# Norton report reveals 186% surge in critical data breaches and rising AI-driven scams in early 2025



The latest Norton Gen Threat Report offers a stark warning as it highlights an alarming rise in cybersecurity threats during the first quarter of 2025. While there appears to be a small decline in the total number of blocked attacks, which could suggest a reduction in overall threat activity, the details within the report paint a much grimmer picture. Cybercriminals have increasingly shifted tactics, leading to a staggering 186% surge in records breached, amounting to over 1.19 million instances of either high or critical severity, including the exposure of plaintext passwords. This significant increase underscores the escalating danger as threat actors gain direct access to user accounts.

Alarmingly, breaches are not only rising in terms of severity but also in sheer volume. The report noted a 36% increase in breach events year-on-year, reflected in nearly a 4% uptick in notifications sent to users regarding identity protection incidents. Furthermore, alerts for potential credit fraud increased by approximately 14%, while signals of criminal record misuse surged nearly 12%. Such statistics illustrate an alarming trend that demands immediate attention. The rise in data breaches coincides with a notable uptick in various scams and social media exploits, marking a significant shift in the cyber threat landscape. For instance, malicious push notifications have shown an increase of over 10% in Germany alone, with even sharper increases in other countries, including 25% in Norway and 22% in Denmark.

The pervasive threat landscape has not only witnessed a rise in breaches, but it has also become considerably more lucrative for criminals. Reputable sources note that financial scams employing artificial intelligence, such as deepfakes, have gained considerable ground. A notable campaign by the CryptoCore group accounted for 2,200 fraudulent transactions, netting approximately $3.8 million. Comments from industry experts reflect the evolving tactics of cybercriminals, as they leverage advancements in technology to exploit trust and target victims more ingeniously. The report highlighted the need for individuals to utilise resources like HaveIBeenPwned and invest in robust identity threat protection services, especially given the personal impact these breaches can have.

In a broader context, other reports corroborate the findings of the Norton Gen Threat Report, revealing a worrying escalation in cyberattacks across industries. According to Check Point’s findings, the education sector has emerged as the most targeted, with an astounding average of 4,484 weekly cyber incidents. Ransomware attacks have surged by 126%, particularly hit hard in North America which accounts for 62% of global ransomware incidents. The manufacturing, retail, and technology sectors are also grappling with a substantial increase in attacks, demonstrating the need for stringent cybersecurity measures across all industries.

Moreover, a review from the Identity Theft Resource Center indicates that over 91 million individuals fell victim to data breaches during the same quarter, highlighting a substantial rise of 26% year-on-year. The financial services sector continues to be particularly vulnerable, exemplified by the compromise of sensitive information in large-scale breaches. The report emphasizes the critical urgency for organisations to strengthen their cybersecurity frameworks, with many experts advocating for improvements in password policies, regular vulnerability assessments, timely updates, and comprehensive training for employees to mitigate risks effectively.

As we navigate this increasingly perilous cyber landscape, it becomes increasingly clear that the emphasis must shift from reactive measures to proactive and preventative strategies, safeguarding both personal and organisational data against the evolving threats posed by cybercriminals.

## Reference Map:

* Paragraph 1 – [[1]](https://www.techradar.com/pro/security/over-a-million-critical-severity-records-exposed-in-q1-2025-alone-make-sure-youre-not-at-risk), [[2]](https://www.techradar.com/pro/security/over-a-million-critical-severity-records-exposed-in-q1-2025-alone-make-sure-youre-not-at-risk)
* Paragraph 2 – [[1]](https://www.techradar.com/pro/security/over-a-million-critical-severity-records-exposed-in-q1-2025-alone-make-sure-youre-not-at-risk), [[3]](https://www.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/), [[4]](https://www.smartindustry.com/benefits-of-transformation/cybersecurity/article/55280831/leading-cyberattack-against-manufacturing-sets-record-in-q1)
* Paragraph 3 – [[5]](https://www.verizon.com/about/news/2025-data-breach-investigations-report), [[6]](https://www.infosecurity-magazine.com/news/us-data-breach-victim-count-surges/)
* Paragraph 4 – [[7]](https://slingscore.com/data-breaches-surge-in-early-2025/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.techradar.com/pro/security/over-a-million-critical-severity-records-exposed-in-q1-2025-alone-make-sure-youre-not-at-risk> - Please view link - unable to able to access data
2. <https://www.techradar.com/pro/security/over-a-million-critical-severity-records-exposed-in-q1-2025-alone-make-sure-youre-not-at-risk> - The Norton Gen Threat Report for Q1 2025 highlights a significant surge in data-stealing threats, with a 186% increase in breached records and a 102% rise in compromised user emails. Over 1.19 million records of high or critical severity were exposed, including plaintext passwords, posing substantial risks of direct account access by cybercriminals. The report underscores the importance of regularly monitoring breach websites like HaveIBeenPwned and considering identity threat protection services to mitigate potential impacts.
3. <https://www.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/> - Check Point's Q1 2025 Global Cyber Attack Report reveals a 47% increase in cyber attacks per organisation, averaging 1,925 weekly incidents. The education sector was the most targeted, with 4,484 weekly attacks, followed by government and telecommunications. Ransomware attacks surged by 126%, with North America accounting for 62% of global incidents. The consumer goods and services sector was the most targeted by ransomware, highlighting the need for enhanced cybersecurity measures across industries.
4. <https://www.smartindustry.com/benefits-of-transformation/cybersecurity/article/55280831/leading-cyberattack-against-manufacturing-sets-record-in-q1> - GuidePoint's Q1 2025 report indicates that manufacturing, retail, and technology industries were most heavily impacted by ransomware, with the nonprofit sector also experiencing a dramatic surge. Actively exploited flaws increased by 75% compared to the same period in 2024, with 12,333 vulnerabilities reported in Q1 alone. Notably, 59% of observed ransomware victims were based in the U.S., underscoring the critical need for robust cybersecurity measures in these sectors.
5. <https://www.verizon.com/about/news/2025-data-breach-investigations-report> - Verizon's 2025 Data Breach Investigations Report reveals a significant increase in cyberattacks, with third-party involvement in breaches doubling to 30%. Exploitation of vulnerabilities surged by 34%, and ransomware attacks rose by 37%, now present in 44% of breaches. The report highlights the critical need for businesses to invest in robust security measures, including strong password policies, timely patching of vulnerabilities, and comprehensive security awareness training for employees.
6. <https://www.infosecurity-magazine.com/news/us-data-breach-victim-count-surges/> - The Identity Theft Resource Center (ITRC) reports a 26% year-on-year increase in individuals impacted by data breaches in Q1 2025, with over 91 million victims. The financial services industry led with 193 reported compromises, highlighting its continued vulnerability. The report underscores the urgent need for enhanced cybersecurity measures to protect sensitive personal and financial information.
7. <https://slingscore.com/data-breaches-surge-in-early-2025/> - Early 2025 witnessed a surge in data breaches, with notable incidents affecting major companies. For instance, UnitedHealth experienced a breach compromising sensitive health insurance information of approximately 190 million individuals, leading to over $3 billion in losses. The report emphasizes the escalating threat landscape and the critical need for organisations to implement robust cybersecurity measures to safeguard personal and financial data.