February 21, 2020 0

42 Cyber Attack Statistics by Year: A Look at the Last Decade

in **CYBER SECURITY**
(**25** votes, average: **3.76** out of 5)

Do you remember what some of the top cyber attacks statistics were over the past decade? We're here to remind you and to provide a comparison for the year 2020

In 2020, cyber attacks seem to be making headlines just about every day. Data breaches, data leaks, phishing scams, ransomware attacks — you name it, somebody, somewhere has fallen

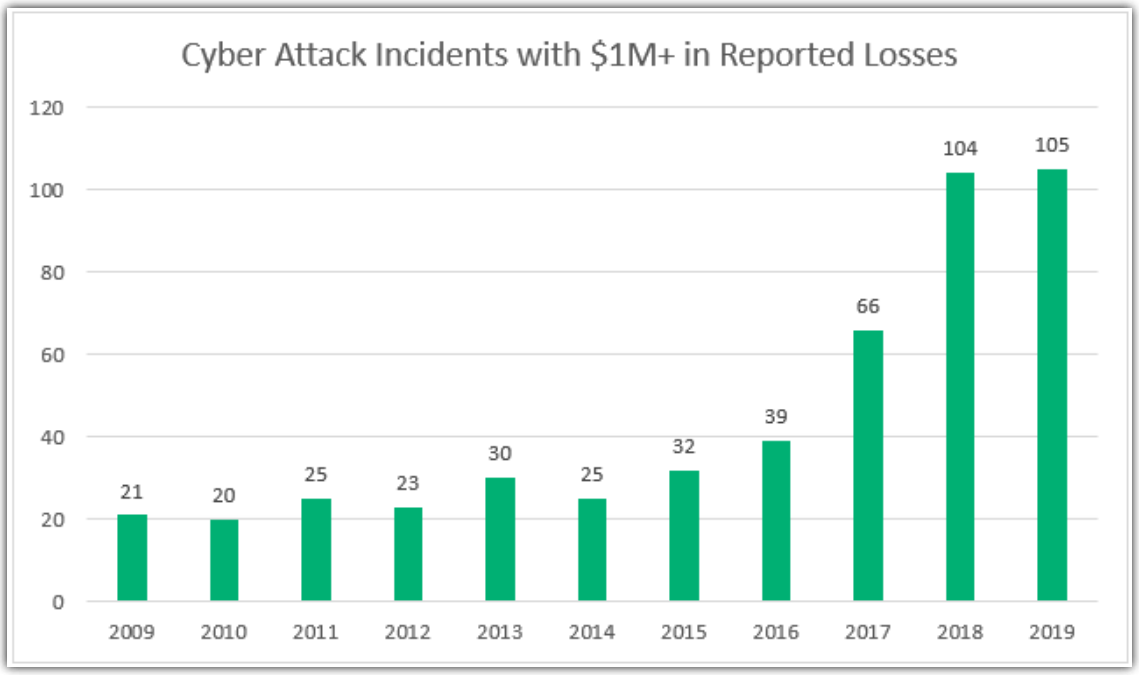
victim to them. This is why we thought it might be cool (and potentially painful) to see the progression of cyber attack statistics over the last decade.

Here are some of the top cyber attack statistics from each year over the last decade. For this article, we're going to draw from a number of notable research publications from government institutions, industry associations, reputable corporations, and news organizations.

