**STUDENT**

"I have a very cynical and pessimistic view on internet security and especially wifi security. Your digital footprint is forever and is impossible to entirely cover up. No matter how hard you work at concealing your identity online it's always possible to be found due to human error. So when browsing online I keep that in mind. When protecting my own information it depends on my location and where I am. When I travel OCONUS I avoid public wifi and rely on my phone carrier for internet while using a VPN unless I am at a family's house I will use their wifi still with a VPN. In CONUS I adopt the same idea. No public wifi and a VPN always. My home wifi password is randomly generated by bitwarden as well. All of that being said I am very cynical and pessimistic and still assume that my data can be viewed in someway" "[name], this is pretty much identical to what I do. I feel as if your judgement is what protects you the most when trying to protect your data online. I'm in the Coast Guard and I laugh at the yearly cyber awareness training we have because of how obvious some of the fake emails are, but I your online security is only as good as your judgement." "[name], The avoiding sketchy places really stuck out to me and it seems like such an obvious thing. Complacency kicks in when you're on your couch and distracted by life. That's where not putting everything online and monitoring bank accounts closely works really well."

**CHATGPT**

Overall Score: 90/100

• Content: 29/30

• Engagement: 30/30

• Mechanics: 31/40

Feedback:

[name], your approach to internet security is pragmatic and realistic, acknowledging the persistent nature of digital footprints and the potential for human error. Your emphasis on staying mindful and cautious while browsing online is wise and aligns with best practices for staying safe in the digital realm.

Your strategy of avoiding public Wi-Fi when traveling and relying on a VPN even when using family members' networks demonstrates a strong commitment to protecting your data, especially in potentially vulnerable situations. Utilizing randomly generated passwords via a password manager like Bitwarden for your home Wi-Fi adds an additional layer of security, which is commendable.

Your engagement with [name]'s post is thoughtful and insightful. Indeed, exercising good judgment is crucial in navigating the complexities of online security. Recognizing the importance of personal judgment over relying solely on automated security measures is a valuable perspective.

Similarly, your interaction with [name] highlights the significance of remaining vigilant and not becoming complacent, even in familiar environments. Your acknowledgment of the dangers of complacency and the effectiveness of limiting online sharing and monitoring financial accounts closely is well-founded and offers practical advice.

In terms of mechanics, your writing is clear and effectively communicates your ideas. However, there are a few minor grammatical errors that could be addressed for improvement. Overall, your contributions to the discussion are valuable and provide valuable insights into internet security practices. Keep up the good work!

**STUDENT**

"Hey Class. keeping your privacy safe is super important, whether you're at home, sitting in class, or high in the sky. So, here's how I make sure my online life stays on lockdown. Firstly, I try to remain vigilant against evolving cyber threats. Staying informed about potential risks enables me to make safe decisions. I rely on antivirus software to safely protect my devices against malicious viruses and diligently apply the latest security patches to maintain resilience. when I'm out in public and am using public Wi-Fi I use something called Virtual Private Networks (VPNs) to encrypt data transmissions, safeguarding sensitive information from potential eavesdropping. I try to steer clear of sharing personal data online and always review privacy settings across social media platforms. safeguarding online privacy makes for a proactive approach, using technological solutions along with safe digital practices is essential to navigating the virtual landscape safely. Let me know what you Think!" " One simple yet effective measure I employ is avoiding public Wi-Fi networks whenever possible. Instead, I opt to connect to my cell phone's personal hotspot, ensuring a more secure internet connection. This practice allows me to maintain control over my online activities, even during downtime between maintenance tasks, like the one I'm utilizing right now. " " While staying up to date on software updates is important for addressing vulnerabilities and patches, it's understandable that you prioritize your online activities based on your usage patterns. However, it's worth considering incorporating regular updates into your routine to further bolster your device security. "

**CHATGPT**

Overall Score: 85/100

• Content: 27/30

• Engagement: 28/30

• Mechanics: 30/40

Feedback:

Your commitment to safeguarding your online privacy is evident in your comprehensive approach outlined in your initial post. It's commendable how you emphasize the importance of staying informed about evolving cyber threats and employing various security measures like antivirus software and VPNs to protect your devices and data. Additionally, your focus on reviewing privacy settings on social media platforms reflects a proactive attitude towards maintaining privacy online.

Your engagement with your classmate's post demonstrates thoughtful consideration of their approach to online security. Your suggestion to prioritize personal hotspot over public Wi-Fi networks is a practical and effective measure to enhance security, especially when in public places. It's great to see you sharing your own strategies for staying safe online while also offering constructive feedback to your peers.

Your comment on the importance of staying up-to-date with software updates further underscores the significance of proactive security practices. While acknowledging individual usage patterns, you rightly advocate for incorporating regular updates into one's routine to strengthen device security continuously.

In terms of mechanics, your writing is clear and articulate, effectively conveying your ideas. However, there are a few minor grammatical errors that could be addressed for improvement.

Overall, your contributions to the discussion are insightful and valuable, showcasing a strong understanding of online privacy and security principles. Keep up the good work!

**STUDENT**

"Good morning class, security is a big thing when it comes down to internet and devices being connected. There's plenty of things to do to protect them that i probably have no clue about. I've never been worried about making sure my devices are private as its already a requirement for most of requirements. My router is private but one thing i do to make sure not to many things are connected is disconnecting old and not in use devices to keep my router with limited access as much as possible. I've realized in the past having too many appliances make everything run slow like gaming which takes up a lot of data. Other ways to help keep yourself more private is not connecting your devices to computers and giving them access to all your photos or even syncing things such as contacts and more to other devices that may ask, same for games or even other apps that may ask for your location and need certain requirements even when you're not using it to run. I'm pretty sure there are more ways to protect your privacy so if you're wondering on what else you may not know look here:https://www.techtimes.com/articles/303859/20240422/top-digital-privacy-tools-of-2024-how-to-safeguard-your-online-presence.htm" "I definitely use vpn but I only discovered the use of Vpn for the wrong reasons lol. Back when you could get on school Wi-Fi but to be able to use the internet and get on certain apps you had to get a vpn but I never knew how great it was or the full purpose of it until a year or so later when it became more convenient." "@[name] I feel you and sometimes public wifi is just convenient do certain things real quick. VPN's are great to use but how do you add or utilize on your computer? I travel outside the country due to my job and I was unable to go to certain sites or even use hulu, max and other apps due to the restrictions in that country."

**CHATGPT**

Overall Score: 80/100

• Content: 25/30

• Engagement: 25/30

• Mechanics: 30/40

Feedback:

Your initial post touches on some important aspects of device and internet security, but it could benefit from more specific and detailed strategies. You mention disconnecting old and unused devices from your router to optimize performance, which is a good practice to prevent network congestion. However, you could elaborate more on other security measures you take, such as password management, software updates, or firewall settings, to provide a more comprehensive understanding of your approach to privacy protection.

Sharing a link to additional resources on digital privacy tools is helpful for your classmates who may want to learn more, but it's important to provide some context or insights from the article to encourage engagement and discussion within the class.

Your engagement with your classmate regarding VPNs adds to the conversation, showcasing your own experience and perspective. However, your response could be more focused on providing guidance on how to add or utilize VPNs on computers, perhaps by recommending specific VPN software or explaining the process step by step.

Overall, your contributions to the discussion demonstrate a willingness to participate and share personal experiences related to online security. To enhance your posts, consider offering more specific advice and insights, and ensure clarity in your writing to improve engagement with your classmates. Keep up the good work!

**STUDENT**

"Hi class, When it comes to safeguarding my information while on the internet admittedly, I don't take as much caution when I am at home as I should, as far as I know, my router is set up with the basic security settings that were included with the package we purchased, that includes a firewall. I do, however, use a VPN that I pay a subscription on whenever using a public network outside my home. Besides that, I pay close attention to the HTTP and ensure that whenever I am putting private information in, that it is on an HTTPS, and stays that way the entire time. I also do everything in my power to be vigilant about what links I click and keep a close eye out for any ads that may try and disguise itself as the link I am looking for. I also try and pay attention to the address of the websites I am looking for incase the address may have some subtle variations that may be a facade of a trusted site. This class has given the inspiration to look into more security while on the internet." "Congrats on the coming of your baby girl! You defiantly start really thinking about the potential dangers that are out in the world once children are in the picture. There is a lot that I try and stay vigilant about with the internet and my boys. Especially being so young they could easily be susceptible to all matters of privacy invasion. I also use a VPN, and I find that it is really a worthwhile investment. Especially out in public, in a MCCS facility, they often time have poor data coverage and you are forced to get on their public Wi-Fi, but once you log on, you can see the amount of other people on the network as well. Having that VPN really does help put your mind at ease." "I have never considered disconnecting the devices that I no longer use but it makes sense. I do however also practice not syncing all of my information but that may be more out of laziness rather that safeguarding! One thing I have always been adamant on is not sharing my location when it is avoidable. It never felt right to me to let Facebook know exactly where I was all the time.

**CHATGPT**

Overall Score: 90/100

• Content: 28/30

• Engagement: 30/30

• Mechanics: 32/40

Feedback:

Your post demonstrates a thoughtful approach to safeguarding your online privacy, particularly when it comes to using public networks and being mindful of website security indicators like HTTPS. Your use of a VPN for public networks and your vigilance in checking website addresses and avoiding suspicious links are commendable practices that enhance your online security.

It's great to see you engaging with your classmate and offering congratulations on the arrival of their baby girl. Your acknowledgment of the increased vigilance required for protecting children's privacy online adds depth to the discussion, highlighting the importance of online security for families.

Your response to another classmate's post adds value to the conversation by reflecting on their suggestion to disconnect unused devices from the network. Sharing your practice of not syncing all information and being cautious about sharing your location further contributes to the discussion, showcasing additional privacy measures you take.

Overall, your contributions to the discussion are insightful and engaging, providing valuable perspectives on online privacy and security. Your willingness to share personal experiences and discuss relevant topics with your classmates enriches the learning environment. Keep up the excellent participation!

**STUDENT**

"I don't have any significant security features with my router. However, I use a lengthy password with multiple special characters to keep my password strength high and use different passwords for myvarious accounts. I also ensure that I never store my bank information, personal information, and other login information in add-ons such as Google Password Manager. I only use my laptop for school, work, and the occasional Steam game purchase/download; out of those three, the only major threat I see is downloading games off Steam. I've researched a few games where developers would sneak files into their video game downloads that allow them to access features such as administrative privileges. However, when caught, the developers will pull the "It's to check the integrity of the players to scan for hacking software" card, to which I say, "Such files should be made clear with a prompt, informing the audience these files exist in the download before hitting the download button." Outside of my home, some of the security practices I take include not connecting to public wifi, putting my trust in an RFID wallet, and not storing card information or bank information on my phone. For traveling, I've never paid for the WIFI airplanes offer, and I usually download movies and shows at home before the flight so I can place my phone in airplane mode for the ride." "The good old barracks' WIFI is not only slow but needs to be more secure. I took a C-School in Great Lakes called Tactoe, a Cisco Unix Networking class, to which the instructors didn't outright say it but taught us the skill to "create" a WIFI backdoor.I deleted my Go-WIFI account that day and luckily transferred within the next two weeks to another C-School Command. On that note, VPNs are secure; however, they do have some privacy cons that are worth taking a look at. I agree that although all the GPS and voice settings are turned offfor my social media apps, they are still listening! Great post; however, there are a few grammar mistakes in your opener and the second sentence; also, the format could be a lot better. You should be able to edit your post before Friday, so save yourself on some point hits. Enjoy your week!" "I agree, not a fan of accessing public networks, especially in airports. Personally I just download my movies and shows prior to flying, along with a game that doesn't require internet access (whenever I can find one). VPNs are great, however I would look into some of the privacy cons that come with them. I would argue that the pro's to outweigh the cons though. Have a great week!

**CHATGPT**

Overall Score: 85/100

• Content: 27/30

• Engagement: 28/30

• Mechanics: 30/40

Feedback:

Your post provides a thorough overview of your security practices both at home and when using public networks, highlighting your awareness of potential threats and your proactive approach to mitigating risks. Your use of strong, unique passwords and avoidance of storing sensitive information in online platforms like Google Password Manager demonstrates a good understanding of basic security principles.

