Task 1:

In my home network I have couple home servers. The most secure one I have taken completely isolated from the rest of the network, and I add data to it through physical means, like through external HDDs. The other server can only be accessed through my main computer.

For my accounts I use different passwords for each one (obviously). I do not use a password manager or some sort, as a successful attack on the manager itself would render everything vulnerable. I do use two factor authentication whenever possible.

At the very least I do not know of being a victim in any serious cybercrime. I probably have been scammed in Runescape when I was young, but I would not count that. I have been a target of phishing and probably malware scams, for example, I once received an email about Ethereum airdrop that had a suspicious PDF. I obviously did not open the PDF, but certainly it was malware. I still have the email so I can study it when I have the time.

Task 2:

Potential targets for cyber criminals for me would be my accounts, any of my computers, IoT devices I have and home servers I host.

Accounts I have range from vital (email, bank account) to trivial (forum accounts). As such, great care should be taken with the vital account information. While having a trivial account fall victim to a cyber crime would be bad, it would not be as disastrous as the vital accounts. Something like the main email account being taken over would be catastrophic.

As accounts are high value targets and there are numerous possible attack vectors against them, they are at a high risk of being attacked. Likelihood of being targeted by an attack is very high, if not almost daily. Most likely vulnerabilities are weak passwords and phishing emails.

Important factors to note is not to any kind of weak passwords with important accounts, and to change them regularly. However, it should be noted that changing passwords often can be rather annoying, so focus on important accounts when changing passwords. Also make sure to enable 2FA whenever possible. Another important thing to note is not to leave sensible information on any public accounts as attackers can find this information with just looking it up. Finding out whether or not an account is compromised can be rather hard if the application that account is related to does not inform of any weird logins and such. However, if such message were to be received, the account should immediately be locked, and password changed.

My home computer contains a large amount of sensitive information and data that should not be allowed to fall into wrong hands. Extra care should be given to secure this. Other computers do not really contain sensitive information, but they should also be properly taken care of. As computers are well protected against attacks, they have smaller risk of being targeted by attackers than accounts, but still likely enough that vigilance is needed.

Attacks that directly target the OS require a payload. Usually these are sent over through malicious files, like executables, zips and PDFs. These are easy to avoid by not downloading weird files or clicking suspicious links. If something suspicious needs to be opened anyways, do it in a sandboxed environment first to see whether or not it is malicious. Another important safety factor that might be overlooked regularly for home computers is the physical side. Leaving the computer open and unlocked in public places spells disaster. Even if the computer is locked, it should never be left alone.

If the home computer would become compromised, the impact would be very bad. A lot of sensitive information could be accessed by the attacker, but fortunately enough, nothing too dangerous should be on the computer. All sensitive data should be moved to an encrypted location, so in the event of an attacker accessing the main computer, the sensitive data would still be more likely to be safe. If any computer would be compromised, nothing less than a full reinstallation of the OS should be done. This would change OS passwords and make sure no malicious programs were left in the system.

IoT devices I have range from wireless sensors to routers. The routers could allow access to the rest of the network and need to be protected. The wireless sensors are also possible attack vector on the network.

The IoT devices are most likely the most vulnerable parts for attacks, but the likelihood of them being targeted is rather small. To attack the wireless devices, the attacker would need to be close to the device, so the amount of people capable of such attack is drastically reduced. Vulnerabilities are also hard to pin down, as I do not have access to the software within the devices, so if the device has vulnerabilities within, I would not know of it. The scope of possible impact if an IoT device were to be compromised ranges from weather information data being leaked to possible network access.

Still, steps can be taken to mitigate any possible attacks. For the router, updating the software will help and making white and blacklists. The router passwords also need to be strong and changed regularly. For the IoT devices, looking up if vulnerabilities have been found and then mitigating those or changing devices will reduce the risk.

Home servers contain large amounts of data that need to be protected. While they are well protected already, there could still be possible attack vectors attackers can use.

One of the home servers contain no useful data for any attacker, just TV shows. If an attacker were to access this home server, the impact would be minimal. The other contains backups, so if the attacker would access it, the outcome would be bad if they deleted those backups, but it does not contain sensitive data.

The show server can be accessed through the network, so an attacker could reach it if they had network access. However, in this case the network access would be more disastrous thing than access to the home server. The other server is isolated from the network, so an attacker could not access it in any other way than somehow get malicious code through a program or if they had physical access to it.

To mitigate any attacks the backup server should be locked up and for the other the network needs to be secured.

Task 3.

Policy on passwords

1. Passwords must be complex enough to satisfy security concerns.
    a. Minimum length: 10 characters

    b. Use of both upper and lower case letters
    c. Include at least two numeric digits
    d. Include at least one special character
    e. Not contain employee names or any basic one word words (ex. Dictionary)
2. Passwords must be stored in safe and secure manner
    a. This means no writing passwords down anywhere like paper or sticky notes
    b. Passwords can't be saved in emails or documents that are not encrypted
    c. Password sharing is strictly prohibited to anyone, be it family, colleagues or IT support
3. Passwords are to be changed every six months and the password is not allowed to be the same as any before used
4. Any passwords given by the IT department must be changed immediately
5. If a password is forgotten, the recovery must be done through the IT department

Policy on social media usage

1. Employees are not allowed to create personal social media accounts using company emails
2. Only authorized personnel may use and create official company social media accounts
    a. Official account lists are to be maintained by the IT department including login credentials in a safe and secure manner
3. Employees are responsible for anything they post on their personal social media accounts and they must not engage in online activities that could hurt the reputation of the company or violate any laws or regulations
4. Employees are prohibited from posting any company information that is confidential or proprietary
5. Employees must get approval from supervisors or from marketing department before sharing any company news, updates or promotional material
    a. Exception is made to reposting material official social media accounts have already posted
6. If an employee sees another employee breach this policy they must report it to the upper management