<u>Scenario 1</u>

**Introduction**: The purpose of this study is to examine the relationship between launch delays and profit losses in the game industry. The objectives are to determine the type, strength, and direction of the relationship between these two variables, and to create a predictive model for losses based on the company's launch delays.

**Research questions**

What type of relationship exists between launch delays and profit losses?
What is the strength and direction of the relationship?
Can existing data help predict profit losses based on launch delays?

**Types of variables:** Continuous and numerically measured at a ratio level.

**Dependent variable:** Profit losses expressed in millions British pounds.
**Independent variable:** Launch delays measured in the number of days from the original launch date for each software.

**Exploration of Raw data- Descriptive statistics:** The scatterplot showed a linear relationship between profit losses and launch delays, indicating a positive correlation that longer launch delays cause larger profit loss. The Shapiro-Wilk normality test revealed the significant value of W = .983, p = .669 (> 0.05). As a result, we fail to reject the null hypothesis, suggesting that the data is normally distributed.

*Figure 1: Scatterplot of profit loss and launch days*

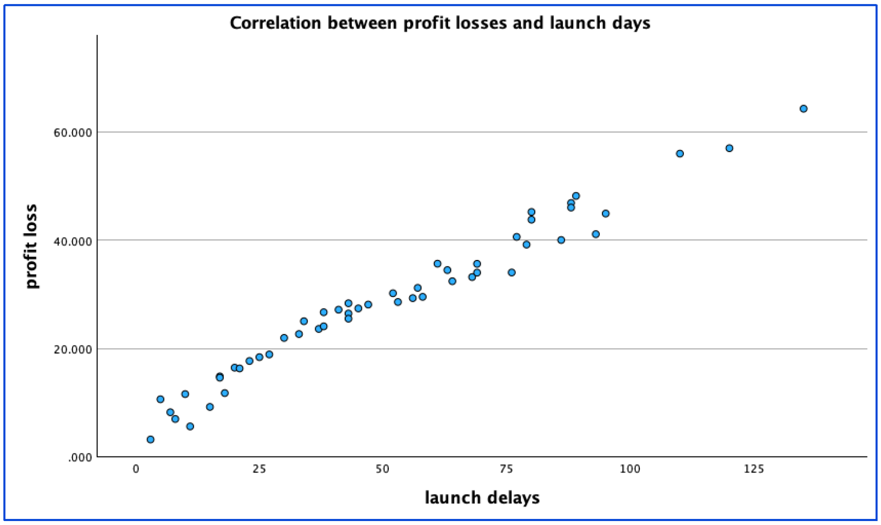


**Table 1: Five-point summary of profit losses (millions) and launch delays ( days )**

| | Profit Loss (millions ) | Launch delays ( days) |
|---|---|---|
| **Minimum** | 3.166 | 3 |
| **First quartile (Q1)** | 17.852 | 24 |
| **Median** | 28.223 | 46 |
| **Third quartile (Q3)** | 38.305 | 77 |
| **Maximum** | 64.300 | 135 |

**Results of statistical tests**

<u>What type of relationship exists between launch delays and profit losses?</u>

**Statistical test and rationale**: Pearson correlation has been used to determine the strength and direction of the relationship between profit loss and launch delays. The test is suitable because the variables are continuous and the dependent variable (profit loss) is normally distributed, which satisfies the requirement for a parametric test.

**Hypothesis**

Null hypothesis (H0): There is no significant correlation between profit loss and launch delays.

Alternative hypothesis (H1): There is a significant correlation between profit loss and launch delays.

**Assumptions for Pearson's Correlation**

1. Both variables are continuous and measured at a ratio level.
2. The scatterplot from Figure 1 showcases a linear relationship.
3. There are no significant outliers as per the scatter plot in Figure 1.
4. Normality of the dependent variable was confirmed in the descriptive statistics section.

Pearson's correlation coefficient (r = .983, n = 52, p = < 0.001) indicates a strong positive correlation between profit loss and launch delays. The relationship is statistically significant because the p-value is less than 0.05, so we reject the null hypothesis.

Can existing data help predict profit losses based on launch delays?

**Statistical test and rationale**: A linear regression was used to determine whether existing data could predict profit losses based on launch delays from the original date. The test is suitable because both variables are continuous, and there is evidence of a linear relationship, indicating that changes in one variable may lead to changes in the other.

