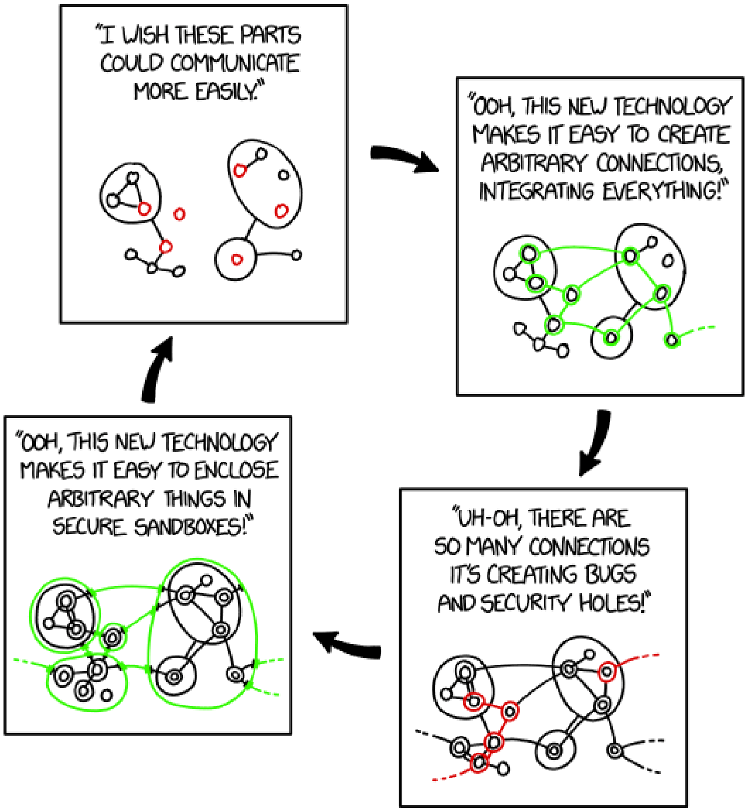
Staying Secure Online

Maxwell Memorial Library's Technology Class
Thursday, October 25, 2018

0 Introduction

This month's program will introduce various apps, techniques, and habits that can help keep your online life as safe as it can be on an inherently unsafe internet.

The lack of safety results from the fact that we want machines and applications that can communicate with each other and send each other commands that get executed.


"I WISH THESE PARTS COULD COMMUNICATE MORE EASILY."
"OOH, THIS NEW TECHNOLOGY MAKES IT EASY TO CREATE ARBITRARY CONNECTIONS, INTEGRATING EVERYTHING!"
"UH-OH, THERE ARE SO MANY CONNECTIONS IT'S CREATING BUGS AND SECURITY HOLES!"
"OOH, THIS NEW TECHNOLOGY MAKES IT EASY TO ENCLOSE ARBITRARY THINGS IN SECURE SANDBOXES!"

Hovertext: "All I want is a secure system where it's easy to do anything I want. Is that so much to ask?"

XKCD #2044 ("Sandboxing Cycle") by Randall Munroe. https://xkcd.com/2044/. Licensed under a Creative Commons Attribution-NonCommercial 2.5 License.

There is, however, an essential tension between this kind of utility and the security we want to maintain. We want apps that can communicate with each other or websites that can deliver active, dynamic content, but we also don't want viruses on our machines, and this conflict establishes the conditions for an eternal arms race or dialectic in which our thesis of a secure but useful cyberspace is countered by the hackers' antithesis of a Wild West where we are their vulnerable victims. Security app developers provide the synthesis that begins the dialectical cycle anew.

1 Types of scams and attacks

1.1 Phishing

Phishing refers to fake emails that appear to be from an organization you do business with. The links in such an email will appear (on the surface) to be to the legitimate organization, but their machinery under the surface will take you instead to a website (also appearing legitimate) whose purpose is to collect the usernames and passwords that victims type in.

There are ways to examine the URLs (web addresses) that links in an email point to, but the safest thing to do is to avoid clicking on links in emails entirely. So, for instance, if your credit card company sends you a notice that your statement is ready, it is safer to go to your browser and use a bookmark that you already know is good than to click on the link in the email.

1.2 “Free” Wi-Fi scams

You may recall that about a year ago in October 2017, some computer scientists at the University of Leuven in Belgium found a way that hackers could crack WPA2 — the most widely used and most secure Wi-Fi protocol around. While there are now patches to protect against such a so-called KRACK attack, the discovery reminded us all that any technology is subject to hacking.

