UNIVERSITY OF DELHI

ATMA RAM SANATAN DHARMA COLLEGE

VAC (Value Addition Course)

Digital Empowerment Assignment

SUBMITTED TO: Dr. Meenakshi Gupta

SUBMITTED BY:

NAME: SOURAV

COURSE: B.Sc. (H) Computer Science

COLLEGE ROLL NUMBER: 24/48044

THREATS IN THE DIGITAL WORLD

: Data Breach and Cyber Attack

The digital world, while offering immense opportunities, also presents a myriad of threats. These threats, often referred to as cyber threats, can target individuals, businesses, and even governments. Here are some of the most common threats in the digital world:

Malware:

- **Viruses: Self-replicating malicious code that can damage systems and data.**
- **Worms: Similar to viruses but spread independently, often through networks.**
- **Trojans: Disguised as legitimate software but contain malicious code.**

- Ransomware: Encrypts data and demands a ransom for its decryption.
- Spyware: Monitors user activity and steals sensitive information.

Social Engineering:

- Phishing: Deceiving individuals into revealing personal information through fraudulent emails or messages.
- Spear Phishing: Targeted phishing attacks aimed at specific individuals or organizations.
- Smishing: Phishing attacks carried out via SMS messages.
- Vishing: Phishing attacks conducted over the phone.

Hacking:

- Unauthorized Access: Gaining access to systems or networks without permission.
- Data Breaches: Stealing sensitive data, such as personal information or financial records.
- Denial-of-Service (DoS) Attacks: Overwhelming a system or network with traffic, making it inaccessible.
- Man-in-the-Middle (MitM) Attacks: Intercepting communication between two parties to steal data or manipulate information.

Other Threats:

- Pharming: Redirecting users to malicious websites.
- SQL Injection: Exploiting vulnerabilities in web applications to access or manipulate databases.
- Cross-Site Scripting (XSS): Injecting malicious code into websites to steal user information or hijack sessions.
- Zero-Day Exploits: Exploiting vulnerabilities that are unknown to software vendors, allowing attackers to gain unauthorized access.

What is a Data Breach?

- A data breach occurs when sensitive information is accessed, used, or disclosed without authorization. This can include personal data like names, addresses, Social Security numbers, credit card information, or even intellectual property.
-

What is a Cyber Attack?

- A cyber Attack is a malicious attempt to damage, disrupt, or gain unauthorized access to a computer system or network. Cyber Attacks can take many forms, including:
- Malware attacks: Using malicious software to infect systems and steal data.
- Phishing attacks: Deceiving individuals into revealing sensitive information through fraudulent emails or messages.
- Denial-of-service (DoS) attacks: Overwhelming a system or network with traffic, making it inaccessible.
- SQL injection attacks: Exploiting vulnerabilities in web applications to access or manipulate databases.
- Ransomware attacks: Encrypting data and demanding a ransom for its decryption.
- The Impact of Data Breaches and Cyber Attacks
- The consequences of data breaches and cyber attacks can be far-reaching:
- Financial loss: Costs associated with data breach investigations, legal fees, and lost business.

- Reputational damage: Loss of customer trust and brand reputation.
- Legal liabilities: Potential fines and lawsuits.
- Operational disruption: Interruption of business operations.
- Identity theft: Misuse of personal information for fraudulent activities.
-

Where do Cyber threats come from?

Cybersecurity threats come from a variety of places, people, and contexts. Malicious cyber threat actors can include:

- Criminal organizations
  Organized groups of hackers aim to break into organizations for financial gain. These cyber threat

actors use phishing, spam, spyware, and malware for extortion, theft of private information, and online scams that are run like corporations, with large numbers of employees developing attack vectors and executing attacks

- Nation-states
  Hostile countries can launch cyber attacks against local companies and institutions to interfere with communications, cause disorder, and inflict damage.
- Terrorist organization
  Terrorists conduct cyber attacks aimed at destroying or abusing critical infrastructure, threatening national security, disrupting economies, and causing bodily harm to citizens.

How to Protect Yourself

- To protect yourself from data breaches and cyber attacks, consider the following tips:
- Strong passwords: Create strong, unique passwords for each account.
- Enable two-factor authentication: Add an extra layer of security to your accounts.
- Be cautious of phishing attempts: Verify the authenticity of emails and websites before clicking links or downloading attachments.

- Keep software updated: Regularly update operating systems and applications to address vulnerabilities.
- Use antivirus and firewall software: Protect your devices from malware and unauthorized access.
- Back up your data: Regularly back up important data to prevent loss.
- Be mindful of public Wi-Fi: Avoid using public Wi-Fi for sensitive activities like online banking.
- By staying informed about the latest threats and taking proactive measures, you can significantly reduce your risk of falling victim to data breaches and cyber attacks.
-