**Hypothesis**

Null hypothesis (H0): Launch delays do not significantly predict profit losses.

Alternative hypothesis (H1): Launch delays significantly predict profit losses.

**Assumptions for Linear Regression**

1. Both variables are continuous, paired and independent.
2. The scatterplot from Figure 1 shows a linear relationship with no univariate or multivariate outliers.
3. The dependent variable is normally distributed.
4. Homoscedasticity failed to meet assumptions. The data showed heteroscedasticity, which may affect the standard error and p-values. Therefore, results should be interpreted carefully.

The regression line matches the data well, with R2 = .967

Launch delays explain 96.7% of the total variation in profit losses.

The regression analysis is statistically significant for predicting profit loss. The p-value is <0.01, which is less than 0.05. As a result, we reject the null hypothesis and accept the alternative hypothesis.

Regression equation (line of best fit) = 6.626 + 0.431 x 110 days.

A 110-day delay predicts a 54.4 million profit loss.

**Conclusions**: The results of the research show a strong positive relationship between launch delays and profit loss. Regression analysis showed that launch delays can predict profit losses with 96.7 % of the total variation explained. For instance, a 110-day delay predicts a 54.4 million loss. However, the data showed heteroscedasticity; therefore, the predicted sum should be interpreted carefully. The evidence also indicates that minimising launch delays will result in less profit loss, meaning assumptions have been met.

## Scenario 1 – Table of errors and corrections

| Error | Correct answer/justification | Reference / Evidence |
|---|---|---|
| Incorrect statistical method | Pearson's correlation measures the strength and direction of the linear relationship between two variables.s | |
| Missing type of variable | Dependent variable: profit losses expressed in millions British pounds.<br>Independent variable: launch delays measured in the number of days from the original launch date for each software. | Types of variables |
| Fig. 1 scatterplot missing | A scatterplot should be added as a visual summary | Figure 1 |
| Statistical test results<br>rs(50) = 0.678, p<0.05 | Persons correlation test results ( r =.983 , n=52, p= <0.001) | Results of statistical tests |
| moderate positive correlation | A strong positive correlation was indicated between the two variables. | |
| Five-point summary missing | The five-point summary should be added to state the maximum, Q1, median, Q3 and minimum of the two variables | Table 1 |
| Student did not check all the assumptions of the Pearson correlation test | Missing assumptions for the Pearson correlation test are:<br>Data pairs need to be independent<br>There should be a linear relationship between the two variables<br>Normality should be distributed<br>There should be homoscedasticity | Assumptions for Pearson's Correlation |
| Missing Normality test | The Shapiro-Wilk revealed the significant value of W = .983, p = .669 (> 0.05). We fail to reject the null hypothesis, so the data are normally distributed. | Exploration of Raw data-Descriptive statistics |
| Incorrect line of best fit | Regression equation = 6.626 + 0.431 x 110 days ( predicts 54.4 million profit loss). | Results of statistical tests |

| | | |
|---|---|---|
| Incorrect R2 coefficient | R2 = .967 with a total variation of 96.7% making the linear regression reliable. | |
| In complete conclusion | Regression analysis showed that launch delays can predict profit losses with 96.7 % of variation explained. For instance, a 110-day delay predicts a 54.4 million loss. However, the data showed heteroscedasticity; therefore, the predicted sum should be interpreted carefully. | |

## Scenario 2

**Introduction:** The purpose of this study is to examine the relationship between employees' cybersecurity awareness levels and the frequency of security breaches in Small and Medium-sized Enterprises (SMEs) to gain insights into improving cybersecurity measures.

**Research Questions:** Is there a relationship between employees' cybersecurity awareness levels and the frequency of security breaches in SMEs?

**Dependent variable:** Frequency of security breaches in SMEs, categorised as high or low. (ordinal/categorical)

**Independent variable:** Employees' cybersecurity awareness level, categorised as low, medium, or high. (nominal/categorical)

**Results of statistical tests**

**Statistical test and rationale**: The Chi-square test was used to explore whether there is a significant association between the categorical variables and whether the observed frequencies in the contingency table are different from what would be expected if the variables were independent.

**Hypothesis**

**Null hypothesis (H0)**: There is no association between employees' cybersecurity awareness levels and the frequency of security breaches in SMEs, which means low and high frequency breaches are the same across all awareness levels.

**Alternative hypothesis (H1)**: There is an association between employees' cybersecurity awareness levels and the frequency of security breaches in SMEs, which means low and high frequency breaches are not the same across all awareness levels.

