15
Jan

ber Security Awareness

131 Cyber Security Statistics: 2024 Trends & Data

Cyber security awareness is an everyday job, and it's easy to fall into a false sense of security once you have a solid plan in place. Every year, statistics are a reminder that hackers and scammers never sleep. New trends and attack types pop up daily, making it difficult to keep track.

This list is a rundown of the most important statistics of the year, allowing you to get a good overview of threats to keep in mind. Moreover, it incorporates some industry-specific statistics for a more detailed perspective.

Cyber attacks and cyber security

The overall cyber security trend is clear, attacks are on the rise, and most companies feel they don't have the proper resources to face the threats. Most users still aren't properly educated and still practice behaviors that put the company at risk.

Cyber security awareness must be a top priority when a majority of users reuse passwords and use easily guessed phrases. Human error is still by far the leading cause of data breaches and most people don't know the safety steps to mitigate them, an easily fixed problem with the proper education.

1. 17% of cyber attacks target vulnerabilities in web applications
2. 98% of web applications are vulnerable to attacks that can result in malware, redirection to malicious websites and more.
3. 72% of vulnerabilities were due to flaws in web application coding
4. The number of material breaches respondents suffered rose 20.5% from 2020 to 2021
5. Cybersecurity budgets as a percentage of firms' total revenue jumped 51%, from 0.53% to 0.80%
6. 30% of executives said their budgets aren't sufficient to ensure proper cybersecurity
7. 31% of executives said their main cyber security challenge was improper identification of key risks
8. 50% of companies outsource their cyber security operations center
9. The most used cyber security framework was ISO 27001/27002 at 48% of companies.
10. 55% of companies run internal cyber security assessments
11. Only 38% of companies say they have made notable improvements after a breach
12. Only 23% of companies say their cybersecurity metrics are well understood by the board and senior executives.
13. The top cyber security investment is upskilling cybersecurity and IT staff with 46% of companies reporting this.
14. 41% of cyber security executives report using Zero Trust architecture principles
15. 63% of companies have some form of email security measure
16. The average time to detect a data breach is 118 days
17. Only 29% of companies reported using multi-factor authentication
18. 26% of companies reported using AI and machine learning solutions to predict and handle breaches
19. 66% of organizations expect their cyber security budget to grow in the coming year.
20. 46% of organizations test cyber incident response time and planning every quarter.
21. 41% of organizations identified hybrid IT situations as their biggest cyber security challenge
22. 46% of companies have identified increased CEO support as a major driver of cyber security-aware work culture.
23. 53% of users haven't changed their passwords in the last 12 months
24. 57% of users reported having a password written down on a sticky note
25. 37% of employees use their employer's name as a portion of their password
26. 44% of users reported recycling passwords across personal and business-related accounts.
27. 62% of users have shared a password over email or text messages.
28. 73% of companies in North America use browsers that are out of date
29. The cybersecurity market is expected to grow to $300 billion by 2024.
30. Global spending on cybersecurity exceeded $1 trillion in 2021.
31. The average security budget of small businesses is 500$
32. 1 in 3 US companies has purchased data-breach insurance coverage or cyber liability insurance.
33. The cyber insurance market is expected to be worth $20 billion by 2025.
34. 1 in 10 small businesses suffers a cyberattack each year.
35. The largest DDoS attack was 1.3 terabytes per second.
36. 540 million accounts were affected in the latest Facebook breach.
37. 60% of small businesses go out of business after being victims of a cyber attack.
38. 95% of data breaches are due to human error.

Search

Search...

Categories

Compliance and Governance (9)
Cyber Security Awareness (298)
Data Privacy Awareness (57)
Events (11)
GDPR (9)
News (25)
Phishing (91)

Recent Posts

What is Baiting in Cyber Security?
7 Smishing Examples and How to Protect Yourself
What is Swatting? What to Look for and How to Defend Yourself
The 2023 Gone Phishing Tournament Results: Everything You Need to Know
Protect your loved ones from phishing, social engineering and other cyber attacks

Tags

byod CISO
Communication tools
Covid-19 Scams
credential stuffing attacks
Cyber Security Awareness
cyber security professional
Data breaches Data Privacy
End user engagement
gartner magic quadrant
GDPR Training governance
Human Risk
information security awareness
information security program
Ilse Iapointe malware
National Cyber Security Awareness Month
NCSAM Password phishing
Phishing scams
phishing simulation ransomware
Remote working
Security Awareness Framework
Security Awareness Training
social engineering
Social Networks Work from home

39. 93% of data breaches are motivated by financial gain.
40. 46% of all cyber breaches are done on companies with fewer than 1,000 employees.
41. 70% of cybersecurity professionals claim that their organization is impacted by the cybersecurity skills shortage.
42. 56% of Americans do not know the steps to take after being a data breach victim.
43. 38% of CISOs expect more serious attacks via the cloud in 2023
44. A study has revealed that just 23% of security leaders monitor their partners and vendors in real-time for cyber security risks.
45. By 2025, it is estimated that 60% of organizations will use cyber security risk as a key factor when determining transactions and business engagements with third parties.
46. The USA had 759% more victims of cyber crime in 2021 than the next-highest country, Canada.
47. 62% of incidents in the System Intrusion pattern involved threat actors compromising partners.
48. 30% of small businesses consider phishing attacks to be the biggest cyber threat.
49. 43% of SMBs do not have a cyber security plan in place.
50. Cybersecurity Ventures tracked more than $23 billion in venture capital devoted to cybersecurity companies in 2021.

