BATTLING THE Dark Side of Technology

With over 900 million internet users, India is witnessing an alarming surge in cybercrime, proving that technology's double-edged sword cuts deeper than ever. The darker side of the digital revolution is growing more sinister, fueled by rising cases of cyberbullying, digital arrests, sextortion, identity theft and financial fraud. Thankfully, warriors like **Akshat Khetan,** founder, AU Corporate Advisory and Legal Services and cofounder, WHT NOW (NGO dedicated to reducing cybercrime in India), are helping us fight this menace. In this eye-opening discussion, he talks about technology's grim underbelly and how we can stay safe


Akshat Khetan

By Ekta Katti

Corporate Citizen: Technology empowers us, but it's also misused for cyberbullying, scams and fraud. Do you think we're losing control over how technology is being weaponised?

Akshat Khetan: Like every coin, technology has two sides. While it's a powerful force for progress, its misuse is spiralling out of control. Yes, I believe we're struggling to keep up with how rapidly it's being weaponised. Be it through cyberbullying, phishing, investment scams, malware or even digital arrests. These threats show just how easily technology can be turned against us, and frankly, our grip on it seems to be slipping.

The problem—innovation moves faster than regulation. Technology evolves at breakneck speed, leaving laws and security measures playing catch-up. Criminals exploit our growing reliance on digital systems, finding loopholes faster than we can patch them.

However, we can overcome this. The first step is awareness. Educate people about online risks and safe practices. Stronger cybersecurity laws and global cooperation can help rein in misuse. If we remain vigilant, advocate for smarter policies, and build a culture of responsibility, we can steer technology back toward its true purpose, which is to empower humanity, not harm it. It won't be easy, but with the right approach, we can reclaim control.

CC: Cybercrimes are rising at an alarming rate. What's driving this surge? Is it greed, anonymity, or just easier ways to exploit people?

Studies suggest that by the end of 2025, cyberattacks are projected to cost the world a staggering $10.5 trillion annually. Just imagine the scale. This kind of money is enough to tempt anyone into crime. A dangerous mix of greed, desperation and technology, is driving this surge. Greed is a major factor, but so is survival, especially in an unequal world. The internet provides criminals with near-perfect anonymity, thanks to AI-generated identities, VPNs and encrypted channels. Worse, technology has lowered the barrier to fraud as phishing, fake websites and scams, now require only basic skills to execute. Yet, despite the growing threat, many remain unaware of even the simplest online safety measures. This results in a perfect storm of greed, anonymity and accessible tools, fuelling an unstoppable wave of cybercrime.

CC: From a psychological standpoint, why do you think some people turn to online harassment or fraud?

Everyone is fighting a battle, some with the world, others with themselves. For certain individuals, psychological triggers

like frustration, narcissism, impulsivity or a lack of empathy, push them toward harmful actions. The online world, with its anonymity and perceived lack of consequences, becomes the perfect breeding ground for such behaviour. Some seek power or validation, others are driven by financial gain or personal agendas. Social influences and toxic online cultures further normalise aggression, while repeated exposure desensitises them to the harm they cause. The digital space lowers barriers. Manipulation, deception and exploitation, become easy and high-reward activities with minimal risk. Ultimately, it's a toxic mix of personality traits, environmental factors, and opportunity that fuels this behaviour. That's why prevention, education and strict accountability, are crucial in combating it.

CC: Many people, especially teens, experience bullying on WhatsApp, gaming platforms or social media. What should victim (or their parents) do first when this happens? Similarly, how can senior citizens handle such situations?

It is unfortunate that you had to face this situation. Here's what you can do next:

Don't respond, instead document:

- Avoid engaging or replying to the message.
- Take a moment to breathe and stay calm.
- Preserve all evidence. Save screenshots, messages and any relevant details.