*Contingency table: Observed value (Table 1)*

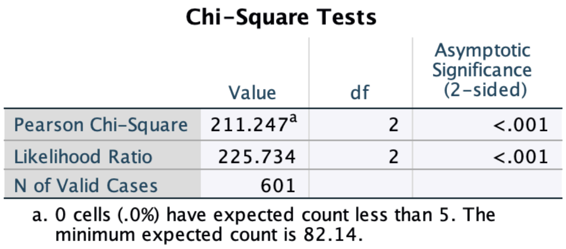
| **Awareness level** | **Low frequency Breaches (less than 50)** | **High frequency breaches ( more than 51 )** | **Total** |
|---|---|---|---|
| **Low** | 47 | 169 | 216 |
| **Medium** | 47 | 140 | 187 |
| **High** | 170 | 28 | 198 |
| **Total** | 264 | 337 | 601 |

**Exploration of Raw Data and Contingency Table:** Employees with low awareness (169 vs. 47) or medium awareness (140 vs. 47) tend to experience high breach frequencies. Whilst employees with high awareness (170 vs 28) are more likely to experience low breach frequencies. For a correct analysis, data will be converted into a proportion of the total employees. An association will exist if the frequencies of low and high security breaches are different across all awareness levels.

*Expected Value: (Table 2)*

| **Awareness level** | **Low Breach Frequency (less than 50)** | **High breach Frequency ( more than 51 )** | **Total** |
|---|---|---|---|
| **Low** | 94.88 | 121,12 | 216 |
| **Medium** | 82.14 | 104.85 | 187 |
| **High** | 86.98 | 111.02 | 198 |
| **Total** | 264 | 337 | 601 |

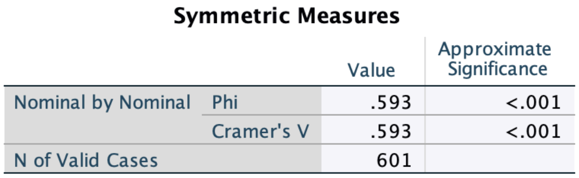
*Fig 1: Chi-square test*



**Chi-Square Tests**

| | Value | df | Asymptotic Significance (2-sided) |
|---|---|---|---|
| Pearson Chi-Square | 211.247[a] | 2 | <.001 |
| Likelihood Ratio | 225.734 | 2 | <.001 |
| N of Valid Cases | 601 | | |

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 82.14.

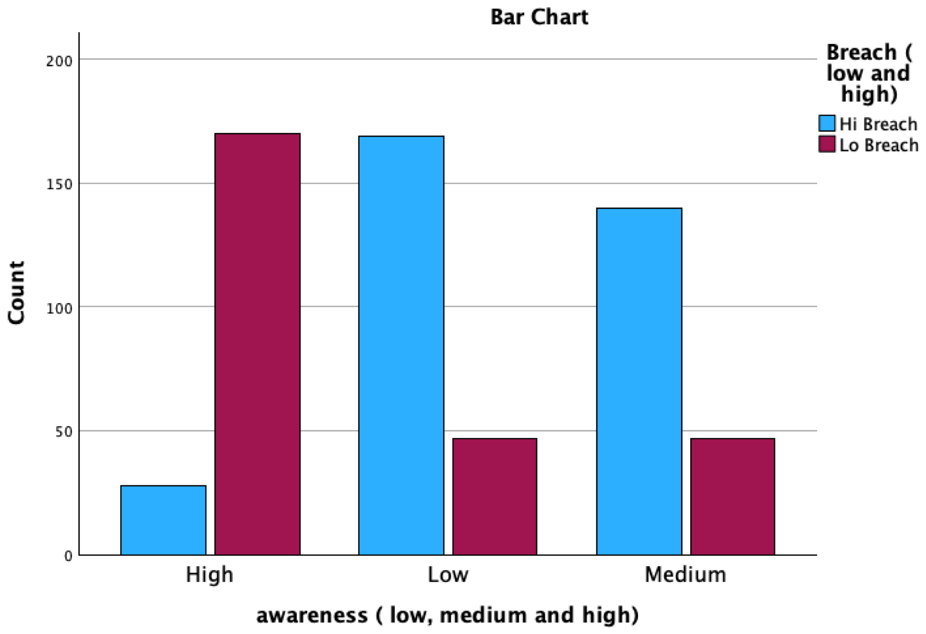


**Symmetric Measures**

| | | Value | Approximate Significance |
|---|---|---|---|
| Nominal by Nominal | Phi | .593 | <.001 |
| | Cramer's V | .593 | <.001 |
| N of Valid Cases | | 601 | |

