Hacker took advantage of the vulnerability in SS7 to steal bank accounts

The SS7 telecommunications vulnerability is no stranger when it not only has the ability to control applications but also steal your bank account information.

Earlier this year, many hackers took advantage of Signaling **7 vulnerabilities** (Signaling System No. 7 (SS7) as the phone protocol used to set up most calls in PSTN) to pass. Two-factor verification and stealing money from bank accounts in Germany, the German newspaper *Suddeutsche Zeitung* said.

Hacker steals login information through fake emails, claiming to come from the victim's bank. Then use the vulnerabilities in SS7 to redirect SMS messages requesting confirmation of money transfer transactions. On *Ars Technica*, representative of O2 Telefonica said: " *Criminals perform attacks from the international mobile network in the middle of January* ." " *The attack will redirect SMS messages from customers to attackers* ."

Ars Technica said security researcher Karrsten Nohl described the potential impact of errors in SS7 late last year by recording calls and tracking the location of US House member Ted Lieu.

Earlier this week, Lieu posted a line on Twitter saying, " *I have urgently requested the FCC and the telecommunications industry to fix the security flaw in SS7. Perhaps losing money in the bank will cause them to act* ."

A warning to the mobile operator

Mark Windle, Mavenir's chief marketing and security manager, told *eSecurity Planet* that the news should be considered a warning to the mobile user community. "The *network has collaborated to understand how to exploit vulnerabilities and eliminate them* ," he said.

" *SS7 technology can eventually be replaced with Diameter or SIP but at least SS7 will last for at least 10 years. And simply canceling such a protocol is not a solution* ." Windle added: " *As long as there is a national and international connection, the door is still there* ."

" *At the same time, by continuing to overcome security problems in signaling protocols through the use of optimized multi-layer solutions, operators can make users more confident, reducing the proportion of customers leaving. The product and most importantly protect mobile devices,* "he added.

Balance between security and convenience

A recent survey of more than 800 representatives from financial institutions around the world showed that 24% of banks face the identification of customers when trading through online services, carefully number.

The survey funded by **Kaspersky Lab** and implemented by **B2B International** also results in 30% of banks encountering security incidents, affecting Internet banking services, and expected increase in financial losses. The main reason for fraud in the next 3 years will be 59%. 38% of respondents said that the balance between prevention methods and customer convenience is one of the biggest concerns.

" *While thinking of other approaches to securing mobile and digital trading channels, banks still have to avoid putting pressure on customers,* " said the head of the fraud protection department. **Kaspersky Lab** Alexander Ermakovich said.