

**hacking of facebook , twitter and  
instagram in 2021**

# Outline

---

introduction

---

---

Case study scenario

---

---

Summary of report

---

---

Conclusion

---



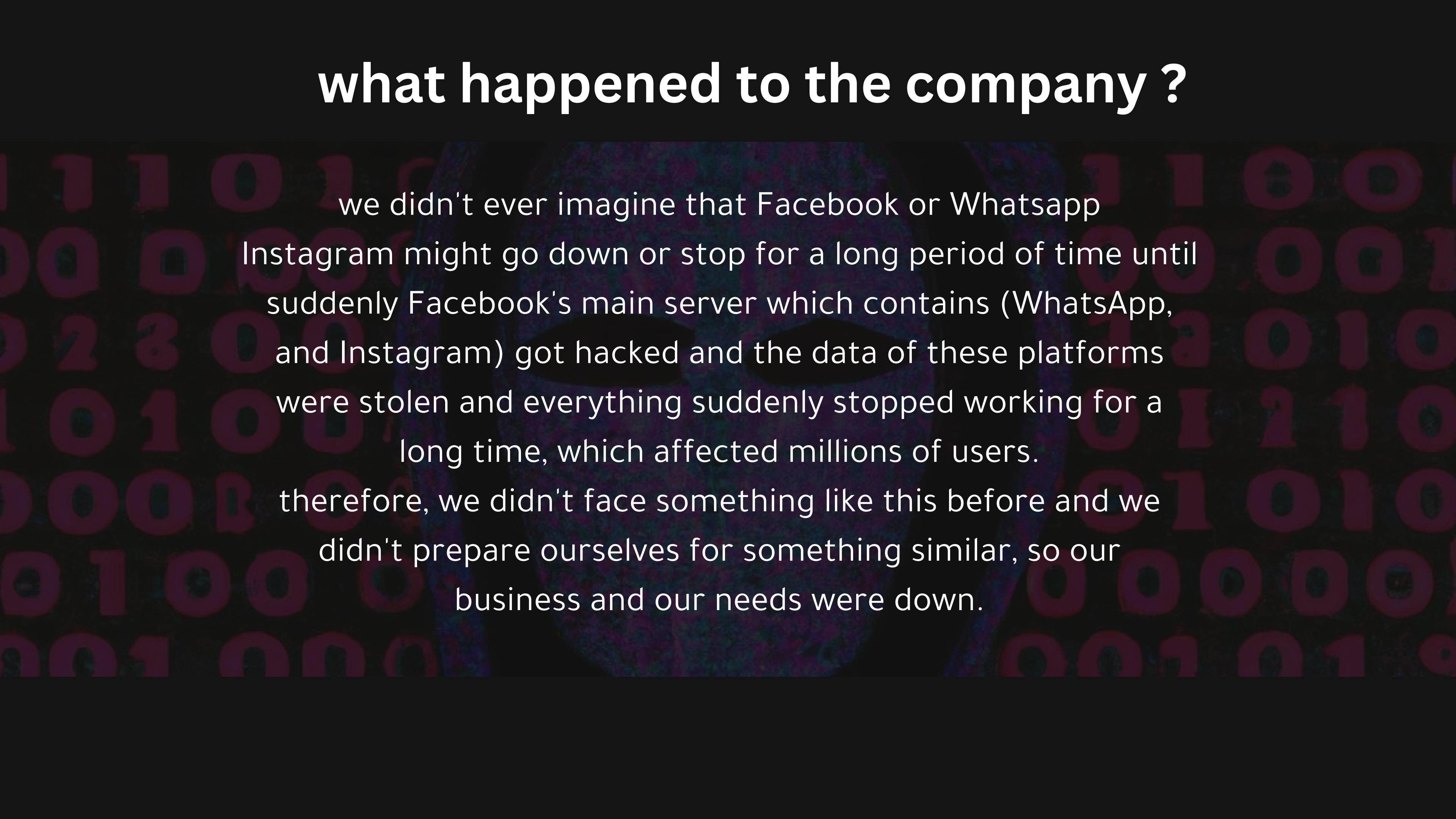
# introduction :



# Company overview:

Meta platforms Inc (meta), formerly Facebook is a provider of social network advertising and business insight solutions. The metaverse focuses on developing a virtual environment that gives people the ability to interact and connect with technologies through its major product (Facebook, Instagram, and WhatsApp). The company has a business presence across the Americas, Europe, the Middle East, Africa, and Asia-Pacific. Meta is headquartered in Menlo Park, California, the US

