

|  |  |
| --- | --- |
| **Intake: APD1F2409CS(CYB)** | **Module Code: CT046-3-1-ISTF** |

|  |  |  |
| --- | --- | --- |
| **HAND OUT DATE: Thursday, 24 April 2025 Week 6** |  |  |
| **SUBMISSION DATE: Thursday, 26 June 2025 Week 14** |  |  |

**TITLE:**

***DATA BREACH INTELLIGENCE***

**Module Lecturer: Ts. Muhammad Amin Sahari**

**GROUP NAME 14**

|  |  |
| --- | --- |
| **AHMED MIRAHUSAIN ALVI** | **TP084807** |
| **ABDALLAH MOHAMED MAHMOUD MOHAMED** | **TP085097** |
| **SULTAN ABDULLA OMAR TAKRORI** | **TP085327** |
| **BADR MAHDI MUBARAK AL-AMRI** | **TP083084** |
| **MOHAMED ABA SAID** | **TP082376** |
| **MOHAMED ABDIFATAH ALI** | **TP082459** |
| **MOHAMMED YOUSEF MOHAMMED MOHAMMED** | **TP085042** |
| **MAHRUS SHAMSUL AHSAN** | **TP085562** |

TABLE OF CONTENTS

[CHAPTER 1: CYBER CRIME & SECURITY BREACHES 1](#_Toc201017319)

[CHAPTER 2: MOAB GROUP OPINION 2](#_Toc201017320)

[***2.1*** *AHMED MIRAHUSAIN ALVI* 2](#_Toc201017321)

[***2.2*** *ABDALLAH MOHAMED MAHMOUD MOHAMED MAHMOUD* 3](#_Toc201017322)

[***2.3*** *SULTAN ABDULLA OMAR TAKRORI* 4](#_Toc201017323)

[***2.4*** *BADR MAHDI MUBARAK AL-AMRI* 5](#_Toc201017324)

[***2.5*** *MOHAMED ABA SAID* 6](#_Toc201017325)

[***2.6*** *MOHAMED ABDIFATAH ALI* 7](#_Toc201017326)

[***2.7*** *MOHAMMED YOUSEF MOHAMMED MOHAMMED* 8](#_Toc201017327)

[***2.8*** *MAHRUS SHAMSUL AHSAN* 9](#_Toc201017328)

[CHAPTER 3: ANALYSIS 10](#_Toc201017329)

[***3.1*** *Specifics of MOAB Breach* 10](#_Toc201017330)

[***3.2*** *Probable Causes of the Breach* 10](#_Toc201017331)

[***3.3*** *Steps to Detect your Group Member Data has been Breached or Not* 11](#_Toc201017332)

[***3.3.1*** *AHMED MIRAHUSAIN ALVI 11*](#_Toc201017333)

[***3.3.2*** *ABDALLAH MOHAMED MAHMOUD MOHAMED MAHMOUD 12*](#_Toc201017334)

[***3.3.3*** *SULTAN ABDULLA OMAR TAKRORI 13*](#_Toc201017335)

[***3.3.4*** *BADR MAHDI MUBARAK AL-AMRI 14*](#_Toc201017336)

[***3.3.5*** *MOHAMED ABA SAID 15*](#_Toc201017337)

[***3.3.6*** *MOHAMED ABDIFATAH ALI 16*](#_Toc201017338)

[***3.3.7*** *MOHAMMED YOUSEF MOHAMMED MOHAMMED 17*](#_Toc201017339)

[***3.3.8*** *MAHRUS SHAMSUL AHSAN 18*](#_Toc201017340)

[CHAPTER 4: IMPACT 19](#_Toc201017341)

[***4.1*** *Potential Impact on Individuals* 19](#_Toc201017342)

[***4.2*** *Potential Impact on Organizations* 20](#_Toc201017343)

[***4.3*** *Societal Implications of Data Breaches* 20](#_Toc201017344)

[CHAPTER 5: PROPOSING SOLUTIONS 22](#_Toc201017345)

[CONCLUSION 26](#_Toc201017346)

[REFERENCES 27](#_Toc201017347)

[WORKLOAD MATRIX 29](#_Toc201017348)

CHAPTER 1: CYBER CRIME & SECURITY BREACHES

The “Mother of All Breaches” (MOAB) epitomizes one of the most shocking and worrisome leaks of sensitive information in the context of cybersecurity incidents. It came to attention in January of 2024 when someone's breach of cyber security gave out sensitive data never seen before, exposing over 26 billion records which compiled sensitive data from numerous previous breaches into an exhaustive collection. Instead of stemming from one central cyberattack, the MOAB is essentially a reservoir of stolen credentials, personal info, and logins from workplace social networks and cloud storage services like LinkedIn, Twitter, Dropbox, Adobe, amongst a host of others. The data set discovered on an open internet exposure by Bob Dyachenko and Cyber news includes login details, email IDs, telephonic contacts, and additional sensitive information that can be used to launch easy phishing, identity fraud, and credential stuffing schemes.

However, because the data scale is so big and so accessible, MOAB is especially dangerous. It is a 12-terabyte archive of years of cybercrime activity that already includes new and recycled data which came from other breaches. Before MOAB, individual datasets had already been leaked, but this consolidation of the records is the first-time cyber criminals could easily exploit exposed individuals and companies. The breach is yet another reminder that repeated data leaks and too long a delay in adopting strong cybersecurity practices is not without consequences but rather has lasting consequences.

