Protect your smartphones, tablets and computers 📱💻 from Spam and Malware, via Antivirus

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

Protect your smartphones, tablets and computers 📱💻 from Spam and Malware, via Antivirus 1
1 Introduction 2
2 One-time: Harden your communications platforms 3
2.1 One-time: Harden your 📱 phone life 3
2.2 One-time: Harden your iPad tablet or 📱 iPhone smartphone 3
2.3 One-time: Harden your Android tablet or 📱smartphone or 💻Chromebook 4
2.4 One-time: Harden your Windows Phone 8 WP8 tablet or 📱 smartphone 6
2.5 One-time: Harden your 💻 computer 6
2.6 One-time: Harden your web presence 10
2.7 One-time: Harden your voice-activated devices: virtual assistants, TVs, toys, and more! 11
2.8 One-time: Harden your Wi-Fi router, cable modem, and nannycam 11
2.9 One-time: Retiring/Donating/Disposing a 📱💻 computing device 12
3 When protesting, targeted by adversaries, or 🛂 traveling in authoritarian areas 13
4 Emergency: Find or clean your 📱💻 computing platforms 14
4.1 Emergency: Find or clean your iPad tablet or iPhone 📱 smartphone 14
4.2 Emergency: Find or clean Android tablet or smartphone, or Chromebook 14
4.3 Emergency: Clean your Windows Phone 8 WP8 tablet or 📱 smartphone 16
4.4 Emergency: Find or clean your 💻 computer 16
4.5 Emergency: Change your 📧 email and other passwords 19
4.6 Emergency: Harden your Wi-Fi router, cable modem, and nannycam 19
5 Monthly/Quarterly: Harden your 📱💻 computing platforms 21
5.1 Monthly: Harden your iPad tablet or iPhone 📱 smartphone 21
5.2 Monthly: Harden your Android tablet or 📱 smartphone or 💻 Chromebook 21
5.3 Monthly: Harden your Windows Phone 8 WP8 tablet or 📱 smartphone 21
5.4 Monthly: Harden your 💻 computer 21
5.5 Quarterly: Harden your 💻 computer 23
5.6 Quarterly: Harden your web presence 27
5.7 Quarterly: Correct your 💳 credit reports 27
5.8 Quarterly: Harden your Wi-Fi router, cable modem, and nannycam 27

TODO: Finish sections on configuring and updating your **Wi-Fi router**, **cable modem**, and **nannycam**.
TODO: For **Android** security, be sure to recommend apps Whispercore, Lookout Mobile or Symantec; and see www.networkworld.com/news/2012/051412-android-259182.html.
TODO: Add steps from www.windowssecrets.com/top-story/start-the-new-year-with-a-clean-windows-pc.
TODO: Look into **OpenDNS**.
TODO: Add other cleanup steps, including Registry cleanup, from my other (but now very stale) RunSafe stuff.

1 Introduction

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, and get it from a known good source, e.g., 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, 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**. 12 or 16 letters is **stronger** (and easier to type) than 8 character combination of lowercase, uppercase, numbers and symbols. Perhaps a string of words like `untidygreenideas`.
    - Or perhaps in camelCase, with numbers or symbols thrown in, like `94greenIdeas`.
    - **Nice password-checker**. Google's suggestions and account checkup.

*If you have a **new** smartphone, tablet or computer*, as soon as practical, please do the one-time harden your computing platforms steps below. *If you are thinking of buying a **new Windows PC***, get it with **Windows 10** pre-installed. If a new Android, you might wish to get it with **Android L/5.1/Lollipop** or above.

*If you have not yet upgraded your **Windows 8.1** or **Windows 7** device to **Windows 10** for free*, please see my full instructions for tablet or smartphone or computer.

And 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 **Microsoft Outlook** to do your email:*
  - Bring up the **offending email**.
  - Get an email ready to go to me, perhaps by **Forward**ing the above.
  - In the offending email:
    - *If you use ✉ **Apple's email client** to do email*, do a `View` > `Message` > `Raw Source` > collect that stuff.
    - *If you use ✉ **Microsoft Outlook** to do email*, 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!
  - **Phone me** that you are sending it, so when I don't see it, I will check my two spamfilters. **Thank you!**

2 One-time: Harden your communications platforms

2.1 One-time: Harden your 📱 phone life

- ☐ NEW Be aware of the **grandma scam**. Be ready with a test for any caller claiming to be a relative with an urgent need for money.
- ☐ Be aware that the **IRS** does NOT call you when you 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 **not** call.

  I consider both of these attacks as variations on spear-phishing.

- ☐ *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 form `aaa-eee-nnnn` (e.g., https://google.com/search?q=123-456-7890), and
  - analyze. Good luck!