1.2.1 Evil twin attack

Someone sets up Wi-Fi with a name similar to the name of the place you’re at. For example, the Baldwinsville Public Library has 2 Wi-Fi networks – Library1 and Library2. Someone nearby (it’s not known who) has a network named Library3. The library warns their patrons not to use that network but only to use one of its 2 legit networks.

In general, find out the actual name(s) of an institution’s networks before accessing.

1.2.2 Not-quite-“free” Wi-Fi

A variation is where the network pops up a page informing you there is a “small” charge and asks for your credit card info.

Results are predictable.

1.3 Man in the middle attacks

Even if the Wi-Fi is legit, hackers might be able to “peek over your shoulder,” so to speak, by inserting their machine between users’ devices and the services that they’re using on the Internet. Such attacks can take place even when encryption is used, but proper use of encryption greatly reduces their chances of harming you.

Note, though, that *proper* in that last paragraph is crucial. Many apps, in order to reduce overhead, don’t properly check security certificates, so they are almost as susceptible to attack as apps that don’t even bother with encryption.

Michael Covington’s recommendations:

- Close/delete unexpected odd communication (whether from email, browser pop-up, or whatever) without responding or interacting,
- Don’t jailbreak devices,
- Don’t use apps unless you know and trust the source of the app (and, presumably, know that the app follows encryption protocols correctly),[1]
- Don’t automatically connect to free, public Wi-Fi,[2] and
- Avoid free Wi-Fi hotspots (note that that would mean not using either your devices here at Maxwell).

In the real world, you will probably have to violate some of these recommendations to some extent. With that in mind, I’ve changed Dr. Covington’s order so that the list is in decreasing order of importance. So though you should probably regard the recommendation to delete unexpected communication as having few exceptions, you might modify “avoid free Wi-Fi altogether” as more of a reminder to vet a hotspot before connecting.

2 What you can do to keep safe

tl;dr:

- Constant vigilance! But don't give in to paranoia.
- Install the HTTPS Everywhere plugin on your Web browsers.
- Use unique, strong passwords and 2-factor encryption.
- Make sure your and apps are set to automatically update.
- You can certainly have your devices remember passwords for public Wi-Fi you use regularly. If you are very security conscious, though, you should adjust your settings such that the devices don't connect automatically.

[1] As recently as 4 years ago, FireEye Mobile Security Team found that 68% of free apps for Android did not properly implement encryption. See both Michael Covington’s post and Charlie Osborne’s article.

[2] Note that this would include Wi-Fi at public libraries like Maxwell. With regard to this point, you have to weigh risk versus convenience.

2.1 Constant vigilance!

You don't need to be paranoid or look for threats everywhere you go online, but you should be mindful of the fact that there are threats out there and that not every “helpful” thing you run into has your best interests in mind.

Indeed, one common scam seems to take advantage of the fact that many people are overly paranoid. One can easily follow links to sites that throw nefarious popups up even if the site belongs to a legitimate organization. One such popup warns in scary tones that your computer has been hacked or infected with a virus and you must call a certain number to get rid of the alleged problem.

Chances are good that this claim is completely false, that you can close the popup (sometimes easier said than done), close the tab for the compromised site that caused the popup, and safely continue with your surfing. Unless you actually called the number and gave the people at the other end of the line access to your machine. Then you *will* have problems.

2.2 Always use HTTPS (secure, encrypted HTTP)

The short version of what follows is that you should use HTTPS rather than HTTP whenever the Website you’re visiting provides it, and to do that, you should get a browser plugin to do it automatically.

As noted in footnote 1, the fact that an app uses encryption does not mean that it uses it correctly. Moreover, though the major browsers (Chrome, Edge, Firefox, Safari) seem to be in compliance with security standards in implementing encryption, the weak link is the sites that you visit. So, for instance, your browser will complain if a site serves up a page under HTTPS that has nonsecure content embedded in it. If an individual page is perfect but other parts of the Website are sloppy, though, the browser will not be able to let you know about that, and it could be that flaws in the site’s implementation allow your information to “leak” or expose you to an attack when you go to nonsecure pages at the site.

Nonetheless, even if a Website’s implementation of HTTPS is flawed, if the site gives the option of connecting by HTTPS as well as by vanilla HTTP, use HTTPS.[3] The question is how to do that. When you type just the Web “address” into the browser, the browser assumes you mean to use HTTP. Also, if you click on a link specifying HTTP, that’s what gets requested. Now if the Website uses HTTPS correctly, there will be no problem as it will use HTTPS regardless of whether it’s specifically requested or not. You could make a habit of typing the whole URL starting with “https://...”, but then when visiting pages that don’t use encryption

[3] A Website that properly implements HTTPS will redirect all plain HTTP requests to HTTPS, but since the point of this section is safety in the event of bad implementation, we’ll ignore that.

at all, the browser will warn you “Your connection is not secure” and that the Website is improperly configured. All of which is technically true, but if you aren’t entering data that needs to stay private, the stakes may be low enough.[4]

Fortunately the Electronic Frontier Foundation has developed a plugin that automates a solution to this conundrum. HTTPS Everywhere has versions for Firefox, Chrome, and Opera. Again, complacency is never warranted, but using something like this can at least help with harm reduction.

