BE CYBER SAFE

Weekly digest of cyber scams to help you stay ahead

AI voice, fake WhatsApp account: How scammers targeted CEO of world's biggest ad firm using deepfake

Mark Read, the CEO of WPP – the world's largest advertising company as of 2023 – has reportedly been targeted by scammers. fraudsters used a deepfake technique to set up a call. They used publicly available photos, videos. The scammers used Read's voice clone and public YouTube footage to set up a Microsoft Teams call with senior executives. A Microsoft Teams call was also arranged between one of his agency heads, another senior executive and the scammers. At the Teams meeting, a voice clone and YouTube footage of the other executive was used while scammers impersonated Read off-camera using the chat function. The pretext was that the individual targeted was being asked to set up a new business with the ultimate aim of extracting personal details and money.

Engineer Duped Of Rs 1.6 Crore By Scammers Impersonating Courier Service Staff

A retired engineer reportedly fell victim to a scam, losing Rs 1.6 crore to fraudsters. The scammers requested 'caution money' from the retiree, purportedly to avoid investigation by the central investigative agency individuals impersonating employees of an international courier service deceived the victim by claiming that the package he had sent contained incriminating documents and drugs known to investigative agencies. Purportedly, to avoid legal trouble, they demanded a caution deposit, assuring its return after the investigation. The alleged transactions totalling Rs 1.6 crore took place in 4 days.

A new cyber fraud trick, criminals send SMS to steal money

Victim recalled that she was on a work call when someone called her, stating the need to send money to her father. Claiming to have problems with his own bank account, he asked for her help in receiving the funds. Shortly after the call, she got a text message alert that looked like standard bank notifications. The caller then told her that he meant to send Rs 3,000 but accidentally sent Rs 30,000 instead. He then asked her to give back the extra money. But when she checked the SMS alerts she got, she saw differences and understood that she was about to be tricked in a financial scam. He was creating a sense of urgency by loudly claiming that he had sent extra money to the doctor and was now sending UPI Ids to receive the remaining amount back. upon examining the SMS messages, that they originate from a 10- digit phone number, not a branded company ID.

The cybercooks lured people, inveigled them to buy products at discounted price.

The victim were lured into purchasing 'heavily discounted' items through links shared on Telegram and to bet on online gaming applications shared on the channel. The accused was in touch with foreign hackers and cyber fraudsters on the dark web to prepare online gambling applications, marketing websites and links. The accused used to invite gullible people through Telegram to bet on gambling applications like Ludo King, and to use e-marketing sites and links. the fraudsters also lured people by sharing fake snapshots of different online payment applications and wallets of winning money and getting expensive items at low prices.

There's a new cyber scam in market, it's covid vaccine feedback calls

A feedback call regarding the coronavirus vaccine enquired the citizens about doses and experience of the vaccination camp. In this, an unknown call comes from any number. A girl reportedly asks you whether you have taken the Covid vaccine or not. If yes then press one otherwise press two. Usually, when people have got the vaccine, they immediately press the button for feedback and get trapped in the net of a scam. t the phone hangs as soon as you press one or two buttons. Cyber hackers get access to the bank account's name and number. Many cases of fraud in the name of Covid vaccine have reached the police.

New Scam, got a friend's WhatsApp message from new number for money

A victim found himself in a precarious situation when one of his friends informed him about a scamster trying to con people in his name. Using victim's DP, the scamster sent messages to four of his friends from college. The scamster then asked them to give him phone numbers of other friends of to build a sense of trust. Two of his friends gave contact numbers to the scamster but then he asked for money. The victim said that he has changed his phone. The scammer then asked his friend to send him ₹2000 on Gpay on this number. His friend suspected something fishy. So he asked him to give him his UPI ID. But UPI ID was of some other name. Then his friend's suspicion got confirmed that he is being scammed. So, he immediately called victim on his number and narrated him the entire incident.

Cyber criminals catch up with IVRS, use latest tech as gateway to fraud

In their latest modus operandi, cyber criminals are making calls to people using Interactive Voice Response System (IVRS) in which a computer-generated voice calls random mobile numbers and threaten the user that their mobile number will be disconnected within two hours. The voice further states that if they want to continue using their mobile number they should press '9'. Many fall in the trap of the fraudsters and siphon their money. A victim received a phone call on his mobile number from an unknown number. As he picked up the call, the computer generated voice said that his mobile number will be disconnected within two hours and if he wants to continue using his mobile number he should press 9. He had recently recharged his mobile number with a six months validity card. For a moment he was about to fall in the trap but he thought and disconnected the call