A Quarterly insight to Cyber Law!

Cyber Niyam means rules of the Cyberspace. This quarterly newsletter aims to create awareness about the rules and regulations of cyberspace, cyber security and data protection. This is also an effort to create awareness about digital safety, trending cybercrimes and effective reporting mechanisms.

V.P SHINTRE & ASSOCIATES
Legacy since 1935.

CYBER NIYAM

By V.P Shintre & Associates *www.vaishalibhagwat.com*

Issue 2 of 2025 – April, 2025

In this Issue

LEGAL LANDSCAPE

A primer on Data Protection and Data Privacy

Chapter 1: Cyber Security and Its Core Principles: People, Process, and Technology

Introduction Cybersecurity is the discipline dedicated to protecting computer systems, networks, data, and programs from digital attacks, damage, or unauthorized access. As cyber threats grow more complex and widespread, cybersecurity is becoming a foundational concern across every sector—from governments and businesses to educational institutions and individuals.

To effectively safeguard digital infrastructure and information, cybersecurity is built on three critical pillars: People, Process, and Technology. These components must operate together to ensure a resilient, secure, and compliant environment.

1. People: The Human Element of Cybersecurity

People are often regarded as the weakest link in the cybersecurity chain, yet they can also be the strongest defence when properly informed and engaged. Employees, IT staff, contractors, and end users all play crucial roles in identifying threats and following good security practices.

.....Continued on page 2

- **Key Elements:**
  - Awareness and Training: Ongoing training programs should teach users how to recognize phishing attacks, malware threats, and safe Browse habits. Simulated phishing campaigns can enhance preparedness.
  - Roles and Responsibilities: Cybersecurity responsibilities must be clearly defined across roles. For instance, a Chief Information Security Officer (CISO) oversees overall security strategy, while system administrators enforce controls.
  - Insider Threat Management: Both malicious insiders and unintentional actions can cause serious breaches. Monitoring access logs, employing behavioural analytics, and restricting data access are vital.
  - Security Culture: Building a culture of security means integrating security awareness into the day-to-day operations of the organization. Rewards and feedback systems can reinforce good behavior.

2. Process: Policies, Governance, and Compliance

Processes refer to the set of structured practices and frameworks that guide how cybersecurity is planned, implemented, monitored, and improved. These are crucial to ensuring consistency, legal compliance, and efficient incident response.

- **Key Elements:**
  - Risk Assessment and Management: This involves identifying critical assets, evaluating potential vulnerabilities, and assessing the likelihood and impact of threats. Risk mitigation strategies should be periodically reviewed.
  - Incident Response Plans: Organizations must be prepared for cyberattacks. A well-documented incident response plan outlines the steps to detect, contain, eradicate, and recover from an attack.
  - Access Control Policies: Least privilege access, role-based access control (RBAC), and periodic access reviews ensure that individuals only access the data necessary for their duties.
  - Compliance and Audits: Regular security audits and assessments ensure alignment with standards such as ISO 27001, NIST, or local laws like India's DPDP Act. Documentation is essential for legal and regulatory reporting.
  - Business Continuity and Disaster Recovery: These processes ensure that critical operations can continue or be quickly restored after a cyber incident.

3. Technology: Infrastructure and Tools

Technology provides the tools necessary to enforce cybersecurity policies and prevent, detect, and respond to attacks. However, technology alone is not sufficient—without trained people and sound processes, its effectiveness is limited.

- **Key Elements:**
  - Firewalls and IDS/IPS: Firewalls block unauthorized access, while Intrusion Detection and Prevention Systems (IDS/IPS) monitor and respond to unusual traffic patterns.
  - Encryption: Data must be protected both in transit and at rest using strong encryption standards like AES-256 or RSA.
  - Multi-Factor Authentication (MFA): MFA adds additional layers of verification, such as biometrics or time-based tokens, reducing the risks of credential theft.
  - Endpoint Security: Every endpoint (laptop, smartphone, server) must be protected with antivirus software, encryption, and policy enforcement.
  - SIEM Systems: Security Information and Event Management (SIEM) tools aggregate and analyse log data in real-time to detect anomalies and support incident investigations.
  - Patch and Vulnerability Management: Automated tools should be used to identify outdated software and apply patches to eliminate known vulnerabilities.
  - Cloud and Zero Trust Security: As organizations migrate to the cloud, new architectures like Zero Trust (trust nothing, verify everything) are essential for securing remote access and SaaS services.

