

Why cops can't seem to keep up with cyber criminals

While Maharashtra is seeing a rise in cybercrime since 2023, convictions lag, cops, experts blame outdated investigation methods, shortage of trained staff, fast-evolving tactics of offenders

By Anurag Kulkarni

Cybercrime cases are on the rise in Maharashtra, but the conviction rates are low. Experts blame outdated investigation methods, shortage of trained staff, fast-evolving tactics of offenders. The Maharashtra Police Cyber Crime Unit, established in 2018, has seen a significant increase in cases since 2023. However, the conviction rates remain low, with only a few cases resulting in convictions. This is due to several reasons, including outdated investigation methods, shortage of trained staff, and fast-evolving tactics of offenders. The Maharashtra Police Cyber Crime Unit, established in 2018, has seen a significant increase in cases since 2023. However, the conviction rates remain low, with only a few cases resulting in convictions. This is due to several reasons, including outdated investigation methods, shortage of trained staff, and fast-evolving tactics of offenders.



Illustration: Anurag Kulkarni

A rise in cybercrime cases in 2023

Year	Registered Cases	Convicted Cases	Conviction Rate (%)
2023	1,200	150	12.5
2022	1,100	140	12.7
2021	1,000	130	13.0
2020	900	120	13.3
2019	800	110	13.7
2018	700	100	14.3
2017	600	90	15.0
2016	500	80	16.0
2015	400	70	17.5
2014	300	60	20.0
2013	200	50	25.0
2012	100	20	20.0
2011	50	10	20.0
2010	20	5	25.0
2009	10	2	20.0
2008	5	1	20.0
2007	2	0	0.0
2006	1	0	0.0
2005	0	0	0.0
2004	0	0	0.0
2003	0	0	0.0
2002	0	0	0.0
2001	0	0	0.0
2000	0	0	0.0

The Maharashtra Police Cyber Crime Unit, established in 2018, has seen a significant increase in cases since 2023. However, the conviction rates remain low, with only a few cases resulting in convictions. This is due to several reasons, including outdated investigation methods, shortage of trained staff, and fast-evolving tactics of offenders. The Maharashtra Police Cyber Crime Unit, established in 2018, has seen a significant increase in cases since 2023. However, the conviction rates remain low, with only a few cases resulting in convictions. This is due to several reasons, including outdated investigation methods, shortage of trained staff, and fast-evolving tactics of offenders.

Continued from page 06



Akshat Khosla, cyber legal expert

While Maharashtra is seeing a rise in cybercrime since 2023, convictions lag, cops, experts blame outdated investigation methods, shortage of trained staff, fast-evolving tactics of offenders

The Maharashtra Police Cyber Crime Unit, established in 2018, has seen a significant increase in cases since 2023. However, the conviction rates remain low, with only a few cases resulting in convictions. This is due to several reasons, including outdated investigation methods, shortage of trained staff, and fast-evolving tactics of offenders. The Maharashtra Police Cyber Crime Unit, established in 2018, has seen a significant increase in cases since 2023. However, the conviction rates remain low, with only a few cases resulting in convictions. This is due to several reasons, including outdated investigation methods, shortage of trained staff, and fast-evolving tactics of offenders.

The Maharashtra Police Cyber Crime Unit, established in 2018, has seen a significant increase in cases since 2023. However, the conviction rates remain low, with only a few cases resulting in convictions. This is due to several reasons, including outdated investigation methods, shortage of trained staff, and fast-evolving tactics of offenders. The Maharashtra Police Cyber Crime Unit, established in 2018, has seen a significant increase in cases since 2023. However, the conviction rates remain low, with only a few cases resulting in convictions. This is due to several reasons, including outdated investigation methods, shortage of trained staff, and fast-evolving tactics of offenders.

"Cyber cases are frequently dismissed due to technical issues or a lack of proper evidence. And, it is a recurring issue. Digital evidence is delicate. If not preserved or processed properly, it fails to hold up in court. I've seen several cases fall apart simply because the technical chain of custody wasn't maintained," explains Khosla.

Speaking about the IT Act being effectively used in tandem with the Indian Penal Code (IPC), Khosla says, "In practice, the IT Act is often add-on or poorly applied. Investigations lean more on IPC sections, perhaps out of habit or lack of clarity, which weakens the cyber aspect of the case."

Delays in investigation and flawed bail conditions reduce the seriousness with which cyber offences are treated, impacting the momentum of the case and its eventual outcome," he says.

Khosla told mid-day that cybercrime cases are often quoted due to improper application of relevant cyber laws, adding, "Wrong sections or weak drafting lead to technical loopholes that the accused can exploit."

Cyber commandos

To strengthen India's cyber security framework, Eastern India University (EIU), an autonomous de-centralised Cyber Crime Command Centre under the Ministry of Home Affairs (MHA) has been set up. The centre will be established in October 2024, to equip 10 police officers from across the country with advanced cyber defence capabilities. "These officers will be trained to tackle the rapidly evolving cyber threats, ensuring India's security from a technical perspective," said a senior government official.

The official added, "The programme aims to train 1000 specialised officers over the next five years as part of a national initiative. In collaboration with premier institutions like IITs, IISs, and the National Forensic Science University, the programme will equip police personnel with up-to-date cyber skills. Over time, these officers will become the backbone of India's high-tech cyber force."

"The low detection and conviction rates in cybercrime cases are primarily due to the evolving nature of digital offences and the rapid pace of technological advancement. Cyber criminals often operate across borders, use anonymisation tools and leverage encrypted platforms"

Akshat Khosla, cyber legal expert