Five Cyber Security Breaches that have happened till now:

1.Facebook

Date: April 2019
Impact: 533 million users

Two Facebook app datasets that were made available to the general internet in April 2019 were made public. Phone numbers, account names, and Facebook IDs were among the data, which pertained to more than 530 million Facebook members. Two years later, in April 2021, the data was made freely available, suggesting new and genuine criminal intent about the data. Security researcher Troy Hunt actually added functionality to his HaveIBeenPwned (HIBP) breached credential checking site that would enable users to check if their phone numbers had been included in the exposed dataset due to the sheer volume of phone numbers that were impacted and easily accessible on the dark web as a result of the incident.

2. Yahoo

Date: August 2013

Impact: 3 billion accounts

Nearly seven years after the initial breach and four years after it was discovered how many records were actually exposed, the attack on Yahoo has taken the top rank. The incident, which the business said occurred in 2013, was first made known to the public in December 2016. It believed that over a billion of its customers' account information had been accessed by a hacker gang at the time when it was in the process of being acquired by Verizon. A little over a year later, Yahoo revealed that the real number of compromised user accounts was 3 billion. Yahoo claimed that the updated estimate did not indicate a fresh "security concern," and it sent emails to all "affected user accounts" as a result.

Despite the attack, the contract with Verizon was finalized—albeit at a lower cost. In response to the then-evolving world of online threats, Verizon's CISO Chandra McMahon stated at the time: "Verizon is committed to the highest standards of accountability and transparency, and we proactively endeavor to protect the safety and security of our users and networks. By receiving support from Verizon's expertise and resources through our investment in Yahoo, that team is able to keep making important security improvements. Investigation revealed that although the attackers gained access to account data such security questions and answers, plaintext passwords, payment card information, and bank information were not taken.

3.LinkedIn

Date: June 2021

Impact: 700 million users

In June 2021, data linked with 700 million of its members was released on a dark web site, affecting more than 90% of LinkedIn's user base. Before dumping a first information data set of over 500 million customers, a hacker going by the handle "God User" employed data scraping techniques to take advantage of the site's (and others') API. They continued by bragging that they were selling the entire 700 million-customer database.Although LinkedIn claimed that because no sensitive, private personal data was exposed, the incident was a violation of its terms of service rather than a data breach, a scraped data sample posted by God User contained information such as email addresses, phone numbers, geolocation records, genders, and other social media details, which would give criminals plenty of data to create convincing, follow-up social engineering attacks after the leak, as warned by the U.S.

4. Adobe

Date: October 2013

Impact: 153 million user records

Adobe revealed that hackers had acquired login information for an unknown number of user accounts and about three million encrypted customer payment card records at the beginning of October 2013. The estimate was then raised by Adobe to include 38 million "active users"' IDs and encrypted passwords. Then, according to security blogger Brian Krebs, a file that had only been posted a few days prior "appears to comprise more than 150 million login and hashed password pairs obtained from Adobe."Weeks of research showed that the hack had also exposed customer names, password, and debit and credit card information. An agreement in August 2015 called for Adobe to pay $1.1 million in legal fees and an undisclosed amount to users to settle claims of violating the Customer Records Act and unfair business practices. In November 2016, the amount paid to customers was reported to be $1 million.

5.Adult Friend Finder

Date: October 2016

Impact: 412.2 million accounts

In October 2016, hackers broke into six databases belonging to the adult-focused social networking service The FriendFinder Network and stole subscriber information spanning 20 years. Given the delicate nature of the services provided by the company, which include casual hookup and adult content websites like Adult Friend Finder, Penthouse.com, and Stripshow.com, the leak of information from more than 414 million accounts, including names, email addresses, and passwords, had the potential to be particularly damaging for victims. And by the time LeakedSource.com published its study of the data set on November 14, 2016, the great majority of the disclosed passwords—roughly 99% of them—had been cracked using the notoriously flawed SHA-1 hashing technique.