Adam Barson
2/28/18

This week's readings are concerned with the security of electronic devices and applications that run on the internet, including cell phones, bank counts, and social media accounts. The first reading is concerned with the trade-off between security and convenience, and what users deem more important in the present day. The second article is concerned with the rising prevalence of biometrics—and the advantages and security risks that they bring.

The statistics garnered in the first article frankly surprised me a bit. As someone who admittedly does not use the best security practice, I myself favor convenience over security. It is refreshing to see that so many young adults and baby boomers alike are placing more emphasis on security, and are not blind to the real risk posed by being hacked, be it their social media account, or bank account.

The second article was an interesting read, as I did not previously know that biometrics posed such a large security risk. It is scary to think that once someone steals your biometric data— data that should belong to you, and only you—they have it forever, and you can no longer safely rely on it for security. I agree entirely with the sentiment that biometrics should only be a partial key in multi-factor authentication, and should not solely be relied upon.

That brings me to my response: I believe multi-factor authentication, including biometrics, should be used by the most "secure" accounts. While I do not consider physical hardware tokens as a good idea (like a USB drive) for use in multi-factor authentication, I think that using mobile phones for two-step authentication is a good solution. I have never actually used a hardware token, but it seems like a huge liability having to carry around a thumb drive that acts as the final key in granting access to your accounts. I already carry around enough stuff—having to worry about a device that can be used against me to access my most secure data is scary enough, and is small enough that I could see myself easily loosing it. Furthermore, everybody almost always is carrying a cellphone around. Cellphones are pretty much considered fundamental in everyday life, and most people (that I know, at least) would never go anywhere without their phone. Using smartphone applications for use in 2-factor authentication is also extremely easy, as most of these applications can work alongside the biometric reading that the phone provides. GPS can also be added as an additional factor.

Passwords alone are clearly not enough, as they rely entirely on users own password etiquette, and are subject to brute force attacks. While 2-factor authentication is still not entirely secure, it removes many risks from the equation. After reading these articles, I am definitely going to look into using 2FA with more of my accounts.