The Top Cyber Attack Statistics Reported in the Last Decade

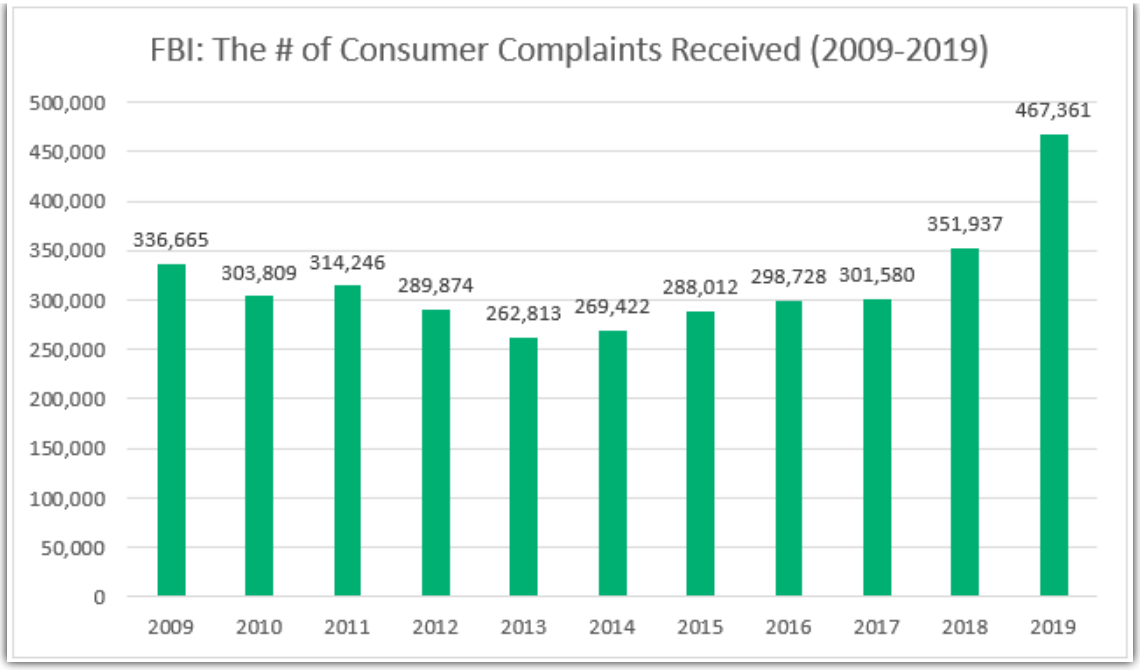
Over the past 10 years, there have been a lot of cyber attack trends we've seen come and go. Some are pretty regular in terms of being counted from year to year. For example, one such cyber security attack statistic that we're able to track from year to year is the number of cyber attacks that result in reported losses that exceed $1 million.

The Center for Strategic & International Studies (CSIS) tracks "cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars." Over the past decade, they've tracked 490 significant cyber incidents.



Below, we've put together a chart that showcases the number of consumer complaints that were reported to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC^3) between 2009 and 2019. They handle complaint reported about a wide variety of internet-facilitated criminal activity and have since the center's inception in May 2000.

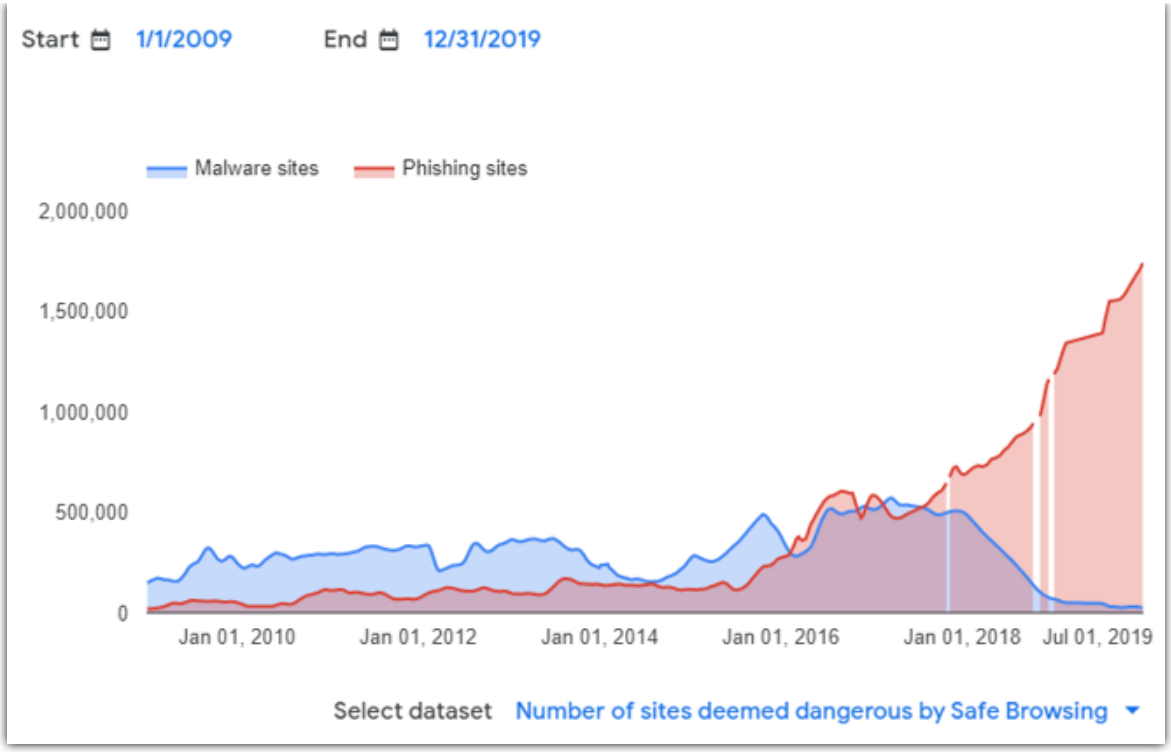
The chart below showcases how this particular cyber attack statistic has changed from year to year:



You know what else has steadily increased over the last decade? The cost of losses from consumer complaints that were reported to the FBI IC^3. See for yourself:

Note: 2010 was a year that the IC3 report did not include its calculation of reported annual losses. As such, we reported it as a "0" but at least wanted to take a moment to explain that it wasn't a matter of there being no reported financial losses — it's just that the FBI didn't disclose that information in its report.

Looking at the year-over-year trends, the number of known phishing websites is also on the rise. Let's take a look at a chart from the Google Transparency Report on Safe Browsing: malware and Phishing:



Between January 1, 2009 and Dec. 31, 2019, you can see a very clear increase in phishing sites that Google's Safe Browsing service detected over time. Now, of course, this could be because of how they define phishing. Or because their algorithms improved and become more capable of identifying such sites. A third option is that it could be because phishing sites have just increased in number so rapidly that it resulted in that big spike between 2016 and 2019.

Or, it could also be a result of all of the above.

But how exactly does Google describe phishing websites? According to their Transparency Report page:

> *These websites pretend to be legitimate so that they can trick users into typing in their usernames and passwords or sharing other private information. Web pages that impersonate legitimate bank websites or online stores are common examples of phishing sites"*

All of this is great, but we know you're here for something more statistic. With this in mind, let's cover some of the most noteworthy cyber attack statistics by year.

The Top Cyber Attack Statistics of 2009

The global economic recession had a big impact on businesses and individuals in terms of cybercrime. A litany of scams and phishing emails promising solutions targeted recession victims, and new cyber attack tactics made their foray into the wild.

Here are some of key cyber attack statistics to note in 2009:

1. **The FBI's IC3 Received a Total of 336,655 Consumer Complaints of Fraud and Scams**

The FBI's Internet Crime Complaint Center (IC3) reported in its 2009 Internet Crime Report that they received more than 335,000 complaints with estimated losses from that year reported at more than $560 million. This jump in the number of consumer complaints is likely due to the recession we mentioned a few moments ago.

2. **Hacking Involved in 60% of Identity Exposure Cases**

In Symantec's Global Internet Survey Threat Report (ISTR) for 2009, the company reported that "60 percent of identities exposed were compromised by hacking attacks."

3. **Botnets Sent 85% of Spam Emails**

The same Symantec Global ISTR report data indicates that approximately 85% of spam emails sent during the year were linked to botnets.

The Top Cyber Attack Statistics of 2010

There were many notable cybersecurity events of 2010. One of the most impactful was the discovery of Stuxnet, a malicious computer worm that was thought to be responsible for causing significant damage to the software of at least 14 nuclear facilities in Iran.