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

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

- ☐ *If you have an **iPad** tablet or **iPhone** smartphone device that does not yet have **antimalware** software*, please install one. I am familiar with **Lookout**; to install it:
  - launch app **App Store** >
  - 🔍 **Search** for "`Lookout`" >
  - select iPad/iPhone 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.

  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.

- ☐ To help if your **iPad** tablet or **iPhone** smartphone device gets **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.

- ☐ NEW Semi-permanently **mark** your tablet or phone 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, make sure 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.

- ☐ *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.griffintechnology.com/survivor. They have other products, such as the Survivor Slim at www.griffintechnology.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.

- ☐ *If you do **not** use your tablet/phone'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.

- ☐ *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**, such as TunnelBear or Avira Phantom VPN.

- ☐ To help you **fall asleep**, consider installing an app to not display blue light near bedtime. On another platform, I use **f.lux**, to good defect so far. Info. ~~If you have or don't mind jailbreaking your iOS device, download~~.

2.3 One-time: Harden your Android tablet or 📱smartphone or 💻Chromebook

- ☐ *If you have an **Android** tablet or smartphone or Chromium OS **Chromebook** device, that does not yet have **antimalware** software*, please install one of:
  - **Lookout**,
  - Sophos Mobile Security for Android or
  - other options.

- ☐ I am familiar with **Lookout**. To install it:
  - launch app **App Store** (icon may be on its own, may be in folder Google) >
  - 🔍 **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.

  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 Evan 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.

- □ To ensure your **Android** tablet or smartphone device does not suffer from the **Stagefright Flaw** of 2015-07-27, please:
  - launch app **App Store** (icon may be on its own, may be in folder Google) >
  - 🔍 **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** tablet or smartphone device does not suffer from the **Heartbleed** Flaw of 2014-04-09, please:
  - launch app **App Store** (icon may be on its own, may be in folder Google) >
  - 🔍 **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.

- □ NEW Semi-permanently **mark** your tablet or phone 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, make sure 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.

- □ *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.griffintechnology.com/survivor. They have other products, such as the Survivor Slim at www.griffintechnology.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.

- □ *If you do **not** use your tablet/phone'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.

- □ *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**, such as TunnelBear or Avira Phantom VPN.

- □ NEW Follow these Android tips.

- □ 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. On another platform, I use **f.lux**, to good defect so far. 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 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.

2.4 One-time: Harden your Windows Phone 8 WP8 tablet or smartphone

- □ *If you have a **Windows Phone 8 WP8** tablet or smartphone device that does not yet have **antimalware** software*, please:
  - Stay informed. As of 2014-07-09, I know of no antimalware available.

- □ NEW Semi-permanently **mark** your tablet or phone 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, make sure 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.

- □ *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.griffintechnology.com/survivor. They have other products, such as the Survivor Slim at www.griffintechnology.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.

- □ *If you do **not** use your tablet/phone'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.

- □ *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**, such as TunnelBear or Avira Phantom VPN.

- □ **Windows 10 Mobile** is now available. When your **Windows Phone 8.1** offers it to you for free:
  - Use that icon or https://microsoft.com/en-US/windows/windows-10-specifications to "**Reserve your free upgrade**" to Windows 10.
- □ When your phone tells you **WP10 is ready to install**, the next time you have it **plugged in** and don't need it for **a few hours**, tell it to **proceed**. *Please let me know your results!*

2.5 One-time: Harden your computer

- □ NEW *If your computer runs **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-EEE-XXXX***. Logon to this account only for large-scale setup of your machine.
  - Create for yourself a secondary personal username, in format ***FirstLast***, with no spaces. 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** to your name and the year you bought it, in format ***FirstLastYYYY***.

- 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**….
- While there, personalize the name of your **harddrive** `C:\` from `Windows` to something with your name and location, in format ***`FirstLastUSA`***.
- 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** > check **Automatically pick an accent color from your background** > set **Show color on Start, taskbar, and 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://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.
- *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 Windows Defender, and make sure it is **on**. Then Update and do a Full Scan, just for practice.