The insight you provide regarding the potential risks associated with downloading games, particularly from less reputable sources, adds depth to the discussion. Your cautionary stance on such practices and your expectation for transparent disclosure of any potentially risky files within downloads is prudent.

Your engagement with your classmate's post contributes to the conversation by sharing your own practices for securing your device and data while traveling. Your decision to download movies and shows beforehand and your avoidance of public Wi-Fi networks, coupled with your use of an RFID wallet, showcase a comprehensive approach to protecting your privacy and security in various scenarios.

In terms of mechanics, there are some grammar mistakes and formatting issues that could be addressed for clarity and readability. Editing your post before the deadline as suggested by your classmate would help improve its overall quality.

Overall, your contributions to the discussion are valuable and demonstrate a strong commitment to safeguarding your online privacy and security. Keep up the good work!

**STUDENT**

"When it comes to protecting and safeguarding my computer and other devices, in all honesty I don't do much. However, I also don't do much to put myself at risk. I try to keep a small social profile online and don't post too many pictures containing myself or info about my life unless its car or motorcycle related. I also don't share where I'm at like a lot of people tend to do. as for my devices, I don't stay up to date on software updates like I should. So that does create a security risk there, however I don't use my devices for much. For the most part I google some stuff, stream apps such as YouTube and Disney+, and I pay my bills. I never engage sketchy emails, text, or calls. I never click random links when surfing the internet and those that pop up on websites and cell phone games. Also, across all of my accounts, all of my passwords are random and don't contain common info from my life. As far as at home router security goes, I have a very unique password, and even though I have the unfortunate opportunity to only have Cox as my Wi-Fi provider, they do offer an enhanced security option which I did turn on. To be honest, I'm not completely sure what it does exactly. Lastly, every once in a while, I will also go through my connected and unconnected devices on my Cox app and scan for devices I do not recognize, as well as pretty much kick all of the devices listed off and go through and reconnect them when necessary." "Me and you are pretty similar. Although I will say I don't use a VPN as much as I should. I'm really curious how many people actually change their passwords that often. I get it's a good safety practice, however it is also very inconvenient. Especially if you already have a strong password to begin with." "Your security measures are what I dream of... if I had the energy and mental capacity to pull it off. Almost makes me want to hire you to set up my stuff. I will definitely take note of your router security settings though as that's where I do spend most of my time online.

**CHATGPT**

Overall Score: 85/100

• Content: 27/30

• Engagement: 28/30

• Mechanics: 30/40

Feedback:

Your post provides a candid insight into your approach to online security and privacy, highlighting both your conscious efforts to mitigate risks and areas where you could improve. Your practice of maintaining a small social profile and being cautious about sharing personal information online is commendable and reflects an understanding of the importance of privacy.

You demonstrate good awareness of basic security practices, such as avoiding sketchy emails and links, using random and unique passwords, and periodically reviewing connected devices on your network. These habits contribute to your overall security posture and help minimize potential risks.

Your engagement with your classmate's post adds depth to the discussion by sharing your own experiences and acknowledging similarities and differences in security practices. Your admission that you don't use a VPN as much as you should and your observation about the inconvenience of changing passwords frequently offer relatable insights into common challenges in maintaining security measures.

The response from your classmate reflects appreciation for your thorough approach to security and indicates a willingness to learn from your practices, particularly regarding router security settings. Your willingness to share knowledge and offer assistance is commendable and enhances the collaborative atmosphere of the discussion.

In terms of mechanics, your writing is clear and effectively communicates your ideas. However, there are some minor grammatical errors that could be addressed for improvement.

Overall, your contributions to the discussion are valuable and demonstrate a thoughtful consideration of online security practices. Keep up the good work!

**STUDENT**

"In an age fueld by technology, privacy is becoming less and less acessible. There are a few things you an do give yourself additonal privacy. I only use apps lile whats app or telegram for textings because they're end to end encrypted. I always use a VPN so my IP adress is secure. I also, don't allow apps like facebook or snapchat to have acess to my location. (I personally think the apps track you irregardless, especially snapchat because I'll use the prompt "McDonalds Near Me" and it will pull the nearest one. When I ask how it knew I was in Ginowan, Okinawa it'll say "I don't have acess to your location" so I ask "how did you know where I was? It responds with "I don't know where you are because I don't have acess to your location." So I ask it how did it know where the McDonalds was, and it says "I must have misspoke, I dont know where you are.") On my macbook, same thing. I use a VPN. Since I live in the barracks, I don't have control over the WiFI router settings." "By combining these security measures with your VPN usage and being mindful of your online activities, you are taking proactive steps towards safeguarding your privacy and data in today's digital landscape. Keep up the good work in prioritizing your cybersecurity!" "Adopting practices like refraining from clicking on suspicious links or pop-ups, as well as attempting to diversify your passwords, are positive steps towards enhancing your personal cybersecurity. As the aviation industry transitions towards a more personalized tech-centric experience, with an emphasis on using personal devices on public networks, it's wise to prioritize security considerations. Sharing public networks in crowded spaces like airports can indeed pose certain risks, making it crucial to bolster your defenses. Stay knowledgable about the security measures implemented by service providers to ensure a safe and seamless user experience. Also, explore additional security measures such as two-factor authentication, regular software updates, and education on recognizing phishing attempts to fortify your digital safety."

**CHATGPT**

Overall Score: 90/100

• Content: 29/30

• Engagement: 30/30

• Mechanics: 31/40

Feedback:

Your initial post effectively highlights the importance of privacy in today's technology-driven world and offers practical tips for enhancing privacy and security. Your emphasis on using end-to-end encrypted messaging apps like WhatsApp or Telegram, along with employing a VPN for secure browsing, demonstrates a proactive approach to safeguarding personal information. Your skepticism about location tracking by certain apps adds depth to the discussion and encourages critical thinking about digital privacy.

The response to your classmate's post is encouraging and supportive, acknowledging their efforts in prioritizing cybersecurity. It reinforces the importance of the security measures they're already taking while also providing positive reinforcement for their actions.

Your engagement with another classmate's post further enriches the discussion by suggesting additional security measures such as refraining from clicking suspicious links, diversifying passwords, and staying informed about security measures implemented by service providers. This demonstrates a comprehensive understanding of cybersecurity principles and offers valuable advice for enhancing digital safety.

In terms of mechanics, your writing is clear and effectively communicates your ideas. However, there are some minor grammatical errors and awkward phrasings that could be addressed for improvement.

Overall, your contributions to the discussion are insightful and valuable, showcasing a strong understanding of cybersecurity practices and a willingness to engage with classmates on important topics. Keep up the excellent work!

**STUDENT**

"Hello class, Ensuring the safety of our online accounts has become more critical than ever in this digital age. It is crucial to take all necessary measures to protect ourselves from cyber threats that are increasing daily. We must proactively protect our valuable information from potential data breaches and unauthorized access. By creating and managing robust and unique passwords, we can significantly increase the security of our accounts. According to Neuways (2024), We can create complex passwords for hackersto crack using a combination of uppercase and lowercase letters, numbers, and special characters. We can also enhance our security posture by avoiding easily guessable information and using passphrases that are easy for us to remember but hard for others to guess. According to Protect (n.d), to ensure the utmost security, we should use a password manager to safely store and generate complex passwordsfor each account. This approach will help us manage our passwords effectively and ensure they are unique to each account. Regularly updating our passwords and refraining from reusing them across multiple accounts further strengthens the security of our online presence.Implementing these strategies not only protects our digital identity but also provides peace of mind, knowing our personal information is secure. Remember, the effort we put into creating and managing strong passwords is a small price to pay for the long-term safety of our online presence. This simple yet effective step can significantly reduce the risk of cyber threats, safeguarding our personal and financial well-being from online scams and fraudulent activities. References Neuways. (2024, April 10). Why do you need to be vigilant with email security? Retrieved May 1, 2024, from https://neuways.com/why-do-you-need-to-be-vigilant-with-email-security/. Protect. (n.d.). Risk Assessment Calculator. Retrieved May 1, 2024, from https://protectnow.info/tools/risk-assessment.html." "You absolutely have an incredibly robust approach to personal cybersecurity, which is commendable in the digital age. Using strong, unique passwords for individual accounts forms a secure first line of defense. In addition, your intentional avoidance of storing sensitive banking and personal information within certain online services, like Google Password Manager, can significantly reduce the risk of unauthorized access. You're correct in being cautious about game downloads. Keeping vigilant about developers' actions and seeking transparency before downloading their games can help prevent unwanted intrusions. Great Job!!!!!" "You bring up an insightful point about the potential risks associated with password managers. Given that they serve as a single storage point for password information, it can pose a serious threat to all accounts if compromised. However, reputable password managers typically use robust encryption and other security measures to protect data. Eventually, no security is foolproof, but every layer added makes breaching security significantly more complicated and often deters the common thief. It's a continual balance between taking sensible precautions and adjusting to potential threats. Your feedback is a reminder of the importance of continually reviewing and updating cybersecurity practices. Thanks for your mindful contribution!" "Your approach to online security is evident through your use of a VPN for added protection and your cautious use of social media. It's important to remember that photographs and online interactions can reveal a lot about us, and while complete privacy and security cannot be guaranteed, taking steps toward protection is always worthwhile. While determined hackers may find ways to bypass security measures, making it more difficult for them is still crucial. Additionally, being mindful of the personal information we share can decrease our potential risk. Good security practices may not make us invincible, but they certainly make us less vulnerable to attacks.

**CHATGPT**

Overall Score: 100/100

• Content: 30/30

• Engagement: 30/30

• Mechanics: 40/40

Feedback:

Your initial post provides a comprehensive overview of the importance of online security and offers practical advice for safeguarding personal information. Your emphasis on creating robust and unique passwords, utilizing password managers, and regularly updating passwords demonstrates a strong understanding of cybersecurity principles. The inclusion of references adds credibility to your points and showcases your commitment to providing reliable information.

Your engagement with your classmates' posts is thoughtful and constructive. You acknowledge their efforts in prioritizing cybersecurity while also offering insightful reflections and additional considerations. Your responses demonstrate a collaborative spirit and contribute positively to the ongoing discussion about online security practices.

In terms of mechanics, your writing is clear, well-structured, and free from grammatical errors. Your use of references and proper citation style enhances the credibility of your post. Overall, your contributions to the discussion exhibit excellence in content, engagement, and mechanics.

Keep up the fantastic work in promoting awareness and best practices for online security within the class!

**STUDENT**

"To protect my privacy and to safeguard my devices I try to be as proactive as possible. I use numerous different passwords that the computer would say are “strong passwords” and have two factor authentication, where I will put my password in then it will either email or text me a code to put in within 60 or 120 seconds so they know it is me. I have my devices set to update software as soon as possible so I am never behind the power curve and making sure my computer does not fall behind. My antivirus and related things are up to date constantly for that damn pesky cyber hackers and nonsense. My privacy settings are whatever the recommended thing is, I do not go overboard or anything, whatever it thinks the settings should be is what I have them as, I have never had an issue this way previously, so if it ain’t broke. I also do not go on any what I would call sketchy websites and I am not playing minesweeper with popup ads and nonsensical things clicking on them left and right randomly so I have not had any issues. As soon as my devices or apps tell me to change my password I try to make up a whole different password entirely instead of just changing one number or one special symbol." "I also thought that putting my phone in "incognito mode" putter me at a higher level of security, so I greatly appreciate you bringing this up. I am honestly not surprised that it is Google that was caught up with monitoring even in that mode. Just by talking to someone about what you want to buy or want, with your phone in your pocket, later that day there will be ads to buy that said thing, it is wild and means everything is being heard. This VPN thing is pretty legit honestly, sounds like a loophole by being able to watch shows not shown in the US and also getting cheaper prices on things, you might be on to something here and may have just got me on that VPN bandwagon. The passwords for wifi for the routers out of the box are how everyone's password should be honestly, alpha numeric and have nothing to do with us personally, and completely random." "You and I are alike when it comes to not being very savvy when it comes to these things. But upon doing this weeks homework I believe I may look into getting a VPN for the security as well as being able to watch more shows and movies when I am deployed, overseas all we have is the gym and Netflix really. I will also be more cognizant when it comes to my passwords as well as what I do on Wifi that is not my own as well as on the plane security measures. This really opened my eyes to people and cyber security attacks and things of that nature. It is crazy how people spend time out of their day to do these kinds of malicious things at airports and such, all I am trying to do is find some comfortable position on this small plane and watch some Netflix."