The breach does not sport new compromises of secure systems, but the massive hoard is potent for widespread mayhem. This serves as a reminder to practice good password hygiene, and to utilize multi factor authentication as well as perform regular monitoring of both personal and organizational cybersecurity posture. MOAB serves as a stark warning that when historical data breaches are not addressed the value of digital identities will only grow more valuable. Cybersecurity is not something that should only happen after high profile incidents; individuals, companies, and institutions need to regard cybersecurity as something that must be treated as an ongoing project.

CHAPTER 2: MOAB GROUP OPINION

## ***2.1*** *AHMED MIRAHUSAIN ALVI*

The “Mother of All Breaches” is a serious issue—huge amounts of personal data and login details were exposed, and that kind of info should always stay private. Stuff like this can lead to phishing scams, identity theft, and financial fraud. It also hits businesses hard, damaging both their reputation and valuable data. As someone studying cybersecurity, I am motivated to help prevent these kinds of incidents. I want to use what I have learned—and continue learning—to protect people online and create a safer digital space where everyone feels more secure. Security should never be an afterthought.

## ***2.2*** *ABDALLAH MOHAMED MAHMOUD MOHAMED MAHMOUD*

The MOAB breach reminds us chillingly of how little privacy we have in the digital domain. It’s not only about a technical failure, to see billions of records dumped online, from emails to passwords. It’s a very clear, massive violation of trust. We hear of better security, and these leaks continue to expand. The worse thing is how this is getting normalized. Users need more control and transparency and while this is a wakeup call, it’s proof that we are already deep in the nightmare. Digital security should never be based on a gamble. It's time for real action, enough with the apologies.

## ***2.3*** *SULTAN ABDULLA OMAR TAKRORI*

As someone trying to understand cybersecurity more deeply, the "Mother of All Breaches" feels like a wake-up call—not just for big companies, but for all of us. What struck me the most is that this wasn’t even a new hack; it was a terrifying reminder of how poorly managed old data can come back to haunt us. The fact that over 26 billion records were just there, publicly exposed, makes me realize how fragile digital privacy really is. It’s not just about having strong passwords anymore—it’s about changing the way we treat our digital identities. I now see cybersecurity as something ongoing, like personal hygiene. We can’t just clean up after getting dirty; we have to maintain safety constantly. I want to learn how breaches like this are discovered, how attackers exploit them, and most importantly, how we can defend ourselves in a world where data never really disappears.

## ***2.4*** *BADR MAHDI MUBARAK AL-AMRI*

The number of 26 billion compromised records during MOAB breaks all expectations for a student like me who studies cybersecurity. Digital life shows its vulnerabilities because servers that are not properly configured can go without any awareness or monitoring. My major concern focuses on people from my country Yemen who lack the means to protect themselves from identity theft attacks. Moab underscored why cybersecurity education needs immediate improvement and I intend to achieve it through APU. Organizations need to establish auditing schedules together with data encryption procedures to stop information from leaking. Better worldwide data protection laws represent my personal motivation to act as an advocate. People's trusts depend on cybersecurity which goes beyond its technical aspects.

## ***2.5*** *MOHAMED ABA SAID*

The MOAB breach is more than just a massive data leak—it’s a loud alarm for anyone who values privacy and digital safety. As someone passionate about cybersecurity, I find it deeply alarming. I use LinkedIn and Twitter and knowing they were affected makes me feel exposed and vulnerable. I always use strong passwords and secure my accounts carefully, but MOAB indicates that even this might be insufficient. This breach proves that no system is too big to fail. It reminds us that we must stay aware, remain vigilant, and take proactive steps to prevent such incidents in our interconnected world.

## ***2.6*** *MOHAMED ABDIFATAH ALI*

With a trailblazing mega-dump such as MOAB a database comprising of 26 billion records credential leaks are not an annoyance, they are a commercial asset. While virtually all of these passwords are expired, billions still work which provides inexperienced attackers immediate access to a searchable toolbox on a grand scale. However, it's less a new breach and more a nasty amalgamation. Instead of separate dumps for Tencent, LinkedIn, Twitter, etc., 'all' of the smaller dumps get attached to a 'working' index where the effort curve balances as expertise moves from dark-web operatives to weekend script kids. The silver lining is that panic often leads to hygiene. Now is the time to turn off MFA, get a password manager, freeze credit, and delete stale credentials.

## ***2.7*** *MOHAMMED YOUSEF MOHAMMED MOHAMMED*

The MOAB breach is a stark reminder of the vulnerabilities inherent in our digital infrastructure. The massive volume of exposed data highlights the need for organizations to prioritize cybersecurity at all levels. As a student of cybersecurity, this incident reinforces the importance of integrating security measures throughout the software development lifecycle. It also emphasizes the role of continuous testing and monitoring to proactively detect and reduce potential threats. In the future, I am committed to advocating and applying cybersecurity best practices to protect users' data and maintain trust in digital systems.