☐ *If your computer does not yet have **antimalware** software*, **install** one. I recommend these free-for-personal-use:

- *For **Apple Macintosh**:*
  - Sophos AntiVirus for Mac Home Edition (as recommended by http://safecomputing.umich.edu/antivirus), or
  - *If you get your Internet via **Comcast***, you can get Norton Internet Security **free**:
    - Install under Comcast, from http://security.comcast.net.
    - Later, it will update itself from anywhere in the solar system with Internet access.
- *For **Windows 10**:*
  - Microsoft **Windows Defender**. Already installed.
    - Verify Windows Defender is running, and updates itself. To do that:
      - Click `Start` > type "**`defender`**" > wait for `Windows Defender Desktop App` to appear > launch it.
      - Look for:
        - **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 Windows Defender 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
  - free **F-Prot** (did they stop offering that?), or
  - Avira **AntiVir** Personal, or
  - **Malwarebytes** (free is a terrific on-demand scan, but I think the prevention module costs $), or
  - *If you get your Internet via **Comcast***, you can get Norton Security Suite **free**:
    - Install under Comcast, from http://security.comcast.net.
    - Later, it will update itself from anywhere in the solar system with Internet access.
  - Or see http://safecomputing.umich.edu/antivirus/ after they update it.
- *For **Windows 8.1**:*
  - Microsoft **Windows Defender**. ~~Alleged to be already installed.~~ Oops, when I checked a friend's machine, MWD was **not** installed--or maybe a subset. Please continue…
    - Verify Windows Defender is running, and updates itself. To do that:

        - Click **Start** > type "**defender**" > wait for **Windows Defender Desktop App** to appear > launch it.
        - Look for:
            - **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 Windows Defender 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
    - free **F-Prot** (did they stop offering that?), or
    - Avira **AntiVir** Personal, or
    - **Malwarebytes** (free is a terrific on-demand scan, but I think the prevention module costs $), or
    - *If you get your Internet via **Comcast***, you can get Norton Security Suite **free**:
        - Install under Comcast, from http://security.comcast.net.
        - Later, it will update itself from anywhere in the solar system with Internet access.
    - Or see http://safecomputing.umich.edu/antivirus/ after they update it.
- *For **Windows 7**:*
    - Microsoft **Security Essentials** MSE (recommended by UM) if free this week, or
    - **Avast!** Free Antivirus Essential > Free Download (trying this now), or
    - free **F-Prot** (did they stop offering that?), or
    - Avira **AntiVir** Personal, or
    - **Malwarebytes** (free is a terrific on-demand scan, but I think the prevention module costs $), or
    - *If you get your Internet via **Comcast***, you can get Norton Security Suite **free**:
        - Install under Comcast, from http://security.comcast.net.
        - Later, it will update itself from anywhere in the solar system with Internet access.
- *For **Windows Vista** or **XP**:* Upgrade Windows now! Until you do, follow the Windows 7 paragraph...

□ Update your **antimalware/antivirus rules**.

□ *If running under **Windows***, **reboot** (**Start** > **Restart**).

□ NEW *If a laptop,* semi-permanently **mark** your 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, make sure the above includes a phone number **other than** that of your device itself.
- Consider making a second tag, hiding it somewhere within the device.

□ *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**, such as TunnelBear or Avira Phantom VPN. Or I use a small router/Wi-Fi-repeater/-extender; at least I get started off encrypted. **TODO:** Investigate this more.

□ For all web browsers, consider:
- NEW Securing access to your **location**.
- Installing plug-in HTTPS Everywhere from the EFF, protecting you against eavesdropping, tampering with or forging content in some websites you visit. So far, trouble-free for me.
- Installing plug-in PrivacyBadger also from the EFF (good, but I have to tell it to exclude some websites), or
- Installing 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.
- NEW 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 **privacy/Incognito/InPrivate mode**.

- NEW There are many ways to **copy files** from an **old machine** to a **new machine**. Using a thumb-/jump-/USB-/flash-drives works fine, but may get a little confusing if you don't have the right tools on both machines. *[Expert] [me]* Assuming 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. NEW 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.

- To help you **fall asleep**, consider installing an app to not display blue light near bedtime. For a while, I used **f.lux**, to good effect. Info. Download for **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*.

- NEW *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 **Windows 8.1** or **Windows 7** to **Windows 10***:
  - NEW You have to 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.
  - 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.
  - 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 . . .
  - NEW Go to https://microsoft.com/en-us/accessibility/windows10upgrade > **Upgrade Now**.
  - 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.
  - On my old Windows 7 machine, W10 kept using my **old username**, local, and same password. Great.
  - But on a new W8.1 machine, W10 insisted on setting me up with a **new username** that is also an email **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.
  - 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.
  - 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.
  - 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.
  - 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.
  - 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 . . .
  - 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 title bar**.
  - 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.
  - After W10 installed, my **Dropbox** icon no longer appeared in my System Tray. After going to https://dropbox.com and logging in again, my Dropbox icon has returned.
  - After W10 installed, many of my **Start pins** were gone. I rebuilt them.
  - 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://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.
  - After W10 installed, Microsoft **Windows Defender** MWD was installed. Seems to be OK, and adequate. Nothing in the System Tray until you **Start** > "**defender**" > **Windows Defender Desktop App** to appear > launch it. Its icon stays in the System Tray 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 Windows Defender, 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** 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 Windows Defender, so I **uninstalled** McAfee. After a **reboot**, **Windows Defender** 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 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."

