BE CYBER SAFE

Weekly digest of cyber scams to help you stay ahead

Beware of free wedding invite WhatsApp scam

The “wedding invite” scam, in which the victim receives a wedding invitation from an unidentified individual urging them to open the attached file to obtain further information about the wedding. The “attached file” is actually an APK that infects the victim’s phone with malware. The malware that exists is designed to steal various types of data from users’ phones .

The app does not appear in the App Launcher due to the Missing Launcher activity category. Once the app is installed on the phone, it stays hidden

As its C2C server, the malware makes use of a Telegram bot. Telegram bots are applications offered by the Telegram chat network. It is configured to deliver real-time information and automate user interactions. The application transfers stolen data to the Telegram bot, making it simple for a hacker to obtain information gathered on Telegram.

Businessman scammed of ₹ 95 lakh after accepting Facebook friend request

The victim had received a friend request from a woman named Steff Mhiz on Facebook last year in October, which he accepted. They later moved their conversations to WhatsApp.
According to the outlet, his friend suggested that he purchase herbal goods from India for ₹1 lakh apiece and sell them to Mhiz’s firm for ₹ 2 lakh.

Once he consented, she urged him to get in touch with a fraudster to obtain the items. Victim and he communicated by email. He paid ₹1 lakh and received a sample packet following their online chat. The box came on schedule, but victim did not open it. He allegedly continued to give money, after that in several accounts per his instructions. When fraudster persisted in requesting more money under fictitious presences, he became sceptical. When he didn’t get the promised sum, victim urged fraudster to call off the agreement and give him his money back. But since then, neither fraudster nor the woman have been in contact.

To his surprise, there were no herbal items within the packages when he finally opened them. They were packed with fried chips and powder.

A 99-Year-Old man lost ₹2.78 lakhs in electricity bill scam

Victim received a message from an unknown number , stating that he had not paid his electricity bill and that his connection would be cut off in next few hours, if he failed to do so. Believing
the message to be from Tata Electricity, the victim contacted the number. Despite informing the person on the other end that he had already paid the bill, he was told that the payment was not
updated in the system.

The fraudster then requested his credit card details and PAN card for rectification, which Agrawal unwittingly provided. As a result, he received messages indicating that Rs2.78 lakh had been
debited from his account.

Cyber fraudsters turned to AnyDesk app to dupe citizens

Cyber fraudsters have now turned to AnyDesk to dupe people. Pretending to be helping the users, fraudsters are sending links using which the latter are directed to install the tool in their mobile phones, after which the devices are controlled by the fraudsters to access the users' bank accounts and siphon money.

A finance professional from Narsingi was searching for a customer care number to inquire for a refund for her watch which she purchased from an e-commerce platform. She received a call from a person claiming to be an executive and he spoke in Hindi. After inquiring about her query, he asked her to download the AnyDesk app to initiate the refund process.

Accordingly, she installed the app from the Play Store, opened it, and provided a number displayed on the app to the caller. She later noticed that 1.2 lakh was debited from her savings account. She tried reaching out to the executive who called her, but there was no response.

Girl Falls Prey to Free iPhone Scam, Loses Over ₹18,000

A girl from has fell prey to a scam promising a free iPhone. Fraudsters tricked her into making multiple payments totaling over ₹18,000 through UPI after receiving a call from an unknown number.

The caller reportedly instructed her to purchase items worth ₹5,048 on Flipkart to qualify for the free iPhone. She then received another call demanding ₹13,990 as GST payment. After making both payments, the caller convinced her to make a further payment to rectify a supposed GST processing issue.

Drugs in parcel fraud: Victims lost ₹1 crore to scammers

The gang members target a section of people and collect the details of a person such as Aadhar card, PAN card and mobile number. Once they have the sufficient information, one of the gang members will approach the victim through a phone call and intimate that a parcel was booked in his/her name from an unknown location and upon inspection they have found drugs or passports in the said parcel.

The accused further threaten the victim of registering cases under NDPS Act and Prevention of Money Laundering Act (PMLA Act) and he alone creates a situation for the victim to negotiate with the officer by connecting to another person, who claims to be their superior officer. "Taking advantage of the situation, they demand money ranging from ₹10 lakh to ₹25 lakh to close the case and stop further proceedings.

The fraudsters have extorted huge amounts by threatening the victims in the name of Enforcement Directorate (ED) and Central Bureau of Investigation (CBI) officials, claiming that they have found drugs in the parcels they have ordered.

Insurance policy scam

The gang targeted victims by posing as SBI Smart Wealth Builder Policy officers. They convinced victims to open new policies or "rectify" existing ones with promises of high returns. The unsuspecting victims were then tricked into transferring money to various bank accounts controlled by the fraudsters claiming to be genuine bank accounts.