**1. What did you do?**

I performed an attack surface analysis for by family and I. To do this I started with all of the locations where my family and I work, live, and frequent. I did not assess the risks in public places like restaurants or shops. I also did not assess the risks in the controlled network environment at work, nor did I assess the risks for my family at their work or school environments; however, I did encourage the adults to perform the same analysis for their personal situations. While I did take their attack surfaces into consideration, the reality is the, especially for my wife and two oldest sons, as adults they have work environments and work usage patterns that I cannot observe or know much about. Even when I inquire for information about this the responses I got were muted and incomplete.

I started with our home as it is the most obvious attack surface. A catalogued the network and a litany of IOT devices we have deployed including security cameras, gaming systems, smart TVs, and even a few smart appliances. Our property comprises two homes and a separate garage with an apartment. My wife and I and three of my children live in the main house, my oldest son intermittently lives in the garage apartment, and my in-laws live in the second house. The main house and the second house are connected via a buried Cat5 ethernet cable. GVTC provides internet to the house via fiber to the curb. The GVTC service lands in a Calix Router/Gateway. I have installed a whole home mesh wifi using a Netgear Obrbi6 system with two satellites. One satellite is in the second house and the other satellite is in the garage. I have a pair of ubiquity bridge nodes that wirelessly carry the signal from the house to the garage. The second Orbi satellite is connected to the ubiquity bridge node in the garage. I ran a port scan on each of the 63 devices on the network and found numerous open ports on many of the devices. As a matter of practice I do use complex passwords on all my devices and use 1Password as a password manager for all of my password requiring multi-factor authentication to login to 1Password.

Of the 63 devices at the house, there is one Ring Doorbell and four Ring cameras, three with solar panels. There are also two Wyze cameras and two Wyze plugs in the house. We have three smart-TVs and four standard TVs with Apple TV, Amazon Fire Stick, or Google Chromecast devices attached. We also have six Amazon Alexa devices deployed throughout the house to serve as alarm clocks or smart speakers. The Whirlpool Washer and Dryer are also connected to the internet. Everyone in the house has at least one PC. The primary use case for these computers is for schoolwork; however two of them are Gaming PCs. There are also three Xbox devices in the house.

I then moved on to the RV, where I live for work during the week. I found a smaller attack surface there. Internet is provided by the RV Park and I use a personal router/firewall to aggregate all of my devices to that device and then connect that device to the publicly exposed wifi. Because I have not disabled SSID broadcast on that device there remains an attack vector for an intruder to attempt to join the network. I have a Ring Doorbell on the door of the RV and several Wyze cameras looking out the windows. I also have an Acurite weather station that uses an RF frequency to communicate with a control panel that uses HTTPS to upload weather data to the internet.

In the second/guest house the attack surface is smaller as my in-laws really only use one of the aforementioned TVs, their cellphones (which I’ll address later), and a Windows Surface Pro & HP Laserjet Printer that my mother in-law uses to run their small business.

Another physical attack surface is the 2020 Ford F-250 that I drive. The truck has a Sync3 system that is integrated with Ford’s FordConnect system. The truck has a built-in WiFi hotspot for passengers to share a mobile internet connection; however, since I usually travel alone I have not paid for this service and, as such, have turned the WiFi hotspot off.

The most significant, and difficult to quantify/capture, attack surface are the mobile devices. While I use parental controls to control what apps my 16yo daughter and 11yo son can use on their iPhones. My iPhone is littered with dozens of apps that I have failed to remove or haven’t removed because “someday” I “might”. My wife’s phone is the same way. I have removed parental controls from my two oldest sons’ devices and so I have very little insight into what apps they’re using and, hence, what risks they bring onto the network when they’re home. The same with my in-laws.

One of the most prevalent attack surfaces for everyone in my family is in relation to email. I have two personal email accounts, one work email account, and one school email account. My wife has one personal email account and one work email account. My daughter has one school email account and one personal account. My youngest son has one school email account and one personal email account. My second oldest son has a school email account, a personal email account, and a business email account. My oldest son has one email account. My in-laws each have a personal email account and a shared business email account. My work email account, my school email account, my wife’s work email account, my two youngest kids’ school email accounts, and my second oldest son’s school email account have any antivirus scanning. That means that 11 out of the 17 email accounts that we have between the eight of us are unprotected from attack.