2.6 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 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 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**.

- ☐ NEW *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.

  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**!

- ☐ NEW Check if you have any accounts **compromised in announced data breaches**, at Have I Been Pwned? (built by an Aussie computer geek) > ***your@email.address*** and ***usernames*** > **pwned?**. And take appropriate action.

- ☐ NEW *If you get creepy messages on your **Facebook** feed*, please follow the procedures in How to Safely Unfriend a Facebook Creeper.

- ☐ NEW 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 **privacy/Incognito/InPrivate mode**.

- ☐ *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 …

2.7 One-time: Harden your voice-activated devices: virtual assistants, TVs, toys, and more!

- ☐ NEW *Manufacturer* warns customers ☹ not to discuss personal information in front of *voice-activated devices*.

  Current examples:
  - virtual assistants (voice butlers):
    - Amazon **Alexa** on Amazon Echo,
    - Apple **Siri**,
    - Google **Assistant** on Google Home,
    - Microsoft **Cortana**,
    - Samsung **Bixby**,
  - smart **TVs**,
  - voice-activated **toys**,
  - more devices soon?

2.8 One-time: Harden your Wi-Fi router, cable modem, and nannycam

- ☐ ***If** your Wi-Fi router's **SSID (network name)** is personalized, (e.g., **HOME-XXXX** or **2Wire999**)*, you can **skip** this step. *If the SSID is generic (the same as all others of its type) (e.g., **Linksys**)*, 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 **Start** > **Run** > "**cmd [Enter]**" > "**ipconfig [Enter]**" > see something like "**10.0.0.1**" next to "**Default Gateway**" > write that down > prefix that 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 good encryption, such as **WPAWPA2-PSK (TKIP/AES)**. --idea 3
- **Apply.**
- Tell **all** your networked devices (computers, phones, tablets, 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).

□ *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.

□ More tips. Some steps require a Wi-Fi Analyzer, of which I love and use this one.
- NEW If your networking is slow, use this Wifi Analyzer to find a better channel number, and tell your router to use that.

□ *If you have **Comcast** and they provide a Wi-Fi network **xfinitywifi***, **TODO:** Write this.

□ **Cable modem**:
- **TODO:** Write this.

□ **Nannycam**:
- **TODO:** Write this.

2.9 One-time: Retiring/Donating/Disposing a 📱💻 computing device

□ NEW **TODO:** Write something about **wiping** your personal information, including possible harddrive 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.

□ **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** (NEW larger appliances to Republic Services).

3 When protesting, targeted by adversaries, or traveling in authoritarian areas

- □ Be professional in exercising your First Amendment rights. NEW Your goals are more likely to be solved by education, understanding, communication and sympathy. These can happen only if your actions are non-violent.

- □ NEW **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.)

- □ NEW Be aware that anywhere the US President goes, and various other places in the USA and around the world, your mobile devices probably will be tracked and attacked by a **Stingray** device.

- □ *If you think your electronic devices may be taken or compromised*, consider **leaving behind** your electronic devices (phones, tablets and computers) and data (thumb-/jump-/USB-/flash-drives).
  However, if you need them:
  - **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 protest/travel, **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** from Open Whisper Systems, and the EFF's older Occupy guide.

- □ 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.
- □ Form a **social media team**.
- □ Form a **legal 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. I also hear that it will be hot enough to badly burn you, and that a sock or something will provide adequate protection if you can complete your chuck within a second or two.

- □ Have a **first aid** team standing by, with training and equipment, including baby shampoo and LOTS of water (to help get pepper spray out of eyes), treatment for rubber bullet wounds, hypothermia if soaked with water, and whatever else you may run into.
- □ Form a **support team**?

- □ NEW **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.)

- □ Good luck!

4 Emergency: Find or clean your 📱💻 computing platforms

4.1 Emergency: Find or clean your iPad tablet or iPhone 📱 smartphone

- ☐ *If your **iPad** tablet or **iPhone** smartphone 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 "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.

- ☐ *If you have an **iPad** tablet or **iPhone** smartphone device that does not yet have **antimalware** software*, please install one. I am familiar with **Lookout**; to install it:
  - launch app **App Store** >
  - 🔍 **Search** for "**Lookout**" >
  - select iPad/iPhone 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.

  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.

- ☐ After you finish these Emergency steps, make a note to come back tomorrow, to continue with the Monthly section below.

4.2 Emergency: Find or clean Android tablet or smartphone, or Chromebook

- ☐ *If your **Android** tablet or smartphone or 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.

- ☐ *If you have an **Android** tablet or smartphone or Chromium OS **Chromebook** device that does not yet have **antimalware** software*, please install one of:
  - **Lookout**,
  - Sophos Mobile Security for Android or
  - other options.