**Decision**: There is a positive association between the two variables. The chi-square test showed a value of 211.25 with a p-value of 0.001, which is < 0.05. This indicates statistical significance at a 95% confidence level; therefore, we reject the null hypothesis and accept the alternative hypothesis. Phi and Cramer's V determined a positive association of 0.593. Both variables are categorical, and observations are in count because each row of the data set represents one employee. Each cell in the contingency table also has more than five observations; therefore, assumptions are met.

*Fig 2: Bar chart showing the association between the frequency of security breaches in SEMs and cybersecurity awareness*



**Conclusions:** The results of the research show a strong positive association between the frequency of security breaches in SEMs and cybersecurity awareness. Employees with high awareness tend to experience fewer security breaches, whilst those with low awareness experience more frequent breaches. Therefore, employees with low awareness should receive more training regarding cyber threats to reduce security breaches for the company.

Scenario 2 – Table of errors and corrections

| Error | Correct answer/justification | Reference / Evidence |
|---|---|---|
| Examination of Raw Data and Contingency Tables: | There were 601 SMEs. 337 experienced high-frequency breaches, while 264 experienced low-frequency breaches. | Table 1 |
| Missing Contingency table | A contingency table should be added to show the observed values of cybersecurity awareness level and the frequency of security breaches in SME. | Table 1 |
| Incorrect hypothesis | Null hypothesis (H0): There is no association between employees' cybersecurity awareness levels and the frequency of security breaches in SMEs.<br>Alternative hypothesis (H1): There is an association between employees' cybersecurity awareness levels and the frequency of security breaches in SMEs | Hypothesis section |
| Incorrect Chi-square interpretation<br>X2 (1) = 0.455, with p>0.05, | The chi-square test showed a value of 211.25 with a p-value of 0.001, which is < 0.05. This indicates statistical significance at a 95% confidence level. | Fig 1 |
| The null hypothesis has been accepted | p-value is < 0.05, so we reject the null hypothesis and accept the alternative hypothesis | Decision section |
| Incorrect φ coefficient, with a value of 0.470 and moderate<br>positive association | Phi and Cramer's V determined a positive association of 0.593. | Decision section |

| | | |
|---|---|---|
| Incorrect/missing assumptions | More than five observations is the assumption that needs to be met.<br>Chi-square tests can handle two or more variables.<br>Observations should be counted. | |
| Missing Fig 2.1 | A bar chart was needed to show the association between the variables. | Fig 2 |

Scenario 3

**Introduction:** The purpose of this study is to investigate how different types of cyber attacks affect detection time (DT) and overall response time (RT) in the cybersecurity system. The objectives are to determine whether different types of attacks result in longer or shorter detection and response times and to explore the potential linear relationship between them.

**Research questions**

Is there a difference in the mean response and detection time across phishing, malware, and DDoS attacks?
Is there a linear relationship between RT and DT for each type of attack?

**Types of Variables:** The dependent variables are continuous and measured at a ratio level, while the independent variable is categorical and nominal.

**Dependent variables:** Response time and detection time.

**Independent variable**: The types of cyber attacks ( malware, phishing, and DDoS).

**Exploration of Raw data - Descriptive statistics:** Tables 1 and 2 show the five-point summary for RT and DT. Malware has the highest median DT, while Phishing has the highest median RT. DDoS has the lowest RT and DT compared to other attacks. The boxplots in Figures 1 and 2 present no outliers.

