Security Updates for your other devices

For devices that are not your Apple Devices (Mac, iPhone, iPad, TV, watch, etc) and their installed Apps.

Introduction:

- Typically, we think of Security updates to only include our Apple Devices.
- We run the Apple updaters to fix bugs, add features, and most importantly apply security updates.
- We also update the supplied Apple software, Safari, Photos, Facetime, etc to get the security updates along with bug fixes and new features.
- Most third-party software has methods to update. Again, along with bug fixes, new features and the like, we get security updates. Just in case you do not know, third party software is software supplied by other companies than Apple.
  - Examples Microsoft Office, Adobe products, Zoom etc.
- However, we forget that other hardware devices have firmware running them, and especially if they live on your home network and/or connect to the Internet do require Security Updates.

Printers:

- This one is something I never thought about, Until the headlines hit about printers.
  - To quote from the Verge article: "Serious security flaws have been found in hundreds of Brother printer models that could allow attackers to remotely access devices that are still using default passwords. Eight new vulnerabilities, one of which cannot be fixed by patching the firmware, were discovered in 689 kinds of Brother home and enterprise printers by security company Rapid7. The flaws also impact 59 printer models from Fujifilm, Toshiba, Ricoh, and Konica Minolta, but not every vulnerability is found on every printer model."
- All I used to think about was the Printer installed on my Macs. In the old days this often meant getting Print drivers from the Printer Vendor, when upgrading to a new version of the Mac OS.
- Airprint introduced back in MAC OS 10.7 largely eliminated this task, with Apple's software engineers taking care of the job for the Printer Vendors and you
- Here we are talking about the Firmware inside the printer.

Printers (Cont'd):

- Looking into support for my Brother Printer HL-L2360DW:
  - A number of security issues were fixed with the latest firmware update
  - There was also an issue with the default password
- To update the printer's firmware, you will need to go to the printer vendors webpage and go to the support webpage.
  - No, I'm not about to research and publish the millions of such pages
- https://support.brother.com/g/b/downloadlist.aspx?c=us&lang=en&prod=hll2360dw_us&os=10083 is the one for my printer. Demo
- As to the password. If you go back to the previous page, you see one vulnerability can't be patched. Actually, Brother said two of them can't be patched and it has to deal with the default password.
  - The issue is that post ~2020 used the printer's serial number to generate a default password. The issue came up when the bad guys figured out how Brother generated the password, and one of the other vulnerabilities allowed remote access to the printer's serial number

Printers (Cont'd):

- It was even worse pre 2020 when the printers used a default common password for all machines.
- The solution is to create a unique strong password that can't be determined and update the password.
- In the case of my Brother printer this means accessing the printer trough your browser to a web page generated by the printer itself.
- The IP in this case is 192.168.1.69 DEMO
  - While this is specific to my printer, for many of the devices talked about in the next set of slides, this is how you will need to access the device.

Routers:

- Well, there is good news and bad news here!
- First off, the Router is a network device that forwards data packets between networks.
- In your home environment this is between the Internet (WAN) and the local computers and devices on your local network. (LAN)
- Today many routers include Wireless home networking, and may include the modem that interfaces with the medium that your internet comes in on. (Cable, telco line for DSL, etc.) this is not a requirement.
- You don’t want the security of your router compromised.
  - Disrupt your connection to the internet
  - Spy on your activities
  - DNS spoofing Send your bank app to a hacker's fake page
  - Botnets Use your router along with thousand of other compromised units to attack or deny services. Send threats to federal folks. Then the FBI shows up at your door!

Routers (cont'd):

- If you have Frontier, Spectrum, Cox, or ATT fiber, and you use the router they give you, they claim to push the security updates to you. If you provide your own router from an approved list, it's a bit less clear, but it seems that the updates are available. Seems you can't manually update.
- Now if you Internet provider just gave you a modem, with just a LAN ethernet jack for one computer and you then added a router for wireless and/or multiple ethernet jacks, then you are responsible to get updates for the router.
- Go to the router vendors website. Get and install the update.
- Now the bad news. If you see the router vendor has ended support of the router there is not much you can do. Toss the router. Sometimes the router vendor says nothing, but note the last update is two or more years in the past, likely they dropped support of that router. Same, toss it.
- https://www.usatoday.com/story/tech/2025/05/09/linksys-internet-routers-cyberattack-fbi/83537973007/

NAS (Network Attached Storage):

- Network Attached storage (NAS) is a shared device on a network that serves files to multiple devices. Often it has multiple hard drives to support redundant backup of the multiple devices.
  - Great for mass storage needs like multi terabyte video files
- Many can be remotely accessed via the internet. This makes security very important.
- Researched this a bit, a very complex subject. I don't have enough time to do further research. Vendors do provide security updates. If you use these it is important that security updates, be applied.

IOT (Internet of Things)

- The Internet of Things has expanded greatly over the years. An incomplete list:
  - Security Cameras
  - Smart Thermostats
  - Smart Lighting
  - Smart TV's
  - Smart (Power) Plugs
  - Burglary sensors
  - Smart Appliances
  - Smart Sprinklers
  - Fitness devices
  - Doorknobs

IOT (Internet of Things) (Cont'd)

- Security Cameras: Useful for protection of your home
- However, you do not want poor security to allow the bad guys to view the contents your cameras, or turn them off to rob your house.
- You want to go with reputable vendors. If they store your cameras recordings on their servers you want to immediately access them if needed and you don't want them viewing your private contents.
- The cameras themselves may need security updates or if the cameras connect to a supplied vendors Hub, then the Hub will need the security updates.
- There is EOL issues for cameras just like the routers mentioned in the previous slides.
  - Wyze announced in 2020 that their 1st Gen cameras could not get any updates and you should stop using them. They discontinued them at the time. Also, they knew about security issues earlier and said nothing.
  - https://tidbits.com/2022/04/01/the-real-reason-wyze-labs-discontinued-its-first-generation-security-camera/

IOT (Internet of Things) (Cont'd)

- Smart Thermostats: Allow you to access them via your Apple device
  - Ecobee says they will auto-update if connected to WiFi
  - Check on other models
- Smart TV's
  - https://www.bleepingcomputer.com/news/security/over-90-000-lg-smart-tvs-may-be-exposed-to-remote-attacks/
- For all the other devices check your user manual and/or go to the Vendors website and look up your model

Final Thoughts:

- https://www.bleepingcomputer.com A good site to find security issues with devices
- Bart Busschots Security Bits show Usually every other week on Allison's Nosillacast podcast Some notable security updates flagged
- Your vendors Website