2.3 Use unique, strong passwords and 2-factor encryption

Ideally, all of your passwords are seemingly random strings of at least 10 characters that mix digits, upper and lower case letters, and symbols. If you use password managing software this is possible, but otherwise it may be an unattainable goal.

However, the experts do provide a harm-reduction strategy: Use the guidelines above for creating your passwords for accounts that absolutely must be secure like those for financial services and email. Then for low-risk accounts, use passwords that are convenient but not necessarily strong or unique (don't reuse any of the passwords you have used for high-security accounts, though!)

As further protection, you should also use **2-factor authorization** for accounts that must be secure. 2-factor authorization means that you get sent a temporary code on your phone or by email when you begin the logon process at a website. That code is required to complete logging on, so the risk of being hacked is reduced since a hacker would have to not only get your password but also your phone or email password.

2.4 Keep your system and apps up-to-date

This measure is the first step for security in general. It is impossible to create an unhackable system, so if you are putting any data or software that you didn’t create yourself into a device, then that device is vulnerable to some degree or other. This is true whether the data or software was downloaded from the Internet or came on a disk of some sort. Moreover, increasing how secure a system is also increases inconvenience for the user, so designers have to balance security against user convenience.

Those facts about computer security get us back to the arms race/dialectic discussed back in the introduction. As vulnerabilities are discovered, it becomes necessary to patch them, and

[4] Since somewhere from a quarter to a third of Web traffic still seems to be served up unencrypted, the stakes seem to be low enough much of the time.

that means reprogramming software and releasing the updated version.

In practical terms, you should go into the settings app for your device and make sure that automatic updates are authorized. Since this is the default setting, they probably are, but it can be worth changing the setting slightly. Since updating apps involves quite a bit of data transfer, updating while away from Wi-Fi can eat into your data allowance significantly. Thus, you can tweak the settings so that automatic updates still happen but only when you're on Wi-Fi. This only increases risk minimally (assuming you will be back to Wi-Fi within a few hours or days) while reducing impact on your data allowance substantially.

2.5 Adjust your networking settings

You should have your device's network settings set such that you at least have to approve joining an unknown network. Better yet, set them so that if no network is available that your device recognizes, then you have to connect manually. That reduces the chance of just automatically approving a questionable network.

Note that your device can still memorize the password for a network even if you have it set not to connect automatically. This means that the cost of security is only the inconvenience of having to find the network and select it and not the full potential cost of having to do that and also remember the network's password.

3 Resources for more help & information

3.1 Apps and plugins

HTTPS Everywhere plugins for Firefox, Chrome, and Opera. https://www.eff.org/https-everywhere

3.2 Articles

Better Business Bureau. (2017, July 7). Scam alert: watch out for 'free wi-fi' scams. Retrieved from https://www.bbb.org/council/news-events/bbb-scam-alerts/2017/07/scam-alertwatch-out-for-free-wi-fi-scams/

Covington, Michael. (2016, October 8). Free Wi-Fi and the dangers of mobile man-in-the-middle attacks, *Beta news*. Retrieved from https://betanews.com/2016/10/08/free-wi-fi-mobile-man-in-the-middle-attacks/

Davis, Gary. (2017, July 7). 10 tips to stay safe online [Blog post]. Retrieved from https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/10-tips-stay-safe-online/

Osborne, Charlie. (2014, August 22). “68 percent of top free Android apps vulnerable to cyberattack, researchers claim”, *ZDNet*. Retrieved from http://www.zdnet.com/article/68-percent-of-top-free-android-apps-vulnerable-to-cyberattack-researchers-claim/

Perez, Sarah. (2017, October 20). “Google says 64% of Chrome traffic on Android now protected with HTTPS, 75% on Mac, 66% on Windows”, *Tech Crunch*. Retrieved from https://techcrunch.com/2017/10/20/https-is-booming-says-google/

Wikipedia. (2018, October 24). HTTPS. Retrieved from https://en.wikipedia.org/wiki/HTTPS

Wikipedia. (2018, October 24). Phishing. Retrieved from https://en.wikipedia.org/wiki/Phishing