I also ran each of those 17 email addresses through the <https://haveibeenpwned.com> utility and found that every one of them has been found in a security compromise. I checked all of the major passwords that I currently use and didn’t find any of them in the database.

**2. What were the results?**

Through this exercise I’m feeling quite a bit of self-condemnation. I know better than this but have done virtually nothing to proactively mitigate these risks. The net result was that my family and I have a very significant attack surface and, while it’s easy to convince oneself that the threat is minimal due to the remote nature of our home, the reality is that our attack surfaces also follow us when we leave there.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk Category** | **Location** | **Type** | **Brand** | **Description** | **Primary TCP Port** |
| Physical | House | IOT | RING | Front Door – Doorbell | 443 |
| Physical | House | IOT | RING | Garage side | 443 |
| Physical | House | IOT | RING | Well side | 443 |
| Physical | House | IOT | RING | Back Porh - Pool | 443 |
| Physical | House | IOT | RING | Back Porch - Stairs | 443 |
| Physical | House | IOT | Wyze | Kitchen | 443 |
| Physical | House | IOT | Wyze | Dog Crate | 443 |
| Physical | House | IOT | Jandy/Polaris | Pool | 80 |
| Physical | House | IOT | Samsung | LivingRoom TV | 443 |
| Physical | House | IOT | Samsung | Master Bedroom TV | 443 |
| Physical | House | IOT | Samsung | Sarah TV | 443 |
| Physical | House | IOT | Vizio | Josh TV | 443 |
| Physical | House | IOT | LG | Patio TV | 443 |
| Physical | House | IOT | Samsung | Poolhouse TV | 443 |
| Physical | House | IOT | Amazon | Echo - SAM | 443 |
| Physical | House | IOT | Amazon | Echo - SARAH | 443 |
| Physical | House | IOT | Amazon | Echo - Kitchen | 443 |
| Physical | House | IOT | Amazon | Echo - Master Bedroom | 443 |
| Physical | House | IOT | Amazon | Echo - Master Bathroom | 443 |
| Physical | House | IOT | Amazon | Echo - Back Porch | 443 |
| Physical | House | IOT | Amazon | Echo - Patio | 443 |
| Physical | House | IOT | Amazon | FireTV | 443 |
| Physical | House | IOT | Amazon | FireTV | 443 |
| Physical | House | IOT | Apple | AppleTV | 443 |
| Physical | House | IOT | Apple | AppleTV HD | 443 |
| Physical | House | IOT | Google | Chromecast | 443 |
| Physical | House | IOT | Microsoft | Xbox One X - Family | 443 |
| Physical | House | IOT | Microsoft | Xbox Series S - Ben | 443 |
| Physical | House | IOT | Microsoft | Xbox Series S - Josh | 443 |
| Physical | House | IOT | Nintendo | Switch - Sarah | 443 |
| Physical | House | IOT | Nintendo | Switch - Sam | 443 |
| Physical | House | IOT | Whirlpool | Washer | 443 |
| Physical | House | IOT | Whirlpool | Dryer | 443 |
| Physical | House | IOT | Calix | Router | 443 |
| Physical | House | IOT | Netgear | Orbi Base | 443 |
| Physical | House | IOT | Netgear | Orbi Satellite | 443 |
| Physical | House | IOT | Netgear | Orbi Satellite | 443 |
| Physical | House | IOT | Netgear | Nighthawk | 443 |
| Physical | House | IOT | Ubiquiti | POE Wireless Bridge | 443 |
| Physical | House | IOT | Ubiquiti | POE Wireless Bridge | 443 |
| Physical | House | IOT | Netgear | 5-Port POE Switch | 443 |
| Physical | House | IOT | Netgear | 5-Port POE Switch | 443 |
| Physical | House | IOT | HP | Laserjet Printer | 443 |
| Physical | RV | IOT | RING | Door | 443 |
| Physical | RV | IOT | Wyze | PAN Cam | 443 |
| Physical | RV | IOT | Wyze | Interior Front | 443 |
| Physical | RV | IOT | Wyze | Left Rear | 443 |
| Physical | RV | IOT | Wyze | Left Center | 443 |
| Physical | RV | IOT | Acurite | Weather Station | RF/443 |
