THE STRAITS TIMES

Monday Feb 19, 2024

Over $34m lost to 1,900 cases of malware scams

Nadine Chua

More than 1,890 cases of malware scams were reported in 2023, the first time this scam type was among Singapore's top 10 scams.

Malware scams were the sixth scam of concern, with at least $34.1 million lost in 2023, according to the police's annual scam figures released on Feb 18. They were practically unheard of previously, as such scams emerged only in 2022 and became widespread in 2023.

The police said the average amount lost per malware scam case was around $17,960 in 2023.

The scammers targeted victims who responded to advertisements on social media platforms for services such as home cleaning or pet grooming.

Under the pretext of getting victims to pay for such services, scammers would send them a file or a link on WhatsApp, requiring them to download an Android Package Kit (APK) file, an app created for Android's operating system.

These APK files contained malware, and when victims downloaded them, the scammers gained access to the victims' devices.

This allowed scammers to obtain the victims' banking credentials and card details by monitoring their usage of the devices. The victims would realise they had been scammed only when they noticed unauthorised transactions made from their bank accounts.

The police said more than 43 per cent of malware scam victims were aged 30 to 49. Facebook and Instagram were the most common platforms used by scammers to contact victims.

Cyber-security expert Raju Chellam said he was not surprised that malware scams were among the top scams of concern in 2023, due to the rapid growth of artificial intelligence (AI).

Mr Chellam, who is honorary chair of cloud and data standards at the IT Standards Committee, said: "Scammers can exploit AI to generate malware, ransomware and other harmful software. Malware acts like a Trojan horse, concealing its nefarious purpose under the guise of a legitimate program or app."

He said scammers can overlay a fake QR code over a real one. If unsuspecting victims scan the QR code and key in their personal details, their phones could get infected with malware.

In May 2023, The Straits Times reported that a woman in her 60s scanned a QR code pasted on the glass door of a bubble tea shop, which had encouraged customers to complete an online survey to get a free cup of milk tea.

After scanning the QR code, the woman downloaded a third-party app onto her Android phone, which allowed scammers to take over her device and transfer $20,000 out of her bank account.

Mr Chellam said malware scams can also cause victims to lose money when they see an attractive online offer advertised as a limited-time deal. "Driven by the fear of missing out, they may hastily download an app with malware to purchase the product," he said.

He added that such malware scams may even be spread inadvertently when a victim tells his friends about the "good deal", without knowing it is a scam.

To combat malware scams, various banks have since August 2023 rolled out upgraded versions of their banking apps with anti-malware measures.

They restrict users' access to banking apps if their devices are detected to have sideloaded apps, which are apps downloaded outside the official app store.

In November 2023, OCBC Bank, DBS Bank and UOB announced new money-locking features for customers to protect themselves against scams.

These were designed to prevent fraudsters from siphoning money out of a hacked account. The money customers choose to lock up can be withdrawn only in person.

The police said that as at January, more than $4.2 billion was set aside across over 49,000 bank accounts.

Ms Loretta Yuen, head of group legal and compliance at OCBC, said that as at Feb 9, $4.4 billion has been locked across more than 40,000 OCBC accounts.

More than a third of these OCBC customers are aged 50 and above, while close to 49 per cent are between 30 and 50 years old. Around 17 per cent are below 30 years old.

Ms Yuen said that while OCBC saw fewer victims falling prey to malware scams towards the end of 2023, everyone should remain alert.

nadinechua@sph.com.sg