Here are some of the top cyber attack statistics of 2010:

4. **The FBI's IC3 Received a Total of 303,809 Consumer Complaints of Fraud and Scams**

The FBI's Internet Crime Complaint Center (IC3) reported in its 2010 Internet Crime Report that they received more than 300,000 complaints that year. However, they did not disclose the estimated annual losses from those internet-based crimes.

5. **Kaspersky Lab Reported 580,371,937 Cyber Attacks Against Users**

The U.S. ranked No. 1 for the highest number and percentage of malware-based cyber attacks that were launched from web resources — 137,487,939 unique web-based attacks, or nearly 26% of all attacks — in 2010.

6. **4 Companies Were Responsible for Kaspersky's Top 20 Software Vulnerabilities**

The same Kaspersky Lab report noted that the Top 20 most common vulnerabilities were found in software developed by four big name companies: Microsoft (8), Adobe (8), Oracle (3), and ACDSee (1). However, it's important to note that some of those vulnerabilities were detected as early as 2007.

The Top Cyber Attack Statistics of 2011

Like 2010 before it, 2011 hit the ground running in terms of major cyber attacks. The attacks against international organizations, businesses, and governments were carried out by hackers and nation-state actors.

Here are some additional cyber attack statistics of interest in 2011:

7. **U.S. Intelligence Performs 231 Cyber Operations**

In 2011, a decade after the Sept. 11 attacks occurred, the Washington Post reported that U.S. intelligence organizations carried out "231 offensive cyber-operations" in a massive campaign of cyber warfare.

8. **The FBI's IC3 Received More than 300,000 Consumer Complaints of Fraud and Scams**

The FBI's Internet Crime Complaint Center (IC3) reported in its 2011 Internet Crime Report that they received 314,246 complaints with estimated losses from that year reported at about $485 million.

9. **Annual Browser-Based Attacks Increase to Nearly 1 Billion**

Kaspersky reports that the number of browser-based attacks they detected increased to 946,393,693 in 2011 — a number that's up from 580,371,937 the previous year.

10. **77 Million Users Impacted by PlayStation Network and Qriocity Breach**

Sony announced that the personal and user information of 77 million PlayStation Network and Qriocity users was stolen by one or more hackers via an attack that occurred over a three-day period in April.

The Top Cyber Attack Statistics of 2012

2012 was a year marked by the targeting of nations' critical infrastructure — particularly the United States. Here are some of the top cyber attack statistics of 2012:

11. **Attacks on Critical Infrastructure Increased 52%**

The U.S. Department of Homeland Security (DHS) reported a significant increase in the number of cyber attacks on critical infrastructure in 2012, according to CNN. The article reports that cybercriminals mainly focused their attacks on organizations within the water and energy sectors and experienced success with "'several' of their nuclear targets."

12. **Browser-Based Attacks Jumps to Nearly 1.6 Billion**

Web-based attacks rose from 946,393,693 to 1,595,587,670 in 2012, Kaspersky Labs reports. This rate of growth is consistent with the previous couple of years.

13. **Botnet of 700,000 Infected Apple Computers Discovered**

2012 marked the year when the "Apple-is-invincible" myth was debunked with the discovery of the Flashfake botnet. According to Kaspersky Labs' 2012 bulletin, this network of infected computers consisted of 700,000 computers that used Mac OS X.

The Top Cyber Attack Statistics of 2013

2013 marked the year when cybersecurity became a central feature in foreign policy and national security as a whole. It saw the rise of the “hack back” industry and was the year when Edward Snowden became an enemy of the state.

Here are some of the most impactful cyber attack statistics of 2013:

14. **The Stock Market Nosedived $136 Billion Due to a Social Media Cyber Attack**

Do you remember reading the fake headline about how there were two explosions at the White House and then-President Barack Obama was injured? The Washington Post reported that the fake tweet was posted by the Associated Press’s (AP) official Twitter account, which became compromised after AP staffers fell for a phishing scam.

15. **3 Billion Yahoo Accounts Hacked in Massive Data Breach**

Verizon, the parent company of Yahoo, announced in a 2017 press release that the initial estimates of the number of user accounts exposed in a 2013 breach — one billion — was vastly underestimated. Their 2017 report states that new intelligence they obtained indicates that “all Yahoo user accounts were affected by the August 2013 theft.”

