171 Cyber Security Statistics: 2025's Updated Trends and Data

This blog post explores key cybersecurity statistics and trends for 2025, providing businesses with valuable insights into the latest cyberattack patterns. Analyze up-to-date cyber security stats and improve your cybersecurity strategies.

2024-09-11

Cybersecurity is evolving rapidly as cyberattacks become increasingly sophisticated, and organizations need to stay informed about the latest trends and threats. Keepnet has compiled 171 key **cybersecurity statistics 2025**, highlighting recent data on emerging threats, advanced attack techniques, and evolving security trends, aligning with broader **cybercrime statistics** reported globally.

This collection provides valuable insights into the shifting landscape of cybersecurity and helps businesses understand the areas where they are most vulnerable. From ransomware and phishing to the growing risks posed by IoT devices, these **cyber security statistics** offer a comprehensive overview of the challenges companies face.

This blog post will help businesses strengthen their cybersecurity strategies by exploring the most up-to-date information and identifying key areas for improvement based on the latest **cyber attack statistics** and trends for 2025.

How often do cyberattacks happen?

Source: *University of Maryland*

Picture 1: Cyberattack Frequency

- A study from the University of Maryland's A. James Clark School of Engineering reveals that cyberattacks occur at an alarming rate of over 2,200 times daily, with someone falling victim every 39 seconds.

- This relentless pace of cybercrime means that hackers are constantly exploiting vulnerabilities across various sectors, putting both individuals and businesses at significant risk.

- Additionally, experts from Cybersecurity Ventures report that ransomware attacks occur, on average, every 11 seconds.

- These attacks, often involving data theft or system lockdowns, are increasingly disruptive and sophisticated, posing severe operational and financial risks. The escalating frequency of these incidents serves as a stark reminder that organizations need to prioritize their cybersecurity defenses to stay ahead of evolving threats.

Cost of Cyber Attacks

- In 2024, the global cost of cyberattacks is projected to reach $9.5 trillion, with **ransomware**, **phishing**, and data breaches driving much of this increase, according to Cybersecurity Ventures.

- These financial impacts go beyond immediate losses, including long-term consequences such as reputational damage, legal expenses, and regulatory fines.

- As Cobalt Magazine points out, the growing complexity of these attacks makes them increasingly difficult to defend against, particularly as ransomware continues to target businesses every 11 seconds.

- The shift to remote work has further increased vulnerabilities, resulting in more costly data breaches as decentralized systems remain open to exploitation.

$9.5
Trillion

In 2024, the global cost of cyberattacks is projected to hit $9.5 trillion, driven by ransomware, phishing, and data breaches.

Source: *Cybersecurity Ventures*

Picture 2: 2024 Global Cost of Cyberattacks

- Insurance Journal reports that, in response to these rising risks, cyber insurance premiums have jumped by 50% in 2022 as companies seek to protect themselves.

- According to Cybersecurity Ventures, the cost of cybercrime is expected to continue rising, potentially reaching $10.5 trillion annually by 2025.

