© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1717774

Why Cybercrime Keeps Winning: A Plain Look at The Root Causes and What the Law Can Do About It

HARNOOR SINGH[1], MINI SRIVASTVA[2]
[1, 2]*BA.LLB(H), Final year, Amity University, Noida*

Abstract*—Every day, millions of people lose money, data, and peace of mind to cybercrime. The standard response — more laws, tougher penalties, better software — has not stopped the problem from growing. This paper argues that the real causes run deeper: most people simply do not know enough about online risks to protect themselves; weak password habits leave accounts wide open; individuals and businesses alike lack the practical skills to respond when something goes wrong; and criminals are quick to twist every new piece of technology into a weapon. None of these are purely technical problems. They are human and institutional ones, and they call for human and institutional answers. The paper examines each cause in plain terms, draws on legal frameworks from India and other jurisdictions, and offers practical steps for lawmakers, law enforcement, schools, and the private sector.

Keywords: *Cybercrime, Digital Literacy, Password Security, Cybersecurity Law, Information Technology Act, Social Engineering, Technology Misuse, Cyber Policy.*

I. INTRODUCTION

The internet has become as essential as electricity, but the same shift that made our lives more connected has also made us more exposed. Every new account we create, every password we reuse, every link we click without checking is a door that a criminal could potentially walk through.

Cybercrime has grown alongside digital life. It is no longer the preserve of solitary, technically gifted hackers. Today it ranges from a teenager guessing a weak password on someone's email account to organised criminal groups running ransomware operations against hospitals and power grids.

Enforcement is hard when criminals operate across borders under pseudonyms. Courts struggle with digital evidence. And the people most at risk — ordinary users with limited technical knowledge — are rarely the audience for legal reform.

This paper takes a different starting point. Instead of asking what new offence should be created or what sentence should be increased, it asks: why does cybercrime keep finding so many willing victims? The answer, as the following sections show, lies less in any particular software vulnerability and more in the habits, knowledge gaps, and institutional failures that make criminal exploitation so consistently easy.

The paper is structured around four root causes. Part II covers the awareness problem: most people do not really understand online risk, and that ignorance is something criminals count on. Part III looks at passwords — the single most widespread security mechanism and the single most widely abused one. Part IV examines the broader knowledge gap in cybersecurity, from individual users all the way to small businesses. Part V turns to the misuse of technology itself — both by deliberate criminals and by ordinary users who inadvertently create vulnerabilities. Part VI draws everything together and suggests what governments, courts, schools, and companies can actually do. A brief conclusion follows.

The approach is straightforward: plain language, grounded in real legal frameworks, with no jargon where plain words will do.

II. THE AWARENESS PROBLEM: NOT KNOWING WHAT YOU DO NOT KNOW

2.1 Awareness Is Not the Same as Knowledge

There is a difference between knowing that something dangerous exists and knowing enough about it to stay safe. A person might have heard that phishing scams are common without having any idea how to spot one. That gap — between vague awareness and practical understanding — is exactly where criminals operate.

Think of it like fire safety. Knowing that fires are dangerous is useful up to a point. But knowing what to do when smoke fills a room, where the exits are, and why you should stay low — that is what keeps you alive. Digital safety works the same way.

General awareness campaigns that say 'be careful online' rarely give people the specific, actionable knowledge they need to make better decisions in real situations.

India's Information Technology Act, 2000 sets out detailed rules about what is and is not permitted online. But its practical value to ordinary users depends almost entirely on whether those users know it exists, understand which situations it covers, and feel capable of using it. Most do not. The statute is well-drafted in many respects; its weakness is not legal but social — the population it is meant to protect largely cannot access its protection.

2.2 Where Awareness Breaks Down

Awareness fails in three consistent ways. The first is that people cannot recognise threats when they see them. Modern phishing emails do not look like obvious scams anymore. They copy the visual design of real banks and government agencies down to the last detail. Domain names differ from the genuine article by a single letter. Messages include personal details scraped from social media. Against this level of craftsmanship, telling someone to 'be alert' is almost useless unless they know specifically what to look for.