16. **Browser-Based Cyber Attacks Surpassed 1.7 Billion**

Kaspersky reports that they neutralized 1,700,870,654 web-based threats in 2013. This number is up from the 1,595,587,670 threats reported in 2012. Almost half (43%) of the attacks they ceased originated from web resources in the U.S. and Russia.

17. **552 Million Identities Exposed by Data Breaches in 2013**

Symantec’s 2013 ISTR report indicates that more than half a billion identities were exposed via data breaches in 2013. An average of 2,181,891 million identities were exposed per event — an increase of 261% over the 604,826 reported the previous year.

18. **“Human Error” Contributes to 95% of Cybersecurity Incidents**

In the IBM Security Services 2014 Cyber Security Intelligence Index, IBM reported that "over 95 percent of all incidents investigated recognize 'human error' as a contributing factor." The most commonly reported errors to make their list?

- Misconfigured and poorly patched systems,
- Use of default usernames and passwords,
- Lost laptops or mobile devices, and
- Disclosure of sensitive information wrong email addresses

19. **Mobile Malware Reaches New Levels with 148,427 Modifications**

Good news for non-Android mobile users: The overwhelming majority of mobile malware — more than 98% — focused on Android devices. These types of malware included trojans, trojan spies, and SMS trojans.

The Top Cyber Attack Statistics of 2014

By virtually all accounts, 2014 was the posterchild year for cyber security concerns. Data breaches and cyber threats seemed to take up permanent residence on the front pages of new publications. Cyber attacks exposed a litany of health records, PII, and financial information.

Here are some of the top cyber attack stats of 2014:

20. **3 Industries Targeted by 62% of Cyber Attacks**

IBM reported in its 2015 Cyber Security Intelligence Index that nearly two-thirds of cyber attacks focused on three industries: finance and insurance, information and communications, and manufacturing.

21. **The FBI's IC3 Received a Total of 269,422 Complaints of Fraud and Scams**

The FBI's Internet Crime Complaint Center (IC3) reported in its 2014 Internet Crime Report that they received nearly 270,000 complaints with estimated losses reported at $800,492,073 in 2014 alone.

22. **More than 1.4 Billion Browser-Based Attacks Reported**

Web-based attacks decreased from 1,700,870,654 to 1,432,660,467 in 2014, Kaspersky Labs reports. Attackers frequently used exploit packs to infect computers by targeting vulnerable applications.

23. **More Than 6.1 Billion Threats Detected & Neutralized in 2014**

The number of cyber threats continue to climb. The same Kaspersky report data indicates that they alone "detected and neutralized a total of 6,167,233,068 threats during the reported period." That number doesn't even include threats that were detected by other IT security solutions providers!

The Top Cyber Attack Statistics of 2015

2015 was a year that resulted in many data breaches of big-name companies, including the affair website Ashley Madison and the healthcare provider Anthem. Here are some of the most notable cyber attack-related stats from the year:

24. **91% of IT Service Providers' Clients Victimized by Ransomware**

More than 90% of Datto IT survey provider survey respondents indicate that their clients were victimized by ransomware in the previous year. The survey of 1,000 ISPs (representing hundreds of thousands of small businesses globally) was eye-opening for sure. In the U.S. alone, Datto estimates that these attacks "cause $75 billion in damages" to SMBs with downtime often costing those businesses more than $8,500 per hour.

25. **431 Million New Malware Variants Discovered**

The number of new malware variants added in 2015 was 431 million. Symantec's ISTR, which reported this number, also says it's equates to a 36% increase over the previous year's number of 317 million.

26. **9 Data Breaches Exposed a Minimum of 10 Million Identities Per Event**

Data from the same ISTR report from Symantec indicates that there were nine breaches that exposed a minimum of 10 million identities per incident.

27. **191 Million Registered Voters PII Exposed**

Due to a database server misconfiguration, the personal information of 191 million registered voters was left exposed on the internet. The exposed information was discovered by a hacker by the name of Chris Vickery.

