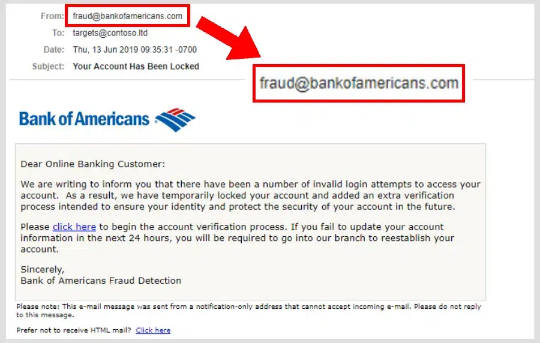
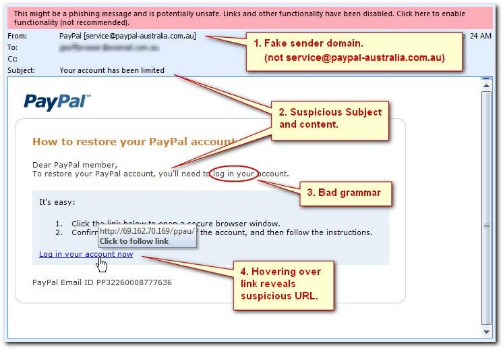
Cyber security is a big part of everyone’s world no matter where you are or what industry you are in. Cyber security is a very important part of today’s society and our lives and the more education you have on this topic the safer your information is. Cyber attacks are a very scary thing and the best way to prevent and reduce them is to know more about them. According to an article “Experts predict that data breaches will cost the global economy 9.5 trillion in 2024” (Hughes, 2024). This is an outrageous amount of money and there are things that can help you in your everyday lives. My summer project at Brookhaven National Laboratory (BNL) was how cyber security policies, procedures and best practices are implemented at the National Synchrotron Light source II. I’ve learned so many things and I’m going to explain the things I learned and educate you about keeping a safe system and preventing cyber-attacks and vulnerabilities.

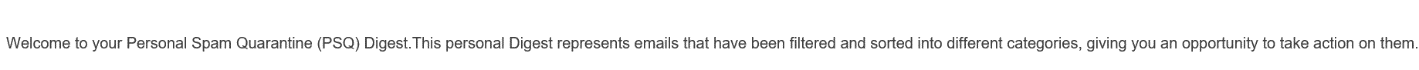
The first topic I want to talk about is making sure equipment and technology is set up to policy standards. BNL and most federal facilities have plans and rules they must follow to make sure everything is running to their standards. One of the things I did this summer was setting up a telepresence robot and since it’s a federal facility they are strict with their rules and the steps to getting it set up on the network were very tricky. First, we had to contact the IT department and get an IP address for the robot. An IP address is the unique identifying number assigned to every device connected to the internet. Once it gets assigned an IP address now, we can xxxxxxxxxx

The second topic I’d like to talk about is the most common cyber threat, which is the phisher attack. What a phisher attack is, is an attack that tricks the victim(s) into giving away personable data or information. There are various types of phisher attacks, email phishing which is doing by sending through email, Smishing which is similar to email but through SMS message that has fake clickable link or number, Spear phishing which is a targeted attack about looked up victim, and lastly vishing which is an attack through phone calls to pretend being someone they are not by sending a fake web page that looks identical to a legitimate site. Phisher attacks are very dangerous and can be very convincing so it’s important to read and look at what you’re clicking on before jumping to conclusions. According to Safety Detectives website they state “Phishing was the most reported cybercrime in 2023, causing losses of more than 18.72 million” (Jovanovic, 2024) this is showing the statistics phisher links have caused in 2023 and they predict it to be worse in 2024. Let’s talk about some important things to keep an eye out for in some of these emails to protect you.



**Figure 1 and 2**. Are examples of fake emails that are pretending to be popular companies.

Both sources are highlighting key examples of what to look for in a fake email. Looking at Figure 1 you would think it is a legit email but in fact it isn’t. In the from section, you can see that the email is suspicious. It states fraud@bankofamericans.com, which to someone might seem real but in fact it’s not, Bank of America real email is just bankofamerica.com. That is a great way to figure out if the email is real or not and if you are not certain if it is, you can look for misspellings or you can google search for the companies email and compare. Referring to Figure 2 more things to look for are bad grammar such as bad spelling and if there is a link on that email if you hover over a clickable URL, you can see if it has the same destination path. So, a best practice would be to look over everything on your emails and while you’re reading your emails look out for misspellings and hover over every link and get the destination. This one of the most common attacks on federal companies and two ways Brookhaven Haven National Laboratory do to prevent these attacks happening on their accounts, is one having an email digest system that reads for emails that might be spam or harmful and block them and sends you a separate email about the attack that allows you to block the sender or allow them. A second way is requiring a twostep authentication which means when you log into a BNL associated account it prompts you to use a third-party application to authorize the log in. What this means is the only way to log into an account with someone credentials are also having their phone, so for example if a hacker gains your username and password to BNL you would also need to click accept on your phone at the same time.



Graphical user interface, text, application

Description automatically generated

**Figure 3 and 4**. Are examples of email system BNL uses to prevent a lot of unwanted spam emails.

The second attack I want to mention is a malware attack. Malware attacks is any program or code that is created with the intent to harm a computer, network or server. There are many different types of malwares. One of the most common forms of malware is called ransomware. Ransomware is an attack that encrypts a victim’s data and the only way to decrypt that data is by paying them off. You might wonder why you would trust a hacker and give them money. Most of the time they do actively decrypt it because it gives them reputation and the more people, they get the more people know to get their stuff back is by paying. According to the FBI’s website their tips to avoid ransomware is “keep operating systems, software, and applications up to date… Make sure anti-virus and anti-malware solutions are set to automatically update and run regular scans… Back up data regularly and double check that those backups were completed” (FBI, n.d.) I’m going to explain why each one of these things are important and why most companies such as BNL follow those exact same tips. First, making sure everything is updated to do is very important because having out of date operating systems, software, and applications can pose a serious threat to your system. This causes what they call “holes” which is an away an attacker can get in and harm your system. Second, anti-virus and anti-malware needs to be up to date because they rely on signatures or signals and if it’s not up to date it can’t pick up new signals which would lead to getting breached without even knowing. Lastly in the article they talked about backups. Backups are a copy of the data used for a recovery in case original data is lost or corrupted, ways that can happen is through failure, cyberattack, or natural disaster. So even besides the point of cyber it’s good to have backups in case of other incidents. Regularly checking to make sure the back ups are up to date and full completed is important to make sure no data goes missing when the time comes of needing it.