The second failure is that people underestimate consequences. Sharing a one-time password over the phone feels minor. Clicking a link that looks like it came from a courier company feels harmless. The connection between these small actions and losing an entire bank balance, or having personal photographs stolen and threatened for release, is not obvious until it is too late. Research in behavioural psychology has consistently shown that people are poor at estimating the real cost of low-probability, high-impact events — and cybercriminals have learned to exploit exactly that tendency.

The third failure is geographic and demographic. In India, the rollout of cheap smartphones and affordable data has brought hundreds of millions of new users online in rural and semi-urban areas. Many are first-generation internet users. They have not had years of informal exposure to online norms that might have built up some instinctive caution. They are often the targets of the crudest and most damaging scams, precisely because nobody has sat them down and explained the basics.

2.3 The Legal and Institutional Gap

When victims do not know they have legal recourse, the justice system cannot help them.Others assume nothing will come of a report. The result is systematic underreporting that makes the official picture of cybercrime look far smaller than it really is — and gives legislators and police forces a distorted basis for deciding where to focus resources.

The responsibility for closing this gap does not rest with any single institution. Schools need to teach digital literacy as seriously as they teach road safety. Employers need to train their staff. Community organisations working in rural areas need to reach people who may never interact with formal educational institutions as adults. The law can help by creating incentives — or requirements — for these things to happen, rather than assuming they will happen on their own.

III.THE PASSWORD PROBLEM: A DAILY SECURITY FAILURE

3.1 Why Passwords Matter So Much

Before anyone can access a digital service — a bank account, an email inbox, a company database — their identity has to be verified. For the vast majority of services, that verification rests on a single password. The password is simultaneously the most universal security tool in existence and the one that people handle most carelessly.

A genuinely strong password — random, long, unique to each account — is extremely difficult to crack by automated means. The problem is that almost nobody uses one. Remembering dozens of strong, unique passwords is cognitively demanding, and most people, when faced with that burden, take the path of least resistance. They pick something familiar. They reuse what they already have. They write it on a sticky note. The result is a layer of security that looks solid in design but is riddled with holes in practice.

3.2 The Three Ways Passwords Go Wrong

The first way is simple weakness. Every year, after major data breaches expose millions of credentials to analysis, the same story emerges: an enormous proportion of users rely on passwords like '123456', 'password', their own name, or their date of birth. These can be cracked in seconds by automated tools that work through common options first. This is not just a problem among older or less tech-savvy users.

Studies have found predictable passwords throughout all age groups and education levels, suggesting the issue is structural — the way services are designed — as much as individual.

The second way is reuse. When the same password protects an email account, an online banking portal, and a shopping website, a breach of any one of them puts all of them at risk. Attackers know this and routinely test stolen credentials against popular services — a technique called credential stuffing. It works because reuse is so widespread. A leak from a minor website thus becomes the key to something far more serious.

The third way is negligence over time. People keep passwords long after they should have been changed. They share them with family members or colleagues without thinking about what access that actually grants. These habits may seem harmless in any individual case, but collectively they keep the door to criminal exploitation permanently ajar.

3.3 How Attackers Exploit It

Brute force attacks run through possible combinations systematically until they hit the right one.All of these are fast and effective against weak credentials, slow and prohibitively expensive against strong ones.

3.4 Legal Responsibility

Who bears responsibility when a weak password leads to a breach? The answer is not straightforward. Users who adopt manifestly inadequate passwords may, in certain civil proceedings, be found to have contributed to their own loss. But service providers also carry obligations. Both sides of this equation matter, and the law is still working out the right balance

IV.THE KNOWLEDGE GAP: WHEN AWARENESS IS NOT ENOUGH

4.1 The Distance Between Knowing and Acting

Being told that phishing exists is not the same as being able to spot a phishing email. Understanding that ransomware is dangerous is not the same as knowing how to respond when your organisation's files are suddenly encrypted. The gap between surface-level awareness and the practical knowledge needed to act effectively is where most cybersecurity education currently falls short — and where cybercriminals reliably find their opening.