Malware

Malicious software is still a common threat with thousands of attacks recorded every day. Certain industries like retail are more often targeted, but malware is often coupled with other tactics such as phishing. In most situations, adware is the target, but traditional data breaches are still something to look out for.

51. There were 5.4 billion malware attacks in 2022
52. The US sees the most malware attacks per year, 9x more than #2 the UK
53. In a recent survey, 53% said they were victims of adware
54. 71% of malware attacks have a specific target
55. 17% of malware attacks target individuals
56. 40% of malware attacks result in confidential data leakage
57. The most common malware type used for individuals is spyware.
58. Cyber attacks on the retail sector increased by 117% in 2021
59. 70% of attacks on the retail sector led to customer data theft
60. A database of gift cards to multiple retailers totalling $38 million was put up for sale on the dark web in 2021
61. 5,520,908 mobile malware, adware and riskware attacks were blocked.
62. Adware accounted for 25.28% of all mobile threats detected.
63. 405,684 malicious installation packages were detected in 2022, the leading type being mobile banking trojans.
64. Iran was the leading target of malware attacks, accounting for almost 27% of all attacks in 2022
65. 70% of organizations have users being served malware ads on their browser
66. 48% of organizations experienced information theft via malware.
67. Ursnif/Gozi and IceID were the most popular trojans of 2022

Phishing

Phishing is perhaps the most well-known cyber security threat and statistics prove that it is top of mind for most cyber security professionals. The goal is still majorly to steal credentials and younger users seem to be less prepared for this type of attack.

68. 96% of phishing attacks are delivered via email
69. 90% of data breaches are the result of phishing attacks
70. Phishing and business email compromise results in over 500 million dollars in losses per year, according to the FBI
71. In a recent survey, 77% of respondents said their main cybersecurity fear was a targeted phishing attack
72. Credential theft is the top goal of phishing attacks at 51.8% in 2021
73. Phishing emails are the leading delivery method for ransomware attacks
74. Security firm Slashnext estimates there will be 255 million phishing attacks in 2022
75. 18-24 is the age group that fell for phishing emails the most in 2022
76. 50% of people who fell for a phishing email said it was because they were tired or distracted
77. 85% of mobile phishing attacks happen outside of email whether through messaging apps, social networks or games.
78. The financial services industry saw 5 times more phishing attempts than any other industry in 2022
79. 682 brands were the target of spoofing phishing attacks in November 2023 alone
80. 43% of spoofing attacks impersonated Microsoft
81. 32% of phishing attacks involve the impersonation of a social network

Ransomware

Ransomware has seen an important increase in recent years since it is one of the most lucrative hacks. Industries where technology access is mission critical such as healthcare and government remain the top targets.

This type of attack has become one of the most well-known by consumers, and it's top of mind to them because it so often results in data leakage and interruptions of service. Industries targeted by this type of attack should be wary since it is increasingly linked to the abandonment of services.

82. Ransomware breaches have seen a 13% increase in the last 5 years
83. According to firewall maker SonicWall, ransomware attacks surged by 105% in 2021
84. 2022 saw 623.3 million ransomware attacks around the world
85. The two most targeted industries for ransomware are healthcare and government with 121% and 94% increases in 2021, respectively.
86. There were 20 ransomware attacks every second in 2020
87. The average cost of a ransomware attack is 4.54 million, excluding the cost of the ransom itself.
88. The average downtime experienced after a malware attack is 21 days
89. Ransomware is the #1 malware threat
90. CryptoLocker is the leading ransomware variant affecting 52% of respondents to a survey
91. 63% of cyber attacks against government agencies use ransomware
92. 79% of attacks on the retail sector involve ransomware
93. 45% of security and IT execs expect a further rise in ransomware attacks

94. 59% of consumers said they would avoid doing business with a company that has suffered a data breach in the last year.
95. 70% of consumers believe companies aren't doing enough to secure their personal data.
96. 25% of consumers will stop using a product or abandon it if it has been the target of a ransomware attack.

Finance

The finance sector has always been an attractive target for all types of criminals. With money becoming increasingly digital, hackers have increased their efforts targeting banks and other financial institutions.

Ransomware remains a leading trend due to the critical nature of the software being used in the financial sector, but companies in this industry also hold a lot of sensitive data making data breaches a popular cyber attack.

