Beware of unique types of frauds

Experts share safety precautions

ANJALI KOCHHAR

A week ago, a man from Delhi was trying to book a train ticket through a reputed travel website. In the process, he called their customer care number, and the call got diverted to another number. The other party asked him to install an application on his phone, and connect his credit/debit cards with the app. As soon as the call was cut, a sum of ₹1.2 lakh was syphoned out from his account. Who knew a ticket from Delhi to Jalandhar would cost such a vast amount? Who knew fraudsters are coming up with unique techniques to dupe innocent people?

Well, to tell you the truth, the victim in this case was none other than my father!

To make sure that people don't keep falling prey to such fraudsters, I have tried to create a guide about some little-known types of frauds and how to deal with them, after speaking with several industry experts. Here you go!

OTP-BASED FRAUDS

Messages purportedly from non-banking financial companies (NBFCs) are sent out to targets, offering loans or credit limit enhancements, along with a contact number. When victims call the number, they are asked to fill out forms containing financial details and are coerced into sharing OTP (One-Time Password) or PIN details. This information is then used by fraudsters to conduct unauthorized transactions and cause financial losses.

HOW TO AVOID OTP FRAUD

CrossFraud's Dedhia has the following tips:

- Never share OTP, PINs, or personal details with anyone in any form.
- Regularly check SMS and emails to ensure that no OTP is generated without your knowledge.

JUICE JACKING

Juice jacking is a hardware-focused fraud tactic where attackers infiltrate public charging stations or connection cables with malware. They hope that unsuspecting individuals will use these doctored devices to charge their gadgets, and thus unknowingly expose their personal information or allow unauthorised access to their details. The crime exploits the trust users place in public charging stations.

HOW TO AVOID JUICE JACKING

Dhiren V Dedhia, head of Enterprise Solutions, CrossFraud, shares the following tips:

- Avoid using public charging stations, including at airports.
- Use power banks instead of relying on public charging stations.
- Disable the option for automatic data transfer when connecting via USB.
- Consider using a USB passthrough device that only allows charging and blocks data transfer.

TURN TO PAGE 10

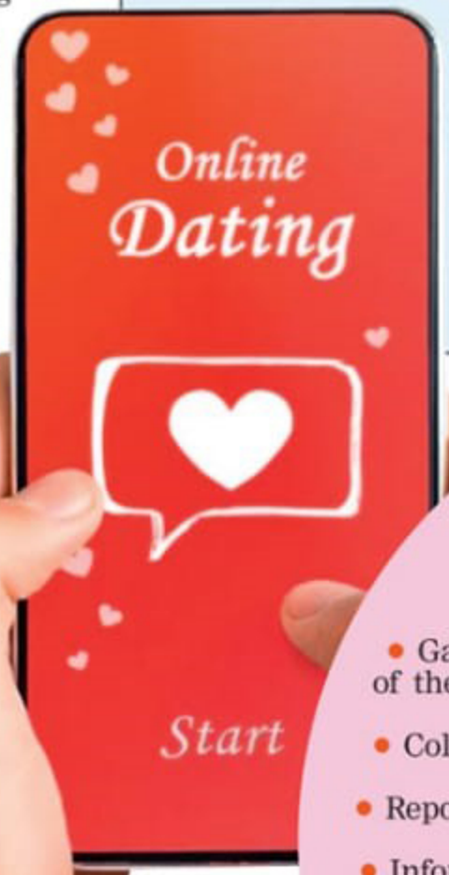
BEWARE OF UNIQUE TYPES OF FRAUDS

ROMANCE FRAUDS

This is a type of online fraud where criminals deceive the unwary on dating websites, social media platforms, or through email by pretending a romantic interest. These scammers often create fake profiles and develop emotional connections with their victims to gain their trust. Once trust is established, they exploit the victims by manipulating them into sending money, and personal information, or even engaging in illegal activities on their behalf.

HOW TO AVOID ROMANCE FRAUD

- Maintain a healthy level of scepticism when engaging with people online.
- Avoid sharing sensitive personal information, such as your address, financial details, and Government ID numbers with individuals you've only met online.
- Watch out for warning signs, such as inconsistent or evasive answers, reluctance to video chat or meet in person, or excessive declarations of love early in the relationship.



REMOTE ACCESS SCAMS

Scammers convince victims to install remote access software on their devices, claiming to provide technical support. Once installed, the fraudsters gain control over the victim's device and steal personal information or commit financial fraud.

HOW TO AVOID REMOTE ACCESS SCAMS

Dr. Sanjay Katkar, the Managing Director and Chief Technology Officer of Quick Heal Technologies, has this to say:

- Exercise caution when interacting online; avoid suspicious links, and verify identities before sharing sensitive information.
- Educate yourself and your employees about fraud techniques through regular cybersecurity training.
- Activate 2FA (Two Factor Authentication) whenever possible, especially for important accounts like email and banking. This adds an extra layer of security by requiring a verification code in addition to your password.
- If you have granted remote access to someone you are suspicious of, disconnect your computer or device from the internet to prevent further access or data theft.