## ***2.8*** *MAHRUS SHAMSUL AHSAN*

Mother of all breaches (MOAB) showed us how vulnerable humans are in terms of digital privacy. Many individuals have had their identity stolen and others are victims to cybercrimes. This massive data leak exposed the fragility of organisations as they didn't secure their clients and customers data safely. It was a wakeup call for us and we realised the urgent need for a robust cybersecurity framework worldwide. Organisations and governments need to implement stricter rules and regulations in order to protect innocent individuals who are victims to not just cybercrime but irresponsible organisations not securing their systems and data properly.

CHAPTER 3: ANALYSIS

## ***3.1*** *Specifics of MOAB Breach*

A 12-terabyte data breach known as the "Mother of All Breaches" (MOAB) was reported by Cybernews on January 29/2024 as it contained 26 billion records distributed across 3,800 folders of past breaches (Petkauskas, 2024). Leaked information consists of usernames and passwords as well as email addresses and phone numbers and complete payment records. The unexposed data segments which constitute 10% of the total make the situation riskier (Diachenko, 2024). Public data breaches of platforms Tencent (1.5 billion records), Weibo (504 million), Twitter (281 million), LinkedIn (251 million), and Adobe (153 million) stem from this incident. Government institutions from the US alongside Brazil and Germany among others were all subjected to this breach. The large number of breaches unified into MOAB creates a valuable database which criminal hackers use to execute email scams and commit identity theft and fraud schemes. Sweeping user information exposure highlights the necessity for powerful cybersecurity systems that need immediate implementation (Cybernews 2024).

## ***3.2*** *Probable Causes of the Breach*

The MOAB dataset was discovered on an open instance, likely due to a misconfigured firewall, as reported by Leak-Lookup, the data owner (Petkauskas, 2024). This suggests improper server settings allowed unauthorized access. Common breach causes include:

* **Misconfigured Software Settings**: Unsecured databases or cloud servers, like MOAB’s, expose data due to overlooked configurations (Kaspersky, 2023).
* **Social Engineering**: Phishing or pretexting tricks users into sharing credentials, though less likely here as MOAB aggregates existing breaches (Moore, 2024).
* **Application Vulnerabilities**: Unpatched software or weak APIs can be exploited, potentially contributing to the original breaches in MOAB (Grimes, 2024). The unidentified culprit—possibly a hacker or data broker—complicates attribution (Cybernews, 2024). MOAB highlights how aggregated breaches amplify risks, emphasizing the need for regular audits, patch management, and employee training to mitigate such vulnerabilities.

## ***3.3*** *Steps to Detect your Group Member Data has been Breached or Not*

**3.3.1** AHMED MIRAHUSAIN ALVI

Figure 1 Hasso Plattner Institute Identity Leak Checker

***A screenshot of a computer

Description automatically generated***

Using the **Hasso-Plattner-Institute’s Identity Leak Checker**, I conducted a search on a group member's email address — masterthreeboy@gmail.com — to determine whether their personal data had been exposed in any known security breaches. By entering the address into the secure search field, the tool scanned a massive archive of compromised data across thousands of leaks.

After submitting the query, no breach records were found associated with this email. This means the address has not appeared in any known public data leaks, and there is no indication that sensitive information linked to it — such as passwords, phone numbers, or personal identifiers — has been exposed.

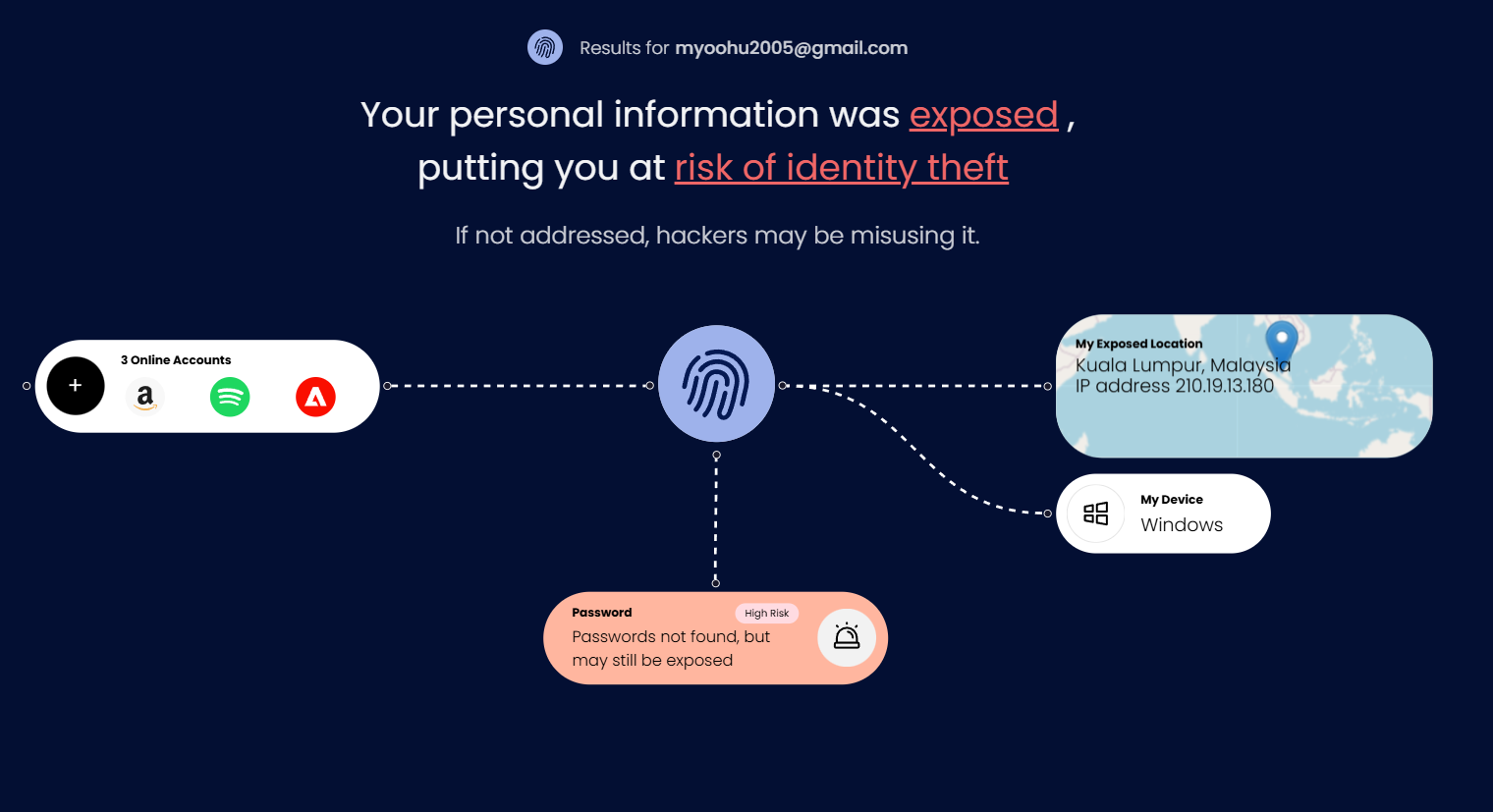
Even though this result is positive, it is still critical to follow best practices:

* Keep strong, unique passwords for each service.
* Enable two-factor authentication wherever possible.
* Avoid sharing login credentials or sensitive info through insecure channels.

This check reinforces the importance of proactive cybersecurity, and it is good to confirm that at least this group member’s digital identity appears to be secure — for now.

**3.3.2** ABDALLAH MOHAMED MAHMOUD MOHAMED MAHMOUD

Figure 2 Malwarebytes Digital Footprint Scanner



Use a trusted tool like **Malwarebytes Digital Footprint Scanner** to determine whether the group member's data has actually been compromised or is it safe. First, type the group member's email into the scanner at malwarebytes.com/digital-footprint-app. The tool will then search in the dark web and breach databases looking for any indication of exposed personal information. Look out for red flags: exposed account names, IPs, or devices attached to some breach. Notice the platform icon displayed (like Amazon, or Spotify) that indicates an account being compromised. There are times when it could state "Passwords not found, but may still be exposed" to give a warning even if no passwords have been listed. Glance at location and device exposure (such as Windows PC), as these may help in tracking the breach. Change all respective ones immediately and activate two-factor authentication in case anything suspicious emerges. Keep an eye out for updates and inform your group members concerning the threats of phishing and safe online behaviour.

**3.3.3** SULTAN ABDULLA OMAR TAKRORI

Figure 3 F-Secure Identity Theft Checker

A screenshot of a computer

Description automatically generated

Using **F-Secure Identity Theft Checker**, I conducted a search on one of my friends personal e-mail to check if his personal data had been exposed in any known data breaches. By entering his email address, To find any indication of compromised data, the tool searched breach databases and the dark web. We searched it and we got 9 separate breaches, indicating that this address and possibly associated details—such as usernames, passwords, or leaked information were exposed. While the tool doesn’t show full breach details on the screen, it sends a report via email highlighting where and how the data might have been leaked. Sometimes, passwords may not appear but could still be at risk, especially if linked to exposed accounts or devices. These results raise concerns and should be treated the right way. For extra security, two-factor authentication should be turned on and any associated account passwords should be changed. It is also important to stay careful for signs of suspicious activity or phishing attempts. To avoid extra compromise, group members must be informed about safe online activities. All things taken into account, this F-Secure procedure highlighted the significance of protecting digital identities and exposed possible risks.

**3.3.4** BADR MAHDI MUBARAK AL-AMRI

A screenshot of a computer

Description automatically generated

I used Hack Check tool of Avast to do the security scan of my group member email account mohamedabdifatah619@gmail.com. Avast is a tool that scans a vast amount of credentials to learn whether they have been leaked, information associated with such accounts as a password, phone number, or other specifications. The verdict was clear after the scan was completed:

The email did not show any password leaks.