Five-point summary

*Table 1: Response time ( Appendix 1 & 2)*

| **Attack type** | **Malware** | **Phishing** | **DDoS** |
|---|---|---|---|
| **Maxium** | 380 | 547 | 285 |
| **Q1** | 308.00 | 448.00 | 198.00 |
| **Median** | 327.00 | 498.00 | 222.00 |
| **Q3** | 337.00 | 537.00 | 251.00 |
| **Minimum** | 298 | 432 | 177 |

*Table 2: Detection time ( Appendix 3 & 4)*

| **Attack type** | **Malware** | **Phishing** | **DDoS** |
|---|---|---|---|
| **Maxium** | 247 | 183 | 182 |
| **Q1** | 205.00 | 145.00 | 130.00 |
| **Median** | 208.00 | 162.00 | 152.00 |
| **Q3** | 233.00 | 175.00 | 178.00 |
| **Minimum** | 187 | 135 | 122 |

*Figure 1: Response time boxplot*

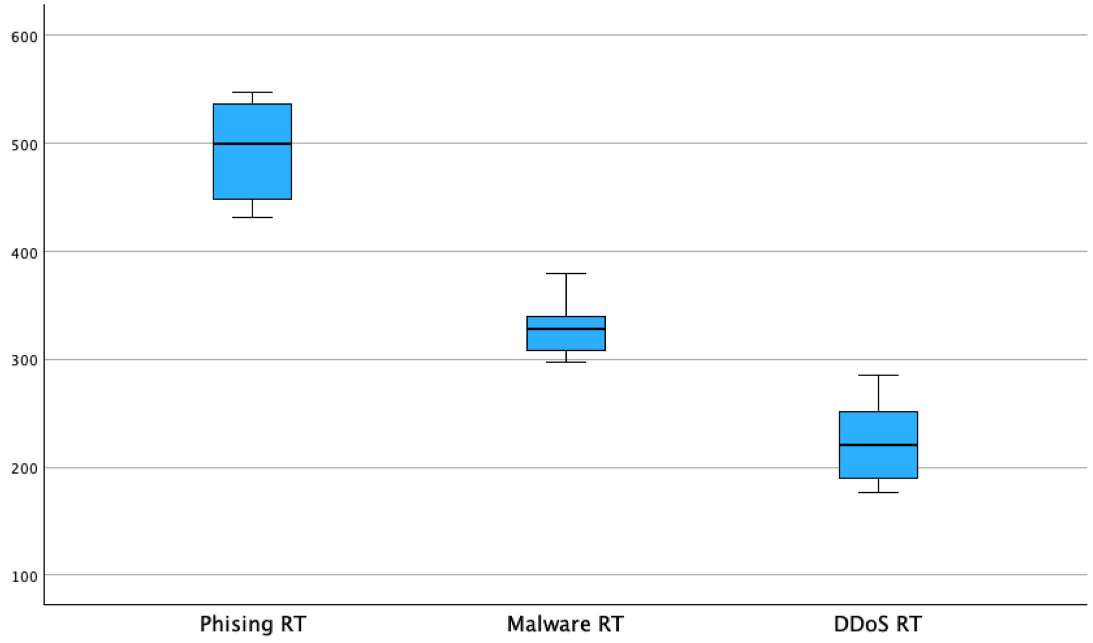
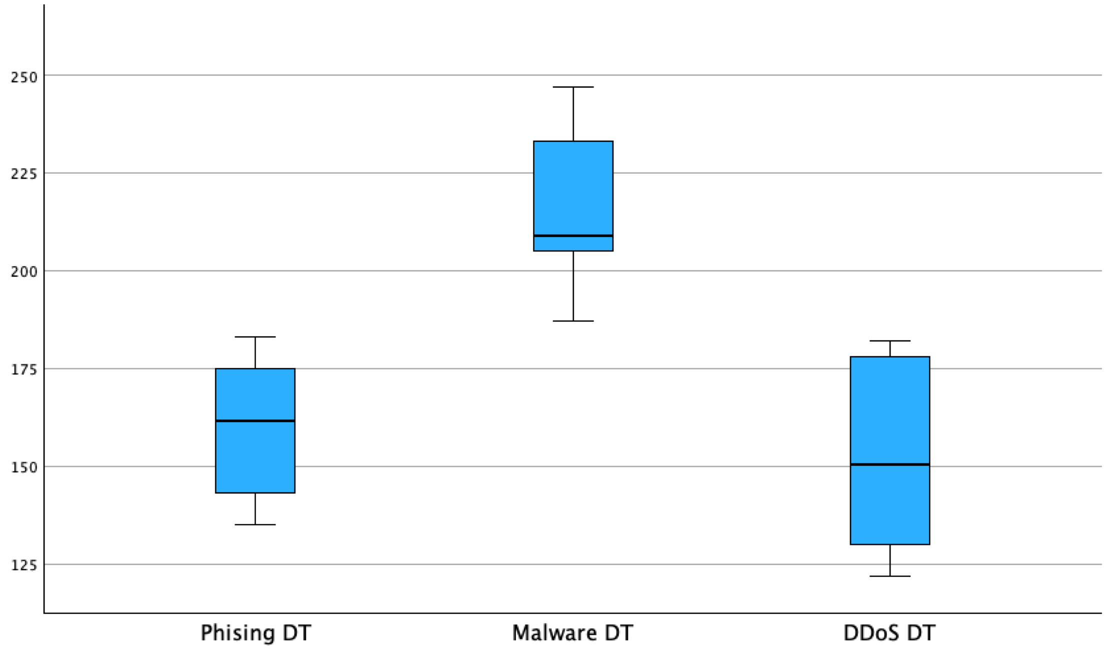