| Physical | RV | IOT | Netgear | WISP Router | 443 |
| Physical | RV | IOT | Apple | AppleTV | 443 |
| Personal | Jim | IOT | Ford | F-250 - FordConnect | 443 |
| Personal | Jim | IOT | Apple | iPhone | MANY |
| Personal | Jim | IOT | Apple | Watch | BT |
| Personal | Jim | IOT | Dell | Laptop | MANY |
| Personal | Jim | App | Various | Social Media | 443 |
| Personal | Jim | App | Microsoft | Web Browser - School | 443 |
| Personal | Jim | App | Microsoft | Web Browser - Work | 443 |
| Personal | Jim | App | Microsoft | Remote Desktop | 3389 |
| Personal | Jim | App | Microsoft | Visual Studio | MANY |
| Personal | Jim | App | Microsoft | SQL Server | 1433 |
| Personal | Jim | App | Wyze & Ring | Camera Apps | 443 |
| Personal | Jim | App | Fidelity | Investing | 443 |
| Personal | Jim | App | Microsoft | Office365 | 443 |
| Personal | Jim | App | Microsoft | Outlook | 443 |
| Personal | Jim | App | Autodesk | Desktop Connector | 443 |
| Personal | Kristie | IOT | Microsoft | Surface Laptop | MANY |
| Personal | Kristie | IOT | Apple | iPad | MANY |
| Personal | Kristie | IOT | Apple | Watch | MANY |
| Personal | Kristie | IOT | Apple | iPhone | MANY |
| Personal | Kristie | App | Various | Social Media | 443 |
| Personal | Kristie | App | Microsoft | Web Browser - Work | 443 |
| Personal | Kristie | App | Custom | Banking | 443 |
| Personal | Kristie | App | Wyze & Ring | Camera Apps | 443 |
| Personal | Kristie | App | Microsoft | Office365 | 443 |
| Personal | Kristie | App | Abbott Labs | Blood Glucose Monitoring Software | 443 |
| Personal | Kristie | App | Microsoft | Outlook | 443 |
| Personal | Kristie | App | Apple | iTunes | 443 |
| Personal | Ben | IOT | Dell | Laptop | MANY |
| Personal | Ben | IOT | Custom | Gaming Desktop | MANY |
| Personal | Ben | IOT | Apple | iPhone | MANY |
| Personal | Ben | App | Microsoft | Office365 | 443 |
| Personal | Ben | App | Microsoft | Web Browser - School | 443 |
| Personal | Ben | App | Microsoft | Web Browser - Personal | 443 |
| Personal | Ben | App | Various | Social Media | 443 |
| Personal | Ben | App | Steam | Steam | 443 |
| Personal | Ben | App | Discord | Discord | 443 |
| Personal | Ben | App | Epic | Fortnite | 443 |
| Personal | Ben | App | Microsoft | Minecraft | 443 |
| Personal | Sarah | IOT | Microsoft | Surface Laptop | MANY |
| Personal | Sarah | IOT | Microsoft | Surface Go | MANY |
| Personal | Sarah | IOT | Apple | iPhone | MANY |
| Personal | Sarah | App | Google | Web Browser - School | 443 |
| Personal | Sarah | App | Various | Social Media | 443 |
| Personal | Sarah | App | Discord | Discord | 443 |
| Personal | Sarah | App | Microsoft | Office365 | 443 |
| Personal | Sam | IOT | Custom | Gaming Desktop | MANY |
| Personal | Sam | IOT | Apple | iPhone | MANY |
| Personal | Sam | IOT | Microsoft | Surface Go | MANY |
| Personal | Sam | App | Various | Gaming | 443 |
| Personal | Sam | App | Epic | Fortnite | 443 |
| Personal | Sam | App | Microsoft | Minecraft | 443 |
| Personal | Sam | App | Microsoft | Office365 | 443 |
| Personal | Josh | IOT | Apple | iPhone | MANY |
| Personal | Josh | IOT | Microsoft | Surface Laptop | MANY |
| Personal | Josh | App | Various | Social Media | 443 |
| Personal | Josh | App | Microsoft | Office365 | 443 |
| Personal | Kathy | IOT | Microsoft | Surface Pro | MANY |
| Personal | Kathy | IOT | Apple | iPhone | MANY |
| Personal | Kathy | App | Microsoft | Office365 | 443 |
| Personal | Kathy | App | Various | Social Media | 443 |
| Personal | Kathy | App | Intuit | Quickbooks | 443 |
| Personal | Kathy | App | Microsoft | Office365 | 443 |
| Personal | Gerald | IOT | Apple | iPhone | MANY |
| Personal | Gerald | App | Meta | Facebook | 443 |

