# **Personal Cybersecurity Audit – Example**

|  |  |  |
| --- | --- | --- |
| Device or Account | Password Strength | Security Actions |
| Personal Computer | Strong | * Updated antivirus protection on my machine * Verified the strength of my password |
| Personal Cell Phone | Strong | * Downloaded the latest software update on my phone * Updated my passcode |
| Bank Account | Strong | * Verified my password strength * Implemented 2FA to provide more security beyond my passcode |

Sites to check your password strength

* NordPass is a safe place where you can verify your password strength
* There are many other websites but it is important that you verify the site’s credibility before accessing the site

## **Phishing**

### What is Phishing?

In cybersecurity phishing is a cyberattack that utilizes fake emails and phone numbers to trick people into sharing sensitive data or downloading malware.

A common phishing scam that is prevalent in our world today is sometimes we may receive text messages saying that our package had not been delivered and we should click on the link and verify our information. Clicking an unverified link from an unknown source is a key indicator that it could be a scam.

When I conducted my personal audit, I noticed that with my school email, I was constantly getting emails from unknown sources asking that if I wanted a research position, I should respond to the email with my information so I could be registered. Since I could not verify the email user, it was clear that it was very risky to provide data if not a scam.

Understanding key indicators of what could be a phishing email is a great to protect your personal information and most importantly yourself.

## **Conclusion**

After going through my personal devices and accounts I noticed that a lot of the passwords I had created needed to be changed. Passwords that I had once believed were strong, were not as strong when I checked them using a password strength testing website. To also help provide more security to my accounts, I enabled two factor authorization where I could. For example, for my school email, in order to access my universities pages using my login info, after I type in my password, the extra step of security is Duo Mobile sends me a message on my phone asking to confirm that it is me logging in. By using Duo Mobile, I am alert when my email is being logged into a new device. For my devices, I made sure to install the latest software to ensure all security patches were up to date. Reviewing the security on my accounts and devices has shown to me how easily it could have for me to be hacked had I not been more careful. It taught me the proper steps I need to take in order to make sure my information is secure from now and into the future.