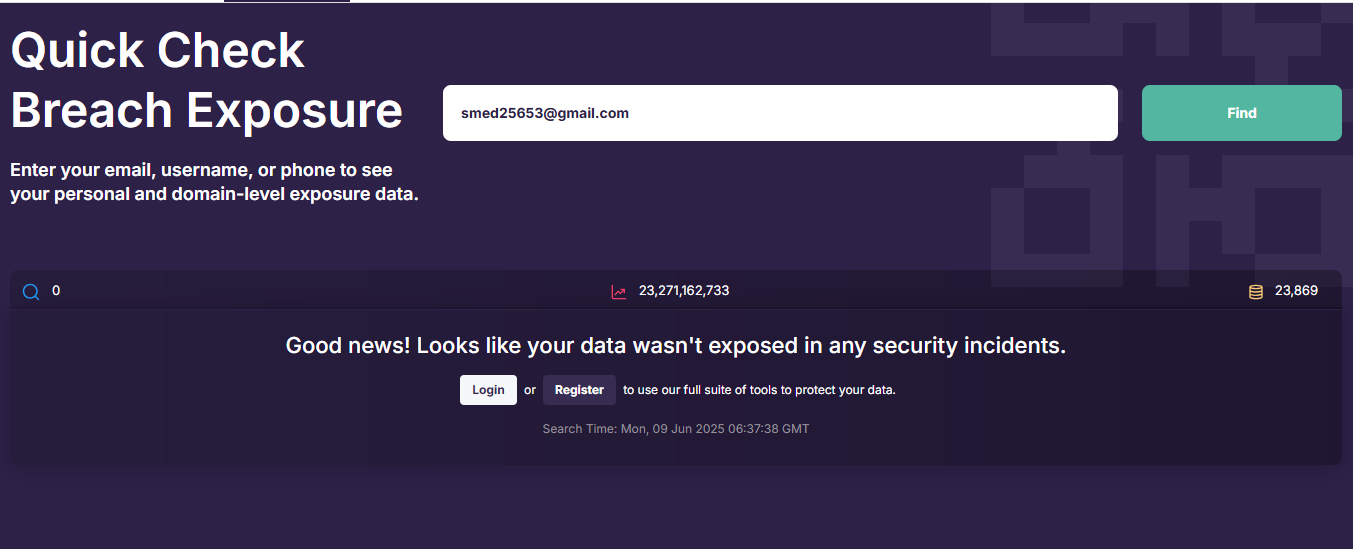
That means, my group member credentials have not appeared in any known structure data leakage in the present time, and it also does not find any evidence of previous disclosure. Although this brings relief, it is important not to forget about digital hygiene such as:

* Having different and strong passwords for each account.
* Enable two-factor authentication where it is possible.
* Do not send credentials on unreliable sites.

This is a clean report that highlights the benefit of frequent security checks. My group member online identity is currently safe at the moment, but constant monitoring is of the essence.

**3.3.5** MOHAMED ABA SAID

Figure 4 DeHashed Identity Leak Checker



To check if my data was compromised, I used **DeHashed**, which analyses billions of leaked records to find any exposed information associated with your email address. I did a search using my email address: smed25653@gmail.com, and the result was positive: no records were found. This means that my email has not been exposed to any known data breaches, and no personal information, such as passwords or my account information, has not been leaked. Although my data is currently safe, I will continue to take the necessary precautions, such as using strong and unique passwords, activating two-factor authentication on my accounts, and being vigilant against phishing attempts. It's also good to check my data regularly. I advise all group members to do the same to ensure the security of their information.

**3.3.6** MOHAMED ABDIFATAH ALI

**Step 1**

* I have collected and email of my colleague, the email name: mohamedabdifatah619@gmail.com
* Then browsed <https://surfshark.com/> to manually check the email for breaches.

**Step 2** Writing the email on the Email checker:

Figure 5 Email Address Verification via Surfshark Data Leak Checker

A screenshot of a computer

AI-generated content may be incorrect.

**Step 3**. Nothing was found; luckily, nothing was found:

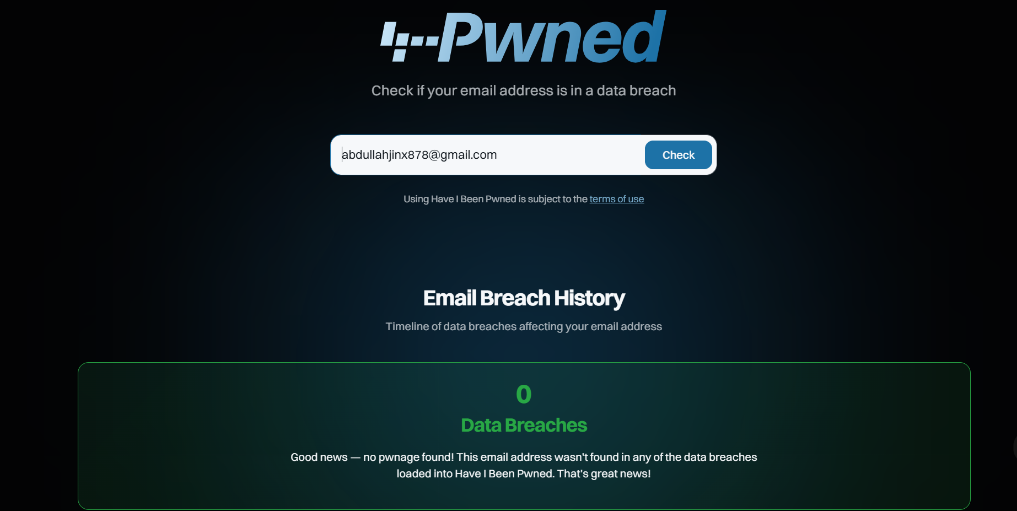
Figure 6 Confirmation of No Data Exposure via Surfshark Leak Checker

A screenshot of a computer

AI-generated content may be incorrect.