.....Continued on page 3

GOOD TO KNOW!

Cyber Cell at Police Station

A Cyber Cell at Police Station is a specialized unit that investigates crimes committed using computers and the internet. These units handle a wide range of cyber crimes including hacking, online fraud, cyber stalking, and data theft.

Key Functions of a Cyber Cell –
1. Investigating Cyber Crimes
2. Providing technical assistance to other police units in cyber-related cases
3. Raising awareness
4. Co-ordinating with other agencies like law enforcement agencies to address cyber crime
5. Registering FIR's and conducting investigations

One can report the cybercrime/online fraud to the nearest cyber cell police station along with reporting it on cyber.gov.in or 1930

Conclusion

Cybersecurity is not merely a technical challenge—it is a multidisciplinary endeavor requiring careful coordination among people, processes, and technology. Organizations must view cybersecurity as a strategic function and allocate adequate resources to all three pillars. Only by building a comprehensive and integrated cybersecurity framework can institutions ensure the confidentiality, integrity, and availability of their data and digital services in an increasingly hostile cyber environment.

Chapter 2: Common Cyber Security Threats

Malware Attack

Malware is malicious software designed to damage, disrupt, or gain unauthorized access to computer systems.

Example: iClicker, a digital classroom tool used by thousands of instructors and millions of students in the U.S., was compromised in a "Click Flix" attack. A fake CAPTCHA with instructions to press "I'm not a robot" appeared. Clicking this silently copied a malicious PowerShell Script to the user's Windows clipboard. Users were then instructed to press Win+R to open the Windows Run dialogue, paste the script, and execute it by pressing Enter. This installed malware, enabling remote access to their systems. The likely installed malware was an Infostealer, capable of extracting browser-stored passwords, cookies, credit card data, Browse history, cryptocurrency wallets, and sensitive files. Such stolen data can be used to compromise faculty and student credentials, leading to identity theft, financial fraud, and ransomware attacks.

Ransomware

Ransomware is a type of malware that encrypts a victim's files and demands a ransom payment, typically in cryptocurrency, for the decryption key.

Example: A Pune-based multinational biopharmaceutical company was targeted in a ransomware attack where cybercriminals compromised and encrypted vital data on their servers, demanding 80,000 USD for the decryption key. The attackers threatened to post private information on the dark web if the ransom was not paid. The ransomware likely infiltrated the company's internal network through a phishing attack that deceived an endpoint device into executing a malicious payload. Once inside, the attackers deployed the ransomware across the company's primary and secondary servers, encrypting sensitive data, including proprietary formulas and manufacturing processes. The investigation is ongoing, with police urging organizations to adopt better cybersecurity protocols, including regular data backups and robust protection measures.

Phishing Attacks

Phishing attacks are cybercrimes where individuals are tricked into revealing sensitive information. They often involve fraudulent emails, text messages, or websites that appear legitimate.

- **Email Phishing:** Mass emails impersonating trusted entities (e.g., banks, government) urge recipients to click on fake links or submit sensitive data. This can lead to malware infections, stolen login credentials, and unauthorized access to bank accounts.
- **Spear Phishing:** Targeted emails are crafted using personal information of specific individuals to appear legitimate. It often involves links or documents hosted on cloud services. This can result in the loss of personal and corporate data, including login credentials and financial information specific to the target.
- **Whaling:** High-level executives are targeted with highly personalized attacks, often involving fake calls or emails from trusted partners. Attackers gain trust by infiltrating company networks, following up with phone calls routed through reputable agencies, and sending emails that appear to come from legitimate business organizations. Once the executive's email is compromised, sensitive authentication data is gathered, and fraudulent wire transfers are carried out. This can lead to the theft of executive credentials, financial authorization data, and sensitive employee information, often resulting in wire fraud or public exposure.
- **Smishing (SMS Phishing):** Fraudulent SMS messages with malicious links disguised as offers or alerts. Clicking these links can lead to malware downloads or harvesting of personal data such as login details or banking info.
- Social Media Phishing: Attackers create fake brand accounts or interact with users through tailored messages to trick them into clicking harmful links. This can lead to the breach of login credentials and personal details, potentially granting access to connected apps or payment information.
- **Vishing (Voice Phishing):** Fake phone calls using VoIP services impersonate legitimate institutions and create a sense of urgency to trick individuals into revealing sensitive information such as credit card numbers, bank credentials, insurance details, and other personal data.

