2FA or Nay?

Assignment Due Date: 2/9/15

A growing trend in the realm of authorization and authentication is 2FA, or two-factor authentication. A two-factor authentication scheme is one in which a user must enter a password at the usual login point, but then must also enter a second form of identification such as a second password sent to a mobile phone, or the input of a USB security key. This authentication scheme has the benefit of requiring not only something the user knows (a password), but also requiring something the user has (a phone or security token). While this is a distinct increase in the amount of security against would-be imposters, it can also be a significant inconvenience; if a 2FA service uses your smartphone as the second form of authentication and you don't have you're phone, you're probably not going to get access to that service!

I would like you to enable two-factor authentication on a service of your choosing. You can find a relatively comprehensive list of services utilizing 2FA here: https://twofactorauth.org/ Use the 2FA scheme for approximately 48 hours. After you've used the 2FA scheme, you may disable the scheme… but you may find that you enjoy the extra layer of security it provides!

When you have used the 2FA scheme for at least 48 hours, write a brief report on your experience. In your report, you should include:

- The service you enabled 2FA on
- The frequency with which you use that service
- The number of times you used the service with 2FA enabled (this can be a rough estimate if you select a service that you use many times per day)
- What device you used 2FA with
- Your thoughts on having to use 2FA with your chosen service
    - Did you like/dislike it, was it an inconvenience, did you feel like it provided more security for your account, etc
- Will you be keeping 2FA enabled on your chosen service?
- Will you use 2FA on a different service now that you know more about it and its benefits?

While you are free to choose any service that has a 2FA scheme, please note that some services only support 2FA using physical security tokens such as the YubiKey. There are, however, many services that use SMS messaging for 2FA.

If I may take the proverbial soap box for a moment, I would urge you to consider purchasing a YubiKey or other physical security token that supports current and/or emerging 2FA standards (the current widely supported scheme is U2F, or universal two factor, but the YubiKey line supports a few other proprietary and widely trusted protocols). The YubiKey runs from $25 to $50 and can be purchased on Amazon with Prime shipping (you have Amazon Prime for Students, right?) If that price tag is too high, there are cheaper security tokens that support U2F. While 2FA might be a slight PITA, it *does* provide a significant layer of additional security for services that support it; as you enter into the professional world, you'll have bank accounts and other online services that will mean a lot more than your average social media account. Perhaps you already do!

I am in no way paid by anyone in the 2FA game, I just want to share my passion for online security. ☺