Rampant NID data trade: Mobile banking institutions alert law enforcement

March 5, 2024

Online *Desk*: In a concerning development last year, personal information of individuals registered with the country's Smart National Identity Card (NID) system was reportedly available on several Telegram channels, with instances of buying and selling such data coming to light.

A quarter with vested interest has recently emerged, engaging in the illicit trade of customer data. To elevate the prominence of such data trading, there have been attempts to associate the names of reputable mobile banking institutions.

Sources indicate that what began with the exploitation of Telegram bots has evolved into a more organized operation, with perpetrators setting up a dedicated website alongside Telegram channels to facilitate this illicit trade. These individuals are also actively advertising on social media platforms, falsely claiming to hold customer information from reputable Mobile Financial Services (MFS), thus aiming to mislead and deceive customers through various tactics.

The modus operandi involve circulating specific links through Telegram channels that purportedly allow access to personal details of individuals by inputting their NID numbers and birthdates. Despite skepticism about the authenticity of such claims, due to the absence of verification mechanisms, the alleged data breaches have stirred concern among the public, already wary from previous incidents involving the national ID card database.

ICT experts emphasize the vulnerability of the populace to misinformation regarding new leaks, amidst conflicting statements and opportunities for fraudulent activities. They note that while opening an account in any financial institution requires national ID information and a photo, the allegedly leaked information on digital platforms is deemed non-exploitable for fraudulent purposes within Bangladesh.

The national ID database, a critical repository of personal information for approximately 120 million citizens, remains a target for cybercriminals. IT expert Tanvir Hassan Zoha warns, "Those selling information online and those purchasing it are both committing offenses and could face legal consequences under the vigilant oversight of law enforcement agencies. Interestingly, there's no real profitability in buying such information in Bangladesh."

A significant data breach in July last year exposed sensitive information of millions through the website of the Office of the Registrar General, Birth and Death Registration, searchable via Google. Subsequent leaks involving smart card data have seen such information circulated as belonging to customers of mobile banking institutions and banks. However, verification efforts have unveiled inconsistencies, with varying pieces of information available in different groups.

This proliferation of customer information on digital platforms has sown discomfort and fear among citizens, potentially eroding trust in financial institutions and fostering a climate of insecurity. Mobile banking entities, while yet to issue formal statements, have reportedly notified law enforcement agencies about these breaches.

A senior official from a leading mobile banking institution highlighted the challenges of combating digital platform propaganda related to data breaches, emphasizing their prompt communication with law enforcement upon becoming aware of the recent incidents.

Md Hassan Shahriar Fahim, managing director of Octagram Limited that specializes in cybersecurity, underscores the risks to individuals enticed into purchasing such data. Collaborative analysis with law enforcement has revealed that information thieves also retain data on buyers, exposing them to potential hacking, blackmail, and other complications. Victims, in turn, find themselves in a predicament when seeking legal assistance, often unable to disclose the circumstances of their online harassment.