SECURITY

13 CYBER SECURITY STATS

Cybersecurity matters are fast becoming a daily struggle. Side effects of the global pandemic and recent security trends are leading to an increase in security threats. Unprotected data, poor security practices and a rise in remote workers is also leading to vulnerabilities. To give you an idea of the current security landscape, we've compiled some statistics. Hopefully this will show you how prevalent the risks are, and how important it is to have a sound security strategy in place.

The worldwide information security market is forecast to reach $170.4 billion in 2022. (Gartner).

According to Cybint, 95% of cybersecurity breaches are caused by human error.

45% of breaches feature hacking
17% involved malware
22% involved phishing

43% of all cybersecurity attacks are targeted at small business (Fundera).

70% of organizations said remote working would increase the cost of a breach (IBM).

ARE YOU AWARE OF THE MOST COMMON SECURTITY THREATS?

68%

of business leaders feel their cybersecurity risks are increasing. (Accenture)

86%

of breaches were financially motivated and 10% were motivated by espionage. (Verizon)

88%

of organizations worldwide experienced spear phishing attempts in 2019. (Proofpoint)

ARE POOR SECURITY PRACTICES PUTTING YOUR BUSINESS AT RISK?

$3.86 million

The average cost of a data breach is $3.86 million as of 2020 (IBM).

207 days

The average time to identify a breach in 2020 was 207 days (IBM).

Average cost $133,000

The average cost of a ransomware attack on businesses is $133,000. (SafeAtLast)

94%

94% of malware is delivered by email. (CSO Online)

77%

More than 77% of organizations do not have an incident response plan. (Cybint)

IBM, SafeAtLast, Cybint, CSO ONline, Proof Point, Accenture, Verizon, Fundera, Gartner. 134 Cybersecurity Statistics and Trends for 2021 | Varonis