DIGITAL LITERACY
COMPUTER CLASSES

DIGITAL HOUSEKEEPING

SEPTEMBER 13, 2019

A LITTLE OF THIS AND A LITTLE OF THAT

SmorgasBORK.

Today, a grab bag of information and advice on keeping your digital house in order. A smörgåsbord, if you will.

Let me take a guess, and forgive me for profiling: you *do* want to be involved in the digital world—to some degree, at least. You *don't* want to be overwhelmed with a waterfall of jargon, and you *don't* have the time or inclination to learn basically a professional's entire career worth of nerdy trivia and security information.

I get it! This information is for you.

YOUR DIGITAL DOOHICKEYS
AND HOW THEY COHABITATE

INTERNET OF THINGAMIES

Your computer, tablet, and phone all connect to the Internet. Well, *duh*. Of *course* they do. But in our marvelous push-button future, your various security cameras, smart speakers, lightbulbs, washing machines, refrigerators, and assorted doodads are all jostling for a chance to go online.

"Woah, woah," you say. "Those of you who can't connect to cell networks, look, there's only *one* internet connection to this house and we all have to share." How do we accomplish this? By building a **home network**.

NETWORK

He's mad as hell and he's not going to take it anymore!

To facilitate talking to *each other* and not all screaming randomly in a cacophony, every device on a network[1] is assigned a unique IP address. True nerds[2] will often assign "static" IPs to devices on networks over which they exercise their dweeby mastery, but often, devices are assigned an IP by some server providing DHCP.[3] Never mind the acronyms; what this means is when you connect to a router, either with an Ethernet cable (they look like big fat phone jacks) or by Wi-Fi, after a bit of handshaking and negotiation, it just works. We'll look at networks more closely in other classes, but for now, let's look at a typical setup:

Okay, I lied. In a truly typical setup, the modem, router, and access point are all wrapped up in one device called a wireless gateway that your "friendly" "local" ISP[4] oh-so-generously *lets* you use—for $10-15 a month. Forever.

I'll break it to you now that *this is how they get you.*[5] After a while, you'll quickly pay much more for that dumb thing with poor Wi-Fi performance than you would for various cool devices you own and control—in fashion, they might call these "separates." But your choice!

MAKING YOUR NETWORK WORK

Work it, girl! When you first get going with that gateway straight from Comcast HQ in the land of Mordor, where the shadows lie, it will be primed and ready to give all your devices a way to talk to each other and the Internet at large. But how? I presume the brute who installed it grunted and set up a computer or two without explaining what he was doing

---

[1] A TCP/IP network, that is. There are other network schemes, but … you'll never see one. I mean, have you ever been in a 1980s Token Ring? Of course not.

[2] Yes, I confess I do this with most devices that remain stable on my own network at home. It's nice to always know the printer is at 192.168.0.6.

[3] Dynamic Host Configuration Protocol. Aren't you glad you asked?

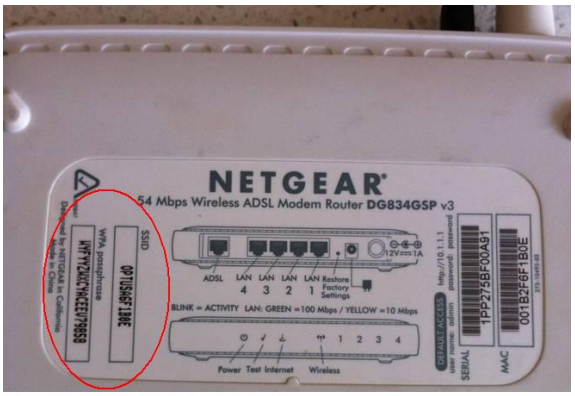
[4] It's Comcast, isn't it? Bah! You may as well get your Internet from *Satan*.

[5] Well, one of many, *many* ways, among overcharging, underdelivering, throttling your speeds, limiting your bandwidth, steering you evilly to their own monopolistic services, and selling your DNS queries to advertisers. A pox on their house!

before departing, but what if you get a new printer and want it to be available to all your other thingamies?

Lift your gateway in a mighty, Samsonian grip and peep at the bottom:

See that "SSID" and "WPA passphrase" business? "SSID" is the nerd way of saying "name" of your Wi-Fi network and "WPA passphrase" is the password you'll need to enter to join the network and enjoy the protection of its encryption. WPA2/PSK[6] is the current standard of encryption and protection. Exploits for it exist, but it's the best we have at the moment and its successor, WPA3, isn't even out in the world yet and people have already discovered exploits for it, so ...



