginalProductKey" and save the results in one of the files above.
  - A copy of [file:///C:/Windows/Logs/CBS/CBS.log](#).
  - Then when we get together, we will ...
- [Run](#) the various tools (free on Windows) in "[msconfig](#)" [Enter] tab [Tools](#), including [mmc](#).
- Run **Win+X** (or right-click of **Start** icon) > [Windows PowerShell \(Admin\)](#) or [Command Prompt \(Admin\)](#) > type "[sfc /VERIFONLY](#)" (no quotes) [Enter].
  - If it shows anything bad, stay in the Admin command prompt, enter "[sfc /scannow](#)" [Enter]. It will take a while — a half-hour or so.
    - [This article says you may have to run it 3 times](#). In between, reboot, until it runs clean (fixes no errors).
- And:
  - "[dism /Online /Cleanup-Image /CheckHealth](#)",
  - "[dism /Online /Cleanup-Image /ScanHealth](#)",
  - "[dism /Online /Cleanup-Image /RestoreHealth](#)",
  - reboot, and
  - run "[sfc /scannow](#)" a fourth time.
- If all this didn't correct everything, look for guidance on commands [chkdsk](#), [sfc](#) and [dism](#) at <https://duckduckgo.com/?q=chkdsk+sfc+dism> or <https://google.com/search?q=chkdsk+sfc+dism>.
- Then have your local techie look at the output of your commands and their logs [file:///C:/Windows/Logs/CBS/CBS.log](#) and [file:///C:/Windows/Logs/DISM/dism.log](#).
- Determine that you have your **computer** manufacturer's *Support Assistant* (if under Windows, **Start** > scroll down list of programs), or install it now.
  - For example:
    - [HP Support Assistant](#), and
    - [HP PC Hardware Diagnostics](#).
  - Run relevant of its/their:
    - **Updates** to any software or firmware,
    - **Operating System checks** (if any Fail, keep logs),
    - **System tests** (if any Fail, keep logs),
    - **Hardware tests** (if any Fail, keep logs),

- **Diagnostic tests** (if any Fail, keep logs), and
- **Optimizations.**
- Determine that you have your computer **chip** manufacture's *Support Assistant* (if under Windows, [Start](#) > scroll down list of programs), or install it now.
  - For example:
    - [Intel® Driver & Support Assistant DSA](#).
    - [AMD Catalyst Control Center](#).
  - Run relevant of its:
    - **Updates** to any software or firmware,
    - **System tests** (if any Fail, keep logs), and
    - **Diagnostic tests** (if any Fail, keep logs).
- [Remove the Fluff From Windows 10 With Windows Decrapifier & Debloater](#).
- If you have MS Outlook, [repair your MS Outlook .pst files](#) using command `scanpst`.
- For **each** of your web browsers, consider:
  - [Test your browser against tracking](#).
  - [Secure access to your location](#).
  - To help ProPublica track displays of political ads, download their browser extension/add-on [Facebook Political Ad Collector](#) (scroll down to Download box).
  - To protect you against eavesdropping, tampering with or forging content in some websites you visit, install plug-in [HTTPS Everywhere](#) from the EFF. I have used it for years, trouble-free for me.
  - Install plug-in [Privacy Badger](#) also from the EFF (good, but I have to tell it to exclude some websites), or
  - Install plug-in [www.ghostery.com](#) > set to block web tracking types **Advertising**, **Analytics**, **Beacons**, **Privacy** and **Widgets**. A cousin recommended this. I love it, too. I currently block everything, except for one Analytics that I use occasionally. So far, so good.
  - [Block ads on YouTube](#).
  - To have your web browser **forget** your **browsing history**, **cookies**, **cached files**, and **passwords** at the end of each session, whenever accessing important sites (bank, ✉ email, Facebook, etc.), get used to launching your web browser in mode **privacy/Incognito/InPrivate**.
  - Then once a month or so, [delete your browser's cookies](#) and [clear your browser's cache](#), and [on your iOS iPhone or iPadOS iPad](#).
  - If you have browser *Chrome*, follow the few steps in <https://support.google.com/chrome/answer/2765944> > tab **Computer**.