.....Continued on page 4

Man-in-the-Middle Attack (MitM)

A Man-in-the-Middle attack occurs when cybercriminals intercept ongoing communication between two parties, often altering the communication to their benefit.

Example: In a recent MitM attack, the director of a Pune-based IT and dry fruits import firm unknowingly transferred ₹6.49 crore to fraudsters. The cybercriminals intercepted email communication between the director and a U.S.-based dry fruit exporter. They created a spoofed email address with slight changes—altering one letter and modifying the bank account details. Believing the email to be genuine, the director authorized the large payment across five transactions. The fraud was only discovered weeks later when the real exporter denied receiving the payment, which reduced the chances of recovering the stolen funds.

Data Breach

A data breach is a security incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.

Example: Equifax, one of the three largest credit reporting agencies in the U.S., managing sensitive financial data of millions, experienced a significant breach in 2017. Hackers exploited a flaw in the Apache Struts web application framework that Equifax neglected to fix, allowing the intrusion to occur for 76 days before detection. Approximately 146 million Americans were impacted, with personally identifiable information such as names, Social Security numbers, birth dates, addresses, driver's license numbers, and credit card numbers made public. Equifax suffered severe financial and reputational losses, and the impacted individuals also experienced significant harm. This resulted in a settlement of up to $700 million with the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and 50 U.S. states and territories.

Identity Theft

Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.

Example: On December 19, 2024, a victim received a WhatsApp call from an individual pretending to be a representative of the Telecom Regulatory Authority of India (TRAI). The caller falsely claimed that a mobile number registered in her name was linked to serious criminal activities, including child abduction and molestation. The victim was told that her KYC (Know Your Customer) documents were involved in a ₹68 crore fraud. To intensify fear, another individual posing as a customs officer named Rajeev Sinha provided a fabricated case number to lend credibility to the claims. The victim was manipulated into believing she was facing immediate arrest. The fraudsters staged a fake courtroom video call with one individual acting as a judge. The victim was even asked to wear white clothes to simulate a court appearance. During this staged hearing, she was falsely convicted and threatened with arrest. Under pressure to "settle" the matter and avoid arrest, the elderly woman was coerced into transferring ₹4.82 crore to the fraudsters over a period of time. This case highlights the growing threat of cybercrime involving impersonation of government authorities and the urgent need for public awareness and digital vigilance.

Denial of Service (DoS)

A Denial of Service (DoS) attack aims to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Example: Following the Pahalgam terror attack, India witnessed a wave of cyber offensives launched by pro-Pakistani and Bangladeshi hacktivist groups, targeting both government and private entities. Between April 22 and May 8, 2025, over 200 cyberattacks were documented by cybersecurity intelligence platform FalconFeeds.io, affecting more than 500 Indian entities. Nearly 96% of attack planning and coordination occurred on Telegram, where hacktivist groups communicated, recruited members, and hired DDoS-for-hire services. Some high-traffic platforms, such as the Income Tax portal, experienced brief slowdowns due to DDoS attacks. However, no major service was taken offline permanently, thanks to real-time monitoring and resilient infrastructure. According to cybersecurity experts, no critical data was stolen and no core infrastructure was compromised during this campaign.

.....Continued on page 5

Chapter 3: Common Cyber Safety Practices

Top 10 Cyber Safety Practices for Academic Institutions

In the digital age, academic institutions are increasingly reliant on technology, which also exposes them to various cyber threats. Cyberattacks on educational institutions can compromise student and staff data, disrupt operations, and lead to legal and reputational consequences. The following ten essential cyber safety practices should be implemented to strengthen cybersecurity in academic environments.

