BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

A 66-YEAR-OLD MAN DUPED OF RS 1.88 CRORE IN A CYBER-FRAUD.

The victim was added to a WhatsApp group after he clicked on a link while watching a video on an online platform. The group was named 'customer care ICICI Ambani shares' and had over 80 participants when he had joined. She was guided on investing money in various shares and also directed to download an application.

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. She 'invested' Rs 50,000 on April 9 and Rs 2.50 lakh the next day. Unaware of the fraud being committed on her, the complaint sent Rs 18 lakh on April 13, Rs 16 lakh on April 14, Rs 21 lakh on April 19. In a transaction on April 26, she even deposited Rs 80 lakh in one go. The complainant said in return, she had initially received Rs 3,302 back in her bank account. Her request to withdraw the amount was rejected. By the time he realised she was being duped, she had already transferred Rs 1.88 crore to the bank accounts as directed by fraudsters in the WhatsApp group.

VISHING: NEW DEEPFAKE-ENABLED CYBER ATTACK TECHNIQUE HAS INDIA WORRIED

In vishing, adversaries use phone calls to trick victims into opening malicious emails sent on their government email IDs. The adversaries pretend to be high ranking officers to trick victims into opening malicious files. The problem is compounded as the threat actors may also use deepfake techniques to hoodwink such officials.

The adversary often impersonates as a defence personnel or a higher ranking official from a legitimate organisation, and contacts the victim through an Indian phone number," it read. Then the caller uses techniques, such as referencing to accurate personal information or quoting high ranked officers, to build trust and to seem credible.

In one particular instance, a PIO (Pakistani Intelligence Operative) claiming to be SO to a very officer contacted the victim through an Indian phone number and asked the victim to open a NIC mail from their PC . The caller then creates a sense of urgency claiming that there is an urgent email which needs to be responded to. The adversary instructs the target to check their email for a message from the organization which is actually a phishing email.

A CYBERCROOK POSING AS AN RBI OFFICIAL DUPED A 66-YEAR OLD FARMER OF RS 4.49 LAKH ON THE PRETEXT OF RETURNING CASH

A cybercrook posing as an RBI official duped a 66-year-old Parbhani farmer of Rs 4.49 lakh on the pretext of returning cash handling charges on May 2 for the money the latter paid earlier. A Wakad police officer said the complainant runs a liquor and an agro product shop in Parbhani. "On May 2, he received a link similar to his bank application. He clicked on the link, filled in the details and shared an OTP. He then got a call from an RBI officer asking for an OTP. Though he did not it, Rs 4.24 lakh were siphoned of .

Powered by GRAMAX CYBERSEC
A GAR AERO SERVICES INITIATIVE

WHAT IS 'DIGITAL ARREST', A NEW FORM OF CYBERCRIME?

In what could possibly be a movie script, scammers held a woman, a resident of Noida, under 'digital arrest' over a Skype call for an entire day by pretending to be cops. The result: they duped her of Rs 11 lakhs. The scammer told the woman that her Aadhaar card had been used to buy a SIM card, which is connected to a money laundering case in Mumbai. They told her that an arrest warrant had been issued in her name.

Digital Arrest involves the virtual restraint of individuals. These suspensions can vary from restricted access to the account, and digital platforms, to implementing measures to prevent further digital activities or being restrained on video calling or being monitored through video calling.

74 YEAR MAN DUPED OF ₹2.80 LAKH BY CYBER-FRAUDS POSING AS CBI OFFICERS

A 74-year-old Mahim resident was duped of ₹2.80 lakh on Sunday by cyber frauds who posed as Central Bureau of Investigation (CBI) officers and claimed that his son, who lives in the US, was arrested in a rape case and the money was required to secure his release. Police have also managed to freeze ₹1 lakh transferred by the victim to a bank account whose details were provided by the frauds.

On Sunday morning, at around 9am, the complainant's wife got a call from a number whose profile picture was that of a policeman. The caller claimed that he was a CBI officer and told the complainant that his son had been arrested in connection with a rape case. He said the son could be freed as he had no direct role in the case, but officials would have to be bribed for that.

'BEWARE OF JUICE-JACKING': USB CHARGER SCAM

USB charging ports at public places are being misused by cyber criminals for malicious activities. "Cyber-criminals may use USB charging ports installed at public places like airports, cafés, hotels and bus stands for malicious activities. Charging your electronic device at such infected USB charging stations may make you a victim of juice-jacking cyber attack.

Cyber criminals through juice jacking, can install malicious apps; encrypt devices and demand ransom to restore data and they could even steal data from devices. The agency advised the public to be cautious while using public charging stations or portable wall chargers. It also advised the public to use electrical wall outlets for charging mobile devices and carrying personal cable and power bank. Lock your mobile device and disable pairing with a connected device. Try to charge your phone when it is in switched off state.

RETIRED MECHANICAL ENGINEER IN PUNE LOSES LIFE SAVINGS OF ₹4 CRORE

A 59-yearold retired mechanical engineer in Pune duped of nearly ₹4 crore in an online share trading scam. The fraudsters contacted the victim in October 2023 over the phone with an online share trading offer. They allegedly assured him of huge returns on investments in online share trading.

The fraudsters gained his trust by interacting with him multiple times. As per their instructions, the victim transferred ₹3,95,85,204 from his bank account to various other bank accounts till December 9, 2023

But when he did not get the assured returns, he realized he had been cheated and approached the police.