□ I am familiar with **Lookout**. To install it:
- launch app **App Store** (icon may be on its own, may be in folder Google) >
- 🔍 **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.

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 Evan 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.

□ To ensure your **Android** tablet or smartphone device does not suffer from the **Stagefright Flaw** of 2015-07-27, please:
- launch app **App Store** (icon may be on its own, may be in folder Google) >
- 🔍 **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** tablet or smartphone device does not suffer from the **Heartbleed** Flaw of 2014-04-09, please:
- launch app Google **Play Store** >
- 🔍 **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.

□ After you finish these Emergency steps, make a note to come back tomorrow, to continue with the Monthly section below.

4.3 Emergency: Clean your Windows Phone 8 WP8 tablet or smartphone

- ☐ *If you have a **Windows Phone 8 WP8** tablet or smartphone device that does not yet have **antimalware** software*, please:
  - Stay informed. As of 2014-07-09, I know of no antimalware available. I do not yet know if **Windows 10 Mobile**, now available, makes any difference.

- ☐ After you finish these Emergency steps, make a note to come back tomorrow, to continue with the Monthly section below.

4.4 Emergency: Find or clean your computer

*If you **lost** your computer*:
- ☐ For **Apple Macintosh**, please see "Find My iPhone, iPad, iPod touch, or Mac".
- ☐ **Windows**: **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. Unplug it. 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 drive caddy.
  - 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.

*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*.
- ☐ NEW *How To Fix a Computer That Won't Turn On*.
- ☐ NEW *How To Fix a Computer That Turns On But Displays Nothing*.
- ☐ The notes I have somewhere on what I did in the past.

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

- ☐ *If your computer does not yet have **antimalware** software*, **install** one. I recommend these free-for-personal-use:
  - *For **Apple Macintosh**:*
    - Sophos AntiVirus for Mac Home Edition (as recommended by http://safecomputing.umich.edu/antivirus), or
    - *If you get your Internet via **Comcast***, you can get Norton Internet Security **free**:
      - Install under Comcast, from http://security.comcast.net.
      - Later, it will update itself from anywhere in the solar system with Internet access.
  - *For **Windows 10**:*
    - Microsoft **Windows Defender**. Already installed.
      - Verify Windows Defender is running, and updates itself. To do that:
        - Click `Start` > type "`defender`" > wait for `Windows Defender Desktop App` to appear > launch it.
        - Look for:
          - **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 Windows Defender 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
    - free **F-Prot** (did they stop offering that?), or
    - Avira **AntiVir** Personal, or
    - **Malwarebytes** (free is a terrific on-demand scan, but I think the prevention module costs $), or
    - *If you get your Internet via **Comcast***, you can get Norton Security Suite **free**:
        - Install under Comcast, from http://security.comcast.net.
        - Later, it will update itself from anywhere in the solar system with Internet access.
    - Or see http://safecomputing.umich.edu/antivirus/ after they update it.
- *For **Windows 8.1**:*
    - Microsoft **Windows Defender**. ~~Alleged to be already installed.~~ Oops, when I checked a friend's machine, MWD was **not** installed--or maybe a subset. Please continue…
        - Verify Windows Defender is running, and updates itself. To do that:
            - Click `Start` > type "`defender`" > wait for `Windows Defender Desktop App` to appear > launch it.
            - Look for:
                - **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 Windows Defender 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
    - free **F-Prot** (did they stop offering that?), or
    - Avira **AntiVir** Personal, or
    - **Malwarebytes** (free is a terrific on-demand scan, but I think the prevention module costs $), or
    - *If you get your Internet via **Comcast***, you can get Norton Security Suite **free**:
        - Install under Comcast, from http://security.comcast.net.
        - Later, it will update itself from anywhere in the solar system with Internet access.
    - Or see http://safecomputing.umich.edu/antivirus/ after they update it.
- *For **Windows 7**:*
    - Microsoft **Security Essentials** MSE (recommended by UM) if free this week, or
        - If Windows Defender 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
    - free **F-Prot** (did they stop offering that?), or
    - Avira **AntiVir** Personal, or
    - **Malwarebytes** (free is a terrific on-demand scan, but I think the prevention module costs $), or
    - *If you get your Internet via **Comcast***, you can get Norton Security Suite **free**:
        - Install under Comcast, from http://security.comcast.net.
        - Later, it will update itself from anywhere in the solar system with Internet access.
- *For **Windows Vista** or **XP**:* Upgrade Windows now! Until you do, follow the Windows 7 paragraph...

□ Update your **antimalware/antivirus rules**.
□ **Reboot** (if under Windows, `Start` > `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.

□ *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.

□ *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.

