Explain why someone who used the same password for several sites would need to change all those passwords. In your opinion, was LinkedIn negligent in protecting its main asset? Explain

Step 1:

Passwords are your computer's and personal information's first line of defence against unwanted access. Your computer will be safer from hackers and bad malware if you use a strong password. For all accounts on your computer, you should use strong passwords.

Step 2:

According to a new Google study, internet users should cease using the same password for different websites unless they want their data to be stolen, their identity stolen, or worse. When you use the same password for multiple websites, you are yourself vulnerable to hackers having access to your personal information.

If you use the same password for all of your accounts, a single password breach anywhere puts them all at risk. Hackers will also be able to access your other internet accounts.

Using the same password for many accounts is akin to having a single key that unlocks all of your doors. Every door is vulnerable if a bad actor obtains or replicates the key. Make it difficult to access your information if one of your accounts is compromised.

Step 3:

There are various effects on Linkedln's popularity and credibility, including a significant loss of money, regulators imposing massive fines for violating privacy laws and guidelines, and a significant loss of revenue in cleaning up and upgrading the data. The lack of security and failure to identify the intrusion would have severely harmed Linkedln's trust and discouraged potential users from joining, resulting in lower-than-expected ad revenue. Millions of dollars were spent cleaning up the damage and investing in IT infrastructure as a result of the incident. As a result, the security compromise was more than just a public relations disaster.

Linkedln was encrypting data with an out-of-date method. As a result, they were unable to detect the data breach, but IT security specialists were able to do so ahead of them.

linkedln took a sloppy approach to data security. The data was Linkdln's most valuable asset, and failing to preserve it made no sense for business. In the business world, IT security assumes responsibility for providing cyber protection for data. When LinkedIn became aware of hacking and data breaches, nearly 6.5 million user passwords were leaked, resulting in millions of dollars in losses and violations of privacy. The entire information was then published on the Russian website.