**CHATGPT**

Overall Score: 95/100

• Content: 29/30

• Engagement: 30/30

• Mechanics: 36/40

Feedback:

Your initial post showcases a proactive approach to online security, highlighting various measures you take to protect your privacy and safeguard your devices. Your use of strong, unique passwords, two-factor authentication, and regular software updates demonstrates a good understanding of basic security practices. Additionally, your cautious approach to privacy settings and avoidance of sketchy websites contribute to your overall security posture.

Your engagement with your classmates' posts adds depth to the discussion by sharing personal experiences and reflections. Your acknowledgment of the potential limitations of incognito mode and your interest in exploring VPNs for enhanced security and accessing geo-blocked content demonstrate a willingness to learn and adapt to evolving security challenges. Your agreement with your classmate regarding the importance of strong, randomly generated router passwords further reinforces the significance of robust security practices.

In terms of mechanics, your writing is clear and effectively communicates your ideas. However, there are some minor grammatical errors and awkward phrasings that could be addressed for improvement.

Overall, your contributions to the discussion are insightful and valuable, demonstrating a commitment to enhancing online security awareness and promoting best practices within the class. Keep up the excellent work!

**STUDENT**

"Hi Class, When it comes to staying safe online and protecting our devices, a couple simple steps can go a long way. Personally, I make sure to always do the following: Online Privacy: It's important to be mindful of what we share online and adjust our privacy settings accordingly. For example, avoiding sharing personal information like our full address or phone number publicly on social media can help keep us safe from prying eyes. Never share where you are in that exact moment wait until later. Device Security: Just like we lock our doors at home, keeping our devices secure is essential. Using antivirus software and keeping it updated is like having a digital lock on our computer, keeping out unwanted intruders. I have two-factor authentication enabled for all my social media, banking accounts and email. By being cautious about what we share online and taking steps to secure our devices, we can better protect our privacy and stay safe in the digital world. It's all about simple but effective measures that help keep us secure online." "Yes snapchat can be scary forsure. I asked the Snapchat AI the same thing and it was honestly so scary. WhatsApp is also a great alternative for texting as it is also end-to-end encrypted. Using a VPN is great idea, I'm going to start using one on my MacBook as well. Thank you for the tips and great post!!" "Yes before this class, I've also never really paid close attention to protecting myself online. Thank you for sharing your insights! Using a VPN and HTTPS websites is a very smart choice, I personally don't utilize them but will look further into it as we progress with technological advancements we can't risk compromising our information. Great post!!

**CHATGPT**

Overall Score: 95/100

• Content: 29/30

• Engagement: 30/30

• Mechanics: 36/40

Feedback:

Your initial post effectively emphasizes the importance of online privacy and device security, providing simple yet valuable tips for staying safe in the digital world. Your emphasis on being mindful of what information we share online and adjusting privacy settings accordingly demonstrates a proactive approach to protecting personal data. Additionally, your comparison of device security to locking doors at home is a relatable analogy that reinforces the importance of keeping devices secure.

Your engagement with your classmates' posts adds depth to the discussion by sharing personal experiences and reflections. Your agreement with the potential risks associated with certain social media platforms like Snapchat and your intention to start using a VPN on your MacBook showcase a willingness to learn and adopt new security measures. Your acknowledgment of the importance of staying updated with technological advancements further demonstrates a proactive attitude towards online security.

In terms of mechanics, your writing is clear and effectively communicates your ideas. However, there are some minor grammatical errors and awkward phrasings that could be addressed for improvement.

Overall, your contributions to the discussion are insightful and valuable, demonstrating a commitment to enhancing online security awareness and promoting best practices within the class. Keep up the excellent work!

**STUDENT**

"Hello Everybody Internet privacy is something I take very seriously. There are many ways and techniques I use to secure my internet connection and ensure my privacy is protected. When it comes to any of my devices, I ensure they don’t have the ability to connect to open networks or any network in general without my authority. This is accomplished by simple network setting on the devices. I also use a paid subscription of AVG internet security which controls any threats to my computer or me. I also have windows defender running which acts as another great barrier. I also run scheduled scans and clean my devices as needed. When it comes to the use of an account online, I ensure to have a mix of password options so it will not be easy to be completely hacked into. A secondary security system like SMS code or Duo push to approve certain access to some of my account has been set up. My network router setting are set up as such recommended by ISP. I use a Netgear router and my access is set for WPA and WPA2 for my wireless connections. My WiFi is secured with a password. I also have setup a program on my computer which shows if any other devices are connected to or is using my network. Thank you" "I am impressed by your proactive stance towards digital security, especially your implementation of robust and distinct passwords, as well as your avoidance of storing critical data in online managers. Your meticulous examination of game downloads for concealed files that may jeopardize system security demonstrates your exceptional vigilance. In addition, your prudent measures while traveling, such as abstaining from public Wi-Fi usage and prearranging entertainment, effectively mitigate your vulnerability to cybersecurity threats. These measures are essential for safeguarding personal data. " Your judicious approach to online security demonstrates a pragmatic comprehension of the digital environment. Utilizing a Virtual Private Network (VPN) is a prudent decision, particularly when connecting to the internet over public networks, as it safeguards privacy and circumvents geographical limitations. Adopting a strategy to uphold a limited online presence, such as restricting social media engagement and refraining from disclosing location data, is indeed prudent. This mitigates the likelihood of personal information being utilized in an improper manner. You have brought up a crucial aspect regarding the constraints of security methods. Although we can employ diverse technologies and techniques to mitigate vulnerabilities, a resolute individual can frequently circumvent these obstacles. This highlights the fact that although we cannot completely remove all hazards, we have the ability to greatly diminish them. Your recognition that our phones function as tracking devices brings a significant aspect to the discussion on privacy, serving as a reminder of the unavoidable compromises we encounter in our interconnected society. Your approach serves as a reminder that security encompasses more than just robust passwords or cutting-edge technology. It entails being cognizant of our digital presence and handling it with caution.

**CHATGPT**

Overall Score: 100/100

• Content: 30/30

• Engagement: 30/30

• Mechanics: 40/40

Feedback:

Your initial post demonstrates a comprehensive approach to internet privacy and device security. You clearly outline various measures you take to protect your devices and ensure your online accounts remain secure. Your use of multiple layers of security, including antivirus software, distinct passwords, and secondary authentication methods, reflects a strong commitment to safeguarding personal data. Additionally, your proactive approach to monitoring network activity and adhering to recommended router settings further reinforces your dedication to maintaining a secure digital environment.

Your engagement with your classmate's post is insightful and constructive. You commend their proactive stance towards digital security and highlight specific aspects of their approach that demonstrate exceptional vigilance. Your acknowledgment of the limitations of security methods and the inevitability of some compromises in our interconnected society adds depth to the discussion and prompts reflection on the broader implications of digital privacy.

In terms of mechanics, your writing is clear, articulate, and free from grammatical errors. Your responses effectively convey your ideas and contribute to a meaningful exchange of insights within the class discussion.

Overall, your contributions to the discussion showcase a sophisticated understanding of internet privacy and device security, as well as a commitment to promoting best practices in digital safety. Keep up the excellent work!

**STUDENT**

"Hello everyone. So in the instructions it says to discuss how we protect ourselves internet wise and I am here to tell you, I don't. I suck at safeguarding my privacy on the internet. I have no idea what my security settings are on my router and honestly, the more I think about it, that scares me. I live on a military installation, we all live like right on top of each other and we all use the less than stellar base internet/wifi that they have. I feel like there is someone spying on my internet use now. Be warned spy, there is a lot of funny cat videos. I definitely think I just gave myself homework, like intensive homework to check/change all of my security settings to make sure my devices and internet use are all protected. You would think that having a father in law that works for a government contracted network security company, that I would have a better understanding of how to figure this stuff out." "Have no fear because you are doing way better than I am. I should probably change my passwords more often or even have them contained somewhere that I can look at them so I can at least remember what passwords I'm using. I have no idea even how to set up a VPN so from my perspective, you're doing great!" "I have also noticed this same thing, and I keep saying I'm going to do better about safeguarding my privacy. I have Alexa devices in my house that I synced mine and my husband's voice to so that it would recognize us, only to realize that they record everything that gets said. So not only does it hear us talk about anything under the sun, I have a young daughter now and I feel like it's hearing me talk to her and about her; that scares me. Thank you for reminding me to reset it and take our voices out of its programming.

**CHATGPT**

Overall Score: 95/100

• Content: 29/30

• Engagement: 30/30

• Mechanics: 36/40

Feedback:

Your initial post is refreshingly honest and relatable. You candidly acknowledge your shortcomings in internet privacy and express a genuine concern about the potential consequences of neglecting security measures. Your humor adds a light-hearted touch to the discussion while still conveying the seriousness of the topic. Your realization that you need to take action to improve your security measures demonstrates a proactive mindset, and your willingness to learn and make changes is commendable.

Your engagement with your classmates' posts adds depth to the conversation. Your empathy towards others who also struggle with internet privacy and security issues creates a supportive atmosphere within the class. Offering encouragement and solidarity, you contribute to a sense of camaraderie among classmates who may share similar concerns.

In terms of mechanics, your writing is clear and effectively communicates your thoughts. However, there are a few minor grammatical errors and awkward phrasings that could be refined for clarity.

Overall, your contributions to the discussion are valuable and genuine. Your willingness to openly discuss your challenges with internet privacy and security encourages others to reflect on their own practices and take steps towards improvement. Keep up the great work!

**STUDENT**

"Right now, as I sit writing this in my living room, I have 7 devices hooked up to the internet. Most homes now adays have just as many or more connected to the internet. Privacy and Security are always a concern, leaving a trail of personal data behind. Growing up when the internet became big, I did make mistakes early on that I learned from. Ways I combat this is using strong unique passwords, stopped sharing personal information on social media, and use a VPN when possible. I never log into any other wifi but my own. My router at home has an incredibly long and crazy password that I change every few months. The wifi is encrypted WPA2. I have set up a guest wifi for visitors. Overall, I try and do my best to keep my data safe. Every day it gets harder to keep it from the wrong hands." "You are doing a great job at keeping your information safe from the seedy underworld. It is hard to keep up with all the extra measures needed to keep our information safe these days. I am always slow to update firmware which puts me at risk." "You are doing a great job at keeping your information safe from the seedy underworld. It is definitely a nutty world with some pros and cons to it. I can't keep up with how fast the technology changes. Congrats on the new Baby. Enjoy it while you can."

**CHATGPT**

Overall Score: 25/30

• Content: 9/10

• Engagement: 8/10

• Mechanics: 8/10

Feedback:

Your initial post provides a concise overview of your approach to internet privacy and security, highlighting the measures you take to protect your personal data. You effectively convey the challenges of maintaining privacy in an increasingly connected world and demonstrate awareness of potential risks. Your commitment to using strong passwords, avoiding public Wi-Fi, and regularly updating your router's firmware reflects a proactive approach to safeguarding your information.

Your engagement with classmates' posts adds value to the discussion by offering validation and encouragement. By acknowledging their efforts to prioritize privacy and sharing your own experiences, you contribute to a supportive learning environment. Additionally, your congratulatory message demonstrates thoughtfulness and contributes to a sense of camaraderie within the class.

In terms of mechanics, your writing is clear and coherent, with minor grammatical errors that do not significantly detract from comprehension. However, paying attention to punctuation and sentence structure could enhance the overall readability of your responses.

Overall, your contributions demonstrate a solid understanding of internet privacy and security concepts, and your engagement with classmates fosters a collaborative learning environment. Keep up the good work!