**3.3.7** MOHAMMED YOUSEF MOHAMMED MOHAMMED

Figure 7 Verification of Email Security Using Have I Been Pwned?



To assess the current security status of my group member data, I used the online tool Have I Been Pwned? to check whether my group member email address - abdullahjinx878@gmail.com - had been involved in any documented data breaches.

Scan Results:

The tool has completed its scan and has not reported any data breaches or record compromises associated with this email. In other words, based on a database of known incidents, there is no evidence that this account has been subject to any major leaks or cyber attacks.

What This Means:

This result indicates that my email did not appear in any of the compromised data sets tracked by the service. It's a good sign, as it indicates that my credentials and related personal information, such as passwords or account details, haven't been publicly leaked—at least in the breaches reported so far.

Recommended Security Practices:

Even with no current breaches detected, staying secure requires continued attention. Here are some steps I follow to maintain good cybersecurity hygiene:

1. Use strong, unique passwords for every account

2. Avoid clicking unknown links or sharing credentials online

3. Perform regular checks for new breach notifications

Conclusion:

Although no threats were detected during this scan, digital security is not a one-time task. Being vigilant is the best way to protect your accounts and personal data.

**3.3.8** MAHRUS SHAMSUL AHSAN

A purple and white website

Description automatically generated

Figure 8 Mozilla Monitor Homepage for Personal Information Exposure Check

Figure 9 Mozilla Monitor Scan Results Showing No Data Exposures

A purple circle with black text

Description automatically generated

Using Mozilla Monitor, I conducted a search on a group member’s email address — mahrusahsan2005@gmail.com — to check whether their personal data had been leaked in any known security breaches. Mozilla Monitor, powered by the “Have I Been Pwned” database, scans through a large database of leaked credentials and records from across the internet. After entering the email address in the website, the system ran a scan across hundreds of known data breaches. The results came back with no breach records associated with this email. This shows that the email has not been part of any public leaks.

CHAPTER 4: IMPACT

## ***4.1*** *Potential Impact on Individuals*

Mother of all breaches (MOAB), a massive data leak that exposed well over 26 billion records gave rise to serious threats to those affected. These threats range from identity theft, financial fraud, and violation of privacy, with identity theft being the most immediate threat. Examples of the data exposed are names, emails, passwords, and possibly more sensitive personal information. With these data leaked, identity fraudsters can easily impersonate the victims and access bank accounts, commit fraud and many more. These crimes may cause the victims consequences such as damaging their credit history and many more.

Invasion of privacy is another grave concern. Criminals not only can exploit details such as location history, communication logs or behavioural habits, but unethical marketers and data brokers can also do the same. Social engineering attacks could also leverage this data, where criminals pressure victims into revealing private information. The toll of stress, fear, and mistrust can drag people’s quality of life and their use of digital services down.

## ***4.2*** *Potential Impact on Organizations*

Organisations in the public and private sectors are also threatened by the MOAB breach. This kind of leak can result in a loss of competitive advantage, especially if trade secrets, strategic documents, or confidential customer information are exposed to the public. cybercriminals or competitors might use this information to undermine company plans or create counteroffers.

Furthermore, credit ratings may decline for organisations. Cybersecurity risk is taken into account by rating agencies when determining a company's creditworthiness. The inability to safeguard data could lead to higher borrowing rates or less attractive investment opportunities. The cost of cyber insurance will also probably increase. Insurers may reassess the risk profile of affected organizations or entire industries, leading to stricter coverage terms or higher costs.

National security threats may also affect government organisations, particularly when it comes to critical public infrastructure or citizen data. All things considered, the operational, financial, and reputational harm may be permanent.

## 

## ***4.3*** *Societal Implications of Data Breaches*

**1. Decrease of social trust and privacy**

Users cannot just "change the locks" when highly sensitive data, such as location histories, medical records, or financial credentials, are exposed by a breach. The risk of identity theft, medical fraud, and doxing is constant because stolen identifiers have been sold on underground markets for years. The public eventually comes to believe that every click, transaction, and private message is being recorded somewhere. This presumption undermines trust in both public and commercial platforms; people are reluctant to use telehealth portals or digital government services because they do not think anyone can protect their data. Reduced trust undermines collective benefits that rely on large, representative datasets by reducing participation in data-driven initiatives like public health registries or smart city programs.

**2. Threat on civic engagement and free expression**

Exploring ideas and developing opposing viewpoints require privacy. Researchers see a decrease in "risky" online activity following headline breaches or surveillance disclosures: Wikipedia edits about terrorism decline, social media posts on delicate subjects decrease, and journalists return to in-person meetings. This threat goes beyond politics; whistle-blowers may remain silent out of concern for their safety that their communications will be leaked, and youth may refrain from looking into important health resources. The end effect is a more limited public conversation and a democratic process that lacks the critical of free expression

**3. Limitations on economic expansion and innovation**

Market research indicates that breaches cause multi-year revenue to drag and an immediate stock price decline, but they also have a wider economic impact because they change incentives. Boards reallocate funds from R&D to compliance, cyber-insurance, and settlements. There Under pressure to "do something," regulators enforce more stringent data-protection laws or localization requirements that disrupt international information flows. While incumbents with larger budgets absorb the costs of compliance and consolidate market power, start-ups in data-intensive industries like AI, genomics, and ad-tech now face greater entry barriers. An economy that is always on defence innovates more slowly than one that is free to try new things without worrying about disastrous leaks, but the upside is a growing cybersecurity sector and advancements in privacy-enhancing technologies.