1. **Establish Strong Access Controls:** Use role-based access control (RBAC) and multi-factor authentication (MFA) to ensure only authorized users can access sensitive systems and data. Implement password policies that require complexity and regular updates.
2. **Educate and Train Staff and Students:** Regular training programs should educate users about phishing, password security, social engineering, and responsible internet behavior. Awareness reduces the likelihood of human error leading to a breach.
3. **Implement Robust Data Backup and Recovery Plans**: Automate data backups regularly and store them securely offsite or in the cloud. Have a tested disaster recovery plan to restore operations quickly in the event of data loss or ransomware attacks.
4. **Keep Systems and Software Updated:** Ensure all devices, operating systems, and applications are updated with the latest security patches. Vulnerabilities in outdated software are a common entry point for attackers.
5. **Use Firewalls and Antivirus Software:** Deploy network firewalls and endpoint antivirus solutions to monitor and filter malicious traffic. Enable automatic scanning and threat detection features.
6. **Secure Wi-Fi Networks:** Use WPA3 encryption for campus wireless networks and change default router passwords. Segment the network (e.g., student, staff, guest) to limit exposure in case of a breach.
7. **Develop and Enforce a Cybersecurity Policy:** Create clear institutional policies for the acceptable use of devices, email, internet, and data storage. Ensure all stakeholders understand and agree to these policies.
8. **Monitor Network Activity and Conduct Audits:** Use intrusion detection and prevention systems (IDS/IPS) and SIEM tools to continuously monitor network traffic. Conduct periodic security audits and vulnerability assessments.
9. **Protect Personal Data and Ensure Compliance:** Adopt data minimization and encryption practices. Ensure compliance with data privacy laws like India's DPDP Act or GDPR for international collaborations. Handle student data responsibly.
10. **Establish an Incident Response Plan:** Have a predefined and practiced protocol to handle data breaches, cyberattacks, or accidental disclosures. This plan should define roles, communication channels, and response timelines.

Conclusion - By adopting these cyber safety practices, academic institutions can create a secure digital environment that protects the privacy and integrity of student, staff, and institutional data. Cybersecurity is not just an IT issue—it is a shared responsibility that involves governance, education, technology, and ongoing vigilance

Chapter 4: Power of Data

Data-driven companies have a significant competitive advantage, utilizing data to improve decision-making, optimize processes, and gain a deeper understanding of their customers and markets. This approach leads to increased profitability, customer acquisition, and retention, ultimately driving business growth and innovation.

Key Advantages of Data-Driven Companies:

- Improved Decision-Making: Data provides a more accurate and objective basis for decisions, leading to better outcomes and reduced risks.
- Enhanced Customer Understanding: Data allows companies to personalize customer experiences, tailor products and services, and build stronger relationships.
- Optimized Processes: By analyzing data, companies can identify inefficiencies and implement improvements to streamline operations and reduce costs.
- Increased Profitability: Data-driven insights can lead to more effective marketing campaigns, better product development, and overall operational efficiency, contributing to higher profits.

.....Continued on page 6

NEWS CORNER

AI-powered Cyber Threats surge in India amid deepfake and ransomware concerns

India is facing an accelerating wave of cyber threats fuelled by artificial intelligence (AI), with ransomware attacks, deepfakes, and phishing campaigns becoming increasingly targeted and scalable. Sundar Balasubramanian, Managing Director, Check Point Software Technologies (India & South Asia), told CNBC-TV18 that cyberattacks are now “growing more complex and widespread,” driven by advances in AI and the vulnerabilities created by hybrid work.

News Source – CNBC

NEWS CORNER

16 Billion Logins Stolen in Mega Data Breach Threatening Apple, Google and more

In one of the largest data breaches in history, cybersecurity researchers have confirmed the leak of 16 billion login credentials, including passwords. The information leak can open the door to "pretty much any online service imaginable, from Apple, Facebook, and Google, to GitHub, Telegram, and various government services", according to a report in Forbes.

The development comes in the backdrop of multiple reports highlighting the presence of a "mysterious database" containing 184 million records -- sitting unprotected on a web server. The latest research suggests that it may have been just the tip of the iceberg. As per the outlet, the researchers have uncovered 30 datasets, with each of them containing up to 3.5 billion records. The information, which includes social media and VPN logins as well as corporate and developer platforms, is contained in datasets that have been found since the start of 2025.

This is not just a leak - it's a blueprint for mass exploitation. These aren't just old breaches being recycled. This is fresh, weaponizable intelligence at scale," said the researchers.
Researchers suggest that credential leaks at this scale can be exploited for phishing campaigns, account takeovers and business email compromise (BEC) attacks.

News Source - NDTV

.....From page 5

- Innovation and Growth: Data can reveal new market opportunities and potential growth areas, enabling companies to innovate and expand their reach.
- Competitive Advantage: Data-driven insights provide a significant edge over competitors, allowing companies to better serve customers and adapt to market changes.
- Faster Time to Market: Data analysis can help identify and address potential roadblocks in product development, leading to faster time to market.

