Beware of these 8 digital payment-related scams

04 Nov 2019, 12:06 PM IST

1/8 How to avoid payment-related scams

Several payment-related scams have come to light in recent months. ET unravels the modus operandi involved and tells you how to avoid being taken for a ride. **1. The remote access mobile application scam Modus operandi:** Fraudsters, who had listed fake numbers online under an NGO's name, gained access to a Mumbai resident’s debit card details by asking her to download Anydesk, a remote desktop software tool, which provides a third party a complete view of the user’s screen. She wanted to transfer funds to the NGO to cremate her pet. Instead, her debit card details were compromised and Rs 30,000 was withdrawn from her bank account. **Lessons to learn:** Do not seek help from strangers to complete payment transactions. Do not download apps, except official ones, recommended by seemingly-helpful people, even if they claim to be bank staff.

2/8 2. Trap for gullible insurance seekers

Modus operandi: In this, scammers prey on an individual's inability to spot the difference between the official and fake portals of the insurance regulator. A counterfeit portal going by the URL www.irdaionline. org managed to sell fake policies to insurance seekers until the Irdai issued an alert, and the URL was blocked.

Lessons to learn: Irdai does not sell insurance policies. Stay away from portals misusing domains that are akin to regulators' official ones to swindle funds.

The crypto startup has stayed afloat and even clocked growth in a hostile r...

Organic farming can cut direct greenhouse-gas emissions, but it would also ...

3/8 3. Phishing smses promising income tax refund

Modus operandi: A Mumbai-based private sector employee received a link, purportedly from the income tax department, regarding a tax refund he was eligible for. Once he clicked on the link, he was directed to a mobile application that got downloaded on his phone. Tricksters elicited his account access details and siphoned off money.

Lessons to learn: The income tax department directly credits the refund to the bank account mentioned in your I-T return form. Do not trust any messages, links, online forms or calls seeking additional account/card details.

4/8 4. The KYC update hoax

Modus operandi: An IAS officer in Udaipur lost Rs 6 lakh when she clicked on a fraudulent link asking her to update her KYC. She was prompted to enter her account details and the OTP received, following which she received messages from her bank notifying her of debits worth Rs 6 lakh.