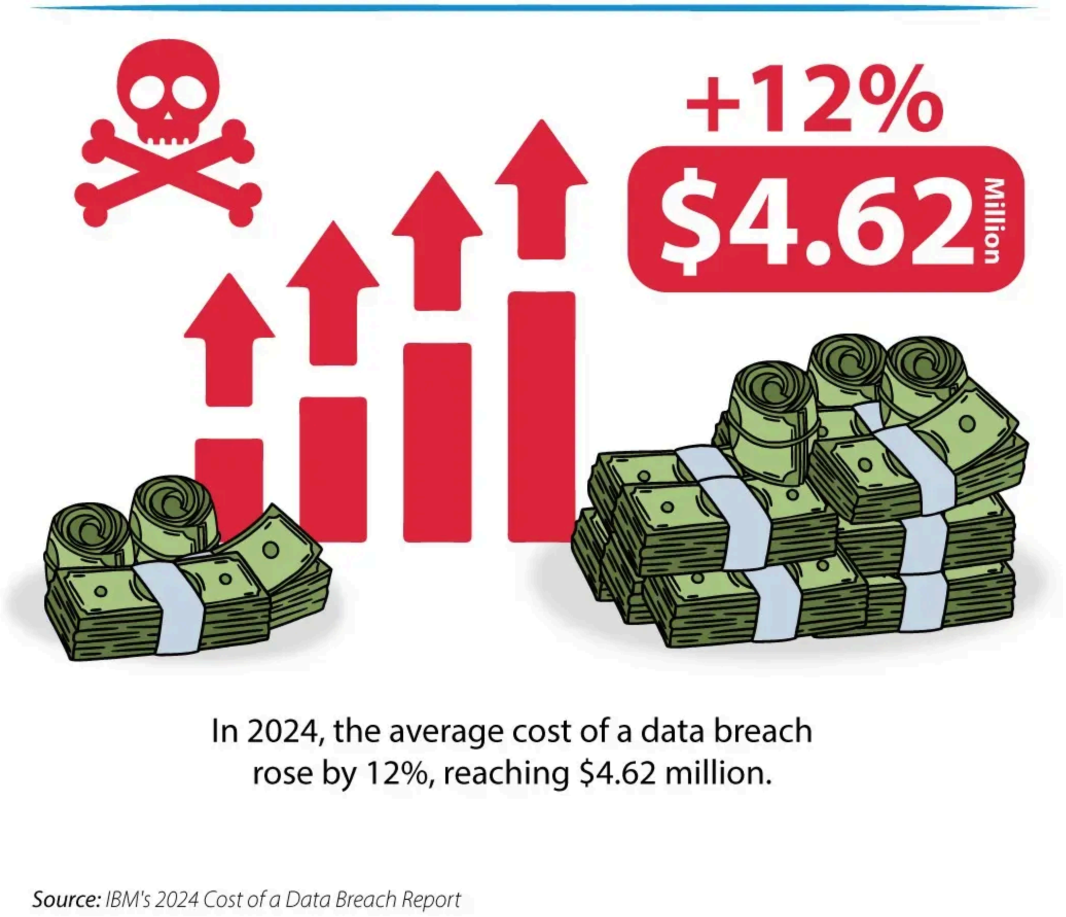
- This **cyber security stats** from Cybersecurity Ventures emphasizes the critical need for businesses to implement robust cybersecurity strategies to protect themselves from escalating financial damages and operational risks in the years ahead.

- The average ransomware payout has increased dramatically from $812,380 in 2022 to $1,542,333 in 2023

Critical Data Breach and Hacking Statistics

- In 2024, **data breaches** continue to be an expensive challenge for organizations globally. According to *IBM's 2024 Cost of a Data Breach Report*, the average cost of a breach increased by 12% from the previous year, reaching $4.62 million.

- The healthcare industry remains the hardest hit, with breach costs averaging $10.93 million per incident due to the sensitive nature of the data involved.


+12%
$4.62
Million
In 2024, the average cost of a data breach rose by 12%, reaching $4.62 million.

Source: *IBM's 2024 Cost of a Data Breach Report*

Picture 3: 2024 Average Cost of a Data Breach

- **Phishing** and business email compromise (BEC) attacks are among the most frequent and costly, averaging $4.88 million per breach. A key factor driving these rising costs is the time required to detect and respond to breaches.
- The report notes that the average breach lifecycle—time to identify and contain a breach—is now 277 days, further escalating financial impacts for affected organizations.
- Moreover, companies that deployed AI and automation to their security operations significantly reduced their costs, saving an average of $2.22 million per breach compared to those that did not use these technologies.
- This demonstrates the growing importance of investing in advanced security tools to mitigate the financial and operational fallout of data breaches.

Phishing Statistics

- **Phishing attacks** have become an even more common threat in 2024, accounting for nearly 30% of all breaches globally, according to IBM's 2024 Cost of a Data Breach Report.
- These attacks are highly effective because they exploit human trust, tricking victims into providing sensitive information or access credentials.
- The average cost of a phishing-related data breach now stands at $4.88 million per incident, highlighting its financial toll on organizations (Verizon DBIR).
- Phishing campaigns are evolving, with attackers leveraging AI to create increasingly convincing emails and websites, making it harder for individuals and businesses to detect fraud.
- Additionally, phishing-related breaches often take up to 206 days to detect and contain, according to IBM's **2024 Cost of a Data Breach Report**, which significantly prolongs the operational and financial damage.

