WERKSMANS
ATTORNEYS

REGULATORY

The Twitter data hack

1 March 2023 *4 min read*

Data Privacy & Cybercrime

by Ahmore Burger-Smidt, Head of Regulatory Practice and Chiara Ferri, Candidate Attorney

In the first week of January 2023 hackers scraped the e-mail addresses and usernames of over 200 million Twitter users and published them on the black market. This data breach has been traced to a vulnerability existing as far back as 2021 and is the latest in a string of cybersecurity breaches to have affected Twitter. The significance of the Twitter data hack is inextricably linked to the detrimental effects it could have on users' privacy, the loss of their personal data, and the misuse of such data, which illustrates the need for urgent intervention.

Although the scraped database does not include users' passwords, it poses a significant security threat to those who have fallen victim. While a portion of the data is publicly accessible information, the database includes users' e-mail addresses and phone numbers which, by all legal standards, are private and protected data. This will inexorably lead to a spike in targeted phishing, hacking and doxing attacks.

The hackers are said to have threatened Twitter owner, Elon Musk, with the ultimatum of paying for the ransomware before it becomes subject to a large fine under European GDPR privacy law. A fine for a breach that involves this many users could cost Twitter millions of dollars, compounded by claims by victims who wish to seek compensation for damages. It is important to note that even where the victims of ransomware attacks make payment and succumb to hackers' demands, copies of that data are not necessarily deleted. There are multiple cases where data is still made available for sale on the dark web, after the ransomware has been paid by victims.

The 2023 data hack constitutes a significant breach for Twitter, which has long struggled to protect its users' data. Where Twitter has its EU headquarters in Ireland, the Data Protection Commission as well as the US Federal Trade Commission have already started investigations. Based on initial reports dating back to July 2022, Twitter is alleged to have been non-compliant with European data protection policies and US consent orders.

Peiter Zatko, Twitter's former head of security, is a hacker turned cybersecurity-expert turned whistle-blower on the company and in August 2022, he issued alarming allegations with the US government in which he claimed that the company was concealing egregious deficiencies in its cybersecurity defences. He alleged that Twitter has not only covered up negligent security practices but has also misled federal regulators about its safety and omitted to disclose the number of bots on the platform. Twitter's primary vulnerability, according to Zatko, is that too many employees have access to sensitive user data and internal software, which is not vigilantly monitored.

Scraping of data involves hacking a piece of software linked to Twitter called an API (application programme interface) which in turn reveals hidden account details. The data is then used for further malicious hacking campaigns. What is important to note is that these hackers are not infiltrating the servers of Twitter, they merely scrape the public-facing surface of platforms, which illustrates the negligence of the media platform in securing and protecting its users' data. The same method was used in November 2021, whereafter, in January 2022, Twitter publicly stated that it had fixed the issue. The media platform noted that there was no evidence to suggest that hackers had taken advantage of the vulnerability, however experts in the field subsequently discovered various databases of Twitter credentials for sale in July later that year.

Not every crime is a cybercrime – The dichotomy of cyber-enabled crimes and cybercrimes

The distribution of personal data, particularly private e-mails and telephone numbers, is a universal violation of a data subject's rights, as the misuse of personal information / data could result in, to mention a few –

- identity theft or fraud;
- financial loss;
- damage to reputation;
- loss of confidentiality of personal data protected by professional secrecy; or
- any other significant economic or social disadvantage to the natural person concerned that limits their data subject rights.

The consequences of the nefarious dissemination and abuse of this information has become abundantly apparent over the years. Cybercrime has increased exponentially over this period and unless pro-active and interventional measures are taken, we can expect this to become endemic.

Ahmore Burger-Smidt

Head of Regulatory

View Profile