Examples of How Data-Driven Companies Are Successful:

- E-commerce: Companies like Amazon use data to personalize product recommendations, optimize pricing, and improve customer service.
- Marketing: Businesses utilize data analytics to target specific customer segments, track campaign performance, and optimize advertising spend.
- Retail: Retailers use data to optimize inventory management, analyze sales trends, and predict customer demand.
- Healthcare: Healthcare providers use data to improve patient care, optimize treatment plans, and predict disease outbreaks.

.....Continued on page 7

Conclusion In conclusion, data-driven companies are more likely to be successful because they leverage data to make better decisions, understand their customers better, optimize their operations, and innovate more effectively.

Chapter 5: How Companies Use Your Data Without Privacy Laws

In the absence of comprehensive privacy laws, companies have broad freedom to collect, use, and exploit your personal data. This section outlines major practices and includes real-world examples to illustrate the risks.

Use of Personal Data

- Behavioral Profiling: Influencing purchases, opinions, and even emotions.
- Targeted Advertising: Selling and sharing data to advertisers, political campaigns, and insurance companies.
- Price Discrimination and Manipulative Pricing: Offering different prices based on perceived willingness to pay.
- Opaque Algorithmic Decisions/AI Models/Biases: Automated decisions that can be discriminatory and lack transparency.
- Surveillance and Location Tracking: Continuous monitoring of movements and online activity.
- Manipulation and Nudging: Influencing user behavior through design and algorithmic feeds.

Case Studies

Behavioral Profiling & Targeted Ads:
Facebook–Cambridge Analytica Scandal (2018): Data of 87 million users was harvested to influence political opinions. Likes were used to infer psychological traits without consent. Cambridge Analytica, a political consulting firm, harvested personal data from 87 million Facebook users without their consent through a Facebook quiz app created by researcher Aleksandr Kogan. This quiz was claimed to be a personality detector for research. Data collected included name, gender, location, ethnicity, education level, pages liked, and brand of clothing worn. Profiles were categorized based on this data, including geographical area. For example, users near border areas concerned with immigration were grouped into anti-immigration voter profiles. Political affiliations were also derived from clothing brands; e.g., Wrangler and L.L. Bean were associated with conservative voters, while Kenzo was linked to liberal voters. Through profiling from quiz data, Cambridge Analytica aimed to swing neutral voters towards a particular candidate.

Price Discrimination:
Orbitz (2012): Displayed more expensive hotels to Mac users, assuming higher spending capacity. Orbitz Worldwide Inc. found that iOS and Mac users were likely to spend 30% more on hotels, so the travel agency showed higher prices for them compared to Windows users who were charged nominally less. Mac users searching for accommodation would only see upgraded rooms, believing these were the only options, while Windows users conducting the same search would get results with less expensive standard rooms. In such scenarios, travellers are led to believe they are getting the best deal, but they are only receiving the best deal the company offers based on their presumed spending capacity.

AI/Algorithmic Decisions:
Amazon Hiring Algorithm (2018): Penalized resumes with the word 'women's', reflecting biased training data. Automated decisions can be opaque and discriminatory.

Manipulation & Nudging:
Instagram: Algorithmic feed manipulation can affect mental health and attention span. While Instagram can temporarily improve mood and reduce boredom, it also increases anxiety, depression, and feelings of loneliness after short usage. Compulsive use is influenced by social factors such as the need for social connection, the fear of missing out (FOMO), and the desire to increase views or popularity. Users frequently compare their looks and lifestyles to those of influencers, which can result in negative self-image and body dissatisfaction. Obsession, escapism, and a lack of control are behavioural factors that motivate Instagram use. Procrastination and depression are linked to excessive app use. Users from remote locations and lower socioeconomic backgrounds often engage more due to fewer entertainment options. Instagram's personalized algorithms and interactive features activate brain reward systems, increasing user engagement and potentially causing habitual and addictive use that frequently interferes with social, personal, and academic lives.

.....Continued on page 8

Health and Fitness Apps:
Flo Health App (2021, U.S.): Shared sensitive reproductive health data with Facebook and Google without user consent. Flo Health, a fertility tracking app, shared private health information of millions of users with marketing and analytics companies. Millions of users felt betrayed as highly sensitive information was disclosed. The FTC charged Flo for misleading users about how their data was handled.