**STUDENT**

"Right now, as I sit writing this in my living room, I have 7 devices hooked up to the internet. Most homes now adays have just as many or more connected to the internet. Privacy and Security are always a concern, leaving a trail of personal data behind. Growing up when the internet became big, I did make mistakes early on that I learned from. Ways I combat this is using strong unique passwords, stopped sharing personal information on social media, and use a VPN when possible. I never log into any other wifi but my own. My router at home has an incredibly long and crazy password that I change every few months. The wifi is encrypted WPA2. I have set up a guest wifi for visitors. Overall, I try and do my best to keep my data safe. Every day it gets harder to keep it from the wrong hands." "You are doing a great job at keeping your information safe from the seedy underworld. It is hard to keep up with all the extra measures needed to keep our information safe these days. I am always slow to update firmware which puts me at risk." "You are doing a great job at keeping your information safe from the seedy underworld. It is definitely a nutty world with some pros and cons to it. I can't keep up with how fast the technology changes. Congrats on the new Baby. Enjoy it while you can."

**CHATGPT**

Overall Score: 83/100

• Content: 90/100

• Engagement: 80/100

• Mechanics: 80/100

**STUDENT**

"I make it a priority to keep all my devices updated with the latest software and security patches, as staying updated helps close any vulnerabilities that might be exploited by hackers. Alongside regular updates, I use reputable antivirus software to safeguard against malware and ensure that I conduct regular scans. For login security, I create strong, unique passwords for each of my accounts and manage them through a password manager. This practice is complemented by enabling two-factor authentication wherever it’s available, adding an extra layer of security beyond just passwords. At home, I’ve customized my router settings away from the default to more secure configurations, including a unique username and password. I secure my Wi-Fi network with WPA3 encryption, the most robust available, and keep my router’s firewall enabled to monitor traffic. Additionally, I’ve set up a guest network for visitors to protect access to my main network. When online, I am very cautious about the personal information I share, particularly on social media platforms. I always ensure that the websites I visit use HTTPS, especially when I’m entering sensitive information. For added security, particularly in public or unsecured networks, I use a VPN to encrypt my data and obscure my IP address, safeguarding my online activities. Physically, I keep my devices secure and within sight, especially in public places, and use biometric locks and secure passcodes as extra safeguards. I also stay alert to my surroundings when accessing sensitive information to prevent "shoulder surfing." To stay ahead of potential threats, I regularly follow security blogs and websites to stay informed about the latest in cyber threats and how to protect against them." " I completely agree with your updated approach to online privacy. It's a common misconception that incognito mode offers complete privacy, but as you've discovered, it doesn’t protect against all forms of tracking. Your shift towards using a VPN is a smart move. It not only enhances your privacy but also opens up possibilities like accessing geo-restricted content, which is a great perk. Regarding your router settings, it’s definitely a good idea to change the default username and password to something more secure. Sometimes, these settings can be tricky to adjust, but reaching out to your provider for assistance can help secure your network effectively. It’s a small step that can make a big difference in your overall network security." It’s really understandable to feel a bit out of your depth when it comes to the nitty-gritty of home network security—many people share that sentiment. Using public Wi-Fi is often unavoidable, especially when traveling. It’s great to hear that you use a VPN on your laptop and desktop; even if initially for entertainment access, it inadvertently boosts your security by encrypting your internet connection. You’re already practicing some essential security habits, like avoiding random links and pop-ups, which are common vectors for malware and phishing attacks. Also, striving to use different passwords for different sites is a good practice, even if it's tough to maintain consistently. Maybe consider a password manager to help manage and generate strong passwords without the hassle of remembering each one!

**CHATGPT**

Overall Score: 95/100

• Content: 95/100

• Engagement: 90/100

• Mechanics: 100/100

**STUDENT**

"I make it a priority to keep all my devices updated with the latest software and security patches, as staying updated helps close any vulnerabilities that might be exploited by hackers. Alongside regular updates, I use reputable antivirus software to safeguard against malware and ensure that I conduct regular scans. For login security, I create strong, unique passwords for each of my accounts and manage them through a password manager. This practice is complemented by enabling two-factor authentication wherever it’s available, adding an extra layer of security beyond just passwords. At home, I’ve customized my router settings away from the default to more secure configurations, including a unique username and password. I secure my Wi-Fi network with WPA3 encryption, the most robust available, and keep my router’s firewall enabled to monitor traffic. Additionally, I’ve set up a guest network for visitors to protect access to my main network. When online, I am very cautious about the personal information I share, particularly on social media platforms. I always ensure that the websites I visit use HTTPS, especially when I’m entering sensitive information. For added security, particularly in public or unsecured networks, I use a VPN to encrypt my data and obscure my IP address, safeguarding my online activities. Physically, I keep my devices secure and within sight, especially in public places, and use biometric locks and secure passcodes as extra safeguards. I also stay alert to my surroundings when accessing sensitive information to prevent "shoulder surfing." To stay ahead of potential threats, I regularly follow security blogs and websites to stay informed about the latest in cyber threats and how to protect against them." " I completely agree with your updated approach to online privacy. It's a common misconception that incognito mode offers complete privacy, but as you've discovered, it doesn’t protect against all forms of tracking. Your shift towards using a VPN is a smart move. It not only enhances your privacy but also opens up possibilities like accessing geo-restricted content, which is a great perk. Regarding your router settings, it’s definitely a good idea to change the default username and password to something more secure. Sometimes, these settings can be tricky to adjust, but reaching out to your provider for assistance can help secure your network effectively. It’s a small step that can make a big difference in your overall network security." It’s really understandable to feel a bit out of your depth when it comes to the nitty-gritty of home network security—many people share that sentiment. Using public Wi-Fi is often unavoidable, especially when traveling. It’s great to hear that you use a VPN on your laptop and desktop; even if initially for entertainment access, it inadvertently boosts your security by encrypting your internet connection. You’re already practicing some essential security habits, like avoiding random links and pop-ups, which are common vectors for malware and phishing attacks. Also, striving to use different passwords for different sites is a good practice, even if it's tough to maintain consistently. Maybe consider a password manager to help manage and generate strong passwords without the hassle of remembering each one!

**CHATGPT**

Your response demonstrates a comprehensive understanding of various aspects of online security and privacy. You've outlined a robust approach to safeguarding your devices and data, covering areas such as software updates, password management, router configuration, VPN usage, and awareness of online threats. Your proactive stance towards staying informed about cybersecurity best practices is commendable.

Additionally, you've provided thoughtful responses to others' contributions, offering insights and encouragement. Your feedback is supportive and constructive, acknowledging their efforts while also suggesting potential improvements or alternative approaches where relevant. This fosters a collaborative learning environment and encourages further discussion on the topic.

One suggestion for improvement could be to provide more specific examples or anecdotes from your own experiences to further illustrate your points. Sharing personal anecdotes can make your contributions more relatable and enhance the overall engagement of the discussion.

Overall, your contributions reflect a strong grasp of cybersecurity principles and a willingness to engage meaningfully with your peers on the topic. Keep up the excellent work!

**STUDENT**

"My approach to online security is pretty middle ground. I am not changing passwords every 30 days or always using 16-character passwords, but I also am not doing nothing. I use a VPN on my phone because it is the device i connect to the internet the most with. I originally got the VPN while in deployment so I could watch shows that were blocked in the foreign countries I was in. It was just a nice addition that the VPN help protect me while on public networks while away from home. Another thing I do is try to have a very minimal online presence. I rarely post on Facebook or snap chat and never tie my location with the posts i do make. Security is not just passwords and firewalls, so much information about you can be deciphered just from a photo of you. My favorite example of this is Jose Monkey, where people will send a short video of their surroundings and he can find exactly where they were just by landmarks or stores. I think it is important to note that all the things we do to protect ourselves on the internet are kind of pointless to defend from somebody that really wants YOUR information. Locks just keep honest people honest. Also our phones are basically a GPS tracking device with a camera and a phone." "I agree with your point about having multiple complex passwords for each account, but I think that putting too much faith in password managers could be problematic. Attackers only have to breach the security of the manager instead of each individual account. But all the protection in the world is only good at keeping the common thief out. If they really want your info they will get it." "It's good that you're mindful about your online activity and take some precautions like avoiding oversharing personal information and being cautious with links and emails. However, I do think keeping your devices updated with software patches is crucial for security. Updates might include better encryption or protections from known exploits."

**CHATGPT**

Your approach to online security demonstrates a balance between practicality and vigilance, which is commendable. It's understandable that you prioritize convenience while still taking steps to protect your privacy and security. Using a VPN on your phone, especially during deployment, not only allows access to geo-blocked content but also enhances security on public networks.

Your awareness of the importance of minimal online presence is crucial. Limiting the personal information you share, especially on social media, can help mitigate risks associated with data exposure. Additionally, your example of Jose Monkey highlights the potential risks posed by sharing location-based information online.

Regarding password managers, your skepticism is valid. While they offer convenience, they can also be vulnerable if compromised. It's essential to weigh the benefits of convenience against the potential risks and consider additional security measures, such as two-factor authentication, for sensitive accounts.

Lastly, your acknowledgment of the limitations of security measures is insightful. While strong passwords, software updates, and other precautions are essential, they may not deter determined attackers. However, implementing these measures still provides valuable protection against common threats and enhances overall security posture.

**STUDENT**

"My approach to online security is pretty middle ground. I am not changing passwords every 30 days or always using 16-character passwords, but I also am not doing nothing. I use a VPN on my phone because it is the device i connect to the internet the most with. I originally got the VPN while in deployment so I could watch shows that were blocked in the foreign countries I was in. It was just a nice addition that the VPN help protect me while on public networks while away from home. Another thing I do is try to have a very minimal online presence. I rarely post on Facebook or snap chat and never tie my location with the posts i do make. Security is not just passwords and firewalls, so much information about you can be deciphered just from a photo of you. My favorite example of this is Jose Monkey, where people will send a short video of their surroundings and he can find exactly where they were just by landmarks or stores. I think it is important to note that all the things we do to protect ourselves on the internet are kind of pointless to defend from somebody that really wants YOUR information. Locks just keep honest people honest. Also our phones are basically a GPS tracking device with a camera and a phone." "I agree with your point about having multiple complex passwords for each account, but I think that putting too much faith in password managers could be problematic. Attackers only have to breach the security of the manager instead of each individual account. But all the protection in the world is only good at keeping the common thief out. If they really want your info they will get it." "It's good that you're mindful about your online activity and take some precautions like avoiding oversharing personal information and being cautious with links and emails. However, I do think keeping your devices updated with software patches is crucial for security. Updates might include better encryption or protections from known exploits."

**CHATGPT**

Apologies for the oversight. Here are the scores along with the feedback:

1. Score: 85/100: Your approach to online security demonstrates a balance between practicality and vigilance, which is commendable. It's understandable that you prioritize convenience while still taking steps to protect your privacy and security. Using a VPN on your phone, especially during deployment, not only allows access to geo-blocked content but also enhances security on public networks. Your awareness of the importance of minimal online presence is crucial. Limiting the personal information you share, especially on social media, can help mitigate risks associated with data exposure. Additionally, your example of Jose Monkey highlights the potential risks posed by sharing location-based information online. Regarding password managers, your skepticism is valid. While they offer convenience, they can also be vulnerable if compromised. It's essential to weigh the benefits of convenience against the potential risks and consider additional security measures, such as two-factor authentication, for sensitive accounts. Lastly, your acknowledgment of the limitations of security measures is insightful. While strong passwords, software updates, and other precautions are essential, they may not deter determined attackers. However, implementing these measures still provides valuable protection against common threats and enhances overall security posture.