WHAT TO DO IF ONE IS SCAMMED

IN CASE YOU HAVE FALLEN PREY TO FINANCIAL FRAUD, EXPERTS SAY:

- Gather all available information and contact details of the fraudsters and any evidence of the fraud, such as screenshots of conversations or emails.
- Collect records of all the payments made to the fraudsters.
- Report the fraud to authorities such as the police, cybercrime cell or the Consumer Court.
- Inform bank and credit card companies about the fraud and take necessary steps to secure your accounts.

And finally, do make sure you are dealing well with the anxiety and stress that might result from the financial abuse. **Mynoo Maryel,** an accomplished author and thought leader, recommends the AAA approach to overcome trauma or distress from financial fraud - Acknowledge the situation, Accept it and Accomplish great things by moving on.

Mynoo Maryel

WORK-FROM-HOME FRAUDS

Work-from-home frauds are schemes that target individuals seeking remote employment opportunities. These scams often promise high earnings and flexibility while working from the comfort of your own home, but in reality, they aim to deceive and defraud unsuspecting individuals.

HOW TO DEAL WITH WFH FRAUDS

Sudhakar Raja, Founder and CEO of the Human Risk Mitigation platform TRST Score, presents the following tips:

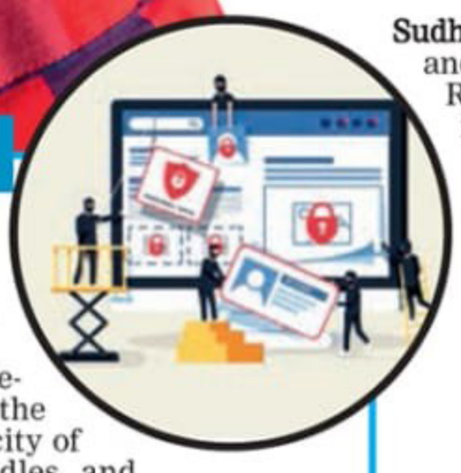
- Candidates need to be extremely suspicious of offers from unknown sources. Reputed companies will never approach you with job offers via WhatsApp when you have not applied for one.
- A demand for money to provide a job or participate in the selection process is a red flag.
- If you are being pushed to participate quickly, be aware that a false sense of urgency is being created to prevent you from spotting loopholes. Take a step back and think through what you are being asked to do.
- Use holistic Risk Mitigation Platforms to check the employers and the companies that you are being approached by. This allows you verify the person approaching you instantly.

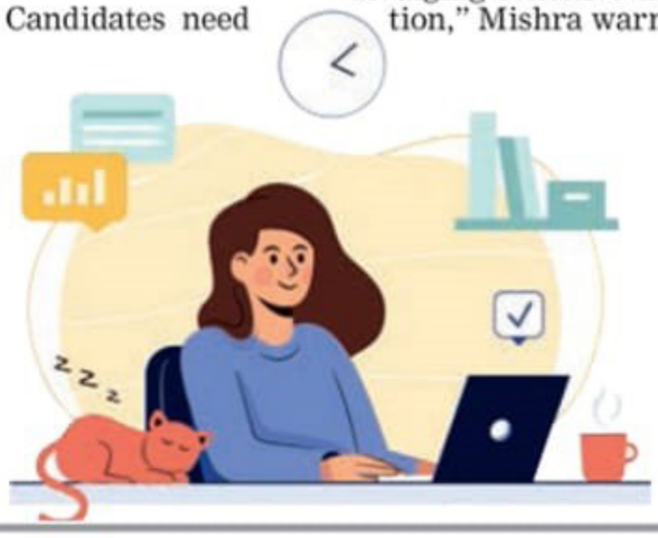
HOW ARE SCAMMERS PULLING OFF THESE SCHEMES?

Scammers can pull the wool over people's eyes easily, despite precautions. Even the most educated or highly-graded professional gets scammed.

Amit Relan, Founder and CEO of a global ad fraud detection and prevention company, mFilterit, says fraudsters bank on a person's trust to pull off phishing scams. They use social engineering techniques to manipulate victims to take a certain action. Usually, they pretend to be authentic and trusted sources by crafting deceptive messages or emails that appear legitimate, like posing as a trusted organization or individual. Also, fraudsters continuously adapt their techniques to exploit vulnerabilities in technology.

Manish Mishra, CA and virtual CFO, believes that frauds succeed by exploiting vulnerabilities in behaviours and online practices. "Hackers capitalize on our consideration, interest, and desire for comfort. They may use state-of-the-art social engineering techniques to govern victims into divulging sensitive information," Mishra warns.





SYNTHETIC IDENTITY FRAUDS

This type of fraud involves creating a new identity by combining real and fake information. Fraudsters use these synthetic identities to open fraudulent accounts or obtain credit, making them difficult to detect.

HOW TO AVOID SYNTHETIC IDENTITY FRAUD

Preekshit Gupta, Vice President, APAC & MEA of no-code decisioning platform Bureau has the following advice:

- Be cautious and sceptical of unsolicited communications that request personal or financial information.
- Take the time to verify the legitimacy of the sender or caller before sharing sensitive details. Make sure you verify the numbers online to check if they are actually from the business name they are using.
- Always ensure that you have reliable security software installed on your devices and keep it updated to detect and prevent new fraud techniques.
- Double-check the authenticity of UPI handles and websites before making any transactions.
- Stay informed about the latest fraud techniques and scams, and regularly monitor your transaction history for any suspicious activity.