**4. Inequality and systemic repercussions**

Following a series of massive breaches, cyber-insurance premiums have skyrocketed to the point where some carriers have left the market or refused coverage for critical infrastructure, leaving smaller businesses vulnerable. Meanwhile, wealthy people can afford private-browser services, reputation management, or ongoing credit monitoring, while those with lower incomes must deal with the full financial and emotional disasters of identity theft. Even the creation of public goods is negatively impacted: universities find it difficult to create open data repositories, and patients who are concerned about leaks choose not to participate in medical research. These domino effects weaken society's ability to learn from accumulated data and deepen already existing social divides.

CHAPTER 5: PROPOSING SOLUTIONS

**5.1** What You Should Do If You Identify Your Group Member Data has been Breached

Upon discovering the breach, initiate a private incident response immediately to contain and assess the situation. Begin by identifying the affected platforms—determine which PCs were compromised and revoke session permissions across all connected devices. Next, conduct a credential audit: issue strong, unique new passwords for all users, implement biometric authentication where possible, and enforce two-factor authentication (2FA) as a baseline security measure. To monitor for further exposure, use tools like Have I Been Pwned and Firefox Monitor, and set up Google Alerts to track any name-based breach mentions online. Notify all relevant parties, including essential institutions and the university IT department, to ensure coordinated action and transparency. Meticulously document every step taken throughout the response to support future forensic analysis and to maintain accountability. Following containment, reinforce digital hygiene practices by establishing regular password change intervals, adopting safe file encryption standards, and using email aliases for public-facing communications. Finally, use the incident as an opportunity to educate involved parties and implement stronger, long-term cybersecurity measures, turning the crisis into a catalyst for resilience and improvement.

Figure 10 F-Secure's Online Tool for Scanning and Removing Viruses on Windows PCs

A screenshot of a computer

Description automatically generated

Figure 11 Google Alerts Interface with "Mother of All Breaches" Search Query

A screenshot of a computer

Description automatically generated

***5.2*** *Preventive Measures*

To avoid MOAB like data breaches, individuals and organizations must have proactive measures in place. Essential such safeguards include a multi factor authentication (MFA), strong passwords as well as encryption of sensitive data. Access controls in organization should be strictly controlled, organization should undertake routine security audits and organization should apply timely software patches.

Phishing and social engineering attacks can be prevented by the employee awareness training. Further defences include the implementation of firewalls, antivirus software, threat detection tools. Finally, data minimization is crucial: only collecting the necessary user information to make that product work, and there you minimize the exposure you have if the company does take a breach down the line.

Passing a password manager and making an effort to stop using the same password across platforms. Incorporating security into every part of your business and remaining abreast of new threats are the best ways to reduce breach risk and devastation in the future.

***5.3*** *Effective Strategies*

Prepare before breaches: keep an up‑to‑date asset map, risk inventory, and a management‑approved incident‑response plan aligned with ISO 27035 or NIST SP 800‑61. When a SIEM alert, EDR hit, user report, or intelligence tip appears, triage swiftly; if thresholds are met, declare an incident, and open a master evidentiary ticket. Contain attackers while preserving proof—isolate hosts, capture live memory, image disks with SHA‑256 hashes, export raw logs—and watch statutory deadlines (CIRCIA 72‑hour/24‑hour ransom, NIS2 24‑hour, SEC four‑day). Eradicate root causes, rebuild from hardened golden images, verify clean configurations, then restore critical services first. Communicate facts, obligations, and mitigation offers to executives, regulators, and affected customers through pre‑drafted statements. Within ten days, run a lesson‑learned review, update controls, metrics, and exercise plans to continually strengthen the cyber resilience program.

CONCLUSION

Massive platforms remain exposed to cyberattacks that cause billions of users to lose their data according to the MOAB security breach. Research findings indicate that inadequate setting management and software flaws combined with social engineering techniques are the primary causes of extensive data security breaches. Insufficiently strong passwords turned out to be inadequate for protecting information from unauthorized access. When an incident occurs users must immediately act by replacing passwords while activating the "Have I Been Pwned" alert together with reporting the breach to relevant authorizing entities. The proposed solution from the group included digital hygiene practices supported by standard password updates and two-factor authentication alongside encryption technology to protect systems. Response plans prove most essential for the organization because defining protocols before crises happen proves their worth. The organization must be prepared at all times. This message indicates that everyone has digital safety responsibility and effective defense requires both awareness and secure tools with solid digital tools and safe practices.