*Figure 2: Detection time boxplot*



The descriptive analysis in *Appendix 1 and 3* also reveals that phishing attacks have a higher variability, SD = 47.98, while malware has the lowest SD = 25.38. As a result, a significant difference in mean response time is indicated; however, detection time shows less variation across attack groups.

**Results of statistical tests**

Is there a difference in the mean response and detection time across phishing, malware, and DDoS attacks?

**Statistical test and rationale**: A one-way ANOVA test was used to explore the differences in mean response and detection time across phishing, malware, and DDoS attacks. This test is suitable because the research question consists of three independent categorical variables.

**Detection time hypothesis**

Null hypothesis (H0): There is no significant difference in mean DT across malware, phishing, and DDoS attacks.

Alternative hypothesis (H1): There is a significant difference in mean DT across malware, phishing, and DDoS attacks.

**Response time hypothesis**

Null hypothesis (H0): There is no significant difference in mean RT across malware, phishing, and DDoS attacks.

Alternative hypothesis (H1): There is a significant difference in mean RT across malware, phishing, and DDoS attacks.

**Assumptions for one-way ANOVA**

1. RT and DT are continuous variables.
2. The independent variable has three levels ( malware, phishing, DDoS).
3. Observations are independent within and between groups.
4. There are no significant outliers. *( Figures 1 & 2)*
5. Shapiro-Wilk confirmed that RT and DT are normally distributed ( $p > 0.05$). *( Appendix 5 and 6)*
6. Variance for DT is more homogeneous than RT.

The one-way ANOVA test indicated a difference in mean between RT and DT across the attack groups. As a result, we reject the null hypothesis and accept the alternative hypothesis.

Response time

F value = 119.53   p value = 3.86E-4 (<0.001)  *( Appendix 7)*

Mean difference: phishing = 492.6 (mins)  malware = 330.7(mins)  DDos = 225 (mins)

Detection time

F value = 25.47 p value = 6.09E-07 (<0.001) *(Appendix 8)*

Mean difference: phishing = 159.3, malware = 213.9, DDos = 152.6

The F value was statistically significant for both variables because the F Crit = 3.35 was met.

Post hoc test comparisons signified a significant difference between response and detection times. The p-value across all attack types is less than 0.05. *(Appendix 9-14)*

Is there a linear relationship between RT and DT for each type of attack?

**Statistical test and rationale:** Pearson correlation was used to assess the strength and direction of the relationship between RT and DT across different attack groups. The dependent variables are continuous and normally distributed, which makes a parametric test suitable.

**Null hypothesis (H0)**: There is no significant correlation between RT and DT regarding phishing, malware, and DDoS.

**Alternative hypothesis (H1)**: There is a significant correlation between RT and DT regarding phishing, malware, and DDoS.

**Assumptions for Pearson Correlation**

1. RT and DT are continuous variables.
2. Each RT and DT pair is associated with an attack group.
3. Data pairs are independent across attack groups.
4. The scatterplots indicated some extreme values for RT and DT in malware and phishing attacks, which may affect the correlation and variance across groups.
5. DDoS shows no outliers, indicating a linear relationship. *(Appendix 18, 19 & 20)*
6. Shapiro-Wilk confirmed that RT and DT are normally distributed ( $p > 0.05$). *(Appendix 5 & 6)*

Phishing (RT) and (DT):  r  = .08, n = 10, p = .822 (Weak positive correlation)

Malware (RT) and (DT):  r  = - 41, n = 10, p = .234 (Moderate negative correlation)

The relationship between (RT) and (DT is not statistically significant across phishing and malware. So we fail to reject the null hypothesis because the p-value is more than 0.05. *( Appendix 15) (Appendix 16)*

DDoS (RT) and (DT):  r  = .95, n = 10, p = <.001 (Strong positive correlation)  *(Appendix 17)*

The relationship between RT and DT is statistically significant among DDoS attacks. We reject the null hypothesis and accept the alternative hypothesis because the p-value is less than 0.05.

