20 Shocking Statistics About Cybercrime

THE CYBERTHREAT LANDSCAPE IS GETTING RISKIER AND COSTLIER BY THE DAY

Just how massive and destructive has cybercrime become? Here are 20 statistics that paint a shocking picture — like InfoSec World's version of Edvard Munch's **The Scream**.

1. The cybercrime economy has grown to $1.5 trillion a year. [Source]

2. Security breaches in 2018 climbed 11% from 2017, and they have increased 67% since 2013. [Source]

3. The volume of malicious PowerShell scripts increased by 1,000% in 2018. [Source]

4. Unpatched and outdated software is responsible for 22% of security incidents. [Source]

5. Third-party app stores host 99.9% of all discovered mobile malware. [Source]

6. Small and Mid-Size Businesses (SMBs) are targeted in 43% of cyberattacks. [Source]

7. Email is responsible for distributing 92% of all malware. [Source]

8. The overall damage caused by cybercrime will reach $6 trillion a year by 2021, up from $3 trillion a year in 2015. [Source]

9. The average cost of a data breach is $7.91 million for companies in the U.S., and $3.86 million for companies worldwide. [Source]

10. It takes an average of 196 days to discover a data breach. [Source]

11. It takes an average of 49.6 days between discovering a data breach and reporting it. [Source]

12. Every 14 seconds there is a new ransomware attack, which will cost victims $20 billion by 2021. [Source]

13. Hackers can purchase cybercrime toolkits on the dark web for as little as $1. [Source]

14. The #1 country that cybercriminals target is the U.S. [Source]

15. By 2023, cybercriminals will steal an estimated 33 billion records. [Source]

16. 88% of companies with more than 1 million folders lack appropriate access limitations, and 58% of companies have more than 100,000 folders accessible to all employees. [Source]

17. 95% of HTTPS servers are vulnerable to Man-in-the-Middle (MitM) attacks. [Source]

18. Phishing attacks posing as SaaS platforms increased 237% in 2017. [Source]

19. 46% of websites have high security vulnerabilities, and 87% of websites have medium security vulnerabilities. [Source]

20. 70% of employees don't understand basic cybersecurity. [Source]

Things Are Getting Worse

OK, you can come out from under your desk now — we've stopped with the scream-inducing cybercrime statistics (for now). Regardless of how you crunch the numbers and analyze the trends, this much is abundantly clear: the cyberthreat landscape is getting riskier and costlier by the day. And not just for large corporations, either. Since they are easier to target and have valuable data to steal, small businesses are now ground zero for cyberattacks — and 60% of small businesses fold within six months of a cyberattack.

Minimizing Cyberattacks

With this in mind, is it possible to 100% prevent a cyberattack? Unfortunately, the answer is no. If cybercriminals are motivated, skilled and well-funded, it is only a matter of time before they break down (or break through) endpoint and network defense tools and systems.

However, companies can — and frankly, they must — make it as difficult as possible for cybercriminals to raid their digital fortresses. It is similar to safeguarding a home. Seasoned burglars can break into virtually any home they want to, but they are much more inclined to target homes with weak security than those with state-of-the-art surveillance and alarm systems. Cybercriminals are just as pragmatic. They aren't looking to win any creativity awards. They're looking to steal data and make money — and the easier, the better.

Best Practices for Preventing Data Hacks

Our Product Marketing Specialist, Jenny, recently published a list of best practices for preventing data hacks that you can find here. Its timely information and advice can help your organization stay at least a step or two ahead of the bad guys — and lower your chances of becoming a terrifying cybercrime statistic.