## 7.5 Quarterly: Harden your web presence

- [Remove from social media anything about drinking, drug use, other embarrassing information, kids' names, current location, vacation plans, home location, and full birthdate](#).
- Review the **Privacy Settings** in your ✉ email provider, [Facebook](#), and web browsers. They occasionally change them.
- If you have a Google account (you might, even though you have no Gmail account), follow [Google's Privacy Checkup](#) and [Security Checkup](#).
- After Facebook disclosure of 2019-03-21, [change your Facebook and Instagram passwords](#). And those from all apps from Meta Platforms, Inc.
- Check if you have any accounts **compromised in announced data breaches**, at [Have I Been Pwned?](#) (HIBP) (built by an Aussie </> computer geek) > `your@email.address` and `usernames` > **pwned?**. And take appropriate action:
  - To get notified when **future** pwnage occurs and your account is compromised, [Have I Been Pwned?](#) > nav **Notify me** > `your@email.address`.
  - If you have custom email addresses in form `you@yourDomain`, you can get notified of pwnage of any of them via [Have I Been Pwned?](#) > nav **Domain search** > `yourDomain` > etc.
  - If you are considering a new password, [Have I Been Pwned?](#) > nav **Password** > `yourPassword` > **pwned?**.
  - [Helps on correcting your credit Reports](#).
- Follow Kim Komando's "[Google yourself to protect your reputation--online and off](#)".



## 7.6 Quarterly: Correct your credit reports

- Read and act on [my article on !\[\]\(a22ba4e13c745edbf29e51af246c4c12\_img.jpg\) Credit Reports](#).

## 7.7 Quarterly: Harden your Wi-Fi router, cable modem, and doorbell camera

- See if your **Wi-Fi router** needs a **firmware update or configuration change**:
  - **Netgear** > [www.routerlogin.net](http://www.routerlogin.net) or <http://192.168.1.1> > "admin" "*whateverYouChangedItToAbove*" > tab **Advanced** > left navigation bar **Administration** > **Firmware Update** > **Check**. If there is an Update, you might want your local geek to put it on (me, if I am at your house anyway). --[idea 2](#)
  - **Others** > your router's **administrative URL you found above** > your router's **administrative username and password you found above** > bop through the admin pages until you find how to get a firmware update. If there is an Update, you might want your local geek to put it on (me, if I am at your house anyway). --[idea 2](#)
- Follow <http://cnet.com/how-to/tips-to-stay-safe-on-public-wi-fi>.
- Or <http://komando.com/tips/370327/your-router-needs-this-one-thing-manufacturers-dont-tell-you/all>.
- Ensure your Wi-Fi firewall is on, and set correctly. Mine from Comcast Xfinity is set to Typical Security (Medium). **TODO:** Read more about this at <https://www.lifewire.com/how-to-enable-your-wireless-routers-built-in-firewall-2487668> and <https://www.lifewire.com/how-to-test-your-firewall-2487969>.
- If you have **Comcast** and they provide a Wi-Fi network *xfinitywifi*:
  - **TODO:** Write this. A start: [review your use of its SSID](#).
  - I use it, but sparingly, and only at remote locations (way down the list).
- See if your **cable modem** needs a **firmware update or configuration change**:
  - **TODO:** Write this.
- See if your **doorbell camera**, **nannycam**, or **Tile** or  **Apple AirTag tracker device**, needs a **firmware update or configuration change**:
  - **TODO:** Write this, including stalkerware.
- If your networking is slow:
  - Use a **Wi-Fi Analyzer** (I love and use [this one](#)), to find a better channel number, and tell your router to use that. <https://duckduckgo.com/?q=my+router+change+channel>.
  - [Change your computer's DNS Servers](#). **TODO:** Look into **OpenDNS**.
- You might want to review section ["3.7 One-time: Harden your Wi-Fi router, cable modem, and nannycam" above](#), in case I added any new items.
- [Expert] Study the latest [Microsoft Security Intelligence Report](#) and [Krebs on Security blog](#).

## 7.8 Semiannually: Harden your phone life

- Update your info at [Smart911](#).
- If you get junk **robocalls** on your  **landline**:
  - Set up call-blocking call-blocker app [Nomorobo](#) (awesome!), free on most VoIP landlines (a landline provided digitally — perhaps from your cable TV provider).
  - Or, I hear, apps [Truecaller](#) or [RoboKiller](#).
  - [Other options](#)
- If you get junk **robocalls** on your  **smartphone**:
  - Block all suspected spam calls, or send them directly to voicemail:
    - If through Republic Wireless, see [How to Block Robocalls/Spam Calls & Voicemails Using the Republic Wireless App](#).
    - If through any other mobile company, look into call-blocking call-blocker app [Hiya](#) or [others](#), or pay for [Nomorobo](#). Or perhaps, apps [Truecaller](#) or [RoboKiller](#), or [other choices](#).
  - If using an Android, version 7.0 Nougat or above (likely if your phone is from 2016 or later), block **individual numbers** via [How to Block Calls/Numbers on Phones with Android Nougat 7.0 or Higher](#).

-End.- [send comments to the author](#)