Ransomware Statistics

- In 2024, **ransomware attacks** continue to surge, with incidents rising steadily across various industries.
- According to a report by the United Nations Office on Drugs and Crime (UNODC), these attacks are happening at an alarming rate, with a new incident occurring approximately every 11 seconds.

ransomware breaches in healthcare cost an average of $10.93 million per incident.

- Additionally, ransomware-induced downtime leads to significant financial losses, with businesses losing an average of $8,500 per hour due to disrupted operations, according to Egnyte. These long recovery periods add to the financial and operational difficulties faced by affected companies.
- Despite large ransom payments, recovering data is not guaranteed. As reported by TechRepublic, many organizations struggle to fully restore their systems after paying a ransom.

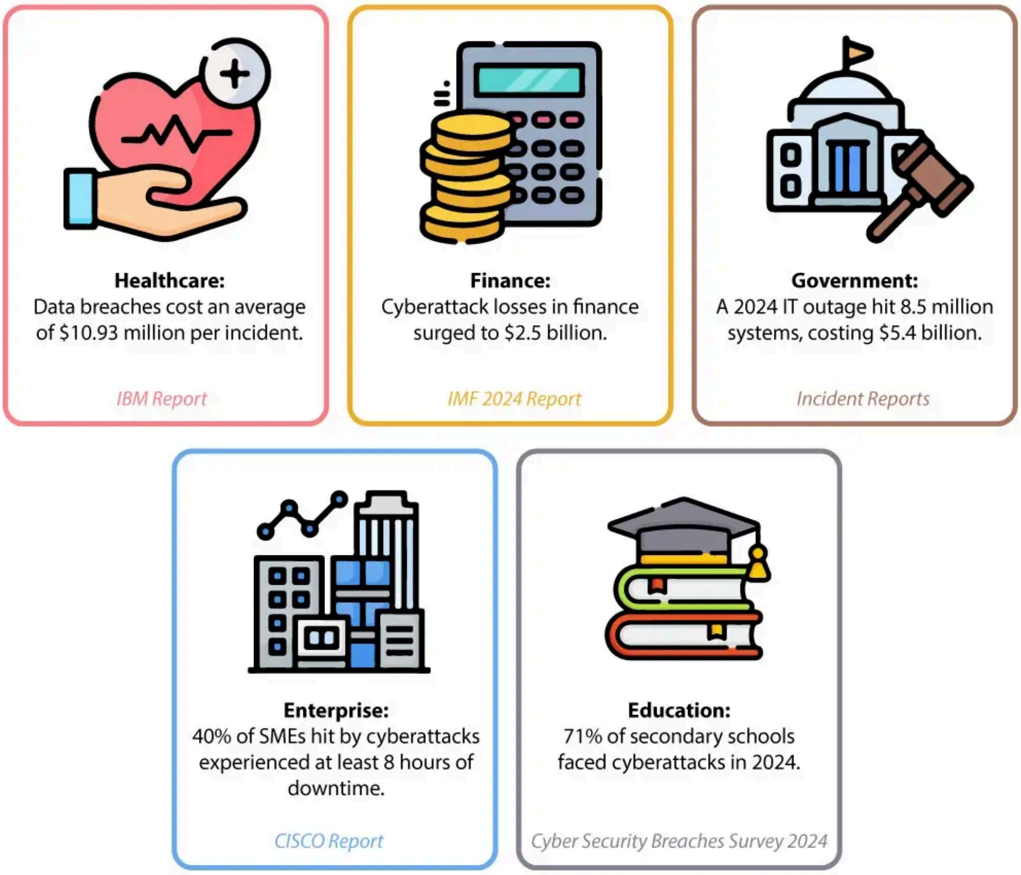
These cyber security statistics underscore the urgent need for businesses to invest in stronger cybersecurity measures and effective incident response strategies to tackle the rising ransomware threat.