# what happened to the company ?

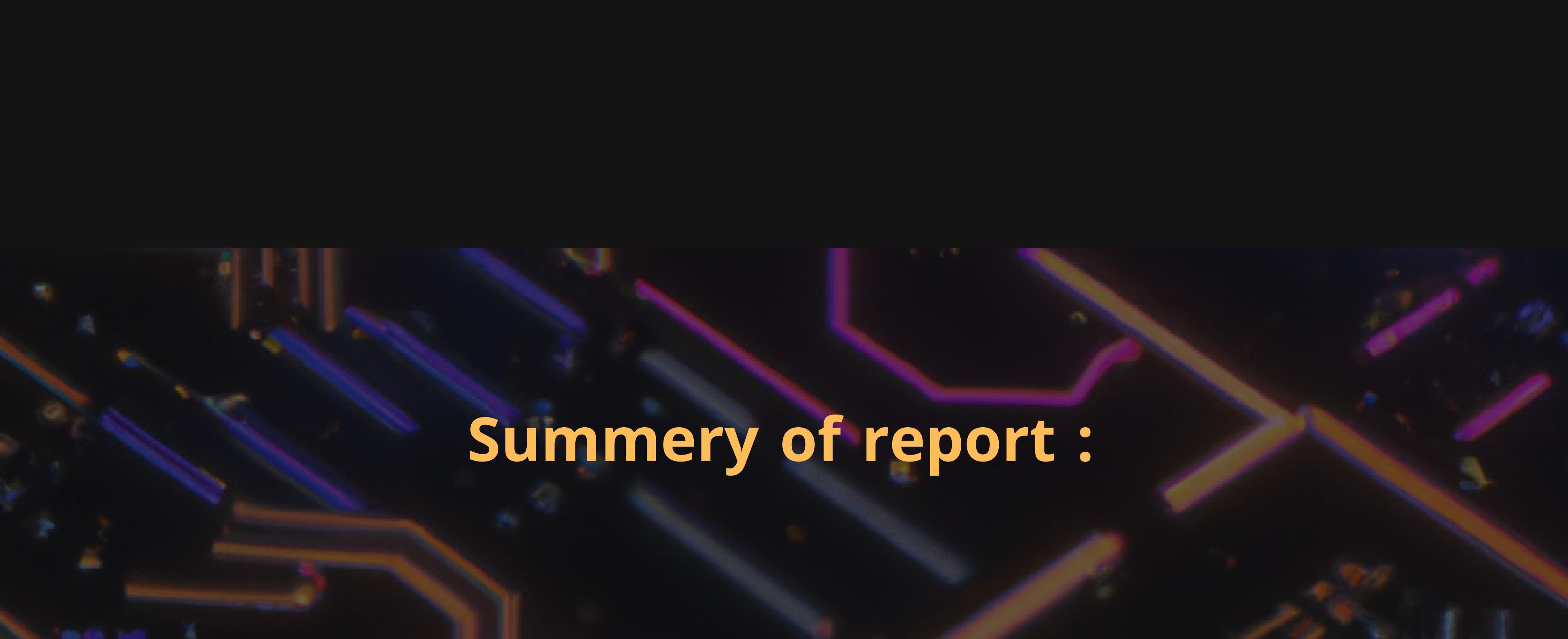


we didn't ever imagine that Facebook or Whatsapp Instagram might go down or stop for a long period of time until suddenly Facebook's main server which contains (WhatsApp, and Instagram) got hacked and the data of these platforms were stolen and everything suddenly stopped working for a long time, which affected millions of users. therefore, we didn't face something like this before and we didn't prepare ourselves for something similar, so our business and our needs were down.

# Scenario Of hacking :

The hack occurred when hackers exploited a vulnerability in Facebook's systems and software, which allowed them to gain unauthorized access to user data,

The hackers were able to steal personal information such as email addresses and phone numbers from around 90 million Facebook users. They also gained access to the accounts of around 50 million users, allowing them to view  
•private messages and other sensitive information



**Summery of report :**

# Analysis of the Ethical Issue:

---

## Issue category

The Hacking falls under the category of security ethical issues because it involved unauthorized access and theft of user's personal information, which can be used for unethical purposes,

# Analysis of the Ethical Issue:

---

## Consequences

The hacking resulted in a number of significant consequences.

One of the immediate consequences was the loss of trust in these social media platforms.