Retail and Loyalty Programs:
Target (U.S.): Used analytics to identify a teenage girl's pregnancy and sent her maternity ads before her family knew. This case illustrates how strong data analytics can result in intrusive outcomes. Target's algorithm correctly deduced the pregnancy based on purchase history and behavioral data. The business then started sending her maternity and baby-related ads. The incident demonstrated how seemingly innocuous information, such as purchasing unscented lotion or calcium supplements, can disclose delicate life events. Concerns regarding consumer privacy, ethical data usage, and the possibility of emotional harm when businesses act on personal insights without express consent were raised.

Impact: Sensitive personal insights were inferred and acted upon invasively.

Credit and Loan Decisions:
Lenddo (Philippines/India): Assessed creditworthiness based on social media activity, including friends and posts. Lenddo, a financial company, generates credit scores based on psychometric credit assessment, using data like social media, tagged photos, Browse, search, and geospatial data from mobile phones to assess customer creditworthiness. Many users are unaware they provide sensitive personal information (location, online activity, social connections) to companies like Lenddo by using specific apps or services. Discriminatory lending decisions may result from social connections or online content reflecting socioeconomic background, race, or culture. Without context, algorithms may misinterpret behaviors (e.g., frequent location changes) as instability, leading to unfair credit scores. The system is opaque and unaccountable, as users are frequently not informed of reasons for loan denial or how to raise their credit score. The risk of data breaches and misuse increases when vast amounts of personal behavioral data are tracked and analyzed. Impact: Risk of biased, opaque lending decisions with no way to appeal.

Educational Technology (EdTech):
Proctoring Apps (Global): Monitored students' homes, eye movements, and keystrokes during exams. Proctoring apps are software used to monitor online exams to prevent cheating during remote assessments. These apps identify cheating instances by monitoring keystrokes, eye movements, and possibly recording audio and video, including of the student's home environment. This involves gaze tracking, facial recognition, and using cameras and microphones for a 360-degree panorama of the space. Many proctoring tools don't clearly explain what data is collected, how it's used, or who it's shared with. Students often cannot opt out or provide meaningful consent, making the process coercive. A breach could leak home environments, academic records, and live exam content. Impact: Raised concerns over biometric data collection and home surveillance.

Why and How Users Need to Be Aware About Their Personal Data Privacy Rights
Users need to be acutely aware of their personal data privacy rights because, in the absence of comprehensive privacy laws, companies have extensive freedom to collect, use, and exploit personal data. This broad access to personal information can lead to various risks and manipulations.

Why Users Need to Be Aware:
- Behavioural Profiling and Manipulation: Companies can collect data to infer psychological traits and build detailed behavioural profiles, which are then used to influence purchases, opinions, and even emotions.
- Targeted Advertising: Personal data is frequently sold and shared with advertisers, political campaigns, and insurance companies by data brokers, leading to highly targeted ads.
- Price Discrimination: Companies can use data to charge different prices to different users based on their perceived spending capacity.
- Opaque Algorithmic Decisions and Biases: AI models often make opaque algorithmic decisions that can be discriminatory.
- Surveillance and Location Tracking: Without privacy laws, companies can engage in extensive surveillance and location tracking, gathering vast amounts of sensitive personal information.

.....Continued on page 9

- Emotional and Psychological Impact: Algorithmic feed manipulation can negatively affect mental health, increasing anxiety, depression, and feelings of loneliness, and fostering negative self-image and body dissatisfaction through comparisons.
- Invasive Inferences: Seemingly innocuous data can reveal sensitive life events, such as a teenage girl's pregnancy being inferred from her purchasing habits.
- Lack of Control and Accountability: Users are often unaware of what data is collected, how it's used, or with whom it's shared. This means users frequently cannot opt out or provide meaningful consent.
- Increased Risk of Data Breaches and Misuse: When vast amounts of personal behavioral data are tracked and analyzed, the risk of data breaches and misuse significantly increases.

