Harsh Dhingra

Dr. Stephen Farrell

Security and Privacy

April 21, 2021

T-Mobile Faces a Data Breach Again

T-Mobile, a US-based company currently the most prominent wireless voice and data communications services provider in the United States and has more than 80 million customers. T-Mobile has its operations in Europe in countries like Austria, UK, Germany, etc., globally T-Mobile has approximately 230 million users. T-Mobile International, a T-Mobile subsidiary, is the world's thirteenth largest mobile phone service provider by subscribers. T-Mobile, the Bellevue Wash–based wireless company, posted a revenue of $19.3 bn, and profited $1.3 bn in Q3 2020. Looking at the posted revenue and profit, it is hard to comprehend that more money could not be spent protecting user data.

Telecommunication providers have become a key target for scammers because of the customer's large databases and the high value that the data possesses on the black market. On February 26, 2021, T-Mobile released a statement stating that they had information about a security breach. Many T-Mobile customers were affected by SIM swap attacks or SIM hijacking, while T-Mobile did not release the number of affected customers. On investigation, it was found that the attackers seem to have penetrated T-Mobile's system and exposed data about customers, including their names, addresses, phone number, account numbers, rate plans, email addresses, PIN (personal identification number), account security questions, and answers and date of birth. This is T-Mobile's third breach in less than a year; unlike the previous ones, this is more serious because it involves the user's important personal information.

This incident can't be neglected because it involves porting or SIM-swapped cases (also called SIM hijacking). If a scammer has hijacked the SIM, it can easily control your phone number and can use it to obtain sensitive information (such as OTP – one time passwords for logging in); basically, it is the kind of attack that targets a weak two-factor authentication therefore once a sim is hacked the scammers can receive victim's messages and calls which allows them to bypass SMS-based authentication easily. The scammers can easily access victims' financial accounts, steal money, cryptocurrency, commit fraud, and even lock the victim out of their account. Since scammers have all the necessary personal information about a user, they can steal a user's identity, threatening the user and the country. T-Mobile quickly identified and terminated the unauthorized activity. A text message was sent to affected users, and they were advised to change their account password, PIN, and their security questions and answers. T-Mobile also has offered two years of free credit monitoring and identity theft detection service as compensation.

Security breaches and data breaches have become pestilence issues; after the shift from paper records to advanced databases worldwide, these scams are burgeoning. Every organization should be proactive with security breaches; regular security audits should be conducted regardless of whether there was a data breach or not. Organizations should devote at least 5% of annual budget in IT security. Security is an investment cheaper than a data breach.