**STUDENT**

"When it comes to protecting my devices while at home or in public, first thing I start with is what wifi connection I use. At home I have it set up to where I can use a VPN. Or most commonly I like to change up passwords every now and then. In public I never connect to any WIFI spots, unless I am 100% certain its a secured connection. To often I see stories about how people make fake WIFI connections and get peoples information. While using devices, I avoid any links that have no relation to what I am doing, and if the computer says its an unsecured link, I don't click it! But as far as software, my MacBook has the anti-virus software (Xprotect). It updates usually when the MacIOs does. Or at least I am certain thats how it works. But if anyone knows it better than me, please share! All together, i make sure I am using a WIFI connection I trust, don't click on things that seem fishy, and keep my Mac updated when updates come out for the anti-virus software." "great post! I agree that using unique passwords, two factor authentication are a good start to protecting your information! But I see you pointed out having a primary network and a secondary for guests. I am going to have to look into that myself!" "great post and insight on how you protect yourself while online! Strong passwords and two factors are a great first step in my opinion. I do the same thing. Also another great thing is to not click on things you probably shouldn't be opening. I know if I don't recognize it, I don't open it!

**CHATGPT**

1. Score: 90/100: Your proactive approach to device security both at home and in public is commendable. Utilizing a VPN at home and being cautious about connecting to public Wi-Fi networks demonstrate a strong awareness of potential security risks. Changing passwords regularly and avoiding suspicious links further enhances your security posture. It's great to see that you prioritize software updates for your MacBook's antivirus software, although seeking clarification on the update process is wise. Your willingness to learn and improve your security practices is commendable, as evidenced by your interest in setting up primary and guest networks. Overall, your strategies for safeguarding your devices are sound and demonstrate a proactive attitude toward protecting your digital information. Keep up the good work!

**STUDENT**

"Hello everyone, When traveling abroad I like to keep my personal electronics safe by not using any public wi-fi networks or guest accounts. Hackers have been know to be able to access those wi-fi networks/ create them to capture your personal data and information. To prevent this from happening I solely connect to my own personal hotspot through my phone or purchase a internet puck to travel with me. Another important feature I use is a VPN for my personal laptop. This protects me from further from any hackers that might try to take my personal information. This is extra critical for when using my Army government computer. At home I use a normal spectrum router and modem, I do not have any extra implementation of protective equipment and gear. I avoid suspicious emails and web traffic from sites and people I do not know and try to only visit and click on links that I know for sure are safe and legitimate." "I am with you, in the fact that I am not the most well read or knowledgable on my computer network security. I simply just try to not log onto sites that are not well known or seem fishy. I to use a VPN when I am using networks out and about." Great work on your discussion post, I really like how you utilize a separate guest network that will keep your primary network and information safe. I will definitely be doing that in future. I think your approach to network security is really comprehensive and safe. Great work!

**CHATGPT**

1. Score: 95/100: Your approach to safeguarding your personal electronics, especially while traveling abroad, demonstrates a strong understanding of potential security risks. By avoiding public Wi-Fi networks and using your own personal hotspot or an internet puck, you're taking proactive steps to protect your data from potential hackers. Additionally, utilizing a VPN on your personal laptop, especially when accessing your Army government computer, further enhances your security posture. Your awareness of suspicious emails and web traffic, as well as your cautious approach to clicking on links, reflects a responsible attitude toward online safety. While you may not have additional protective equipment at home, your emphasis on safe browsing practices and utilizing a separate guest network showcases a thoughtful approach to network security. Overall, your strategies prioritize privacy and protection, making your digital environment more secure. Keep up the excellent work!

**STUDENT**

"Sup y'all, Module 7 lets go! We're almost there class, For this discussion I am going to start off with my own personal experiences from traveling, rather than a google answer. I hope this is sufficient. So basically traveling is my hobby. Im a seasonal wildland firefighter and when I get my lay off, I make a point to go on a 2-4 week trip to multiple foreign countries. Traveling is 100% my biggest hobby, and it is always adventure related. I grew up before all of this modern technology, so I was raised to be accustomed to: #1 listen to music or #2 read a book. Old habits die hard, and I greatly enjoy both of these things, so typically when I travel these are my main go-to's. That being said, as both myself and technology have grown, Netflix and mobile streaming apps became a thing so I grew to pre-download cinematic experiences rather than using the airlines software. Nothing against them, just throughout my life I have become very self sufficient so I try not to rely on tings like that; even today there are airlines without a touch screen TV screen. That being said, my most absolute favorite thing abut airline technology is the GPS tracker of where the airplane is currently. Regardless of if it is a long fight or a short fight, I constantly follow that thing and personally it makes my trip so much more enjoyable. Especially for the long hauls like SE Asia or Dubai." Solid post man and you bring up some very valid points. I have been considering switching to a VPN recently and after reading your post, it has helped solidify that it is probably a good choice. The marketing tactics and privacy violations are getting out of hand. This evening, my wife was talking to me about how a coworker used an app to print off a crossword puzzle for everyone at work today. Since then, I keep getting facebook advertisements for "build your own crossword" apps. That should not be okay.

**CHATGPT**

Score: 90/100

Your personal experiences with traveling offer a unique perspective on the topic of technology and entertainment during flights. It's interesting to hear how you've adapted to modern technology while still maintaining some traditional habits like listening to music or reading books. Your preference for pre-downloading content rather than relying on in-flight entertainment systems is understandable, especially given your self-sufficiency mindset. The mention of using the GPS tracker on airplanes to enhance your travel experience adds a nice touch and shows how technology can augment our enjoyment of the journey.

The discussion about considering switching to a VPN and the privacy concerns raised by targeted advertisements is relevant and adds depth to the conversation. Your example of receiving Facebook advertisements related to a conversation your wife had about crossword puzzles highlights the invasive nature of online tracking and targeting. Overall, your post provides valuable insights and prompts further reflection on the importance of privacy protection in today's digital age. Keep up the thoughtful contributions!

**STUDENT**

"Greetings class! I am sure you all noticed that my post was a tad late but I hope you enjoy it all the same and I look forward to some criticism. Flying is something that I only did a few times growing up but it wasn't until the Navy that I became a frequent flyer. The information provided to us was very informative and it really got me thinking about things I never would have thought of. My first and only layer of defense for my electronic devices is as simple as a normal 4 digit passkey. However, the next time I travel on an airplane I will take a much different approach to include a VPN to try and prevent anyone from acquiring my personal information while we are connected to the same wifi. I think that this is a cool thing that airlines are doing to help adjust to the technology dependency and the ability to let this generation entertain themselves." "I really enjoyed your discussion post, it was very different and interesting. Your simplistic defense when it comes to not using public wifi is something that I will do from time to time and it definitely works. However, it can be a drag if there is a poor connection to the hotspot. Well done!" "Your post was very relatable to me. Not only do I too, take basic precautions while connecting to public wifi but I also agree with your scary thought that companies like google have the power to do anything they want if they really wanted to. Good job explaining your thoughts and organizing your post!"

**CHATGPT**

Score: 85/100

Your acknowledgment of the importance of protecting personal information while connected to public Wi-Fi shows a proactive approach to cybersecurity. Implementing a VPN during air travel to safeguard against potential privacy breaches demonstrates a willingness to adapt and embrace technology for enhanced security. It's great to see you reflecting on your own habits and considering improvements for future trips.

The comments from your classmates highlight the relatability and relevance of your post. They appreciate the simplicity of your approach to protecting personal information and share similar concerns about the power of technology companies. However, there could be more depth in your post regarding the potential risks associated with public Wi-Fi and the benefits of using a VPN, which could further enrich the discussion.

Overall, your post initiates meaningful dialogue on cybersecurity practices during air travel and encourages others to reflect on their own habits. Keep up the thoughtful contributions!

**STUDENT**

"Good evening class, I am a frequent flyer, constantly having to travel for work and due to me being overseas this is well needed to get extra training for my job. I bring my laptop with me to either touch up on some work that I kind of forgot about or haven't work on. In addition, I try to stay updated with my schoolwork so while in flight I work on them to kill time while in flight. Stating the obvious there isn't any service being in the air so naturally, I connect to the airlines Wi-Fi. Yes, it is kind of expensive and yes it is an open network so there is always a potential for someone to spy on whatever you are doing and steal information. As a contingency, I paid and installed "Nord VPN". This application allows me to hide my IP address, hide my current location, and to make my connection to a Wi-Fi more secure. In short, to have a safer experience whilst being online. Relating to security, when it comes to my router at home, I try to keep it simple. Being simple doesn't mean be sloppy and have a weak security setup, you should invest in your router constantly. For myself, I have a very long password that I have to write down because I can not simply remember it off the top of my head. For myself i am very paranoid about security due to the amount of times that I get hacked. I seem to be very unlucky or just careless in some way. In result I went ahead and installed a third party firmware, "DD-WRT". This will strengthen not only the capabilities of your router but will replace the default firmware so make it more secure and protect all of your private information. Good thing about it, is that it is free!" "Regarding the topic that was covered, using a VPN feels almost crucial these days due to people always wanting to steal your information. I use Nord VPN and was wondering what kind of VPN you utilize. I am so bad at clicking pop ups because they can sometimes be very convincing that I need to have a coffee mug. Great job on this post, Felt relatable to me because I also go on planes a lot so I typically bring my personal laptop for work/entertainment." "So my only question about "WhatsApp" is this, due to its alleged ability to be encrypted, does this restrict the creator/ developer of the app from accessing messages? Myself being in the barracks I use to live the struggle of having boingo but then later switched to buying my own router due to the ability to have a private connection. This will allow you to install a third party firmware into it, this will in result better your security. Great job on your post, really cracked me up on the comment of how it knows where you are even when it shouldn't.

**CHATGPT**

Score: 90/100

Your post effectively highlights the importance of cybersecurity practices, especially during air travel and at home. Your proactive approach to protecting your devices both in-flight and at home demonstrates a commendable commitment to security. Utilizing a VPN like Nord VPN while connected to public Wi-Fi networks adds an extra layer of protection, which is crucial in today's digital landscape where cyber threats are rampant.

Your decision to invest in your home router's security by using a long password and installing third-party firmware like DD-WRT shows a thorough understanding of the importance of securing your network. The fact that you're willing to take these extra steps despite previous hacking experiences reflects a proactive attitude toward mitigating potential risks.

Your engagement with your classmates, particularly inquiring about their VPN usage and raising questions about WhatsApp's encryption, adds depth to the discussion and encourages further exploration of cybersecurity topics. Overall, your post is informative, relatable, and contributes positively to the conversation on digital security. Great job!

**STUDENT**

"Hey class! My approach to protecting my when I am online is always to enable my two-factor authenticator such as temporary code to sent from email or my number. And I always checked the taskbar if there is any trouble or or not belong to the software like password cracking tools and application. Lastly, I don’t put my personal information in my own personal computer. Because, you never know who is going or after with your belongings stuff. What measures do I take to safeguard my computer and other devices? It is very simple but very effective. First off download and install antivirus software. This will help to detect malicious software and viruses to compromise my devices. Secondly, enable automatic updates. Regular updates help is to avoid the unknown vulnerabilities. Thirdly, I don’t use my personal email address when I am buying stuff like let say a third party seller. Because, it will spam my email and put something malware software. Lastly, I am making that my WiFi is secured and also I considered to hide my network SSID to make it visible and less problem. Details and explanations about my router security settings: Connect to the router's administration interface using the default IP address. Change the default administrator username and password to unique, strong credentials. Enable encryption and set a strong WiFi password. Enable MAC address filtering to allow trusted devices on the network. Regularly update the router's firmware for security patches and improvements." "I agree with your perspective on the importance of ensuring the safety of online accounts. Creating and managing robust and unique passwords, using a combination of uppercase and lowercase letters, numbers, and special characters, is indeed a crucial step in enhancing security. Additionally, utilizing a password manager to generate and store complex passwords for each account can further strengthen our online presence. Regularly updating passwords and avoiding reuse across multiple accounts are essential practices for safeguarding personal and financial well-being in the digital age." "Whitney, you're taking important steps to prioritize privacy and security in this interconnected world. Using strong, unique passwords, refraining from sharing personal information on social media, and utilizing a VPN are all effective strategies. Your precautions with Wi-Fi, such as a long, regularly changed password and separate guest network, further enhance protection. It's a constant battle, but your efforts are commendable. Keep up the good work!"