Malware Statistics

- A recent Statista report shows a steady rise in malware incidents, with over 6.06 billion attacks detected worldwide in 2023, particularly concentrated in the Asia-Pacific region.
- This surge in malware reflects the increasing sophistication and frequency of attacks targeting both businesses and individuals.
- Among the most commonly blocked malware types were trojans, worms, and ransomware, which continue to pose significant threats across various sectors.
- In 2024, 81% of organizations faced malware threats, according to Station X. This statistic underscores the widespread and persistent nature of malware as a key cybersecurity challenge.
- With such a high percentage of businesses affected, addressing malware through advanced detection and prevention strategies is more critical than ever to minimize risks and protect sensitive data.
- Over 6.06 billion malware attacks were detected globally in 2023.
- 81% of organizations faced malware threats in 2024.

Cybersecurity statistics by industry

- Cybersecurity risks differ greatly across industries, with certain sectors facing more severe threats, according to various **cybersecurity statistics 2024.**
- Healthcare remains highly vulnerable, with the average cost of a data breach reaching $10.93 million, as noted in IBM's **Cost of a Data Breach Report.**
- The financial sector, based on **cybercrime statistics**, is heavily targeted by business email compromise (BEC) and ransomware attacks. In manufacturing, 35% of confirmed breaches involve ransomware, while espionage-related breaches in public administration have increased from 5% to 7%, as highlighted by Verizon's 2024 **Data Breach Investigations Report.**



Healthcare:
Data breaches cost an average of $10.93 million per incident.

IBM Report

Finance:
Cyberattack losses in finance surged to $2.5 billion.

IMF 2024 Report

Government:
A 2024 IT outage hit 8.5 million systems, costing $5.4 billion.

Incident Reports

Enterprise:
40% of SMEs hit by cyberattacks experienced at least 8 hours of downtime.

CISCO Report

Education:
71% of secondary schools faced cyberattacks in 2024.

Cyber Security Breaches Survey 2024

Picture 4: 2024 Cybersecurity Statistics by Industry

In the following sections, we will delve deeper into the specific cybersecurity challenges faced by each sector.

Healthcare Cybersecurity Statistics

- The healthcare sector has become a top target for cybercriminals, largely due to the vast amounts of sensitive data it handles and the life-critical services it provides.
- In 2023, the average cost of a data breach in healthcare soared to $10.93 million per incident, nearly double that of the financial sector, which averaged $5.9 million per breach. These cyberattacks not only compromise confidential patient data but also pose serious risks to the safety and well-being of patients.
- According to the World Economic Forum, such attacks can disrupt entire healthcare systems, putting lives and operations at risk. With the increasing digitization of healthcare services, strengthening cybersecurity has become an urgent priority for the industry.

Finance Cybersecurity Statistics

- Cyber attacks in the financial sector have more than doubled since the pandemic, putting companies at greater risk. Some, like Equifax, faced significant penalties, paying over $1 billion after a major breach in 2017.
- According to the IMF's April 2024 Global Financial Stability Report, extreme losses from cyberattacks have increased significantly since 2017, now reaching $2.5 billion. These losses can threaten a company’s financial stability and create funding issues.
- Additionally, indirect costs such as reputational damage and the need for enhanced security measures further increase the financial pressure on affected companies.

Government Cybersecurity Statistics

- In 2024, cyberattacks on government systems have caused significant disruption and financial damage.
- In January, Australia imposed sanctions after a breach exposed the data of 9.7 million customers of its largest private health insurer, marking the first use of its cyber sanctions framework. In December 2023, an attack disrupted 70% of gas stations in Iran, leading to widespread outages and payment issues that lasted several days.

- Cyberattacks disrupted 70% of gas stations in Iran, leading to financial and operational crises.
- A global IT outage affected 8.5 million systems, causing $billion in damages.

