

People lose ₹3 crore to cybercrime across Maha daily, says DIG Shintre

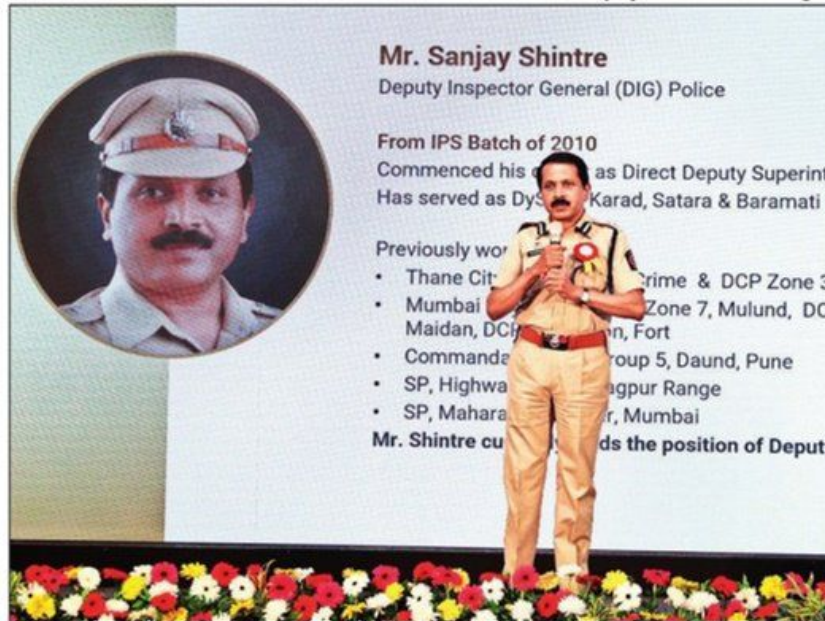
Shashank.Didmishe
@timesgroup.com

Pune: Barely Rs 134 crore or 10% of the total Rs 1,300 crore lost to cybercrime in Maharashtra since 2019 have been recovered through police investigations, deputy inspector general of police Sanjay Shintre in the city said on Saturday.

“The police force has a working system to tackle cybercrimes, but it is not strong enough. The cybercrime police in the state receive roughly 4,000-5,000 calls every day from the cybercrime victims. The daily monetary loss to cybercrimes is Rs 3 crore in Maharashtra,” Shintre said at an event organised by cybersecurity solution firm Quick Heal Technologies.

The event was aimed at increasing cybersecurity awareness and recognition efforts of students, teachers and institutions in spreading cybersecurity initiatives.

Maharashtra saw 8,249 cybercrime cases in 2022, which was 48% higher than 5,562 incidents recorded in the previous year, National



Pic courtesy: Quick Heal Technologies

WIDE NET: DIG Sanjay Shintre says the cybercrime police units in the state receive roughly 4,000-5,000 calls every day from victims

Crime Records Bureau (NCRB) data showed. At the national level, as many as 65,893 cases were reported in 2022, the data revealed.

The Maharashtra govt's cybersecurity project is expected to be rolled out in the coming months, Shintre said, adding that there were six verticals under the project, including command, security operations and network operations centres.

Around 140 engineers will take complaints on a helpline under the project. These

complaints will be directed to respective police stations, while a major number of case will be investigated in the central cell.

In many cases, migrant workers fall for online scams while looking to augment their incomes. When a fresh graduate from a rural area comes to the city in search of a job, s/he realises that monthly salary is not enough to make ends meet. This is when s/he starts looking at

ways to make additional money. Cybercriminals latch on to such people by using prevalent baits on social media and other websites, he said.

Shintre also referred to 'sunk-cost fallacy'. The term means that despite the victims suspecting that they are likely to be duped, they continue to engage in the 'suspicious' activity as they have invested time and money into it and partly in expectation of getting something out of it. “The criminals have recognised this behaviour of the victims and they exploit it fully to their advantage,” Shintre said.

Cybercriminals have even created fake online profiles of police officers and other authorities, which they use to intimidate the victims. “These criminals lure the victims to join on a video call. Criminals posing as police officers then ask them [the victims] to make payments,” Shintre said.

In India, cybercriminals target 1-2 crore people every day. There are 120 crore internet users in India, 80% of these use smartphones, data available with various agencies showed.