**CHATGPT**

Score: 85/100

Whitney, your proactive approach to protecting your online accounts and devices is commendable. Enabling two-factor authentication and regularly checking for suspicious activity on your computer demonstrate a strong commitment to security. Your strategy of avoiding sharing personal information on your personal computer is also wise, as it adds an extra layer of protection against potential threats.

Your measures to safeguard your computer and other devices, such as installing antivirus software, enabling automatic updates, and being cautious with personal email addresses during online purchases, are effective and practical. Utilizing encryption and setting a strong WiFi password, along with regularly updating your router's firmware, contribute significantly to enhancing your network security.

Your engagement with your classmates, offering feedback and sharing perspectives on online security practices, adds depth to the discussion and fosters a collaborative learning environment. Overall, your approach demonstrates a good understanding of cybersecurity principles, and your commitment to implementing best practices is evident. Keep up the excellent work!

**STUDENT**

"Hello class, I want to preface this by saying that I don't worry about my privacy online nearly as much as I should; as in, I will take basic precautions such as never posting my name or specific location unless absolutely necessary, but I don't normally use a VPN or other extensive security measures to maintain my privacy. TO be completely honest, I think that companies like Google and Microsoft can track you down no matter what if they wanted, and precautions are more directed towards other internet users. Obviously, one of the best ways to protect your privacy against targeted attacks is to change up your passwords for different websites. It can be a bit tough to track all your passwords, but using the proper tools can be beneficial. Additionally, antivirus services like Microsoft Defender help prevent viruses from being downloaded on my computer, but I would never download something from a website that I'm not familiar with. Also, I try not to click on links from other websites unless I know exactly where it leads. On our Wi-Fi router, we use the WPA2 (Wi-Fi Protected Access 2) setting to prevent hackers and other unsolicited attacks from gaining entry into our network. It's the next generation of WPA, and it supposedly uses some of the best encryption algorithms today in order to protect the network. " "I'm also fairly guilty of not staying too wary of my privacy when it comes to security. However, I try not to connect to public Wi-fi pretty much ever, as I can use a personal hotspot for most things. However, if I do connect to public Wi-fi, I think it's safer to practice standard safety precautions like not revealing personal information or logging into sensitive websites. A VPN would also definitely help, as it increases your own personal security, and that's something that I need to work on as well." "I think that using a VPN, even at home, can be incredibly helpful to keeping your information safe. I also like how you change your passwords up fairly often; it's something that I need to start doing as well, as I only really change it when I'm prompted to do so. Anti-virus software is also helpful, but I would be wary of using a default anti-virus; it's also another thing that I need to look into, but I think it might be worth purchasing a high-quality anti-virus."

**CHATGPT**

Score: 80/100

Your awareness of basic privacy precautions is commendable, although you acknowledge room for improvement. Utilizing different passwords for various websites and being cautious about clicking on unfamiliar links are essential steps to safeguarding your online accounts. However, considering the potential capabilities of large companies like Google and Microsoft to track user data, it's understandable that you feel limited in your ability to fully protect your privacy.

Your use of antivirus software like Microsoft Defender is a positive step towards protecting your computer from malware. However, being selective about downloading from unfamiliar websites and avoiding clicking on unknown links altogether can further reduce the risk of encountering malicious content.

Using WPA2 encryption on your Wi-Fi router is a good practice to prevent unauthorized access to your network. It's encouraging to see that you're mindful of securing your home network against potential threats.

Your acknowledgment of the benefits of using a VPN, both at home and on public Wi-Fi networks, demonstrates an understanding of the additional layer of security it provides. Considering investing in a reputable VPN service could further enhance your online privacy and security.

Overall, your willingness to recognize areas for improvement in your privacy practices and your openness to exploring additional security measures are positive steps towards strengthening your online security posture. Keep exploring and implementing new strategies to enhance your privacy and security online.

**STUDENT**

"Class, When it comes to internet privacy I choose to take a simpler route. I really just don't put my personal business out on the internet. I started using social media back in 2008 but really only used it regularly for about 4 years. Once I was out of high school I realized that I just didn't care about other friends business and if I did I would ask. Since my information is on the internet somewhere I really just insure I try not to accept cookies and regularly go through my email and unsubscribe from any spam. So far I really feel comfortable with just using the internet less to prevent my privacy from being targeted. When it comes to security I used to be more in tune with my electronic devices and insuring I was caught up with he latest virus protection. As I got older I really started using the internet differently and really 90% of my internet activity comes from my smart phone. I don't play games on my phone and I'm not really downloading anything other than email attachments that I would send myself. I take a really simplistic approach to internet security now but that is primarily because I feel like my internet activity is simplistic. I regularly check my bank accounts so I also know if my money is being taken. I did have an instance where a credit card that I never use ever had a tiny charge. I was able to rectify the issue and I was able to remove my cards from being used again on the website they had been used on. In this case my simple approach worked and have worked for my since but I do think I am fortunate with what has happened with me and my experience. I approach internet security how I would in the physical world really. I mind my own business and if it looks like a sketchy place then I will go somewhere else." "you are so much more thorough with your security. What is more impressive is that what you do does not go above and beyond but creating small habits that add to your overall enhanced security. Something we both have in common is using VPN's. I did purchase a VPN for a year but I found that I wasn't using it as much as I thought I would. Most of the time I don't like using public Wi-Fi. I don't come into many situations where my unlimited cellular data gets throttled to a point where I can't download or stream something on my phone. If you do know some good VPN's that are free send them my way!"

**CHATGPT**

Score: 85/100

Your approach to internet privacy and security is grounded in simplicity and practicality, which can be effective for many users. By minimizing your online presence and being selective about what information you share, you reduce the likelihood of your privacy being compromised. Regularly unsubscribing from spam emails and avoiding cookies are proactive steps to manage your online footprint.

While you acknowledge a shift in your internet usage primarily towards your smartphone, you maintain a simplistic approach to security. This includes not engaging in risky online activities like downloading unknown apps or games, which reduces the potential exposure to malware and security threats. Your experience with monitoring your bank accounts and promptly addressing suspicious charges demonstrates vigilance in safeguarding your financial information.

It's commendable that you approach internet security with a mindset similar to how you would navigate the physical world, focusing on minding your own business and avoiding potentially risky situations. However, considering the prevalence of online threats, such as data breaches and phishing attacks, it may still be beneficial to explore additional security measures beyond your current practices.

Regarding VPN usage, it's understandable that you haven't utilized it extensively, especially if you primarily use your smartphone for internet access. While there are free VPN options available, it's essential to research and select reputable providers to ensure adequate protection without compromising privacy. If you're interested, I can provide recommendations for reliable free VPN services.

**STUDENT**

"Measures taken to safeguard computer and other devices. Privacy protection and device security have gained more importance in the digital era, more so with the connectivity of humans to home, class, and even flights (Reportlinker, 2020). This paper discusses my approaches to protecting my online privacy and securing my devices while providing an in-depth overview of the security settings for my router at home. Device Security Measures My essential security strategies include robust passwords, encryption, and regular updates. In the first place, I consider periodic updates to the OS software and apps on my gadgets. Such updates are fundamentally crucial because these often include security patches that may help existing security issues specific to a given time frame. Secondly, I guarantee that I have installed powerful antivirus and anti-malware softwares. Installing reputable security programs, I create a barrier that hinders malware intrusion, which might harm my security. I continuously run real-time protection and sometimes opt for regular scans to detect and terminate any risk. Finally, I rely on Virtual Private Networks (VPNs) when I connect to public Wi-Fi networks in public places such as airports or cafées. VPN provides me with internet traffic encryption, which enhances overall data transmission security, making me the only person who can read or see my sensitive information. These strategies make the mainstay of my approach to device security, covering all kinds of incidents in the modern life of us who use devices. Router Security Settings After setting up the router, one of the things I do with precision is configure its settings. The first thing that I do is change the default username and password. Since the default credentials are common knowledge and can be found over the Internet, the routers can be accessed without authority if the default passwords are retained. I then activate WPA3 encryption, one of the latest encryption technologies available, which is useable for personal and enterprise use. Generally, WPA3 significantly improves security, making it a means of network security from foreign attacks. Also, I turn offthe Wi-Fi Protected Setup (WPS) feature. Although WPS is put in place to ease the connection of devices to the network without a user having to get into the hassle of password entry, it can be a security liability, asattackers could exploit this feature. I switch this feature off. Another vitalmeasure I undertake is to have a separate guest network apart from the one managing my personal devices and sensitive information. In so doing, I've isolated the traffic that the visitors bring, thus reducing the potential risk they can introduce to my network inadvertently. All these measures combined boost the defense of my network against any unauthorized access and cyber threats. Approaches to Online Privacy I act carefully to protect my online privacy. I carefully manage my online footprint by paying explicit attention to the information I post on social media and adjusting settings for who can access my posts and personal data. I also use privacy-centric browsers and their add-ons as ad blockers and anti-tracking tools to manage my online movements and security better. Further, wherever available, I utilize Two-Factor Authentication (2FA) as services offer. A second level of validation through 2FA makes security tighter and reduces the likelihood of infiltration (Boeing, 2011). These, among others, form part of the practice of ensuring digital privacy and the safety of personal information in an ever-connected world. In today's highly connected world, the onus of security and privacy for devices is increasingly on the individual user. All that one can do is take these necessary precautions and guard well by following good security practices andmonitoringprivacy settings. When users observe these strategies, they enjoy the immense benefits of digital connectivity without losing their means of security and privacy. References Boeing. (2011, September 22). Pushing 787 in-flight entertainment systems to the limit [Video]. YouTube. https://www.youtube.com/watch?v=JUWJmEuk4Ic Reportlinker. (2020, April 6). In-flight Entertainment & Connectivity Market Size, Share & Trends Analysis Report By Offering Type, Component, Aircraft Type, Region And Segment Forecasts, 2020 - 2028. Www.prnewswire.com. https://www.prnewswire.com/news-releases/in-flight-entertainment--connectivity-market-size-share--trends-analysis-report-by-offering-type-by-component-by-aircraft-type-by-region-and-segment-forecasts-2020---2028-301035736.html" "Your complete online privacy protection is relatively humane and full of measures you think through. Robust, unique passwords for all accounts, followed by the application of two-factor authentication (2FA), would feature at the top of your practices. It is good to hear that you advocate using safe networks or VPNs to protect their data, and indeed, their data needs protection against public Wi-Fi networks. Another good point is that you regularly update your software on your devices. Sometimes, these updates even contain security patches to protect against new vulnerabilities. I am curious to hear how you manage all the passwords, whether you are working off a system that uses a password manager and syncs it between devices or something different. Your router has WPA2/WPA3 encryption and guest network separation. It is an excellent way to segregate traffic and reduce risk from other less secure devices. A firewall adds to its security. That's pretty good. You are backing up your data quite often. Do you back it up into the cloud, or do you use some external drives for that? Let us know so you can help someone else increase their data redundancy. You are overall quite spectacular in ways that others should emulate to improve their security state." "It is impressive and detailed what you have set for securing your devices. Strong and unique passwords and two-factor authentications will be the groundwork for protecting your privacy in this digital world. It is also necessary to update frequently to fix the security vulnerability before it is exploited. I am happy you take so much care about this update to stay one step ahead of the threat. Of course, not browsing suspicious websites and not interacting with doubtful content on the web significantly mitigate the risk. It's somewhat of a miracle that your password changes so often, which also differs from the last one. And here's another tip you probably know, but sometimes, you don't apply, which can increase your security. It would help if you got a password manager to makemanaging passwords easier. These kinds of tools keep your passwords safe and create strong and unique passwords for each of your accounts, thus reducing the chance of a breach related to your password. They simplify your internet life by auto-filling web and app login details, so you only have to remember the master password. Besides, properly reviewing the app permission details in your devices will go a long way towardallowing only what is necessary for the apps and reducing the data leak risks. This is a crucial practice for keeping a hold on your personal information."

**CHATGPT**

Score: 95/100

Your comprehensive approach to safeguarding your devices and ensuring online privacy demonstrates a deep understanding of cybersecurity principles. Utilizing robust passwords, encryption, and regular software updates are fundamental steps in enhancing security. The incorporation of antivirus software and VPNs further fortifies your defenses, particularly when accessing public Wi-Fi networks.

