




Test Test

test

-  Quick Submit
-  Quick Submit
-  Northholm Grammar Canvas

Document Details

Submission ID**trn:oid:::1:2738513669****Submission Date****Nov 3, 2023, 5:32 AM CDT****Download Date****Nov 3, 2023, 5:33 AM CDT****File Name****userfile****File Size****302.7 KB****4 Pages****569 Words****3,823 Characters**

How much of this submission has been generated by AI?

0%

of qualifying text in this submission has been determined to be generated by AI.

Caution: Percentage may not indicate academic misconduct. Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Frequently Asked Questions

What does the percentage mean?

The percentage shown in the AI writing detection indicator and in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was generated by AI.

Our testing has found that there is a higher incidence of false positives when the percentage is less than 20. In order to reduce the likelihood of misinterpretation, the AI indicator will display an asterisk for percentages less than 20 to call attention to the fact that the score is less reliable.

However, the final decision on whether any misconduct has occurred rests with the reviewer/instructor. They should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in greater detail according to their school's policies.



How does Turnitin's indicator address false positives?

Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be AI-generated will be highlighted blue on the submission text.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

What does 'qualifying text' mean?

Sometimes false positives (incorrectly flagging human-written text as AI-generated), can include lists without a lot of structural variation, text that literally repeats itself, or text that has been paraphrased without developing new ideas. If our indicator shows a higher amount of AI writing in such text, we advise you to take that into consideration when looking at the percentage indicated.

In a longer document with a mix of authentic writing and AI generated text, it can be difficult to exactly determine where the AI writing begins and original writing ends, but our model should give you a reliable guide to start conversations with the submitting student.

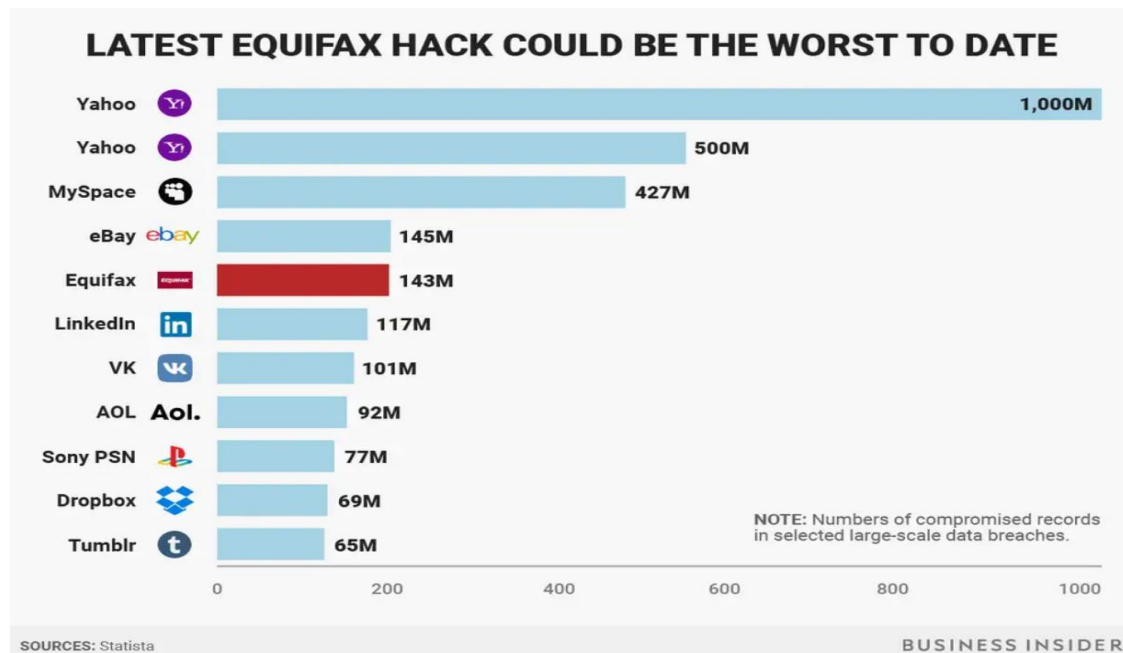
Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify both human and AI-generated text) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Executive Summary

