**In which way both the data breaches & cyber-attacks impact on individuals as well as on organizations for their growth.**

**What is a Data Breach?**

* **Data Breach** means accessing someone's data without knowing them or without any authorization.
* **A**Data Breach **is**also called **data leaking or information leaking**. Data can be of any type; it may be health-related data, business-related data, or any other sensitive data.
* Someone may have done it intentionally or unintentionally and can use it to harm you personally or financially.
* Data breaches now become a very popular attack in the **field of**[**hacking**](https://www.geeksforgeeks.org/types-of-hacking/). Many growing hackers try these types of attacks to enhance their skills.

**How Do Data Breaches Happen?**  
Data breaches happen when someone steals your data. This can occur if your device is lost or taken, or if you click on a fake link or open a harmful file that gives hackers access to your system.

**What is a Cyber Attack?**

* A cyber attack is when someone tries to steal, damage, or take control of computer systems or data without permission. These attacks can affect individuals, companies, or even governments.
* Hackers often use fake emails or infected files to trick people into giving access to their systems.
* It's important not to open suspicious emails and always check who they are from.

**How Does a Cyber Attack Work?**  
Cyber-attacks are mainly of two types:

1. **Untargeted Cyber Attacks:** These attacks aim at many users or devices at once, not one specific target.

* **Phishing:** Sending fake emails to trick people into sharing bank details or passwords.
* **Ransomware:** Stealing and locking your data until you pay money.
* **Scanning:** Randomly checking many systems to find weak spots to attack.

1. **Targeted Cyber Attacks:** These attacks are aimed at a specific person or organization.  
   For example, sending a harmful link or file to one person to steal their data once they click or open it.

**I. Impact on Individuals and Their Growth**

**1. Financial Problems**

* Hackers can steal **money from bank accounts** or use credit cards.
* Victims may lose their savings and take time to recover financially.
* This stops people from **saving for the future** or investing in education or business.

**2. Loss of Job Opportunities**

* If personal data like **emails or private files** are leaked, it can affect someone’s **professional image**.
* It may lead to **job loss or missed opportunities** in the future.

**3. Mental Stress**

* People feel scared, angry, or sad when their personal data is leaked.
* This affects their **mental health** and reduces their confidence to move forward.

**4. Identity Theft**

* Hackers can use someone’s name or documents to **apply for loans or commit crimes**.
* The real person may have to **fight legal cases** or prove their innocence, which wastes time and energy.

**5. Fear of Using Technology**

* After being attacked, people become afraid to use **online services, apps, or cloud storage**. This can stop their **growth in learning or using technology for work**.

**II. Impact on Organizations and Their Growth**

**1. Money Loss**

* Companies lose money due to:
  + **System shutdowns**
  + **Paying ransom to hackers**
  + **Legal fines**
* This stops companies from using that money to **grow or improve their services**.

**2. Losing Customer Trust**

* If customers’ data is stolen, they will **stop trusting the company**.
* This can lead to **loss of customers** and **bad public image**, making it harder to grow.

**3. Work Disruption**

* Attacks can make systems stop working for hours or days.
* This **slows down business** and affects delivery, customer service, or production.

**4. More Spending on Security**

* After an attack, companies need to spend more on **cybersecurity tools, experts, and training**.
* This takes away funds that could have been used for **research, marketing, or hiring**.

**5. Legal Problems**

* If a company fails to protect user data, it may face **fines from the government**.
* Legal cases and compensation claims can **waste time and reduce business focus**.

**6. Loss of New Ideas**

* If secret company information (like product plans or software code) is stolen, **competitors may copy them**.
* This **reduces the company's growth and competitive edge**.

**Prevention of Cyber Attacks**

1. **Use Strong Passwords:**  
   Create passwords using a mix of letters, numbers, and special characters. Avoid easy passwords like “1234” or “password.” Many websites will warn you if your password is weak—make sure to change it to a stronger one.
2. **Don’t Trust Unknown Emails:**  
   Avoid opening emails from unknown senders or clicking on suspicious links or attachments. These could be tricks to steal your information or infect your device with harmful software.
3. **Secure Your Devices:**  
   Always protect your devices by installing reliable antivirus software. Also, use strong device locks like passwords, PINs, or fingerprint recognition. This makes it harder for hackers to access your data if your device is lost or stolen.

**Prevention of Data Breaches**

**For Enterprises:**

1. **Vulnerability Management:**  
   Use tools to scan your systems for security gaps and weaknesses. Regular assessments help you fix misconfigurations before attackers exploit them.
2. **Regular Software Updates:**  
   Always update your software and operating systems. Old or unpatched software can have bugs that hackers can use to access your data.
3. **Limit Data Access:**  
   Only give employees access to the data they need. Avoid sharing sensitive or financial information with those who don’t need it for their work.

**For Employees:**

1. **Secure Your Devices:**  
   Use antivirus software, enable password or fingerprint locks, and keep all applications up to date to prevent unauthorized access.
2. **Protect Your Accounts:**  
   Change your passwords regularly and avoid using the same one across multiple accounts. Use strong, unique passwords.
3. **Be Aware of Social Engineering:**  
   Do not click on unknown links, share personal information, or trust suspicious websites. Cybercriminals use tricks to fool users into giving up information.
4. **Monitor Bank Transactions:**  
   Regularly check your bank statements to ensure no unauthorized transactions have taken place. Early detection can help reduce damage.