□ NEW *If you are having any networking issues, and running Windows 10,* run **Start** > **Network Status** > **Network Troubleshooter**.

□ NEW *If you are having any networking issues,* run:
- "**ipconfig /all**",
- "**ipconfig /release**",
- "**ipconfig /renew**",
- "**ipconfig /all**",
- "**exit**".

□ NEW *If you are still having any networking issues, and running Windows 10,* run **Start** > **Network Status** > **Network Reset** > **Reset**.

□ NEW You might be able to do some of the below, by **Start** > **Settings** > icon **Update & security** > left-tab **Recovery** > section **Advanced startup** > button **Restart now** > wait for reboot > **Troubleshoot** > **Advanced options** > **Startup Repair** > **Diagnosing your PC**.

□ *If your Windows computer runs **slower** than it used to*, and *you don't need your computer for a several hours (overnight or longer?)*, check for dodgy harddrive disk sectors--and fix them--by running:
- **WindowsLogoKey+X** > **Command Prompt (Admin)** > "**chkdsk /F /R /X /B c: [Enter]**" > "**Y**".
  -OR-
- **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**]*.
- **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** > **Restart**) and let her run!
- To see the results, **TODO:** write this. Apparently, redirect operators **>** or **>>** are not enough.

□ NEW *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.

□ Run the various tools in "**msconfig [Enter]**" (free on Windows) tab **Tools**, including **mmc**.

□ NEW Run **WindowsLogoKey+X** > **Command Prompt (Admin)** > "**sfc /VERIFYONLY [Enter]**".
If it shows anything bad, stay in the Admin command prompt, navigate to ***somewhereGood***, enter "**sfc /scannow > *myComputer*_SFC.txt [Enter]**". It will take a while—a half-hour or so. This article says you may have to run it three times.
If it didn't correct everything, look for guidance on commands **chkdsk**, **sfc** and **dism** at https://google.com/search?q=chkdsk+sfc+dism, for example: reboot, and run it again. And reboot and run a third time. And "**dism /Online /Cleanup-Image /RestoreHealth**", reboot, and run **sfc** a fourth time. And if you have MS Outlook command **scanpst**.

□ You can look in the contents of those files, and look at what you have in that files, or discuss them with me.

□ *If you **still** have problems with your PC*, reset your Windows PC to fix major problems, or NEW http://zdnet.com/article/windows-10-tip-reset-your-pc-completely or https://microsoft.com/en-us/software-download/windows10startfresh.

□ After you finish these Emergency steps, make a note to come back tomorrow, to continue with the Monthly section below. Meanwhile, continue here…

4.5 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!

- ☐ **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.

- ☐ NEW *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.

  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!

- ☐ NEW Check if you have any accounts **compromised in announced data breaches**, at Have I Been Pwned? (built by an Aussie computer geek) > ***your@email.address*** and ***usernames*** > **pwned?**. And take appropriate action.

- ☐ 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 …

4.6 Emergency: Harden your Wi-Fi router, cable modem, and nannycam

- ☐ ***If** your Wi-Fi router's **SSID (network name)** is personalized*, (e.g., **`HOME-XXXX`** or **`2Wire999`**), you can **skip** this step. *If the SSID is generic (the same as all others of its type) (e.g., **`Linksys`**)*, 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 **Start** > **Run** > "**`cmd [Enter]`**" > "**`ipconfig [Enter]`**" > see something like "**`10.0.0.1`**" next to "**`Default Gateway`**" > write that down > prefix that 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 good encryption, such as **WPAWPA2-PSK (TKIP/AES)**. --idea 3
- **Apply.**
- Tell **all** your networked devices (computers, phones, tablets, 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).

□ *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.

- **Cable modem**: **TODO:** Write this.
- **Nannycam**: **TODO:** Write this.

□ Follow http://cnet.com/how-to/tips-to-stay-safe-on-public-wi-fi.

□ After you finish these Emergency steps, make a note to come back tomorrow, to continue with the Monthly/Quarterly section below.

5 Monthly/Quarterly: Harden your 📱💻 computing platforms

This monthly section assumes that you previously followed the one-time suggestions in section 2.

5.1 Monthly: Harden your iPad tablet or iPhone 📱 smartphone

- ☐ On your home screen, *if App "**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 iPad tablet or iPhone smartphone" 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**.

- ☐ NEW Periodically, you might want to review section "2.2 One-time: Harden your iPad tablet or iPhone smartphone" above, in case I added any new items.

5.2 Monthly: Harden your Android tablet or 📱 smartphone or 💻 Chromebook

- ☐ If in "2.3 One-time: Harden your Android tablet or smartphone 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**.

- ☐ NEW If your Android smartphone or tablet is **running slow**.