The Top Cyber Attack Statistics of 2016

2016 saw some of the largest cyber attacks in recent history. Companies were getting "pwned" via hacking, DDoS attacks, and ransomware attacks in particular — and it appeared that no one

was safe.

See for yourself. Here are a few of the key cyber attack statistics from 2016:

28. **Only 15% of Organizations Report Ransomware Attacks**

According to a report by cyberscoop.com, “Only an estimated 15 percent of the nation’s fraud victims report their crimes to law enforcement… This 15 percent figure is just a subset of the victims worldwide.” Case in point? In 2016, the FBI’s IC^3 reported receiving only “2,673 complaints identified as ransomware with losses of over $2.4 million” — a number that’s significantly lower than other industry estimates and forecasts.

29. **More Than 750,000,000 Web-Based Attacks Were Thwarted**

Kaspersky’s 2016 bulletin reports that their software was able to repel 758,044,650 attacks from global resources. Nice job, guys.

30. **Cyber Attacks Cost the U.S. Economy Up to $109 Billion in 2016**

The White House’s Council of Economic Advisers released a report “The Cost of Malicious Cyber Activity to the U.S. Economy” in February 2018 that said the economic impact of such activity was estimated to be between $57 billion and $109 billion.

31. **Hacking of Adult Website Resulted in the Exposure of 412 Million Users**

More than 410 million AdultFriendFinder customers found themselves exposed in an undesired way when their user credentials and other information was discovered for sale on the dark web, according to Forbes.

32. **Cyber Attacks Measuring 1 Tbps Affected Service Providers**

The same Forbes report indicates that the DDoS cyber attacks that targeted Netflix, PlayStation Network, Twitter, and others using compromised endpoint IoT devices measured in at nearly 1 Tbps.

The Top Cyber Attack Statistics of 2017

The year 2017 is one that will live in infamy for cybersecurity and IT security experts. It was the year of the WannaCry ransomware attacks targeted businesses, healthcare, and government institutions in more than 150 countries. The attack, which resulted from hackers exploiting the eternal blue vulnerability the NSA discovered in Microsoft’s Windows operating system (OS).

33. **Nearly 1.2 Billion Web-Based Cyber Attacks Repelled**

Kaspersky reports repelling 1,188,728,338 browser-based attacks over the year. The same report data shows that nearly 2 million “unique URLs were recognized as malicious by web antivirus components.”

34. **Cybercrime Cost Global Consumers $172 Billion in 2017**

The Norton Cyber Security Insights Report (Global Results) reported that 978 million people in 20 countries were affected by cybercrime throughout the year. On average, global consumers of these crimes lost $172 billion — an average of $142 per victim — and nearly 24 hours dealing with issues that resulted from their victimization.

35. **41% of Consumers Globally Don't Trust Governments with Their PII**

In some ways, it doesn't really come as a surprise in light of the Eternal Blue exploit by the NSA (a government agency). However, Norton's CSIR report indicates that they're more likely to trust identity theft protection services (76%), email service providers (80%), and financial institutions (82%) than they are their own governments.

The Top Cyber Attack Statistics of 2018

2018 was a busy year for hackers — particularly those who prefer using ransomware attacks. Let's review some of the top cyber attack statistics for the year:

36. **Nearly 1.9 Billion Web-Based Cyber Attacks Repelled**

Kaspersky reports that their products shut down 1,876,998,691 browser-based attacks from around the world. The same data also indicates that more than 550,000 unique URLs were discovered to be malicious by antivirus solutions.

37. **Information on Up to 500 Million People Exposed in Marriott Data Breach**

Marriott found itself in the crosshairs of both hackers and the media when the information of up to 500 million guests was exposed by the unauthorized access of a database. This occurred because of a vulnerability in the guest reservation database of its recently acquired Starwood properties. The hotel giant estimated that a vast amount of personal and payment card information relating to 327 million of those guests was exposed in the breach.

38. **Ransomware Attack Costs the City of Atlanta $2.6 Million**

The city of Atlanta virtually came to a halt due to a SamSam ransomware attack that targeted the city's municipal networks and computer systems. The attackers demanded more than $50,000 in Bitcoin payment. The overall recover costs were approximately $2.6 million once all was said and done. NPR reports that two Iranian hackers were eventually charged with the cybercrime.