97. System Intrusions have doubled from 14% in 2016 to 30% in 2023 (source: Verizon)
98. The finance sector is the second most targeted industry for basic web application attacks (source: IBM)
99. Finance sector data breaches are amongst the most expensive to fix (source: IBM)
100. On average, a financial services employee has access to 13% of the company's total files. (source: Varonis)
101. The two main cyber threats in the education sector are software vulnerability exploitation and phishing, accounting for 29% and 30% of overall attacks, respectively. (source: Infosecurity Magazine)
102. Leak of confidential information and disruption of core activity are the top 2 results of a cyber attack at 64% and 40%, respectively. (source: PT Security)
103. Ransomware accounts for 64% of successful cyber attacks against the financial sector. (source: PT Security)
104. 63% of financial institutions reported an increase in destructive cyber attacks. (source: Blaze Infosec)
105. A data breach in the finance sector costs $5.85 million on average (source: Banking Exchange)
106. 57% of banking executives identified cyber security as a top priority this year. (source: CSI Web)

Healthcare

The healthcare industry faces a dangerous problem when it comes to cyber security. Their systems being down can easily lead to loss of life, which means hospitals often pay ransomware demands.

This habit has, in turn, made the industry as a whole a prime target for cyber attacks. The healthcare industry faces a difficult battle against cyber threats with shrinking budgets and staffing issues, but cyber security awareness training shines even under the toughest conditions.

107. Since 2020, healthcare data breach costs have increased by 53.3% (source: IBM)
108. Healthcare continues to experience the highest data breach costs of all industries, increasing from USD 10.10 million in 2022 to USD 10.93 million in 2023—an increase of 8.2%. (source: IBM)
109. The healthcare sector suffered nearly 337 breaches in the first half of 2022 alone, affecting 19,992,810 individuals. (source: Protenus)
110. Healthcare email fraud has increased by 473% since 2019 (source: HIPAA Journal)
111. Over 93% of healthcare organizations have experienced a data breach in recent years, and 57% have had more than five data breaches. (source: Black Book Research)
112. Data breaches in the healthcare sector are responsible for a 64% increase in advertising expenses to reassure consumers. (source AJMC)
113. The cost of a healthcare breach is about $408 per patient record, without including the cost of the loss of business, productivity and reputation. (source: Healthcare Finance News)
114. Healthcare institutions spend, on average, 4 to 7% of their budget on cyber security, compared to an average of 15% for other industries. (source: Healthcare Finance News)
115. Medical devices have an average of 6.2 cyber security vulnerabilities each. (source: Cybersecurity Ventures
116. 62% of hospital administrators feel unequipped or undertrained to deal with a cyber security breach. (source: Becker Hospital Review)

Education

Education is a relatively recent cyber attack target, but has been very popular with the advent of online schooling in recent years. From K-12 to higher education, these institutions hold a tremendous amount of personal information that can have devastating results if leaked.

With a recent surge in attacks on K-12 schools, it's no surprise to discover cyber security as a priority for school administrators across the globe.

117. Educational institutions experienced a staggering 2,507 attempts per college or university per week in 2023 (source: Educause)
118. 66% of education organizations reported being hit by a ransomware attack (source: Sophos)
119. 50% of education organizations reported having to use multiple restoration methods to restore data after a ransomware attack. (source: Sophos)
120. Only 4% of institutions reported recovering 100% of their data after paying the ransom. (source: Sophos)
121. 62% of education administrators have reported difficulties in hiring cyber security staff. (source: Chronicle)
122. 65% of higher education institutions have designated data security as a top priority this year. (source: Higher Ed Dive)
123. The average cost to remediate a ransomware attack in higher education is $1.42 million. (source: Educause)
124. 1,847,000 students have been impacted by ransomware attacks in the United States alone since the beginning of 2020. (source: US Government Accountability Office)
125. SonicWall reported an 827% spike in attacks on K-12 schools in 2022. (source: Higher Ed Dive)
126. According to the US Government Accountability Office, ransomware attacks result in 3 days to up to 3 weeks in lost learning time. (source: US Government Accountability Office)

Business Email Compromise(BEC)

One of the most potentially damaging hacks, BEC continues to cause billions of damage every year. Thankfully, it is one of the attacks that cyber security awareness solves the easiest.

127. Gift card requests are the most common way to retrieve funds from an attack, constituting 68% of such attacks.
128. 19% of data breaches are the result of BEC
129. 29% of companies have reported losing a client in 2022 due to a business email compromise
130. 52% of people who clicked on a phishing link did so because they thought it came from a senior executive in the company.
131. BEC attacks led to $1.8 billion in damages in 2021

Recap

These statistics show that cyber security still needs to be a top priority for all businesses across all industries. Hackers are constantly innovating to carry out attacks, and the most efficient way to remain ahead of the curve is to be aware and educated.

The dominating trend across these statistics is the lack of user knowledge and preparedness. Almost all cyber attacks can be entirely negated or severely mitigated with the right behaviors. Thankfully, a lot of businesses see the need and are increasing budgets across the board. With cyber security spending expected to exceed a trillion dollars this year, these statistics are bound to become more encouraging with time.

Share:

Newer
Protecting Your Healthcare Organization from Cyber Attacks and Threats

Older
New Attack Allows Hackers Access to Google Accounts Without Passwords

FORTRA
Terranova Security