YOU SHOULD REALLY REALLY DO THESE THINGS RIGHT NOW IF YOU HAVEN'T ALREADY

1. Using information that should also be printed on the device, log in to your router/gateway/whatever's web server[7] and change its administrator account name and password. And for heaven's sake, *write these down*, or tell them to a parrot with an infallible memory and an excellent health prognosis for long life.
2. If your router has new firmware available, get it and install it to fix security problems and improve functionality. The manufacturer's web site will help.
3. This will be on by default, but do make sure an SPI[8] firewall is running.
4. Change the SSID and password to something that's not a bewildering string of random characters. You will not make a lot of friends if people ask to join your Wi-Fi and you tell them, "Sure, just join E19HX2B4#K3776 and the password is LKJNLKJ*Y(%*FN(*%HOIUNF()*Y$HON@#O#IY$*."
5. While you're at it, if your router supports a Guest Network, set one up. This is a second Wi-Fi network that allows people who join it to get to the Internet, but not your precious computers and printers and lightbulbs. Particularly if you rent out rooms or houses, good digital fences make good digital neighbors.

[6] "Wi-Fi Protected Access with Pre-Shared Key." Impress your friends at parties by rattling off these and other acronyms. My friends are already sick of me doing it, so it's your turn.

[7] Basically, its own little web page. Where to find it? Open a browser and where you'd normally type google.com or ihatecomcast.com, type 192.168.0.1 and go. If that doesn't work, 192.168.1.1

[8] "Stateful Packet Inspection." Whew! We're havin' fun now!

I OWN A 13,000 SQUARE-FOOT MANSION AND MY WI-FI DOESN'T WORK WELL

Congratulations, Richie Rich. Hmph. Yes, there are times when a single access point is inadequate to reach every distant corner of your dwelling. You may have thick walls, or lots of interference from other devices flying around. Enter the **wireless mesh router**.

There are now dozens of these, made by eero, Google, Netgear, Linksys, Ubiquiti, TP-Link, etc., etc. The idea is you get to enjoy the convenience of a big fancy distributed Wi-Fi system that lets you roam around and hop seamlessly between access points. They're consumer-oriented, so setup won't be a big problem.[9] In this case, you'd connect one node of the mesh to a modem with an Ethernet cord, and then the nodes talk to each other either over Ethernet (preferable) or wirelessly. Wirelessly, one has to be close enough to the other to have a conversation, but then they can blanket your house in warm, fuzzy Wi-Fi that science hasn't yet proven to be carcinogenic.

CUTTING THE CORD

Oh, the various devices we have now! If you've been paying $200 a month to Comcast[10] for a bloated package of cable TV that's all garbage anyway and want to give those devils the heave-ho, you still have many options. AppleTVs, Rokus, Amazon Fires, Google Chromecasts – all deliver various video content and all offer ways to spend money to rent or buy[11] what you'd like to see. Many TVs cut out the middle man and can do all this themselves. Alls you need is the Internet. And it's out there, waiting!

*Yo: Change the default passwords on **all** your Internet-of-Things devices. Do it now!*

[9] My Linksys Velop is a little *too* trimmed-down and friendly for my tastes, but I had fewer options when I was shopping for my mesh system.
[10] From Hell's heart, I stab at thee; For hate's sake, I spit my last breath at thee!
[11] If you can call an end-user license to view something only until the providing entity loses the rights or goes out of business "buying," that is.

BACK THAT THING UP

Main Issue Two! You have many precious documents and pictures and scanned recipes and things! You want to keep them! Hard drives eventually fail! All these things are true! What do we do?

Back Up to the Cloud – Microsoft, Apple, Google, and various others like Dropbox and Mozy and Carbonite and on and on are lining up at your door, adjusting their bowties and preparing their pitches on why you should have them mirror your important files on distant servers in vast colocation centers, churning away day and night. And it's not a bad idea. Your phones will do this by default, so when you accidentally drop your pricey rectangle into the toilet, you can transfer its mind to a new pricey rectangle.

Back Up to an External Drive – every operating system worth its salt allows for this. Apple's Time Machine and Microsoft's File History can maintain copies of selected files (and even a history of them should you need to revert) in an automated fashion. A point of order: have you heard about **ransomware?** If a crook slips a sneaky program onto your system, he can encrypt all your files and demand payment in those stupid imaginary bitcoins to unlock them, which he may not bother to do anyway. Once ransomware sets to work, it can encrypt anything you have access to and permission to edit, so best practice would be to disconnect the external drive in between backups.

Back Up to Network-Attached Storage – This here is a mini-computer of sorts that lives on your network and can store your files with redundancy like keeping it on two drives or striping data across those drives so that even if one fails you're still okay. This will be pricier and a trickier setup, but it *will* make you feel cool.

The more backups you have in the more locations, the safer you'll be.

WHAT ABOUT THEM VIRUSES?

Third-party antivirus/anti-malware programs are out there, and I think the current leaders are **Webroot**, **Bitdefender**, and, in recent tests – this may surprise you – the clear winner was … Windows's built-in **Microsoft Defender**. I know, right?

The best defense, actually, is not getting in trouble in the first place. Browser extensions and proper online behavior will do most of the work of keeping you safe. But that's a tale for another class …

Until that class, stay frosty, and contact me at fwalther@cityofmillvalley.org for any follow-up questions. Just click on that link, and … oh, right. This is just paper.