Block and report:

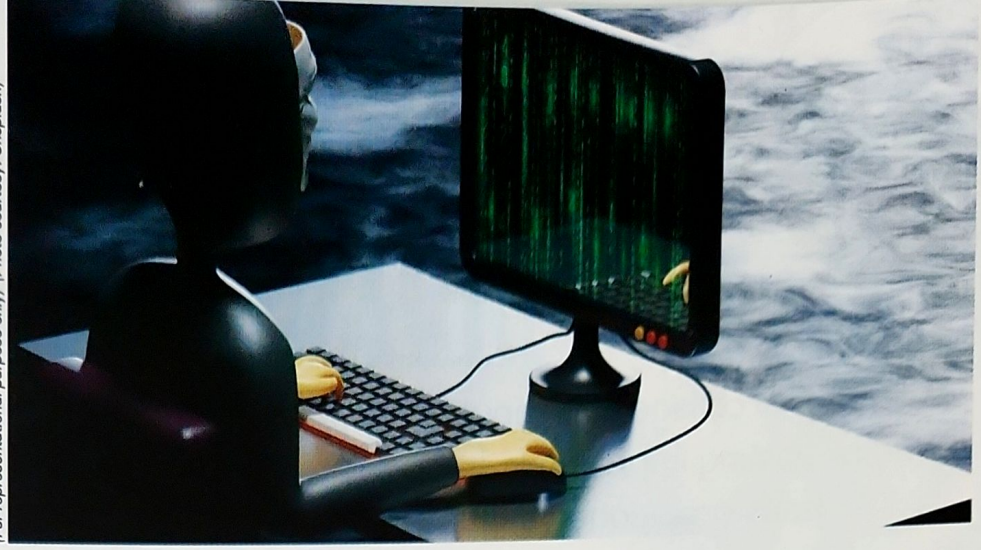
- Block the harasser on all platforms to prevent further contact.
- Report the incident through the platform's official reporting system.

Seek support:

- Reach out to trusted friends or family members for emotional support.
- Get immediate expert assistance, guidance and referral support for cases related to cyber abuse, harassment and online threats.

Contact authorities:

- In India, cyberbullying is punishable under the Information Technology Act 2000, and relevant sections of the Indian Penal Code.
- You can file a complaint with your local cybercrime police for investigation and legal action.
- Early reporting increases the chances of stopping the harassment effectively.



(For representational purpose only) (Photo courtesy: Unsplash)

Technology evolves at breakneck speed, leaving laws and security measures playing catch-up. Criminals exploit our growing reliance on digital systems, finding loopholes faster than we can patch them
— Akshat Khetan

CC: We've seen a spike in scams where fraudsters pose as police or CBI, threatening arrest unless victims pay up. How do these criminals manipulate people so effectively?

Police or CBI impersonation scams exploit fear and urgency. Fraudsters call victims, falsely claiming a case is filed against them, and threaten arrest unless immediate payment is made. Panicked victims often pay via untraceable methods, via bank transfers, digital wallets, before realising it's a scam. These crimes are punishable under IT Act 2000: Sections 66C (identity theft), Section 66D (cheating by impersonation). Under Bharatiya Nagarik Suraksha Sanhita, 2023: Sections 316 (cheating), 317 (fraudulent deeds), 318(2) (criminal intimidation), 351 (false representation).

Stay alert, real officers never demand immediate payments over calls.

CC: These crimes may never fully disappear, but how can we reduce them?

While such crimes may never be fully eradicated, they can certainly be significantly reduced. Raising awareness is crucial, as many people remain unaware of the risks or how to safeguard themselves. Educating the public empowers them to recognise threats and avoid becoming victims.

However, awareness alone is insufficient, stronger laws and better enforcement are equally vital. Strict legislation serves as a deterrent, ensuring harsher consequences for offenders, while well-trained law enforcement agencies must act swiftly and effectively to address these crimes.

Ultimately, the most effective solution lies in a combined approach with public education, robust legal frameworks, and efficient policing. Collaboration among governments, law enforcement and citizens, is essential to create lasting change and fostering a safer society.

CC: Your NGO, WHT NOW, fights cybercrime daily. Can you share a story where your team made a real difference?

WHT NOW, is a bold initiative where we tackle the alarming rise in cybercrime across India. One incident that stands out involved a 16-year-old girl from a tier 2 city, who was being blackmailed by an online predator with her morphed photos. Overnight, her spark faded, grades dropped, and silence took over the once bubbly girl. Her friend anonymously alerted our helpline. Within hours, our team traced the predator's digital trail, coordinated with police for swift arrest and provided counselling to help her heal. Today, she's acing her board exams and educating her peers on digital safety. This is a reminder of why we do what we do.

CC: Any advice for our readers?

Stay vigilant. Guard your data, use strong passwords and avoid suspicious links. Pause before you post, verify sources, mind your digital trail and stop misinformation. Report cybercrimes, demand ethical tech and spread awareness. The internet's power lies in our hands. With vigilance and collective effort, we can build a safer digital world for all.

(ekta.katti@corporatecitizen.in)