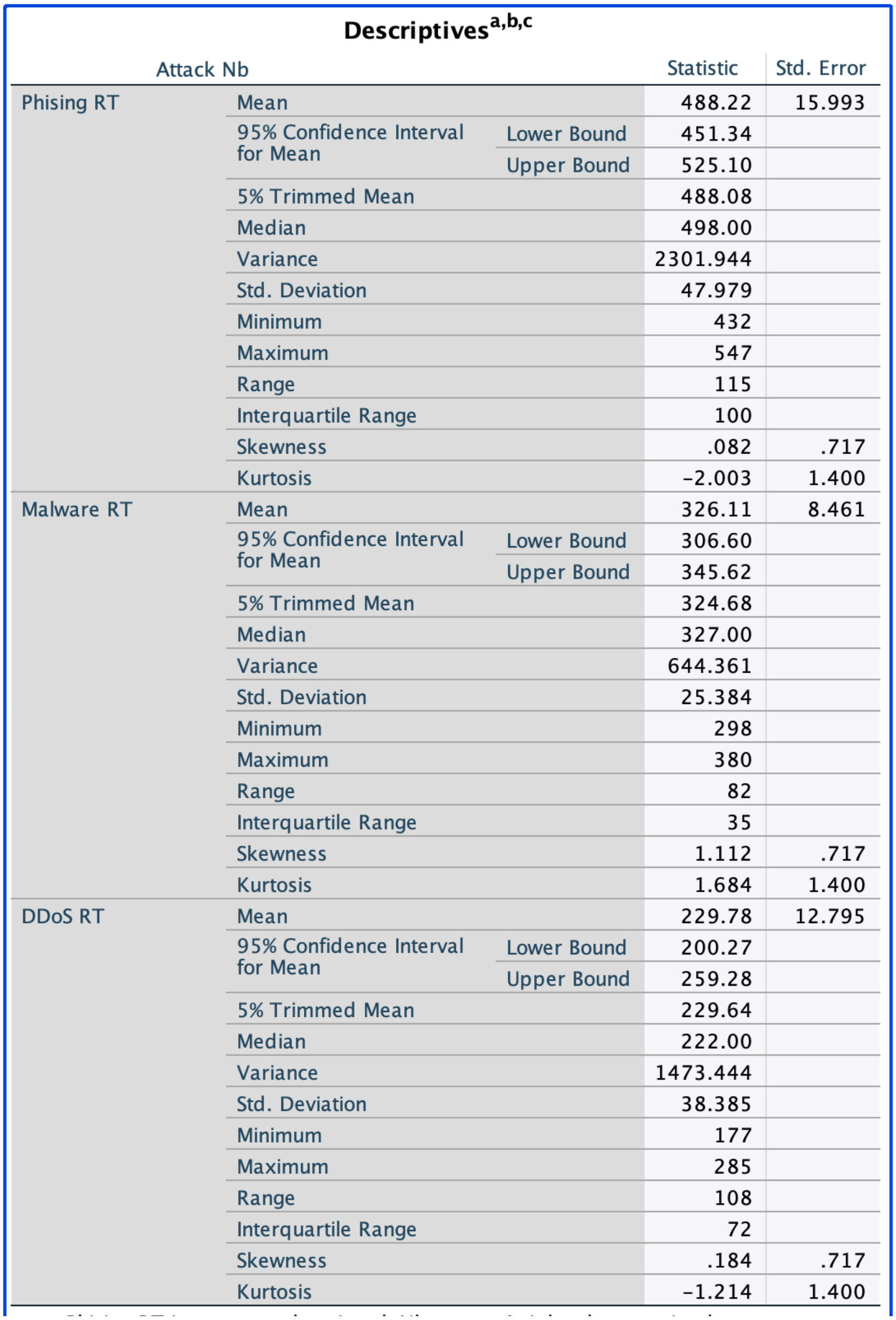
**Conclusion:** The results of this research showed that the response time for phishing and malware is inconsistent and slower, whilst DDoS attacks are quicker and more consistent. The extreme outliers in phishing and malware may affect variances; however, the lack of outliers in DDoS makes the mean difference more reliable. The DDoS group shows a strong positive correlation between response and detection time, while phishing and malware show weak or negative correlations. This suggests response time strategies should be improved for phishing and malware, whilst DDoS attacks can be controlled efficiently based on patterns.