Enterprise Cybersecurity Statistics

- Cybercriminals can successfully penetrate 93% of company networks, according to research reported by Betanews. This alarming statistic underscores the growing vulnerabilities in enterprise security, especially as AI-driven attacks become harder to detect.
- In a study conducted by Positive Technologies, penetration tests across sectors such as finance, energy, government, and IT revealed that attackers could breach defenses and access local networks in 93% of cases.
- Furthermore, CISCO reported that 40% of small and medium-sized enterprises (SMEs) experiencing a cyberattack suffered at least eight hours of downtime, with downtime contributing significantly to the financial damage.
- While 43% of cyberattacks target small businesses, only 14% of these businesses feel adequately prepared to defend against such threats, as highlighted by Accenture's Cost of Cybercrime Study.

Education Cybersecurity Statistics

- According to the Cyber Security Breaches Survey 2024 by the Department for Science, Innovation and Technology (DSIT), 71% of secondary schools and 52% of primary schools reported experiencing cyberattacks in the past year.
- Phishing was the most common method, with 92% of primary schools and 89% of secondary schools encountering phishing attempts.
- Despite increased focus on security, primary and secondary schools are less likely than colleges and universities to seek further guidance on cybersecurity measures.
- Although 75% of primary schools and 81% of secondary schools have implemented cybersecurity policies, the report notes that primary schools generally have less advanced protections.
- 71% of secondary schools and 52% of primary schools reported cyberattacks in 2024.
- Phishing was the most common method, with 92% of primary schools and 89% of secondary schools encountering phishing attempts.

Covid-19 Cybersecurity Stats

- The shift to remote work during the COVID-19 pandemic significantly increased cybersecurity risks, with 47% of individuals falling for phishing scams while working from home, as reported by Deloitte.
- Cybercriminals took advantage of the situation by exploiting the vulnerabilities of remote employees and creating fake COVID-19-related websites to lure victims.
- The average cost of a data breach caused by remote work has surged to $137,000, highlighting the financial risks involved.
- In the UK, the City of London Police reported over £11 million lost to COVID-19 scams since January 2020. Similarly, in Switzerland, one in seven respondents to a survey experienced a cyberattack during the pandemic, emphasizing the global scale of the issue.
- 47% of individuals fell for phishing scams while working from home during COVID-19.
- The average cost of a data breach caused by remote work surged to $137,000.

Business Email Compromise(BEC) Cybersecurity Statistics

- In 2024, **Business Email Compromise (BEC)** remains one of the most financially damaging cyber threats. According to the FBI's Internet Crime Report, BEC attacks led to $2.9 billion in reported losses in 2023, making it the second-most costly cybercrime after investment scams.
- These attacks, which typically involve impersonating high-level executives or trusted partners to deceive employees into transferring funds, have surged by 42% compared to the previous year (Unite.AI).
- In fact, BEC attempts now account for 21% of all email-based attacks, up from 15% in 2023. Moreover, Microsoft reported detecting an average of 156,000 BEC attempts daily between April 2022 and April 2023, highlighting the scale of the threat.
- The growing sophistication of BEC attacks underscores the importance of implementing robust email security practices to mitigate the risks in 2024.

GDPR & Compliance Cybersecurity Statistics

- In 2024, GDPR compliance remains a crucial focus in cybersecurity, with penalties for violations hitting new records.
- DLA Piper's GDPR and Data Breach Survey reports that fines for non-compliance across Europe reached €1.78 billion from January 2023 to January 2024, a 14% increase from the previous year. Ireland issued the highest fine, imposing €1.2 billion on Meta, underscoring how Big Tech is heavily targeted by regulators.
- Data breaches also remain a serious concern, with an average of 335 breach notifications reported daily throughout Europe.
- As regulatory pressures grow, over 70% of organizations expect compliance requirements to keep increasing, making it essential to follow data protection rules to avoid heavy fines and protect sensitive data.

Cybersecurity Spending

- Global end-user spending on security and risk management is projected to reach $215 billion in 2024.
- $90 billion will be allocated to security services like consulting, IT outsourcing, and implementation.

