Five Cyber Security Breach

The five cyber security breach that has happened till now are given below:

1. The Crypto.com Crypto Theft

The crypto.com crypto theft attack took place on 17th January. It targeted approximately around 500 people's cryptocurrency wallets. The hackers succeeded to steal approximately about $18 million worth of Bitcoin along with $15 million worth of Ethereum. The theft was possible due to the ability of the hacker to bypass the two-factor authentication in the user's account and access their wallets. This is an example of why using a password manager is important.

2. The Microsoft Data Breach

Microsoft was targeted by a hacking group called Lapsus$ on March 20th, 2022. The Lapsus$ group had previously targeted Nvidia, Samsung and plenty of other companies. So, Microsoft's security team was ready. The group posted a screenshot on Telegram indicating they had hacked Microsoft. And, along the process, compromised Cortana, Bing, and several other products. The hackers did retrieve some material from Microsoft. However, soon by March 22nd Microsoft announced it had quickly stopped the hacking attempt and that only one account was compromised. Microsoft also claimed that no customer data had been stolen.

3. The News Corp Server Breach

The News Crop Server Breach reported in February 2022, was admitted to server breaches way back to February 2020. News Corp asserted that no customer data was stolen during the breach. They also claimed that the company's everyday work wasn't hindered. However, News Corp uncovered evidence that emails were actually stolen

from its journalists. The attackers have not been identified. However, News Corp has stated that espionage is at the root of this attack.

4. The Red Cross Data Breach

In January 2022, Red Cross Data Breach took place when the hackers carried out an attack on servers hosting the personal information of more than 500,000 people receiving services from the Red Cross and Red Crescent Movement. The data related to the organization's Restoring Family Links services, which works to reconnect people separated by war, migration, and violence was said to be on the hacked servers. Red Cross took servers offline in order to stop this suspected attack by a nation state. The culprit has not yet been identified.

5. The Cash App Data Breach

In April 2022, Cash App was victim of a breach that was done by their own former employee. The hacker clearly had some personal grudges with the business. The hack involved customer names, stock trading information, account numbers and portfolio value, along with the addition of loads of other sensitive financial information. The company had to take some serious action as they contacted more than eight million customers to tell them about the incident. Fortunately, no account credentials were stolen in the attack. The hacker could only steal a limited amount of identifiable information in the said attack.