My personal email has been involved in 7 data breaches according to the *Have I Been Pwned?* website. It is because of these past breaches, that I try to take some extra precautions and best practices when creating my logins so that my email account stays safe. The practices I follow to keep my email account safe include not reusing passwords across multiple sites, using a password manager with randomly generated passwords for each login that needs created, using a unique password for the password manager that adheres to the current standards set forth by both the National Institute of Standards and Technology and Cybersecurity and Infrastructure Security Agency, enabling two/multi factor authentication whenever possible, and also ensuring I am not the victim of any phishing/hacking attempts via spam/malicious emails. If my email were to become compromised though, I would need to immediately change all of my security settings. This means updating your passwords, login recovery options, multifactor authentication, which I would attempt to do from a device that is known to not be compromised or even that is not connected to the internet if possible.

While it is ultimately our own responsibility for keeping our data and accounts safe, there is also an implied responsibility that the companies storing our data have to keep it safe as well. We all acknowledge the risk inherent in giving some of our information to these companies, but that acknowledgement comes with the expectation that they will do everything within their control (to a reasonable extent) to keep that data safe and secure. That being said, the past two plus decades have shown that most companies cannot be trusted to always do the right thing when it comes to keeping your data safe. In fact, I would argue that most companies will do what they can to abuse that given trust and use our data to benefit themselves at almost every turn when given the choice between protecting their customers’ data or profiting off that data.