**3. What did you learn?**

My key takeaway from this exercise is that I need to take personal information security much more seriously. I need to prioritize several activities to protect myself and my family as soon as possible. For the devices listed above as using a Primary TCP Port of “MANY” I will be performing a detailed assessment and removing any unnecessary applications and using a port scanner to confirm that the attack surface is minimized for those devices. For those listed as using “443” I will use the same port scanner to confirm that their traffic is indeed limited to ports 80 or 443. If I find anything odd I will discontinue the use of the device and contact the vendor for instruction on how to limit the attack surface of the device. Next, I will be more intentional when adding new apps and new devices to the network, regularly inspecting the device list captured by the Orbi routers to ensure that there are no rogue or unexpected devices connecting. I will also review the network security settings on the Orbi routers to ensure that only authorized devices can connect to the network. I will work with my family to make sure that everyone understands the risks and potential consequences of installing applications or devices.

One of the most significant threat vectors for the family is our use of Apple iPhones. The good news is that they’re all newer models and all have a reasonably current version of iOS installed; however the devices are not universally configured to automatically update iOS or installed apps. I will gather all of the iPhones and make sure that they are all setup to automatically install the latest publicly released iOS updates and App Updates.

Even though I use a password manager, I need to reinforce to my family that they too need to take advantage of the family subscription we have and they need to take their personal information security more seriously. I will begin changing my passwords on a more consistent basis and will continue to embrace multi-factor authentication and passkey technologies as the apps and services I use implement them.

To protect my kids I already use Apple’s Parental Control features; however, I do need to do a better job of vetting new apps as they are requested. There are several steps that I usually take when they request an app; but if I’m being really honest with myself I need to dig deeper into these apps and understand better how they work, what data they collect, and what they do with that data. I’ve already made sure that nobody is using TikTok; however, we need to have a family review of all social media, paying special attention to what information each of us has exposed through our profiles and what our individual privacy settings are. This will be a slow and cumbersome process, but it needs to be done in detail.

Finally, I need a better way of controlling what new devices can connect to the network, what they can do on the network, and how to know if something is amiss. I will begin investigating an intrusion detection system or something similar so that I can proactively know if something is afoot. Today I would have no way of knowing until it was too late. For that matter, I can’t know that it hasn’t already happened.

**4. How does it relate?**

This is very relatable. Even though I pay for identity protection for my family through LifeLock, I have been using that as a mental excuse for allowing poor personal information security practices to abound in my home. This has left me and my family with a significant attack surface, most of which would not be protected by that insurance. Identity protection services cover Identity Theft; however, they don’t cover information theft or illicit or illegal monitoring or traffic of personal/private information. The only real mitigation for this is to take personal responsibility for my actions and may family’s safety.

The following information will help me to mitigate these risks.

[Introducing Stricter Message Settings for Teens on Instagram and Facebook | Meta (fb.com)](https://about.fb.com/news/2024/01/introducing-stricter-message-settings-for-teens-on-instagram-and-facebook/)

[Parental Guide for Teens on Instagram | About Instagram](https://about.instagram.com/community/parents)

[Snort - Network Intrusion Detection & Prevention System](https://www.snort.org/)

[PRTG Network Monitor – All-in-one network monitoring tool (paessler.com)](https://www.paessler.com/prtg/prtg-network-monitor)

[Protect Your iPhone from Hackers with These Essential Tips | www.iphonelife.com](https://www.iphonelife.com/content/10-tips-to-protect-your-iphone-hackers)