CYBER SECURITY CASE STUDY :

WHY DO PEOPLE NEED TO BE AWARE OF CYBER SECURITY ?

What is Cybersecurity?

Cybersecurity consists of all the technologies and practices that keep computer system and electronic data safe.

In a world where more and more of our business and social lives are online , it's an enormous and growing field.

In simple terms it's an ongoing effort to protect network systems and all data from unauthorized use or harm.

Why do you need to be aware of cybersecurity?

1. **Data Breach** : Data breach or data theft is one of the crucial aspects of cybersecurity. The risk of data theft is high it can ruin the relationship of company and customers .

   In 2018 the popular social media platform Facebook admitted that an unexpected attack on it's computer network exposed the personal data of over 50 million users .

2. **Cyber Attacks** : with the rising cyber threats , it has become difficult to keep a track of cyber – attacks that's been happening every year.
   Few common cyber attacks are phishing , malware attacks, SQL injection etc.

Case Study 1 : Facebook's Data breach Scandal (2018)

According to the report published by **The New York Times and The Guardian on March 17, 2018** . The report said that Christopher Wylie , the creator of 'thisisyourdigitallife' app was behind the data breach .

As per Wylie's claim , private data of users was sold to Cambridge Analytica for targeting users with ads supporting former US President Donald Trump . Facebook's co-founder Mark Zuckerberg revealed that sensitive information of users like their name, hometown, and gender were accessed by hackers through the platform's API's.

Facebook had no clue when the attack began .They officially notified the users about the Data breach on September 25, 2018.

Breach Consequences :

People were not pleased with what they heard and read on the news. Many users were worried and wanted increased regulation around their personal data , while others were even investigating on how to delete their Facebook account.

Financially, the day after the scandal Facebook's share price went down by 7%, and it's market value also fell more than $36 billion.

Facebook's data policy changed :

In 2014, Facebook decided that third – party developers could no longer gain access to new data from an app user's friends.

In 2015 , The Guardian posts an article that Cambridge Analytica helped Ted Cruz's campaign by **'psychographic profiling'**

Facebook responded to the article by banning **'thisisyourdigitallife'** from the platform and asked Cambridge Analytica to remove data that was gained in violation of this policy.

Continuation of Facebook data privacy problems :

Reportedly, Zuckerberg leveraged user data with various competitors and partners as shown through **leaked, internal documents (April 16, 2019)**

They would limit or allow more access to user data with other companies depending on their relationship with them; it was used as a bargaining chip

FB's mishap with email contacts (April 18th, 2019) : 1.5 million email contacts were mistakenly uploaded to FB servers . It was part of a feature where these contacts were used to find friends on the platform.

Case Study 2 : The WannaCry Ransomware Attack of May 2017

The WannaCry attack occurred in the span of four days , however there was heavy damage . Infected systems in over 150 countries resulted in a $100,000 payout for the attackers - however , the losses in productivity and erased files are predicted to have reached into the billions.

The attack was highly effective because it spread across devices by exploiting the Windows **Server Message Block (SMB) protocol**, which enables Windows machines to communicate with each other on a network.

The attack was spread using **EternalBlue** , a Zero – day vulnerability in devices that use an old version of SMB. It was discovered by the **U.S. National Security Agency (NSA)** before being obtained by hacking group Shadow Brokers , which published the exploit within a post on blogging site Medium in April 2017.

How was WannaCry Stopped ?

It can be stopped by downloading a Microsoft patch for the SMB vulnerability, which was made available two months before the attack began.

WannaCry is still a threat for old Windows devices that have not patched to prevent the vulnerability from being exploited.

Key points :

1. WannaCry affected over 350,000 devices in the span of four days in 2017.
2. It exploited a vulnerability in the windows server messenger block.
3. WannaCry used RSA and AES encryption to encrypt a victim's files , demanding a ransom of up to $600
4. Though it was stopped by timely patches and a key retriever , it resulted in billions of dollars in damage.

Cybersecurity Measures :

1. Change your passwords and keep a track of everything. Also use two factor authentication to add extra layer of protection.
2. An easy way for attacker to gain access to your network is to use old credentials that have fallen wayside . Hence delete unused accounts.
3. Keeping the software up to date.

Conclusion :

Today due to high internet penetration , cybersecurity is one of the biggest need of the world. Cybersecurity threats are very dangerous to the country's security . Therefore not only the government even the citizens should spread the awareness among the people to always update the system and network security and also to use anti virus softwares.