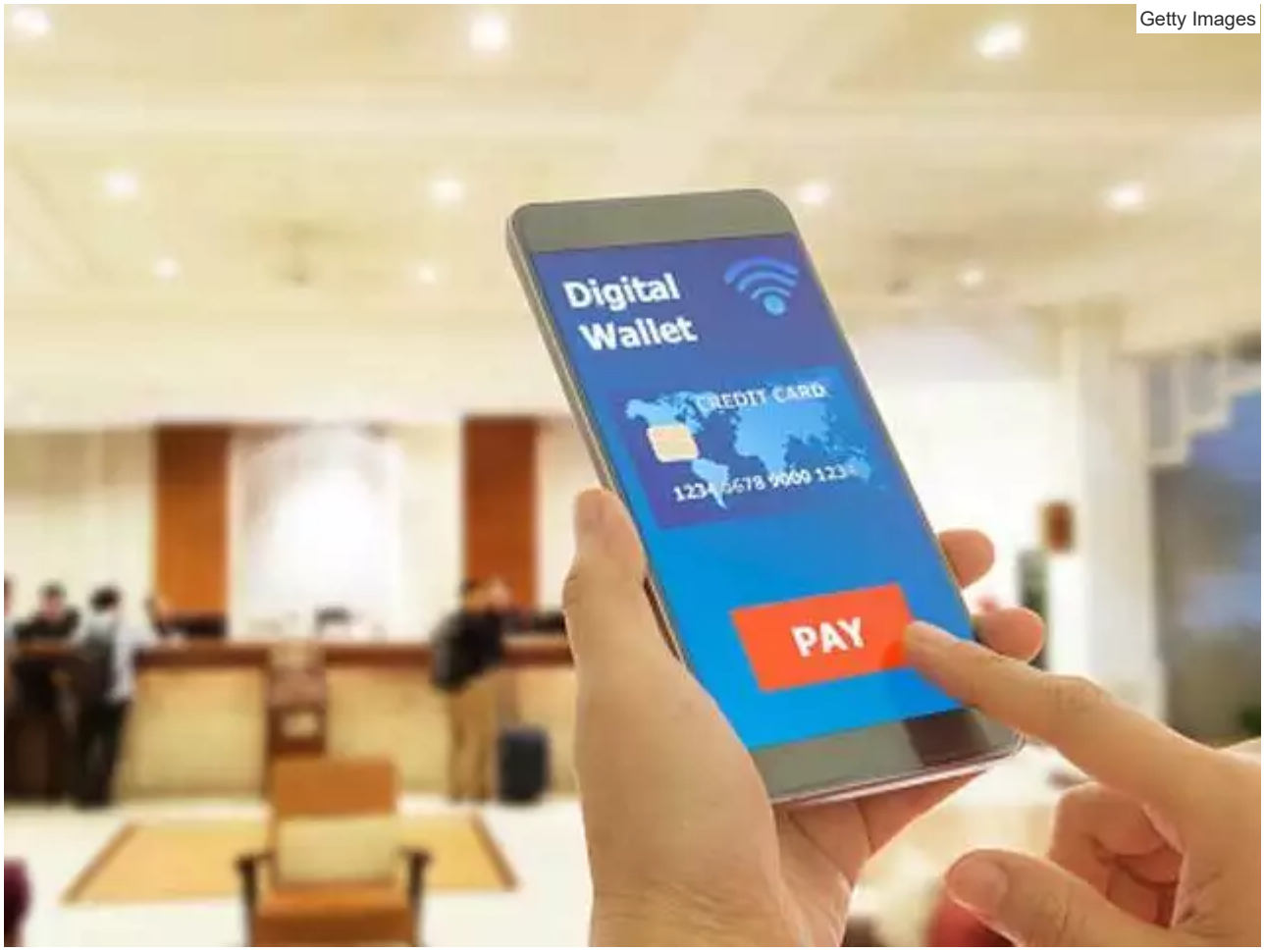
Lessons to learn: Do not click on links received through SMSes. Rely on official websites or bank branches to complete the process, if required.

Getty Images

5/8 5. Simple to-crack passwords

Modus operandi: Here, victims make hacking an effortless job for hackers. The United Kingdom's National Cyber Security Centre (NCSC) recently released a list of 'most hacked' passwords. Over 23 million accounts worldwide were breached as they had 123456 as their passwords.

Lessons to learn: While the data pertains to the UK, it is a pointer to the hazards of using passwords and PINs that are easy to decode.



6/8 6. Fake UPI-based payment links

Modus operandi: Fraudster asked the victim, a Pune-based trader, to transfer a nominal amount of Rs 10 to a mobile number from his digital wallet. It was presented as ‘registration fee’ to initiate the online purchase of a scooter. Subsequently, he received payment links where he had to enter his UPI ID and OTP received and send it back to the fraudster. The information was used to transfer Rs 1.53 lakh out of his accounts.

Lessons to learn: Transact only through the official BHIM or bank UPI apps. Do not use links sent by unknown entities, even if they seem authentic.

7/8 7. Fraudulent NPCI/UPI/BHIM handles and portals

Modus operandi: Myriad Twitter handles masquerading as @NPCI_BHIM official helpline handle have mushroomed on the micro-blogging site. The fake accounts trick customers looking for help to reveal their account, wallet or card details.

Lessons to learn: Look for verified-by-twitter blue ticks while interacting with National Payments Corporation of India (NPCI), bank or payment wallet helplines.

8/8 8. Lack of awareness of UPI pay options

Modus operandi: A Pune resident who wished to sell his air-cooler was tricked by a prospective buyer who agreed to pay Rs 9,000 through a UPI-based app. However, the latter sent a ‘pay’ request to the former, who promptly authorised it without realising that the amount would be debited from, not credited to, his account.

Lessons to learn: Use of newer technologies calls for additional caution. Since UPI-based apps enable push (pay/send) and pull (receive/collect) transactions, newer users could get confused. Understand the processes thoroughly before rushing to use them.