Your meticulous attention to router security settings, including changing default credentials, enabling WPA3 encryption, and segregating guest networks, showcases a proactive approach to network security. Additionally, the decision to disable Wi-Fi Protected Setup (WPS) mitigates potential vulnerabilities, enhancing overall network resilience against cyber threats.

Moreover, your commitment to managing online privacy through social media settings, privacy-centric browsers, and Two-Factor Authentication (2FA) reflects a holistic understanding of privacy protection measures. Your willingness to share insights on password management and data backup practices adds value to the discussion, highlighting the importance of data redundancy and password hygiene.

Incorporating a password manager could streamline password management and enhance security by generating strong, unique passwords for each account. Furthermore, conducting regular reviews of app permissions can minimize data exposure and mitigate potential privacy risks associated with excessive data access.

Overall, your proactive approach to cybersecurity and privacy underscores the importance of adopting multifaceted strategies to mitigate digital threats effectively. Your contributions provide valuable insights that empower others to bolster their security posture and safeguard their digital assets in an ever-connected world.

**STUDENT**

"Unfortunately I am not the most savvy when it comes to security of my home network and I am guilty of using free public wifi from time to time. I do however utilize a VPN on my laptop and desktop sometimes but I did not start using a VPN for security reasons but rather to change my location to watch shows and things of that nature while deployed. Other precautions that I take are common are things like not clicking random links or pop-ups. I also try my best to utilize different passwords for different websites although sometimes I fail at that out of laziness. With the future of flying going towards only utilizing my own personal devices on public networks I will start to prioritize security as the thought of always sharing a public network with thousands of others at an airport sounds a bit scary. While the convenience of always having access to entertainment via your personal devices sounds great, I’m curious to see the security implemented by the providers." "It is both hilarious and scary that your mobile device that you do not want knowing your location shows you that it has your location and then lies to your face about not knowing it. I too will always opt to not share when given the option but I know in all honesty they will will still know. Great post." "Great post! Good to see you actually know your router's security settings as I had no idea what mine were. I usually just leave the settings as they come although I am pretty good about setting up a custom username and password."

**CHATGPT**

Score: 80/100

Your acknowledgment of areas where you could improve your network security demonstrates self-awareness and a willingness to learn. While you may not be highly proficient in securing your home network, your use of a VPN on your laptop and desktop, even if initially for entertainment purposes, reflects a proactive step towards enhancing security.

Taking precautions such as avoiding clicking random links or pop-ups and attempting to use different passwords for various websites, despite occasional lapses, indicates a basic understanding of cybersecurity best practices. However, consistently implementing these practices could further strengthen your overall security posture.

Your recognition of the evolving landscape of in-flight entertainment and the potential security implications of using personal devices on public networks demonstrates a proactive mindset towards adapting to emerging security challenges. Prioritizing security in such scenarios is indeed essential, given the inherent risks associated with sharing public networks with numerous users.

The observation about mobile devices seemingly knowing your location despite assurances otherwise highlights the complexities of privacy in the digital age. Your skepticism and caution regarding data sharing are commendable, even though the reality of data collection may sometimes seem unavoidable.

While you may not delve deeply into router security settings, your awareness of basic configurations like setting up a custom username and password is a positive step. Exploring additional security features and staying informed about router security best practices could further enhance your network's resilience against potential threats.

Overall, your post reflects a balance between recognizing areas for improvement and implementing practical measures to enhance security. Continuously seeking to educate yourself and adopt proactive security measures will contribute to strengthening your overall security posture in an increasingly connected world.

**STUDENT**

"Class, Personally approach I like to take to protecting myself while on public or private Wi-Fi is a big front approach. First approach is turning off auto-connect, saves you a ton of problems. Don't know how many times I have been out in public and seen random networks with some wild names with free access. Additionally, I turn off file sharing. To many stories of friends getting random pictures and sometimes some suspect files that have who knows what attached to them. Occasionally I like to use a VPN, mostly its just safe practice when suffering the internet to find information. Otherwise I keep to a handful of website I visit. Also I try to stick with HTTPS website. You really cant go wrong with browsing on an encrypted website. Lastly keeping an up to date virus subscription is probably the best step to an all around safe approach while surfing." "Smart move on the VPN and HTTPS website choice. Safe use out in public is the best practice to maintaining your personal information from theft. I'm curious to what the future of internet protection will look like, what's next after two step." "Smooth approach on the VPN use and WPA. The two step approach is something I like to use myself. Good move on the unique passwords, despite how frustrating they can be its smart to just sit down and make a good password."

**CHATGPT**

Score: 90/100

Your approach to protecting yourself while using public or private Wi-Fi networks demonstrates a proactive stance towards cybersecurity. Disabling auto-connect and turning off file sharing are effective measures to mitigate potential risks associated with connecting to unsecured networks. These practices help prevent unauthorized access to your device and reduce the likelihood of receiving malicious files or content.

Utilizing a VPN and prioritizing HTTPS websites further enhances your security posture. VPNs encrypt your internet traffic, safeguarding your data from interception by malicious actors, while HTTPS ensures secure communication between your device and the website you're visiting, reducing the risk of data interception or tampering.

Your emphasis on maintaining an up-to-date virus subscription underscores the importance of regular security updates in combating evolving cyber threats. Keeping your antivirus software current helps protect your device from malware, viruses, and other malicious software that could compromise your security.

Overall, your approach reflects a well-rounded strategy that incorporates multiple layers of protection to safeguard your personal information and ensure a secure browsing experience. Continuing to stay informed about emerging threats and implementing proactive security measures will further strengthen your defense against potential cyber threats.

**STUDENT**

"Good afternoon class, My approach to protecting my privacy online used to be "incognito mode". I thought that my privacy was protected by using that. I also thought that apps wouldn't be able to send me ads for stuff I looked up when I was "incognito". It turns out that Google has admitted to tracking data while incognito and has a lawsuit against them. "Google would track users and collect their data while they were browsing privately" (Brokin, 2024). Since I've started using my computers more often I purchased a VPN from Total AV. Along with the VPN, I have a full computer security program from Total AV that was included as a package deal. This gives my devices at home security, like encrypted file sharing and actual browsing privacy. I have the ability to turn it on and off. I also have numerous benefits from utilizing the VPN, my favorite is that the VPN app allows me to select where I would like to connect from, states, cities, and even countries, and with that I can stream Netflix shows that aren't available in US Netflix. I may also get better Amazon pricing. For my router, I don't have anything going on special. It has the same username and password that was given to me by my internet provider. I know I should change it and I've tried like 5 times but for some reason, it won't stick. I'll have to call the provider one of these days." " I also use a VPN for the majority of my streaming. I'm curious about which VPN you use. I have an iPhone so creating new passwords for things is relatively easy because the iPhone will suggest a strong password for you and then keep your saved passwords in your settings. So even if you forget, or log in on another device, you can find them all in one place. " "You have a protocol. You are dialed in on your defenses in cyber security. It's honestly given me more insight on what I can do to protect my cyber awareness. However, I do not think it necessary for me to add another network for guests, because I don't have a spare bedroom, and that means people cant stay long. lol"

**CHATGPT**

Score: 85/100

Your approach to protecting your privacy online has evolved from relying solely on "incognito mode" to adopting more robust security measures such as using a VPN and a comprehensive computer security program from Total AV. This demonstrates a proactive effort to enhance your online security and privacy.

Utilizing a VPN not only provides encryption for your internet traffic but also allows you to bypass geographical restrictions and access content from different regions. Your awareness of the benefits of VPNs, such as accessing region-locked Netflix shows and potentially getting better pricing on Amazon, highlights the practical advantages of using such technology.

Regarding your router, while it's understandable that changing the default username and password can be challenging, it's crucial for improving your network security. Consider reaching out to your internet provider for assistance or exploring online resources for troubleshooting tips.

It's commendable that you're considering implementing separate networks for guests, although it's understandable if it's not feasible due to space constraints. However, even if guests don't stay long, having a dedicated guest network can still enhance your network security by isolating their devices from your main network, reducing the risk of unauthorized access.

Overall, your commitment to improving your cybersecurity practices is evident, and with continued diligence and exploration of additional security measures, you can further strengthen your online privacy and protection.

**STUDENT**

"My approach to Protecting my privacy when online... It can be annoying sometimes, but it is worth it! Using strong, unique passwords for my accounts. Each password is different in some way. I utilize “Passwords” on my apple products to keep track of my accounts and passwords. Enable two-factor authentication (2FA) whenever possible. Regularly update software on my devices. Using a secure network or VPN when I don’t have a secure network. I tend to stay away from websites that are not well known or sorced. I regularly back up my data on my computer. My router Security settings: I have a WPA2/WPA3 encryption that secures my network. I have a customized username and password for my WiFi. I have a separate guest network that isolates guest devices from my primary network. This helps reduce the risk of unauthorized access. I also use the firewall feature to monitor network traffic." "I just wanted to let you know that I think your approach to device security is really impressive. Your focus on using secure Wi-Fi connections, changing passwords regularly, and staying cautious with public networks shows a great awareness of cybersecurity. Your effort towards privacy and security are on point!" "I appreciate your straightforward take on internet privacy and security. It's smart to be cautious with what you share online and to keep a close eye on your accounts. Your approach to steering clear of 'sketchy places' is a great analogy. It's a good reminder that sometimes simplicity is key, and staying vigilant is always important." "Thank you for the kind words! These days it's incredibly hard to be fully secure, but every little bit helps!

**CHATGPT**

Score: 90/100

Your approach to protecting your privacy online is comprehensive and proactive, demonstrating a strong commitment to cybersecurity. Utilizing strong, unique passwords, implementing two-factor authentication, and regularly updating software are essential practices that significantly enhance your security posture.

Using a secure network or VPN when accessing the internet adds an extra layer of protection, especially when connected to public Wi-Fi networks. Your cautious approach to avoiding websites that are not well-known or sourced helps mitigate the risk of encountering malicious content.

Your router security settings are robust, with WPA2/WPA3 encryption, customized login credentials, and a separate guest network. These measures effectively safeguard your home network from unauthorized access and potential threats.

It's evident that you prioritize privacy and security in your digital activities, and your diligence in backing up data further reinforces your proactive approach to cybersecurity. Overall, your efforts to stay vigilant and implement best practices contribute to a strong defense against online threats. Keep up the excellent work!

**STUDENT**

"I wanna start this off by saying something I feel we can all agree on, we live in a pretty nutty world, but everything has its ups and downs right? I strongly believe that we are in the greatest time to be alive in the history of the universe, and also the most confusing time to be alive. Technology is advancing at such a fast rate right now that my daughter (who will be born this month 😎btw) may be able to be among the first humans to live essentially forever. Now that's just a theory but tomorrow they might tell us it's just a thing now. With all of this craziness we all have our own little piece of the internet that villains are constantly trying to steal from us. The few ways I try to keep me and my family safe is using a VPN for all of our electronics at home or on the go. I also try to change up my passwords for different sights so that if the bad guys get one they don't just immediately ruin my whole life lol. I'll end my rambling now, and thanks for reading!" "I agree that we all need to use strong passwords that will make it as difficult as possible for people to figure them out. I totally forgot about immediately updating software. Thank you for the post and have a great weekend." "I love the presentation you created to state all of the possible ways to stay safe online. It is extremely difficult in the time we live in to actually be 100% secure and private. Iam sure doing all of these safety procedures does the trick though! thanks for the post and have a great weekend."

**CHATGPT**

Score: 85/100

Your enthusiasm for the advancements in technology and the potential they hold for the future is evident in your post. It's great to see your proactive approach to cybersecurity, especially considering the importance of protecting your family's online privacy and security.

Using a VPN for all your devices at home or on the go is a wise decision, as it encrypts your internet connection and enhances your overall privacy. Additionally, regularly changing passwords for different sites adds an extra layer of security, reducing the risk of a single breach compromising multiple accounts.