The hacking also had financial consequences for the affected companies. .

The hacking also had social and political consequences. The unauthorized access to personal data raised concerns about privacy and the potential for misuse of personal information.

## Analysis of the Ethical Issue:

---

Reasons: Why did that happen?

The precise cause of the 2021 hacks on Facebook, Instagram, and WhatsApp is still unknown. Yet it's assumed that a weakness in the systems and software of Facebook enabled hackers to access users' personal data without permission, which led to the attack.

## Analysis of the Ethical Issue:

---

Avoidance: what could have they done to avoid it in the first place?

The following steps may have been taken to prevent the hacking

- 1- Frequent Security Audits .
- 2- Stronger Security Protocols .
- 3- Employee Training .
- 4- regular updates .

# Analysis of the Ethical Issue:

---

## Mitigation techniques

to mitigate the effects of the 2021 hacking incident, Facebook implemented a variety of actions :

1. Resetting Access Tokens .
2. inform users who were affected and given guidance to protect their data .
3. Coordinated Response .



# Analysis of the Codes of Ethics :

How its related to the proffessional code of conduct?

## Client and employer

2.05 Respect confidality, Computing experts should protect users' personal information and respect their privacy  
The hacking jeopardizing their privacy by theft personal data .

## Profession

6.02 obey all applicable laws unless, under special circumstances, doing so would be against the public interest , they always thing about laws .

## Self

8.02 computing experts should keep high standards of competency and continually work to expand their knowledge and abilities. This entails keeping up with the most recent security dangers and putting in place the necessary security measures to stop them.

## How the hack is related to Law , regulation , company policies ?

The issue relates to the EU's General Data Protection Regulation (GDPR), which obliges businesses to secure users' private information and notify them of any data breaches. Additionally, the incident went against Facebook's own data security and protection policies, which call on the company to have strong security measures in place to secure user data.





## ISO Standard

What is the Related standard to the hack ?and how it related ?

The issue is related to the ISO/IEC 27001 standard, which provides a framework for information security management systems. Implementing this standard could have helped Facebook, WhatsApp, and Instagram prevent the issue by ensuring that their systems were properly protected and that vulnerabilities were identified and addressed in a timely manner.[2]



## ISO Standard

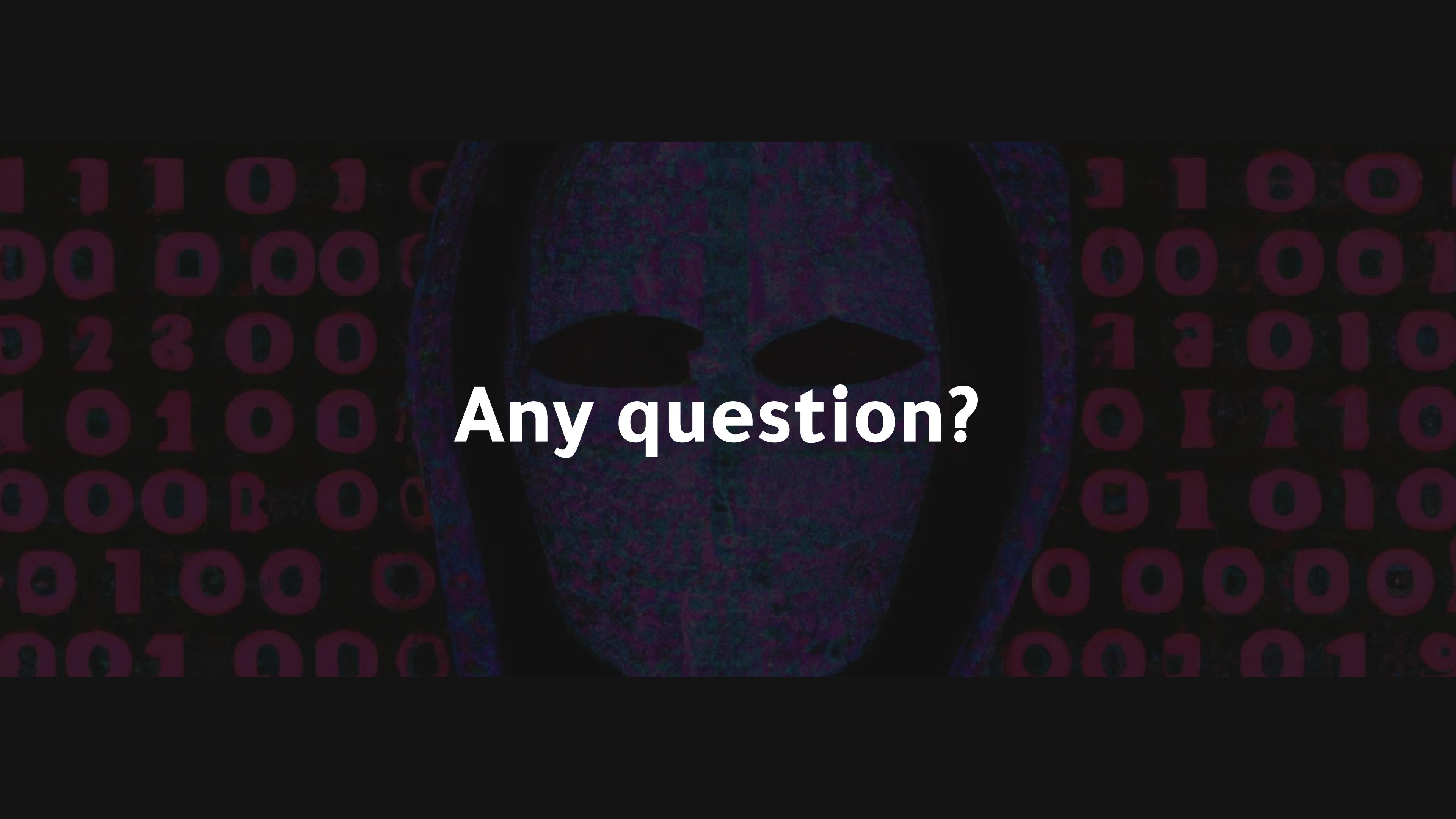
Suggested standard to avoid similar kind of hack

