Thursdays @ Maxwell
Maxwell Memorial Library
Thursday, January 25, 2018

Staying Safe Online in Public

Internet Safety out in the Wild

This month's Tech Program at Maxwell will introduce various tools, techniques, and practices for maintaining digital safety when using mobile devices or laptops at public locations.

You may recall that 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.

That continuous weakening of the effectiveness of security fixes is why you keep up with updates for your devices and their software. But when you venture out from your home, you now have to interact with various devices whose security level is not clear.

Types of scams and attacks

"Free" Wi-Fi scams

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.

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.

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 on the Internet that they're

using. Such attacks can take place even when encryption is used, but proper use of encryption greatly reduces their chances of working.

Note, though, that *proper* in that last paragraph needs to be seen as a weasel word. 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:

- Don't automatically connect to free, public Wi-Fi,[1]
- Ignore unexpected communication (whether from e-mail, browser pop-up, or whatever),
- 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),[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 not to connect automatically to public Wi-Fi as having few exceptions, you might modify "avoid free Wi-Fi altogether" as more of a reminder to vet a hotspot before connecting.

What you can do to be safer

tl;dr:

- Make sure your and apps are set to automatically update.
- You can have your device remember passwords for Wi-Fi you use regularly, but you should set it so that you don't connect automatically.
- Turn Bluetooth off or make it non-discoverable.
- Install the HTTPS Everywhere plugin on your Web browser.

1 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 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.

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 mean that keeping a computer system secure is, in effect, an arms race between hackers and software designers. As vulnerabilities are discovered, it becomes necessary to patch them, and 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.

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.

Set Bluetooth appropriately

If you don't use Bluetooth, you should make sure that it is disabled.

If you do use it, set it to non-discoverable. When you want to pair with another device, you can temporarily set it to discoverable.

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 2, 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 at all,[4] 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.[5]

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.

Resources

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

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.

4 A class which, unfortunately, still includes Maxwell's Website. We're working on it, though.

5 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.

AARP Fraud Watch. (September 20, 2017). "Spot the scam: public Wi-Fi scams", <https://aarpfraudwatch.yahoo.com/spot-the-scam-public-wi-fi-scams-215322410.html>.

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

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

Eckersley, Peter. (June 17, 2010). "Encrypt the Web with the HTTPS Everywhere Firefox extension", <https://www.eff.org/deeplinks/2010/06/encrypt-web-https-everywhere-firefox-extension>.

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

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

Wikipedia. (January 17, 2018). "HTTPS", <https://en.wikipedia.org/wiki/HTTPS>.