Your acknowledgment of the challenges of achieving complete security and privacy online is realistic, but your commitment to implementing safety procedures is commendable. Keep up the good work, and congratulations on the upcoming addition to your family!

**STUDENT**

"Here we are yet again for another discussion and this time about privacy with our PEDs. A very simple thing that I do to protect my privacy is I don't use public WIFI systems, I will connect to my cell phone's personal hot spot and use internet that way. That is how I am able to log into my laptop in my command when I have down time between maintenance and that is precisely what I am doing now. I don't have my phone's airdrop on everybody, all of my social media is set to private or only friend's and family. Like I said in a previous discussion that advancements in technology are both a blessing and a cure, it is a double edge sword with on side of the blade having poison and everything venomous. As security measures become increasingly more proactive at keeping would be identity thieves at bay, so to does their advancements in hacking become increasingly more dynamic as well. Google admitted to people's devices listening to conversations in the room to better assist people with ads on what they wanted more based on an algorithm. I had a similar situation one time in late 2019 early 2020 right before the plandemic, my command was in Air Wing Fallon for about 6 weeks. I was working in the airframe shop on night check from 1800-0600 and we were having a conversation about the S & W .500 Magnum and one of the guys logged onto the computer and got on facebook and the very first video that popped up on his feed was the exact same gun, the exact same make, the exact same youtube video came up. Everyone in the shop said $%#$ that and we all put our phone on airplane mode or turned them off. We knew as a collective that big tech spys on people to "better enhance" their experience but they also sell our information to foreign entities and next thing you know you get spam mail, spam callers and more and more ads on your feed. I limit the use of technology in my household for good reason, especially when we find out the google maps vehicle is on the road. Nope, they aren't spying on me through my wifi. Protect yourself at all costs especially when it comes to electronics and the information that can be stolen from you via electronics." "I agree with you Jacolby on using a VPN for your laptops and updating your passwords whenever possible. I too fall into the trap of using familiar passwords, but in my defence I have a lot of shit on my plate so if it is easier to remember a familiar password then so be it. Do make sure your home wifi is set to privacy, turn off your airdop whenever in public. I've been on two different deployments on two different carriers and I learned that if you don't wan t something airdropped to your phone on the boat turn your airdrop off, lol. Great post brother, keep it up." "Can't say I miss the good ol' barracks wifi but that was trash and slow as hell. My roommate had gotten his own internet with wifi cuz he was a gamer and I found his password so I used it lol, barracks life. Yeah, I don't like the fact that every app you download you have to ask it not to use your location ever, not to give you updates etc. these apps are becoming too much like a trojan horse and you don't know what is inside of the app until it is too late. Using the VPN feature is huge when it comes to privacy because it does make it harder for people to try to get your information. Like the Iphones iOS 17 update when there was a warning about the name drop feature with another phone that was near by. I happened to me and I made sure I turned off that feature. Good job Tyler, keep it up."

**CHATGPT**

It seems like you're all discussing various strategies to maintain privacy and security, especially when it comes to using electronic devices and navigating the online world. Using a personal hotspot instead of public Wi-Fi, setting social media accounts to private, and being cautious about sharing personal information online are all important steps in safeguarding your privacy.

The anecdote about the incident with the S & W .500 Magnum video appearing after a conversation highlights concerns about potential privacy breaches and surveillance by technology companies. It's essential to remain vigilant and take proactive measures to protect your personal information from being exploited or misused.

Additionally, the use of VPNs, updating passwords regularly, and being mindful of app permissions are effective ways to enhance online security. Your discussions reflect a shared understanding of the importance of privacy and the need to stay informed about potential risks and vulnerabilities in the digital landscape.

Overall, your exchanges demonstrate a strong commitment to prioritizing privacy and security in your online activities, and it's great to see everyone sharing tips and insights to help each other stay safe in the digital world.

**STUDENT**

"Here we are yet again for another discussion and this time about privacy with our PEDs. A very simple thing that I do to protect my privacy is I don't use public WIFI systems, I will connect to my cell phone's personal hot spot and use internet that way. That is how I am able to log into my laptop in my command when I have down time between maintenance and that is precisely what I am doing now. I don't have my phone's airdrop on everybody, all of my social media is set to private or only friend's and family. Like I said in a previous discussion that advancements in technology are both a blessing and a cure, it is a double edge sword with on side of the blade having poison and everything venomous. As security measures become increasingly more proactive at keeping would be identity thieves at bay, so to does their advancements in hacking become increasingly more dynamic as well. Google admitted to people's devices listening to conversations in the room to better assist people with ads on what they wanted more based on an algorithm. I had a similar situation one time in late 2019 early 2020 right before the plandemic, my command was in Air Wing Fallon for about 6 weeks. I was working in the airframe shop on night check from 1800-0600 and we were having a conversation about the S & W .500 Magnum and one of the guys logged onto the computer and got on facebook and the very first video that popped up on his feed was the exact same gun, the exact same make, the exact same youtube video came up. Everyone in the shop said $%#$ that and we all put our phone on airplane mode or turned them off. We knew as a collective that big tech spys on people to "better enhance" their experience but they also sell our information to foreign entities and next thing you know you get spam mail, spam callers and more and more ads on your feed. I limit the use of technology in my household for good reason, especially when we find out the google maps vehicle is on the road. Nope, they aren't spying on me through my wifi. Protect yourself at all costs especially when it comes to electronics and the information that can be stolen from you via electronics." "I agree with you Jacolby on using a VPN for your laptops and updating your passwords whenever possible. I too fall into the trap of using familiar passwords, but in my defence I have a lot of shit on my plate so if it is easier to remember a familiar password then so be it. Do make sure your home wifi is set to privacy, turn off your airdop whenever in public. I've been on two different deployments on two different carriers and I learned that if you don't wan t something airdropped to your phone on the boat turn your airdrop off, lol. Great post brother, keep it up." "Can't say I miss the good ol' barracks wifi but that was trash and slow as hell. My roommate had gotten his own internet with wifi cuz he was a gamer and I found his password so I used it lol, barracks life. Yeah, I don't like the fact that every app you download you have to ask it not to use your location ever, not to give you updates etc. these apps are becoming too much like a trojan horse and you don't know what is inside of the app until it is too late. Using the VPN feature is huge when it comes to privacy because it does make it harder for people to try to get your information. Like the Iphones iOS 17 update when there was a warning about the name drop feature with another phone that was near by. I happened to me and I made sure I turned off that feature. Good job Tyler, keep it up."

**CHATGPT**

Apologies for the oversight. Here's your feedback along with a numerical score out of 100:

Score: 95/100

Feedback: You've shared valuable insights and experiences regarding privacy and security measures in the digital realm. Your contributions highlight the importance of remaining vigilant and proactive in safeguarding personal information. Keep up the great work in promoting awareness and sharing strategies for enhancing online privacy and security!

**STUDENT**

"As I've stated before, I'm not very good with technology. When it comes to the internet and security I don't know very much about it. I typically try to stay on reliable sites such as .gov, .org, and .edu. I also use a VPN on all devices that I possibly can. When going through a website I leave if it directs me to any ads and/or sketchy pages. I also try to avoid pages with a lot of ads. For passwords I change them every few months and try to make them as strong as possible. I also try to make my passwords with a capital, a lower case, a number, a special character, and at least 10 characters long. This does become difficult to keep track of, so I keep them listed in a notebook which I do realize isn't very secure. It's either I write them down or I forget them, so I chose the latter." "I forgot to add what my home router settings are. Since I don't know anything about those settings, I've just left them at the default." "Thank you for sharing your post. I really like how you research the latest threats, that will make you more than capable of dealing with them if and when they arise. I also like that you use a VPN on public Wi-Fi." "I appreciate your post. I wish I was as vigilant as you are when it comes to my online security. I just can't seem to get into the whole technology thing. It seems like you have most of your bases covered.

**CHATGPT**

Score: 85/100

Feedback: Your approach to online security demonstrates a good level of awareness, especially with the use of VPNs and caution regarding website credibility. It's commendable that you change your passwords regularly and strive to make them strong. However, relying solely on written passwords in a notebook may pose a security risk. Exploring password manager tools could offer a more secure solution. As for router settings, it's essential to learn about them to strengthen your home network's security. Overall, your efforts to stay informed and implement basic security measures are praiseworthy. Keep exploring and learning to further enhance your online safety!

**STUDENT**

"The internet is everywhere. From coffee shops, to airports, to restaurants, you can usually always find an internet connection. This is great for everyone to have the ability to stay connected, but you also run the risk of leaking your private information or someone hacking into your devices. My work requires me to travel quite a bit so I am constantly hopping on different networks to catch up on work or log in for homework assignments. To protect my privacy online, I always ensure I use the highest level of authentication possible for any login. For websites, I will always use a two factor authentication to login. I ensure my passwords are very unique and not the same for each site I use. I always ensure to keep my authentication methods up to date as well. As for safeguarding my devices, I use antivirus software on my personal computers. I also have a unique password set and an encryption, WIFI protected access (WPA), for my at home WIFI. For work, I use a remote VPN before accessing anything online to ensure I am protecting the information being held within the computer. Bottom line, I always choose the highest level of protection possible for whatever website or device I am using." I completely agree with you on this class giving me some inspiration to look more into what I am doing for internet protection. I am very naïve when it comes to information leaks and hacking because it hasn't happened to me. I would hope this is a result of me being careful of sites I visit and my protection currently in place! Just looking at this discussion, I didn't know so many people use a personal VPN for their personal computers. It is a really great idea that I never thought of doing. Great post! "You seem to be more cautious than I am! It is a very smart idea to invest in a personal VPN due to how much you find yourself connecting to a public network. I just connect without a second thought about my information getting hacked. I like how you keep it simple it home, but your simple is better than mine! Having a password you can't remember might be a good thing as long as you don't lose it. Also, having the idea to install a third party firmware only makes it more secure. I'm sure if you are unlucky when it comes to hacking you have found the best tricks to keep a high level of protection!"

**CHATGPT**

Score: 90/100

Feedback: Your proactive approach to internet security is commendable, especially your emphasis on using the highest level of authentication possible, employing unique passwords for each site, and keeping authentication methods up to date. Utilizing antivirus software, encryption, and VPNs demonstrate your commitment to safeguarding both personal and work-related devices and data. It's great to see your willingness to explore new security measures, such as considering a personal VPN for your personal computers. Engaging in discussions like this can indeed provide valuable insights and inspire further research into enhancing your online protection. Keep up the excellent work in prioritizing your cybersecurity!

**STUDENT**

"Good morning class, I have always been cautious whenever I am purchasing anything online. Whenever I purchase anything online I would only use ApplePay, PayPal, or Klarna since I know my bank account information is encrypted and my information is not shared with the seller. Another extra step I like to keep in mind is to only purchasing items online when I am at home using my own Wi-Fi since I know using public Wi-Fi allows anyone with the right equipment to access my information. I aso appreciate apple because it gives me the option to let an app to use my microphone or camera whenever I am using it and turning off GPS on apps that I know don’t need my location. A security measure that took for protecting my router is using a strong password with capitals, numbers, and special characters. I also like to see which devices are connected and disconnect any devices that i do not recognize." "I think it really smart move of you to disconnect old devices or not in use devices. Since i have spectrum i like to mange the devices through the website. I definitely agree with you that you should be aware with what devices you allow your phone to trust. " "That’s a real smart move of using a VPN when using public Wi-Fi. I do also believe that every one should be aware of the dangers of cyber threats so they can keep their information protected. Would you happen to have the name of the antivirus software you use in order to protect your devices? "

**CHATGPT**

Score: 85/100

Feedback: Your cautious approach to online purchases, particularly by utilizing secure payment methods like ApplePay, PayPal, and Klarna, demonstrates a strong awareness of cybersecurity risks. Avoiding public Wi-Fi for sensitive transactions and actively managing device connections to your router further exemplify your commitment to protecting your personal information. Incorporating measures such as disabling unnecessary app permissions and using strong passwords enhances your overall security posture. Sharing the name of the antivirus software you use could provide additional insights into effective cybersecurity practices for your classmates. Keep up the proactive approach to safeguarding your digital assets!