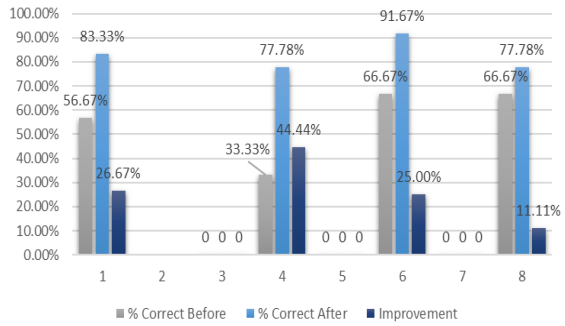

Figure 3. User Results

9. Future Work

Automation

The goal for this solution was to keep automation to a minimum. This goal is to ensure user interaction and predict this would improve the user's long-term memory of the tool. After using this tool for some time, we would add automation to specific areas, including scanning for typos in the test and comparing the hyperlink address value to the embedded link value for equality. Of course, this would come with additional security and privacy measures to be put in place.

More Questions

There are many red flags for an email; it would be wise to add more to the quiz at some point. This addition would ensure each user has covered all their bases regarding how many phishing flags exist in the email in question.

Results to a File

An improvement we found would be helpful after using the extension is to send the data to a file locally after each quiz for auditing reasons. This improvement allowed the user to audit historical activity. This audit would also make it easier to display the results within the tool from a database of entries. Creating the output into a table format from a log entry would make it look more uniform and make it easier to read the data while displaying any additional information to the user.

10. Conclusions

We concluded this process showed a clear improvement between both quizzes. As much of a threat statistically, Phishing involves users clicking malicious links; the group results were relatively high before the tool was given to them. Overall, the method showed improvements in their outcomes as predicted.

Our interactive approach to identifying phishing emails has become a method that we believe can significantly improve the number of clicks and user knowledge over time, especially in conjunction with other methods. The results reveal that users without experience still know which website characteristics to inspect. However, due to the dilemma of users clicking malicious links, perhaps users know what to look for and do not pay close attention at the time regarding some questions to ask themselves. With possible future modifications such as automated detection and improved conventional formatting for the visual references, this has the potential to help users learn what websites are real and which are not.

11. References

[1] Verizon. (2022). 2022 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf. (Access Date 15 November 2022).

[2] IBM. (2022). Ponemon Institute. Cost of a Data Breach Report 2022. IBM Security. https://www.ibm.com/reports/data-breach. (Access Date 15 November 2022).

[3] CS. (23-May-2007). Does Anti-Phishing Training Work? http://www.cs.cmu.edu/~jasonh/publications/apwg-ecrime2007- johnny.pdf. (Access Date 15 November 2022).

[4] Steves,M.P., Greene, K.K.,Theofanos, M. F. (24-Feb-2019). A Phish Scale: Rating Human Phishing Message Detection Difficulty. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/conference-paper/2019/02/24/rating-human-phishing-message-detection-difficulty. (Access Date 15 November 2022).

[5] Chou, N., Ledesma, R., Teraguchi, Y., Boneh, D., and Mitchell, J. C. (2000). Client-side defense against web-based identity theft. https://crypto.stanford.edu/SpoofGuard/web spoof.pdf. (Access Date 20 November 2022).

[6] Milnsbridge. (23-Aug-2022). 5 Characteristics of a Phishing Email. https://www.milnsbridge.com.au/5-characteristics-phishing-email/. (Access Date 24 November 2022).

[7] McCurdy, R. (08-Nov-2022). The biggest phishing breaches of 2022 and how to avoid them for 2023," Security Boulevard. https://securityboulevard.com/2022/11/the-biggest-phishing-breaches-of-2022-and-how-to-avoid-them-for-2023/. (Access Date 16 December 2022).

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0023