Good cybersecurity education is specific. It explains not just that social engineering attacks exist but how they work: what psychological buttons they push, what the warning signs look like, and what a legitimate organisation would actually do in the same situation.

4.2 Social Engineering: Fooling People, Not Machines

Social engineering is the umbrella term for attacks that manipulate human psychology rather than exploiting technical vulnerabilities. It is, by almost every measure, the most effective and most commonly used class of attack in operation today. The reason is straightforward: human beings are easier to deceive than well-designed software.

The most reliable social engineering techniques work by creating urgency, invoking authority, or triggering fear. An email that says 'your account will be closed in 24 hours unless you verify your details' creates panic that short-circuits careful thinking

Protecting people against social engineering requires more than awareness posters. It requires specific, repeated education about the techniques involved, combined with institutional protocols that reduce the scope for manipulation. Banks and government agencies should communicate clearly and consistently that they will never request sensitive information through unsolicited contact — and users need to know this, not just hear it once and forget it.

4.3 Businesses Are Not Much Better

The knowledge gap is not confined to individual users. Small and medium-sized businesses — which make up the majority of enterprises in most economies, including India's
— often have equally significant deficits. The owner of a small shop who has moved their accounts online may have no idea that storing customer data in an unencrypted spreadsheet, using the same password for their banking and their email, or running years-old unpatched software creates serious legal exposure as well as practical risk.

Data protection law imposes real obligations on businesses of all sizes. The fact that many small businesses are unaware of those obligations does not reduce them. Regulators have increasingly taken the

view that ignorance of the law is no defence — and that proportionate enforcement against small organisations is necessary to create genuine sector-wide incentives for improvement. At the same time, the law can only work if the standards it demands are explained clearly and compliance assistance is available to those who want it but lack the expertise to know where to start.

4.4 When a Crime Happens: The Response Knowledge Gap

One of the most overlooked aspects of cybersecurity knowledge is knowing what to do after something goes wrong. Most individuals and many businesses have no plan. They do not know how to preserve digital evidence in a way that will be useful to investigators. They do not know what they are legally required to report, to whom, and within what timeframe. They do not know which immediate actions might contain the damage and which might inadvertently make things worse.

Digital evidence is fragile. Restarting a compromised computer, deleting suspicious files, or running an antivirus scan without guidance can destroy the forensic trail that investigators need. Post-incident response is a skill, not an instinct — and without it, the chances of identifying perpetrators, recovering losses, or successfully prosecuting offenders are significantly reduced. Building this knowledge into business training programmes and consumer guidance is as important as any preventive measure.

V.THE MISUSE OF TECHNOLOGY: WHEN TOOLS BECOME WEAPONS

5.1 Every Tool Has Two Edges

Digital technology is not inherently dangerous. The same platform that lets a small business reach customers across the country can be used to run investment fraud at scale. The same cloud services that allow researchers to collaborate on cures for diseases can be rented by criminals to flood websites with traffic until they collapse. This is the dual-use problem, and it is not new — every major technological advance in history has been turned to harmful purposes by some people. What is new is the speed, scale, and accessibility with which digital tools can be misused.

Regulating this is genuinely difficult. A rule tight enough to eliminate the harmful uses will also restrict the beneficial ones. Striking the right balance requires ongoing, informed engagement between lawmakers, technologists, civil society, and the people most affected —an engagement that is often rushed, underfunded, or captured by the interests of powerful industry players.