The ISO/IEC 27001 standard is a globally recognized information security management system (ISMS) that provides a framework for organizations to manage and protect their information assets.

The ISO/IEC 27001 standard covers a range of areas, including risk assessment, security controls, and incident management..[2]

# Conclusion

we want to emphasize that nothing is 100% protected even if we use it for a long period of time and rely on it, and that every app needs a backup strategy if it becomes hacked or damaged. therefore, the hacking of Facebook, WhatsApp, and Instagram highlights the importance of strict security protocols and regular security assessments to protect users' private data.



A grayscale image of a human brain, centered against a dark background. Overlaid on the brain is a grid of binary digits (0s and 1s) in a light color. The grid is approximately 10 columns wide and 10 rows high, covering most of the brain's surface. The binary code is continuous across the grid.

Any question?

# References :

---

- [1] “Meta Sues Hackers Behind Facebook, WhatsApp and Instagram Phishing Attacks,” amp.thehackernews.com.  
<https://amp.thehackernews.com/thn/2021/12/meta-sues-hackers-behind-facebook.html> (accessed Mar. 24, 2023).
- [2] International Organization for Standardization, “Popular standards,” ISO, 2019. <https://www.iso.org/popular-standards.html> .
- [3] Facebook, Inc. (2021). An Update on Facebook Security. Retrieved from <https://about.fb.com/news/2021/04/an-update-on-facebook-security/>
- [4] Hackett, R. (2021). Facebook, Instagram, and WhatsApp Are Down. Here’s What We Know. Fortune. Retrieved from <https://fortune.com/2021/10/04/facebook-instagram-whatsapp-down/>
- [5] IEEE Code of Ethics. Retrieved from [https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/ieee\\_code\\_of\\_ethics.pdf](https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/ieee_code_of_ethics.pdf)

# References 2:

---

- [6] WhatsApp Security. Retrieved from <https://www.whatsapp.com/security/>
- [7] Instagram Help Center. Retrieved from <https://help.instagram.com/>
- [8] National Institute of Standards and Technology (NIST) Cybersecurity Framework. Retrieved from <https://www.nist.gov/cyberframework>
- [9] ACM Code of Ethics and Professional Conduct. Retrieved from <https://www.acm.org/code-of-ethics>
- [10] Social Engineering Attacks on Facebook – A Case study Retrieved from [https://www.researchgate.net/publication/356908456\\_Social\\_Engineering\\_Attacks\\_on\\_Facebook\\_-\\_A\\_Case\\_Study](https://www.researchgate.net/publication/356908456_Social_Engineering_Attacks_on_Facebook_-_A_Case_Study).



# Thank you

reem alshareef 441200087  
shaden alayed 441201078