The Equifax data breach, disclosed on March 8, 2017, marked a pivotal moment in cybersecurity history, impacting 147 million Americans (1, Puig). Exploiting a vulnerability in Equifax's web application, malicious actors gained unauthorized access to the company's systems and exfiltrated personal data, including names, Social Security numbers, birthdates, and driver's license information. This breach stands as one of the most substantial cyber incidents to date, jeopardizing the privacy and financial security of millions (2, Thomas). Equifax also suffered severe reputational damage and financial losses as a result.

Figure 1: Comparing Equifax data breach with the worst hacks of all time



Analysis of the Equifax Data Breach

The Equifax data breach could be analyzed using different cyber security models and frameworks such as the CIA Triad, the McCumber Model, and the NIST Cybersecurity Framework as follows.

CIA Triad

The Equifax breach had dire implications for the core principles of the CIA Triad. It compromised the confidentiality of sensitive information through unauthorized access, potentially tampered with data integrity, and disrupted the availability of information for a vast number of individuals.

McCumber Model

Analyzing the breach through the McCumber Model reveals vulnerabilities in Equifax's people, processes, and technology. Failure to promptly patch a known vulnerability reflects shortcomings in the human element. Inadequate security controls for detection and prevention expose process deficiencies. Furthermore, improper network segmentation underscores technological weaknesses.

NIST Cybersecurity Framework

Applying the NIST Cybersecurity Framework to the Equifax breach highlights several shortcomings. Equifax failed to sufficiently identify and protect its critical assets. Inadequate security controls hindered detection and prevention. The company's response was slow and ineffective, and full recovery remains a challenge.

Perimeters

Both physical and cyber perimeters were breached in the Equifax incident. Malicious actors exploited a vulnerability in Equifax's web application to breach the cyber perimeter. Additionally, improper network segmentation enabled lateral movement within the company's systems, compromising the physical perimeter.

Lessons TechWorx Can learn from the Equifax data breach

TechWorx can derive essential lessons from the Equifax breach, including the need to promptly address known vulnerabilities, establish a comprehensive security approach that encompasses diverse security controls and user training, enforce network segmentation to restrict lateral movement, and create and rigorously test an efficient incident response plan. These key takeaways can significantly bolster TechWorx's cybersecurity posture and fortify its defenses against potential cyber threats.

Recommendations for TechWorx

TechWorx can enhance its cybersecurity defenses by adhering to several key recommendations. Firstly, the establishment of a proactive vulnerability management program is crucial to swiftly address known vulnerabilities. Secondly, a layered security strategy should be implemented, which involves integrating tools such as firewalls, intrusion detection systems, and comprehensive security training. Thirdly, network segmentation is vital to minimize lateral movement risks in the event of a breach. Additionally, TechWorx should develop, test, and consistently maintain a robust cybersecurity incident response plan. Lastly, conducting routine security audits and assessments will help identify and rectify potential security vulnerabilities, further strengthening the company's overall security posture.

Conclusion

The Equifax data breach serves as a stark reminder for organizations to prioritize cybersecurity. By adhering to the recommendations provided, TechWorx and similar entities can significantly enhance their cybersecurity measures, safeguard sensitive data, and better protect against the ever-evolving threat landscape.

References

1. Alvaro Puig, July 22, 2019 ,Equifax Data Breach Settlement: What You Should Know, Federal Trade Commission, <https://consumer.ftc.gov/consumer-alerts/2019/07/equifax-data-breach-settlement-what-you-should-know>
2. Jason Thomas, December 2, 2019, A Case Study Analysis of the Equifax Data Breach, ResearchGate, <http://dx.doi.org/10.13140/RG.2.2.16468.76161>