- ☐ NEW Periodically, you might want to review section "2.3 One-time: Harden your Android tablet or smartphone or Chromium OS Chromebook device" above, in case I added any new items.

5.3 Monthly: Harden your Windows Phone 8 WP8 tablet or 📱 smartphone

- ☐ Update the operating system and apps if they need it.

- ☐ **Windows 10 Mobile** is now available. When your **Windows Phone 8.1** offers it to you for free:
  - Use that icon or https://microsoft.com/en-US/windows/windows-10-specifications to "**Reserve your free upgrade**" to Windows 10.
- ☐ When your phone tells you **WP10 is ready to install**, the next time you have it **plugged in** and don't need it for **a few hours**, tell it to **proceed**. *Please let me know your results!*

- ☐ NEW Periodically, you might want to review section "2.4 One-time: Harden your Windows Phone 8 WP8 tablet or smartphone" above, in case I added any new items.

5.4 Monthly: Harden your 💻 computer

Please do the following **once a month** or so. Windows might run some of these tasks periodically in the background. But some of you have Windows' **Settings** (formerly **Control Panel**) > **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!*):

- ☐ If since the last time you rebooted (under Windows, **Start** > **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 **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 **Windows***, it should be auto-updating. In case it isn't, also do it manually, via **Start** > **All Programs** > **Windows Update** > "**Check for updates**" > if that works, when it finishes scanning:
  - *If there are **Important** updates listed*, select them.
    - *If not, and there are **Recommended** updates*, click **Recommended** and select them.
  - > **OK** > **Install updates**.
  - 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.
  - *[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.
- □ NEW *If the above didn't work*, see https://www.lifewire.com/latest-windows-service-packs-updates-2624595.

- □ *If running under **Apple Macintosh***, update that. 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 system tray, there is an icon—right-click it > "**Update**" or something.
  - Verify that you are up-to-date.

- □ **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; preferably three. Preferably, one copy off-site.
  - NEW 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 on the cloud, in Facebook, ✉ email via webpage, **Dropbox**, **Microsoft OneDrive**, **Apple iCloud**, **Google Drive**, secure **sync.com**, etc. These are all free for the first few GB. 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.
    - NEW *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 **Apple** devices*, you probably already have access to **iCloud**.
    - *If you have a ✉ **Gmail** email account*, you already have access to **Google Drive** and **Docs, Sheets and Slides** 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 thumb-/jump-/USB-/flash-drive). $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.
  - **TODO:** Add here how to back up **Facebook data**.
  - *For **Apple Macintosh***, 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/.
  - *For **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** > **Settings** (formerly **Control Panel**) > **Backup and Restore**, to that external harddrive. I find MS Backup:
      - Probably backs up everything I want (need to verify).

    - Wasteful on space--a large drive I bought to backup two computers, only does mine.
  - *If you need to be thriftier*, 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., CrypoLocker) from wrecking your backup drive as well:
  - Turn **off** your Internet connection (optional) (if you are paranoid) (me, unless rushed for time) (cannot get infected now).
  - *[Expert] [me]* To prevent Norton from quarantining some of my tools, set `Norton` > `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` > `Settings` > `Removable media scan`=`OFF`, set it back =`ON`.
  - Turn **on** your Internet connection (if you turned it off above).
- *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**, **Microsoft OneDrive**, **Apple iCloud**, **Google Drive**, or secure **sync.com** (up six open-bullets). **TODO:** look into whether SyncBackFree is good for this.
  - NEW *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 **Apple** devices*, you probably already have access to **iCloud**.
  - *If you have a 🖂 **Gmail** email account*, you already have access to **Google Drive** and **Docs, Sheets and Slides** 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!
- **TODO:** See if there is anything else I need to copy from tools.doc and the other doc.

- ☐ **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.

- ☐ NEW Periodically, you might want to review section "2.5 One-time: Harden your computer" above, in case I added any new items.

5.5 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…

- ☐ NEW *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 **Edge**.
- ☐ 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):

- If needed, **Update**.
- If during the install, you see a **checkbox** checked, **consider unchecking** it!
- For your *other* web browser (e.g., Internet Explorer, Chrome, Firefox, Opera, Edge), 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**.

□ 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!

□ Remove **QuickTime**, via `Start` > type "`uninstall`" > wait > `Programs and Features` > wait > if **QuickTime** is there, 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` > `Restart` or `Shutdown`).

□ Scroll through **all your programs** (in 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` > `Restart` or `Shutdown`).

□ Consistent with principles at top, **remove** any programs you **no longer need**. If running under Windows, use `Start` > `Settings` (formerly `Control Panel`) > `Programs and Features` > any program you no longer need > right-click > Uninstall. After every two or three, **reboot** (`Start` > `Restart` or `Shutdown`).