5.2 The Range of Deliberate Misuse

At the sophisticated end, criminal actors write custom malware, identify and exploit vulnerabilities in widely-used software before patches are available, and run phishing operations at industrial scale using rented cloud infrastructure and stolen data. These require real technical skill and deliberate criminal intent, and they tend to produce the largest individual incidents — the hospital brought to its knees by ransomware, the financial institution drained by a coordinated fraud operation.

At the other end, people with minimal technical knowledge use freely available tools to perpetrate harassment, fraud, and blackmail. Creating a fake social media profile to deceive someone requires no coding ability whatsoever. Sending threatening messages anonymously, using a phone number obtained through a prepaid SIM, takes minutes. Distributing intimate photographs of an ex-partner without consent requires only a smartphone and a platform willing to host the content. The legal and institutional responses to high-sophistication attacks and low-sophistication attacks are often poorly calibrated to each other.

5.3 Ransomware: The Clearest Example

Ransomware has become the defining cybercrime of the current decade. In a ransomware attack, malicious software encrypts all of the victim's data and demands payment
— usually in cryptocurrency — in return for the key needed to decrypt it. Targets have included hospitals in the middle of treating patients, municipal governments unable to issue any services, and businesses that lost months of work in an instant.

Several features make ransomware particularly hard to address through existing legal frameworks. Cryptocurrency payments are difficult to trace and recover, though not impossible. Ransomware groups frequently operate from countries where effective legal cooperation with Indian or Western investigators is limited or non-existent. Victims face an agonising choice: pay the ransom and potentially fund future attacks, or refuse and risk permanent data loss — and in some jurisdictions, paying a ransom to

a sanctioned group may itself be illegal. None of these dilemmas are well-served by legal frameworks designed before ransomware existed in its current form.

5.4 Social Media and the Manufacture of Harm

Social media platforms have created extraordinary possibilities for connection and expression. They have also created infrastructure that criminals exploit with remarkable efficiency. Fake profiles impersonate banks, government agencies, celebrities, and individuals. Fraudulent investment schemes use algorithmic amplification to reach millions of potential victims. Harassment campaigns organise strangers against individual targets. Non-consensual intimate imagery is distributed at the click of a button.

Platform liability for this kind of content is one of the most contested legal questions of the moment. The broad immunity that early internet law extended to platforms — on the theory that they were neutral conduits, not publishers — is increasingly hard to justify for companies that actively curate content, profit from engagement, and have the technical capacity to identify and remove harmful material. The direction of legal reform across multiple jurisdictions points toward greater platform accountability, though the precise shape of that accountability remains contested.

5.5 Accidental Misuse

Not everyone who contributes to cybercrime does so intentionally. A user who clicks a malicious link without realising it, downloads an app that turns out to harvest their contacts, or connects to a fraudulent Wi-Fi network at a coffee shop becomes an unwitting participant in someone else's scheme. They are victims, not perpetrators — but their actions have real consequences for others.

This points to a regulatory approach that focuses on the design of technology rather than purely on the behaviour of users. Devices that update their security software automatically, services that require strong authentication by default, and networks that encrypt traffic without requiring users to configure anything — these reduce the scope for accidental misuse without demanding perfect behaviour from imperfect humans. Regulation that mandates secure design is, in this sense, more reliable than regulation that relies on individual vigilance alone.

VI. WHAT NEEDS TO CHANGE: PRACTICAL RECOMMENDATIONS

6.1 For Lawmakers

Cybercrime law needs to be written in technology-neutral language. Statutes that describe specific technical mechanisms become outdated as soon as technology moves on — which it does constantly. Laws that focus instead on the harm caused, and the intent behind the conduct, have a longer useful life and are easier to apply to novel situations.

Procedural law needs updating too. The rules governing how digital evidence is collected, preserved, and presented in court were largely written before digital evidence was common. They need to reflect current forensic practice clearly enough that investigators, lawyers, and judges are working from the same page. Mutual legal assistance treaties with other countries need to be strengthened and made faster to operate, because cybercrime does not respect borders and neither can enforcement.