IoT and DDoS Cybersecurity Statistics

- In 2022, there were over 10.54 million attacks on Internet of Things (IoT) devices ,showing how easily these connected devices can be targeted, according to Statista.
- By 2023, the situation worsened, with IBM reporting a 15% rise in DDoS (Distributed Denial of Service) attacks in the second quarter, particularly focusing on disrupting key applications.
- Additionally, Verizon noted 6,248 DDoS attacks in 2022, demonstrating the widespread nature of these threats. As more devices get connected to the internet, they offer more opportunities for cyberattacks. This highlights the urgent need for better security measures to protect IoT devices and defend against DDoS attacks.
- In 2022, there were over 10.54 million attacks on IoT devices.
- DDoS attacks increased by 15% in 2023, focusing on disrupting key applications.

General & Miscellaneous Statistics

- According to Gartner's forecast report, global end-user spending on security and risk management is expected to reach $215 billion in 2024, a 14.3% rise from the $188.1 billion spent in 2023.

Global spending on security and risk management is projected to reach $215 billion in 2024

Source: *Gartner's Forecast Report*

Picture 5: 2024 Global Spending on Security and Risk Management

- Of this, $90 billion will be dedicated to security services like consulting, IT outsourcing, implementation, and hardware support, reflecting an 11% growth compared to the previous year.
- These services are projected to account for 42% of the total security spending, underscoring their critical role in the overall cybersecurity landscape.
- As the threat environment becomes increasingly complex, organizations are focusing more on outsourced expertise and advanced security solutions to strengthen their defenses. This trend highlights the continued growth of the cybersecurity market as businesses prioritize risk management to safeguard their operations.

Social Engineering

- Only 23% of people over 55 know what smishing is, compared to 34% of millennials who can define it.
- Phishing, smishing, vishing, and pharming scams affected over 240,000 victims in 2020, leading to $54 million in reported losses. On average, smishing scams cost individuals around $800 globally.
- In 2020, smishing attacks skyrocketed by 328%, with 76% of businesses targeted within a year.
- During the first two weeks of the U.S. quarantine, 44% of Americans noticed an increase in scam calls and texts.
- The National Institute for Standards and Technology (NIST) recommends against using SMS-based two-factor authentication (2FA) due to security flaws.
- Hackers often use local phone numbers to make their fake messages seem more credible.
- About 17% of enterprise users encountered phishing links on their mobile devices.
- In the UK, 846,000 people reported fake tax notifications from HMRC in 2020.
- Fake delivery notifications have become a common smishing tactic with the rise of online shopping.
- A hacking group called "Dark Caracal" used apps like WhatsApp and Signal to send phishing links.
- In the U.S., suspicious texts can be reported by forwarding them to 7726 (SPAM), a service supported by major mobile carriers.
- Smishing incidents in the UK jumped by 700% in the first half of 2021.

- Americans lost a whopping $29.8 billion to vishing in 2021, marking a sharp 49.7% increase from $19.7 billion in 2020. On average, each victim lost $502 in 2021, up by 43% from the previous year.
- People aged 18-44 are the most vulnerable to vishing, with men making up 59.4% of victims in 2021.
- Smartphones are now the primary channel for vishing attacks, with 85% of scam calls targeting mobile phones in 2021. In contrast, landline scam calls dropped to just 20%.
- The vishing problem isn't confined to the U.S. In Brazil, known as the most spammed country for four consecutive years, vishing is a rampant issue. In October 2021, Peru recorded over 12 million spam calls, while Mexico experienced 3.2 million.
- A single scammer in India made over 202 million spam calls in 2021, with most related to telemarketing or sales. The KYC (Know Your Customer) scam was especially widespread.
- Around 70% of scam calls in the U.S. involved number spoofing, a technique where scammers mask their caller ID to appear as a trusted source.
- The average duration of a spam call in 2021 was just 12 seconds. This suggests that people are becoming increasingly aware of scams and are disconnecting quickly.
- Scammers often gather personal details about their targets before making the call. In 2019, 75% of victims who lost $1,000 or more reported that scammers already had some of their personal information.
- 96% of online deepfake videos are non-consensual pornographic content, with over 85,000 videos identified by December 2020.
- A worrying 71% of surveyed individuals worldwide admitted they don't know what deepfakes are, highlighting a lack of preparedness.
- 25% of individuals find it challenging to differentiate between deepfake and real audio, increasing their vulnerability to scams.
- 46% of organizations see generative AI, including deepfakes, as a major cybersecurity threat.
- 85% of security professionals believe generative AI has directly contributed to the increase in cyberattacks.
- Due to security risks, 32% of organizations have banned the use of generative AI technologies.
- Frequent deepfake scams are eroding trust among employees, and with most online content predicted to be synthetically generated by 2026, this issue is set to worsen.
- North America, Asia-Pacific, the Middle East, Africa, and Latin America are all experiencing significant increases in deepfake fraud, with the cryptocurrency sector being the most targeted.
- Asia have some of the highest rates of detected identity fraud linked to deepfakes.
- Many organizations have reported incidents of deepfake voice fraud, a threat made easier by advancements in voice cloning technology.
- 78% of deepfake phishing attacks are delivered via email, making this the most common attack vector.
- The cryptocurrency industry is highly targeted by deepfake-related phishing attacks due to its lucrative nature and lack of regulation.

