Vulnerability refers to a weakness or flaw in a system or network that can be exploited by attackers.

Threats are potential risks or dangers that can exploit vulnerabilities to cause harm.

Control refers to measures that are put in place to prevent or mitigate the impact of threats.

2.

Examples of violation of availability:

A power outage causes a data center to lose power and go offline.

A critical system fails due to a hardware malfunction, causing it to become unavailable.

Human error: Human error can also lead to a violation of availability.

Examples of violation of confidentiality:

A data breach occurs and sensitive customer information is leaked.

An employee shares confidential business information with a competitor.

An attacker gains access to a user's personal email account and reads their private messages.

Examples of violation of integrity:

A hacker alters data on a company's database, changing the prices of products to cause financial harm.

A virus infects a system and deletes important files, causing data loss and harm to business operations.

An employee maliciously modifies data in a system to cover up their mistakes or wrongdoing.

3.

A person's financial information being stolen in a data breach and used for fraudulent purposes.

It’s malicious and i was one of the unfortunate victims.

4.

Attackers who might want to attack a program that displays a city's current time and temperature could include hackers looking to steal user data, competitors looking to disrupt a rival's website, or individuals with malicious intent looking to cause harm.

The harm they might want to cause could include stealing user data, disrupting the website's functionality, or even taking control of the website for their own purposes.

Some vulnerabilities they might exploit could include weak passwords, outdated software, or insecure coding practices.

5.

Attackers who might want to attack a program that allows consumers to order products from the web could include hackers looking to steal credit card information or personal data, competitors looking to disrupt a rival's website, or individuals with malicious intent looking to cause harm. The harm they might want to cause could include stealing user data, disrupting the website's functionality, or even taking control of the website for their own purposes.

Some vulnerabilities they might exploit could include weak passwords, unsecured payment processing, or insecure coding practices.

6.

(a) 26^4=456976 possible password combinations, approximately 63.5 hours.

(b) 26^4=456976 possible password combinations, approximately 63.5 hours.

7.

An alternative, less costly means of handling deletion is placeholder which can be used to delete the content of different subject lists.

8.

I choose 2.

The way that password managers work is simple. You save all your passwords to the manager, and then create one "master" password for all of them. When you sign into a site, you just use that one master password — it's the only one you need to remember.

9.

Privacy concerns: Some people think that biometric technology may reveal personal privacy.

Solutions:By implementing strong data security measures, such as encryption and access controls

Security concerns: Biometric data can be stolen or spoofed, potentially leading to unauthorized access.

Solutions:By implementing multi-factor authentication, which requires multiple forms of authentication such as a password and a fingerprint to grant access.

Accuracy concerns: Biometric systems are not perfect and can sometimes fail to recognize authorized users, leading to frustration and inconvenience.

Solutions:By providing backup authentication methods, such as a password or security questions, in case the biometric system fails to recognize the user.

10.

The better method would be sending a new password by email. This is because, most user tend to use repeated passwords for the vast majority of their online accounts. Therefore, sending their old password can cause problems if someone else has access to the user's email and discovers their old password. They may then be able to use this password to access various other accounts that the user possess. The best option would be to send the user a temporary new password and force the user to change the password once they regain access into their account.