Introduction

In cybersecurity, malicious things are often hidden from users and obscured to prevent being detected by intrusion detection systems (Gutzwiller et al., 2024). Also, not every malware or intrusion detection system will always be able to detect something that's hidden and obscured within a file, however, if visualized, humans might be able to perform this detection instead. In this study, the important question is, if raw data is visualized with patterns, could people learn to detect anomalies in this data, which could represent malware?

Experiment Design

In this experiment, data in PDFs was visualized with patterns that represent the raw data in the files. These patterns are called "ambient activity monitors", or AAMs (Gutzwiller et al., 2024). Users are shown a PDF, as well as the AAM for the PDF, then they are asked whether or not the PDF might contain malicious content.

Participants

Participants from this study were government employees at a U.S. DoD lab. Only people who agreed to participate had their answers recorded.

Procedure

Users were introduced to the AAM, and it was explained to them how it worked, but they were not told specifically what to look for. Users were then put into 81 groups to see if they could identify malware within the files by using the AAM. In the control group, 35 people were shown only files without malware and asked if they thought the files contained malware.

Results

In the control group, there was only 66.4% accuracy in detecting if files were malicious or not. However, the experiment group had an accuracy of 78.8%.

Conclusion

In this study, quantitative research was used to find out whether people could identify malware within visualized versions of PDFs. The data that was collected was "Normal", "Anomalous", or "Not Sure". This data was then used to determine the accuracy of people's abilities to detect malware. The research method used in this study was an experiment. The overall contribution of this study to society is that people can be trained to identify malware in files when the raw data inside the files is visualized. The research conducted was as objective as possible by using people of similar skills from the same employer. Parsimony was used to keep the article very short and easily explain what was done and how it was done. Overall, this study didn't relate to the challenges of marginalized groups.

Article Used

https://academic.oup.com/cybersecurity/article/10/1/tyae016/7744929?searchresult=1#479804624