# Staying Secure Online

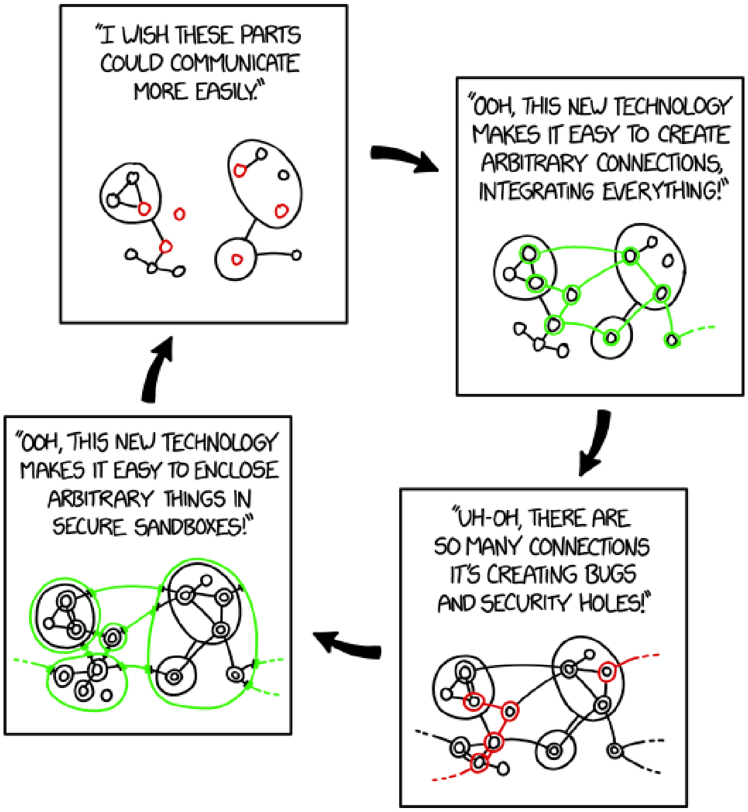
Maxwell Memorial Library's Technology Class
Thursday, October 25, 2018

## 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.

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.


"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/](https://xkcd.com/2044/). Licensed under a [Creative Commons Attribution-NonCommercial 2.5 License](https://creativecommons.org/licenses/by-nc/2.5/).*

## 1 Types of scams and attacks

### 1.1 Phishing

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 an email.

## 1.2 "Free" Wi-Fi scams

### 1.2.1 Evil twin attack

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

- 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).

# 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.

[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.

- 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.

## 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.

## 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.

## 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.

In any case, use strong passwords for things like financial accounts and your email account, and only use those passwords for one account.

As further protection, you should also use **2-factor authorization** for accounts that must be secure.

## 2.4 Keep your system and apps up-to-date

This measure is the first step for security in general. In practical terms, you should go into the settings app for your device and make sure that automatic updates are authorized.

## 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