The Top Cyber Attack Statistics of 2019

The blight of cyber attacks, data breaches, phishing attacks and more seemed to make headlines just about every day in 2019 — and virtually no one was safe. Businesses, city governments, schools, and healthcare organizations all experienced the wrath of hackers through malware and ransomware attacks, and their attacks cost billions globally. In fact, dozens of cities in the U.S., South Africa, and other locations around the world have found themselves the targets of such attacks in the last year.

So, without further ado, here are some of the top cyber attack statistics of 2019:

39. **$26 Billion Lost to BEC/EAC Scams**

The FBI's IC^3 estimates that more than $26 billion dollars was lost between June 2016 and July 2019 due to business email compromise/email account compromise scams.

40. **Nearly 1 Billion Web-Based Cyber Attacks Repelled**

Kaspersky reports that 975,491,360 browser-based attacks from around the world were halted by their products. The same data also indicates that 273,782,113 unique URLs were discovered to be malicious.

41. **More than $675 Million Stolen by North Korean Nation-State Actors**

In March 2019, the UN Security Council reported more than $678 million in foreign currency and cryptocurrency theft by North Korea between 2015 and 2018. The nation-state actors attempted to steal $1 billion via state-sponsored hacking of companies and cryptocurrency exchanges from companies around the world.

42. **400% Increase in Threats to Mac Devices**

In its 2020 State of Malware Report, Malwarebytes reports that the number of threats against Mac devices increased by 40% from 2018 to 2019. They report an average of 11 threats per Mac device, which is nearly double the 5.8 threat average on Windows endpoint devices.

Final Thoughts on Cyber Attack Statistics by Year

It's interesting to see the changes taking place within the industry over the last 10 years. We've seen the growth fluctuations in cyber attacks, the increasingly large reach of the most recent

data breaches and ransomware attacks, and the changing attitudes and decreasing levels of trust concerning data privacy and security.

Needless to say, it'll be interesting to see what the year 2020 has in store. Stay tuned to Infosec Insights and we'll help you stay informed throughout the year to come.

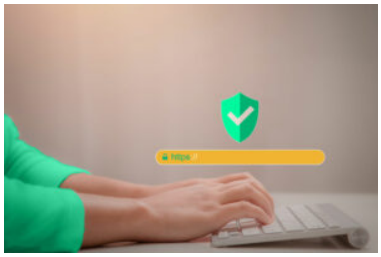
#CYBER ATTACKS #STATISTICS

About the author

Casey Crane

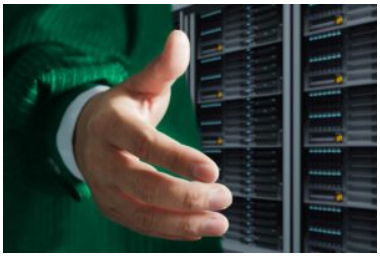
Casey is a writer and editor with a background in journalism, marketing, PR and communications. She has written about cyber security and information technology for several industry publications, including InfoSec Insights, Hashed Out, Experfy, HackerNoon, and Cybercrime Magazine.

You might also like



How to Tell If You're Using a Secure Connection in Chrome

November 15, 2022



TLS Handshake Failed? Here's How to Eliminate This Error in Firefox

November 7, 2022

Years' Old Unpatched Python Vulnerability Leaves Global Supply Chains at Risk

September 22, 2022

No comments

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

Search InfoSec Insights

Search here

Latest Articles

How to Tell If You're Using a Secure Connection in Chrome

TLS Handshake Failed? Here's How to Eliminate This Error in Firefox

Is Email Encrypted? Sometimes… Here's How You Can Tell

What Is a Private Key? A 90-Second Look at Secret Keys in Cybersecurity

Years' Old Unpatched Python Vulnerability Leaves Global Supply Chains at Risk

Recommended Posts

DevSecOps: A Definition, Explanation & Exploration of DevOps Security