□ *If you use web browser **Chrome***, periodically look through tabs:
- `chrome:extensions`
- `chrome:plugins`
  - **Un**check **all** checkboxes `Always allowed`. I find I don't need any of them.
  - **Disable** any plugins you don't use:
    - `AdobeAAMDetect`, **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.

- ☐ 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 (you might have to Paste into your secondary or tertiary web browser, or set **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, via reboot > **Settings** (formerly **Control Panel**) > **Programs and Features** > click and **Uninstall** 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** > reboot.
        - *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 **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 (you might have to Paste into your secondary web browser, or set **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 **Settings** (formerly **Control Panel**) > **Java** > tab **Security** > **un**check **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.
    - *[Expert]* Might need to see **Start** > **Settings** (formerly **Control Panel**) > **Programs and Features** > uninstall programs you don't need.

- ☐ *If your 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 the Norton > Security > Run Scans > Norton Power Eraser utility, and the Norton Bootable Recovery Tool. I have not used these.

- ☐ *If your Windows computer runs **slower** than it used to*, wack or delay unnecessary programs that **start themselves automatically**, using:
    - *[Easy] If you have **Norton Security Suite** (free with Comcast)* > **Tuneup** > **Startup Manager**; or
    - *[Easy]* If running Windows 10, **Task Manager** tab **Startup** (works fine, easier than below); or

- *[Moderate]* If running 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 Windows computer runs **slower** than it used to*, run **CCleaner** Free > 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 > 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
  - **un**check **every checkbox**.

□ *If your 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 thumb-/jump-/USB-/flash-drives (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
    - **un**check **every checkbox**.

□ *If your Windows computer runs **slower** than it used to*, and *you don't need your computer for a several hours (overnight or longer?)*, check for dodgy harddrive disk sectors--and fix them--by running:
- `WindowsLogoKey+X` > `Command Prompt (Admin)` > "`chkdsk /F /R /X /B c: [Enter]`" > "`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` > `Restart`) and let her run!
- To see the results, **TODO:** write this. Apparently, redirect operators `>` or `>>` are not enough.

□ NEW *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.

□ Run the various tools in "`msconfig [Enter]`" (free on Windows) tab `Tools`, including `mmc`.

- ☐ Run **WindowsLogoKey+X** > **Command Prompt (Admin)** > "**sfc /VERIFYONLY [Enter]**".
  If it shows anything bad, stay in the Admin command prompt, navigate to ***somewhereGood***, enter "**sfc /scannow > *myComputer*_SFC.txt [Enter]**". It will take a while—a half-hour or so.
  If it didn't correct everything, look for guidance on commands **chkdsk**, **sfc** and **dism** at https://google.com/search?q=chkdsk+sfc+dism, for example: reboot, and run it again. And reboot and run a third time. And "**dism /Online /Cleanup-Image /RestoreHealth**", reboot, and run **sfc** a fourth time. And if you have MS Outlook command **scanpst**.

- ☐ For all web browsers, consider:
  - NEW Securing access to your **location**.
  - Installing plug-in HTTPS Everywhere from the EFF, protecting you against eavesdropping, tampering with or forging content in some websites you visit. So far, trouble-free for me.
  - Installing plug-in PrivacyBadger also from the EFF (good, but I have to tell it to exclude some websites), or
  - Installing 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.

5.6 Quarterly: Harden your web presence

- ☐ *If you have a Google account* (you might, even though you have no Gmail account), follow Google's Privacy Checkup.

- ☐ NEW Review the **Privacy Settings** in your email provider, Facebook, and web browsers. They occasionally change them.

- ☐ NEW Check if you have any accounts **compromised in announced data breaches**, at Have I Been Pwned? (built by an Aussie computer geek) > ***your@email.address*** and ***usernames*** > **pwned?**. And take appropriate action.

- ☐ Follow Kim Komando's "*Google yourself to protect your reputation--online and off*".

5.7 Quarterly: Correct your credit reports

- ☐ Follow my article on Credit Reports.

5.8 Quarterly: Harden your Wi-Fi router, cable modem, and nannycam

- ☐ See if your **Wi-Fi router** needs a **firmware update**:
  - **Netgear** > 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.

- ☐ *If you have Comcast and they provide a Wi-Fi network* ***xfinitywifi***, **TODO:** Write this.
- ☐ See if your **cable modem** needs a **firmware update**:
  - **TODO:** Write this.
- ☐ See if your **nannycam** needs a **firmware update**:
  - **TODO:** Write this.

- ☐ NEW If your networking is slow, change your router's channel number, using guidance from Wifi Analyzer.
- ☐ NEW If your networking is slow, change your computer's DNS Servers.

- □ NEW You might want to review section "2.7 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.

-End.- send comments to the author