REFERENCES

Arntz, P. (2024, January 23). *“The mother of all breaches”: 26 billion records found online [Updated]*. Retrieved from Malwarebytes: https://www.malwarebytes.com/blog/news/2024/01/the-mother-of-all-breaches-26-billion-records-found-online

Arntz, P. (2024, January 31). *Mother of all Breaches may contain NEW breach data*. Retrieved from Malwarebytes: https://www.malwarebytes.com/blog/news/2024/01/mother-of-all-breaches-may-contain-new-breach-data

Bagwe, M. (2024, December 31). *The Biggest Global Data Breaches of 2024: Lessons Learned*. Retrieved from TheCyberExpress: https://thecyberexpress.com/biggest-global-data-breaches-of-2024/

Bernardone, L. (2024, January 25). *Big brands caught in ‘mother of all breaches’*. Retrieved from InformationAge: https://ia.acs.org.au/article/2024/big-brands-caught-in--mother-of-all-breaches-.html

Brandt, C. (2024, February 22). *What You Should Know About the Mother of All Breaches, 2024*. Retrieved from marco: https://www.marconet.com/blog/what-to-know-about-the-mother-of-all-breaches-2024

Fleury, D. (2024, February 15). *What We Know About the MOAB Data Leak*. Retrieved from SpyCloud: https://spycloud.com/blog/moab-data-leak-what-we-know/

Hewitt, N. (2024, March 1). *What Does The Mother of All Breaches (MOAB) Mean for Organizations?* Retrieved from TRUEFORT: https://truefort.com/mother-of-all-breaches/

Kaspersky. (2024, July 9). *What is Data Breach? How to Prevent Data Leaks*. Retrieved from Kaspersky: https://www.kaspersky.com/resource-center/definitions/data-breach

Key, K. (2025, January 16). *Worried About Data Breaches? Take These Steps to Protect Yourself Now*. Retrieved from PCMag: https://au.pcmag.com/security/88576/so-youve-been-pwned-what-to-do-when-your-private-data-goes-public

Kliashchou, I. (2024, February 28). *The 'Mother of All Breaches' Just Happened — Here's the Security Implications for Businesses*. Retrieved from Entrepreneur: https://www.entrepreneur.com/science-technology/what-business-leaders-need-to-know-about-the-mother-of-all/469510

NETWORKING+. (2024, January). ‘Mother of all breaches’ exposes 26. *NETWORKING+*, p. 1. Retrieved from https://networkingplus.co.uk/Media/Default/archive/Net2401.pdf

Paganini, P. (2024, February 4). *The ‘Mother of all Breaches’: Navigating the Aftermath and Fortifying Your Data with DSPM*. Retrieved from Security Affairs: https://securityaffairs.com/158646/data-breach/mother-of-all-breaches-dspm.html

Parsacala, R. (2024, November 15). *Ten Lessons Learned from The Mother of All Breaches Data Leak*. Retrieved from TRUEFORT: https://truefort.com/mother-of-all-breaches-data-leak/

Petkauskas, V. (2024, January 29). *Mother of all breaches reveals 26 billion records: what we know so far*. Retrieved from cybernews: https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/

Song, V. (2024, January 17). *Mother of All Breaches Exposes 773 Million Emails, 21 Million Passwords*. Retrieved from Gizmodo: https://gizmodo.com/mother-of-all-breaches-exposes-773-million-emails-21-m-1831833456

Winder, D. (2024, January 23). *Warning As 26 Billion Records Leak: Dropbox, LinkedIn, Twitter Named*. Retrieved from Forbes: https://www.forbes.com/sites/daveywinder/2024/01/23/massive-26-billion-record-leak-dropbox-linkedin-twitterx-all-named/

Yacono, L. (2024, February 2). *Navigating the Aftermath of the Mother of All Breaches*. Retrieved from CIMCOR: https://www.cimcor.com/incident-alerts/navigating-the-aftermath-of-the-mother-of-all-breaches

WORKLOAD MATRIX

|  |  |  |
| --- | --- | --- |
| NAME | TASK | SIGNATURE |
| AHMED MIRAHUSAIN ALVI (TP084807) | * **Workload Matrix** * **Overall Document Creation** * **Effective Strategies for Managing Data Breach** | *AHMED ALVI* |
| MOHAMMED YOUSEF MOHAMMED MOHAMMED (TP085042) | * **Show steps to detect your group member data has been breached or not** * **Documentation of Cyber Crime & Security Breaches** | **MO** |
| SULTAN ABDULLA OMAR TAKRORI (TP085327) | * **Documentation of MOAB Data Breach Analysis** * **Conclusion** * **Potential Impact on Individuals** | **STK** |
| MAHRUS SHAMSUL AHSAN (TP085562) | * **Potential Impact on Organizations** * **Documentation of Impact** * **Proposed Solutions** | ***~~MSA~~*** |
| ABDALLAH MOHAMED MAHMOUD MOHAMED MAHMOUD (TP085097) | * **Cyber Crime & Security Breaches** * **Preventive Measures to avoid such breaches in Future** | **Abdo** |
| MOHAMED ABDIFATAH ALI (TP082459) | * **Societal Implications of Data Breaches** * **Table of Contents** * **References** * **Cover Page** |  |
| MOHAMED ABA SAID (TP082376) | * **Conclusion** * **What You Should Do If You Identify Your Group Member Data Has Been Breached** |  |
| BADR MAHDI MUBARAK AL-AMRI (TP083084) | * **Specifics of MOAB Breach** * **Probable Causes of the Breach** |  |