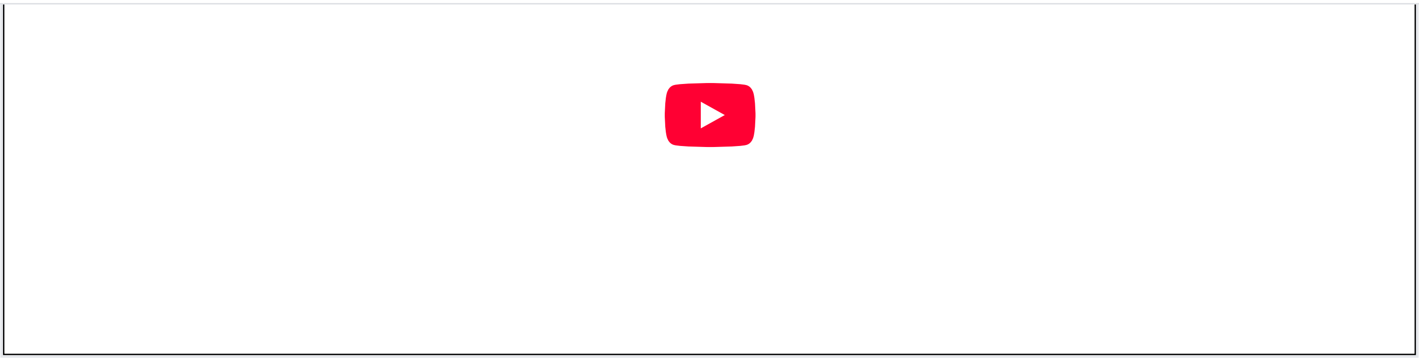
Stay Ahead of Cyber Threats with Keepnet

As cyberattacks grow increasingly complex, businesses must actively address the human element, which contributes to 68% of breaches, according to the 2024 Data Breach Investigations Report. This aligns with current **cyber attack statistics**, which highlight how human error remains one of the largest vulnerabilities in cybersecurity defenses.

Keepnet helps organizations tackle this vulnerability by offering targeted security awareness training and phishing simulations that cover vishing, smishing, and QR phishing, mimicking real-world attacks. These customized simulations enable employees to recognize and avoid advanced phishing tactics, a key component in modern cyber defenses. With Keepnet's behavior-based training, staff learn how to handle specific threats they're likely to encounter, minimizing the risks posed by human error.

This combination of realistic simulations and focused training enhances organizations' ability to defend against evolving phishing techniques and social engineering attacks.

Watch the video below to discover how Keepnet Security Awareness Training can boost your organization's defenses and equip your team with the skills to confidently navigate today's complex cybersecurity landscape.



Watch the video below to see how Keepnet’s Phishing Simulator strengthens your defenses by training your team to quickly spot and respond to phishing threats.

Editor's Note: This article was updated on February 14, 2025.

SHARE ON

Related Blogs