How Users Need to Be Aware:

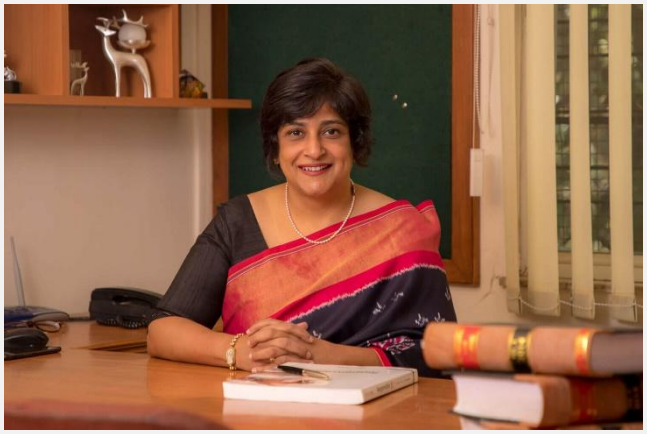
- Read Privacy Policies (Critically): Users should try to understand the key aspects of privacy policies regarding data collection, usage, and sharing.
- Exercise Caution with Permissions: Be mindful of the permissions granted to apps and websites, particularly those requesting access to location, contacts, photos, or microphone/camera.
- Use Strong Privacy Settings: Actively review and adjust privacy settings on social media platforms, web browsers, and mobile devices to limit data sharing and tracking.
- Recognize Phishing and Social Engineering: Be vigilant against suspicious emails, texts, and calls that ask for personal information.
- Understand Data Monetization: Be aware that "free" services often monetize user data.
- Be Skeptical of "Quizzes" and "Personality Tests": Seemingly innocuous quizzes can be sophisticated tools for data harvesting.
- Advocate for Stronger Laws: Support and demand comprehensive data privacy laws from lawmakers that give individuals more control over their personal information.
- Stay Informed about Data Breaches: Be aware of major data breaches reported in the news, and take steps to protect accounts if affected.
- Regularly Review Account Activity: Check bank statements, credit reports, and online account activity for any suspicious behavior.

How Users Come to Know About the Impact of Data Privacy Violations?

Users primarily come to know about the impact of data privacy violations through several key avenues:

- Direct Notification from Affected Organizations: When a company experiences a data breach or privacy violation that impacts its users, laws in many regions often mandate that the affected individuals be directly notified. These notifications typically explain what data was compromised, the potential risks, and steps users can take to protect themselves.
- Media Coverage and Public Reporting: Significant data privacy violations, especially those involving large numbers of users or prominent companies, frequently receive extensive media coverage. News outlets, cybersecurity blogs, and watchdog organizations report on these incidents, detailing how they occurred and their potential consequences for affected individuals.
- Financial Fraud and Identity Theft Incidents: Users often discover the impact of privacy violations when they become victims of financial fraud or identity theft. This could involve unauthorized transactions on their bank accounts, credit cards, or new accounts opened in their name.
- Unusual or Unsolicited Communications: An increase in spam emails, targeted advertisements for products or services they haven't explicitly shown interest in, or suspicious phone calls can sometimes indicate that a user's data has been compromised and is being used for marketing or fraudulent purposes.
- Legal Actions and Settlements: Class-action lawsuits or regulatory actions against companies that have violated data privacy can bring the impact of such violations to light. Settlements, like the up to $700 million paid by Equifax, often include provisions for affected individuals to claim compensation or receive credit monitoring services, directly informing them of their status as victims.
- Changes in Online Experience: Sometimes, subtle changes in online experiences, such as more aggressive or highly personalized advertisements, or unexpected prompts, can be a sign that personal data is being used in ways the user might not be comfortable with.

ABOUT THE AUTHORS



Adv Vaishali Bhagwat

Vaishali Bhagwat is a practicing lawyer with 25 years of experience in civil and cyber litigation and advisory practice in Pune and Mumbai.
Vaishali has a prior degree and work experience in the field of Computer Science, a Post graduation certification in Cyber Security and Information Assurance and is a certified Privacy Lead Assessor.

She is an advisor to several companies on Cyber law and privacy compliance and advisor to various educational institutions on Protection of children from sexual offences.

She has successfully conducted several prominent cases for corporate espionage and Data theft, Data Privacy, Digital Financial Frauds, Cyber-crimes against women and children, take down orders and IP infringement in cyberspace.

Vaishali is a *TCS Chevening Scholar on "Cyber Policy and Cyber Defense" and has earned the Post Graduate certification from Cranfield University UK. She is also a Disha Alumni which is a prestigious program of the British high Commission on Innovative Leadership chaired by UK PM David Cameron and PM Manmohan Singh.*

www.vaishalibhagwat.com

Mrudula Arjunwadkar
BSc., LLB, MPM

POSH Consultant
Helping organizations in end to end POSH Compliance, External member to IC, POSH trainings