Data protection obligations for service providers should be made clearer, more consistent, and more actively enforced. A business that stores user passwords in plain text, or that never requires users to change default credentials, should face real consequences — not because punishment is the goal, but because the credible threat of it creates the incentives needed to drive genuine improvement.

6.2 For Law Enforcement

Police forces at every level need dedicated cybercrime units with real technical capacity. At present, most state and district-level forces in India lack the training, tools, and specialist knowledge to investigate anything beyond the simplest cyber offences. That gap leaves the vast majority of cybercrime victims without meaningful law enforcement support. Investment in training, equipment, and staffing is not optional; it is the minimum required for the law to function as intended in this area.

Coordination between agencies — state police, central bodies, and international partners — also needs to improve. Cybercrime investigations regularly cross jurisdictional lines, and the current fragmentation of authority and communication creates delays and gaps that organised criminal groups actively exploit.

6.3 For Schools and Educational Institutions

Digital literacy should be a core part of school curricula, taught with the same seriousness as mathematics or language. This does not mean technical computing classes, though those have their place. It means teaching children and young people to think critically about what they encounter online: how to check whether a source is genuine, what personal information is safe to share and with whom, what their rights are when something goes wrong, and where to get help.

Adult education matters equally. Many of the people most at risk of cybercrime — older adults, first-generation smartphone users, people in rural areas encountering digital financial services for the first time — are not being reached by current awareness efforts. Community-based programmes, delivered in local languages through trusted local institutions, are more likely to reach these groups than national campaigns delivered through digital channels they may not regularly use.

6.4 For Businesses and Technology Companies

Technology companies have more power to reduce cybercrime than any other single actor, and more responsibility than they currently accept. Requiring strong passwords by default, building multi-factor authentication into all sensitive services, automatically updating security software, and designing products that are secure out of the box rather than requiring users to configure security themselves — these steps would have a larger aggregate effect than almost any legislative measure. Financial institutions should invest seriously in fraud detection systems that can identify unusual patterns before money leaves an account. Clear, consistent public communication about what a bank will and will not ask customers to do would substantially reduce the effectiveness of impersonation-based scams. Civil society organisations have a role in holding both governments and companies accountable for the commitments they make — and in ensuring that the voices of ordinary users, rather than just industry lobbyists, are heard in the policy debates that shape this area.

VII.CONCLUSION

Cybercrime is winning, at least for now, because it consistently finds the same weaknesses: people who do not know enough to protect themselves, passwords that should never have been accepted, organisations that treat security as a compliance checkbox rather than a genuine priority, and a legal system that is perpetually a step or two behind the threat it is trying to address.

None of these weaknesses are inevitable. They are the product of choices — choices made by individuals, by institutions, by legislators, and by companies — and different choices can produce different outcomes. The awareness deficit can be narrowed through sustained, practical education that reaches people where they are, not just where we wish they were. The password problem can be substantially reduced through better service design and clearer legal requirements. The knowledge gap in businesses and institutions can be addressed through accessible guidance, proportionate enforcement, and a regulatory culture that treats security as a shared responsibility. Technology misuse can be constrained through smarter product regulation, greater platform accountability, and international legal cooperation that actually functions.

There is no single fix. Cybercrime is too varied, too adaptable, and too deeply connected to ordinary human behaviour for any one intervention to solve it. But the cumulative effect of serious action across all these fronts would be substantial. The tools, the knowledge, and the legal frameworks to act are largely available. What has been missing, in too many places, is the sustained political will and institutional coordination to use them.

The stakes are high enough to make that investment worthwhile. Digital infrastructure now underpins healthcare, finance, governance, and social life. Its security is not a specialist concern for technologists; it is a fundamental public interest. Treating it as such — with the same seriousness and the same allocation of resources that we bring to physical security — is overdue.

