Cyber fraud in the time of covid-19

sanskritiias.com/current-affairs/cyber-fraud-in-the-time-of-covid-19

(Mains GS 3 : Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges & Basics of cyber security; money-laundering and its prevention)

Context:

- As India grapples with the second covid wave, cybercriminals are working overtime to take advantage of the situation.
- There are already many incidents of fraud involving vaccines, donations, etc.
- Cybercriminals posed as bank officials and offered loan moratorium for a “fee" and there were fake UPI (unified payment interface) handles for the PM CARES Fund.

Growing cybercrimes and vulnerability:

- According to the Norton Cyber Safety Insights Report by NortonLifeLock, a cybersecurity firm, nearly 120 million people experienced cybercrime between February 2020 and 2021.
- It could worsen more in 2021 as people continue to work from home and use online services more often.
- Internet banking penetration has increased as even in rural areas, mobile banking transactions are on the rise.
- But the awareness about cybercrimes has not kept pace in proportion which makes many easy targets.
- New hubs of cybercrimes have mushroomed like the infamous Jamtara in Jharkhand, gangs now operate out of Bharatpur in Rajasthan, Mewat in Haryana, etc.

Cyber frauds and ways to protect:

COVID-19 TESTING:

- As the number of covid cases rises, laboratories are unable to keep up with the demand for tests.
- Cybercriminals are taking advantage of the clogged system.
- There have been cases where people booked tests online with little-known labs, which turned out to be frauds.
- The scammers even visit the victim's house and collect the sample and later, they either don't provide a report or send a fake one.
- **The caution:** Book a test with a lab approved by the Indian Council of Medical Research.
- If someone comes across a new lab, do an online search by typing the company name and adding 'fraud' to it.
- There is a good probability that victims would have talked about it on social media.

JABS AND DRUGS:

- As the vaccination drive started, the government allowed individuals to book appointments online on a platform called Co-WIN for registrations.
- Cybercriminals started releasing apps with Co-WIN as part of their names.
- There have been instances where cybercriminals made fake websites asking people to pre-book vaccines by paying upfront.
- Bogus websites have been selling drugs like remdesivir that are in short supply.
- Scammers even stole data pretending to be government officials wanting to track the progress of those who are vaccinated.
- They ask individuals to upload personal details and identity documents for such tracking.
- In the past year, over 27 million Indians were victims of identity theft, according to the NortonLifeLock report.
- **The caution:**When downloading an app, look at the creator and Verify whether it's from an official source or not.
- "Guard your documents diligently as cybercriminals can use Aadhaar, PAN card and mobile number details in many ways.
- By stealing your identity, they can take loans in your name, open bank accounts and get illegal money transferred and even carry out SIM-swap fraud.

DONATIONS AND CHARITIES:

- Social media is full of people asking for help.
- Many individuals have taken initiatives to provide support to the needy, and they ask their friends on Twitter or Facebook to contribute if they wish.
- Cybersecurity experts warn that it's possible for cybercriminals to fake such initiatives and ask for contributions.
- **The Caution:** If someone wants to donate, preferably give money to an established NGO.

- Criminals are known to have used hacked Facebook or Twitter accounts and reached out to followers or people on the friends’ list and asked for monetary help.
- Thus avoid sending money to someone unless you have confirmed it’s the same person seeking help.

Conclusion:

- Thus for avoiding cyber fraud, add two-factor authentication to your accounts.
- This provides another layer of security by requiring two steps to gain access to your account.
- Avoid putting your mobile number, date of birth and other details online and be suspicious of all unknown incoming messages, emails or calls.