BIBLIOGRAPHY

A. Legislation and International Instruments

[1] Information Technology Act, 2000 (Act No 21 of 2000), as amended by the Information Technology (Amendment) Act, 2008 (Act No 10 of 2009).

[2] Indian Penal Code, 1860 (Act No 45 of 1860), ss 415–420, 463. Personal Data Protection Bill,

2019 (India).
[3] Computer Misuse Act 1990 (c 18) (United Kingdom).
[4] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1. Council of Europe, Convention on Cybercrime (Budapest Convention) ETS No 185 (2001). NIST Special Publication 800-63B, Digital Identity Guidelines (2017, updated 2020).

B. Books
[5] Brenner SW, Cybercrime: Criminal Threats from Cyberspace (Praeger 2010). Clough J, Principles of Cybercrime (2nd edn, Cambridge University Press 2015).
[6] Hadnagy C, Social Engineering: The Science of Human Hacking (2nd edn, Wiley 2018).
[7] Mitnick KD and Simon WL, The Art of Deception: Controlling the Human Element of Security (Wiley 2002).
[8] Wall DS, Cybercrime: The Transformation of Crime in the Information Age (Polity Press 2007). Yar M and Steinmetz KF, Cybercrime and Society (3rd edn, SAGE 2019).

C. Articles
[9] Bada M, Sasse AM and Nurse JRC, 'Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?' (2019) 14 International Journal of Cyber Criminology 79.
[10] Florencio D and Herley C, 'A Large-Scale Study of Web Password Habits' (2007) WWW Conference Proceedings 657.
[11] Hadlington L, 'Human Factors in Cybersecurity' (2017) 3(7) Heliyon e00346.
[12] Hutchings A and Hayes H, 'Routine Activity Theory and Phishing Victimisation' (2009) 9 Current Issues in Criminal Justice 433.
[13] Sasse MA, Brostoff S and Weirich D, 'Transforming the Weakest Link' (2001) 4 BT Technology Journal 122.

D. Reports
[14] National Crime Records Bureau, Crime in India 2022 (MHA 2023).
[15] NASSCOM, Cybersecurity in India: Landscape, Threats and Opportunities (2021). Verizon, Data Breach Investigations Report 2023 (Verizon Business 2023).
[16] World Economic Forum, Global Risks Report 2023 (WEF 2023). ENISA, Threat Landscape 2023 (ENISA 2023).
[17] NITI Aayog, Data Empowerment and Protection Architecture Discussion Paper (2020).

ENDNOTES
[18] [1] Information Technology Act, 2000 (Act 21 of 2000) s 43; Information Technology (Amendment) Act, 2008, s 66 (computer-related offences).
[19] [2] Jonathan Clough, Principles of Cybercrime (2nd edn, CUP 2015) 3–10.
[20] Verizon, Data Breach Investigations Report 2023 (Verizon Business 2023) 6 (74% of all breaches involve the human element).
[21] Maria Bada, Angela Sasse and Jason Nurse, 'Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?' (2019) 14 International Journal of Cyber Criminology 79, 83–84.
[22] National Crime Records Bureau, Crime in India 2022 (MHA 2023) ch 11, Table 11.2.
[23] Dinei Florencio and Cormac Herley, 'A Large-Scale Study of Web Password Habits' (2007) WWW Conference Proceedings 657, 658.
[24] MA Sasse, S Brostoff and D Weirich, 'Transforming the Weakest Link' (2001) 4 BT Technology Journal 122, 127.
[25] Chris Hadnagy, Social Engineering: The Science of Human Hacking (2nd edn, Wiley 2018) ch 2.
[26] Council of Europe, Budapest Convention, ETS No 185, Arts 2–6.
[27] ENISA, Threat Landscape 2023 (ENISA 2023) 12–19 (ransomware identified as prime threat category for the fourth consecutive year).
[28] World Economic Forum, Global Risks Report 2023 (WEF 2023) 8.