## Students' mistakes and missing information

- There is no introduction, variable types, explanation of raw data, written statistical test results, hypothesis, validity of assumptions, or conclusion.
- Students' descriptive output is incorrect for both dependent variables.
- The box plot for both dependent variables across each attack is missing.
- Post hoc test output and tables are missing.
- The scatter plots showing the relationship between RT and DT are missing.
- There is no SPSS output of Pearson's correlation, used to determine the strength and direction of the relationship between RT and DT across different attack groups.
- There is no five-point summary of the dependent variables ( including an appendix of the percentile output).
- The test for normality is missing, including the SPSS output.

Word count - 2189  
Note -  Grammarly was used for grammar errors.

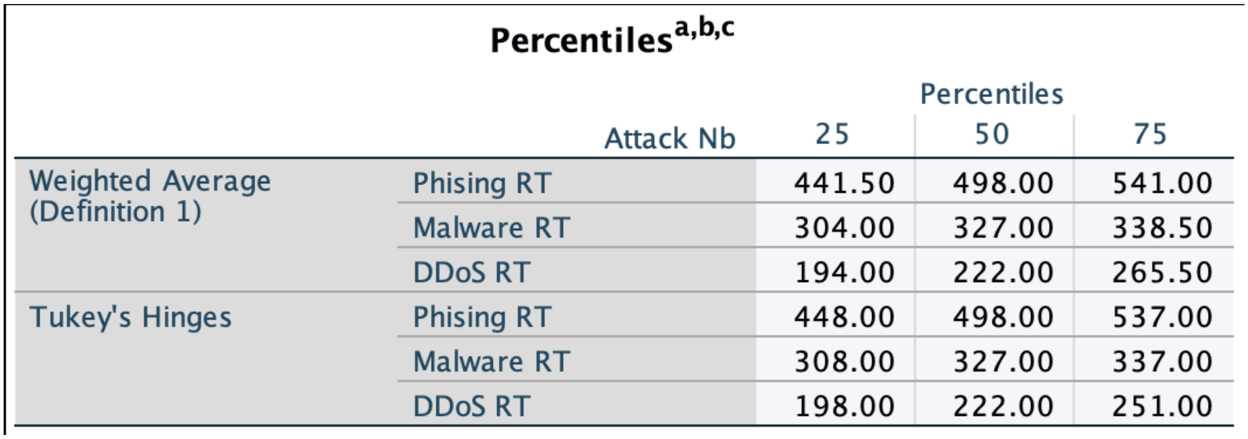
Appendix 1



**Descriptives**[a,b,c]

| Attack Nb | | | Statistic | Std. Error |
|---|---|---|---|---|
| Phising RT | Mean | | 488.22 | 15.993 |
| | 95% Confidence Interval for Mean | Lower Bound | 451.34 | |
| | | Upper Bound | 525.10 | |
| | 5% Trimmed Mean | | 488.08 | |
| | Median | | 498.00 | |
| | Variance | | 2301.944 | |
| | Std. Deviation | | 47.979 | |
| | Minimum | | 432 | |
| | Maximum | | 547 | |
| | Range | | 115 | |
| | Interquartile Range | | 100 | |
| | Skewness | | .082 | .717 |
| | Kurtosis | | -2.003 | 1.400 |
| Malware RT | Mean | | 326.11 | 8.461 |
| | 95% Confidence Interval for Mean | Lower Bound | 306.60 | |
| | | Upper Bound | 345.62 | |
| | 5% Trimmed Mean | | 324.68 | |
| | Median | | 327.00 | |
| | Variance | | 644.361 | |
| | Std. Deviation | | 25.384 | |
| | Minimum | | 298 | |
| | Maximum | | 380 | |
| | Range | | 82 | |
| | Interquartile Range | | 35 | |
| | Skewness | | 1.112 | .717 |
| | Kurtosis | | 1.684 | 1.400 |
| DDoS RT | Mean | | 229.78 | 12.795 |
| | 95% Confidence Interval for Mean | Lower Bound | 200.27 | |
| | | Upper Bound | 259.28 | |
| | 5% Trimmed Mean | | 229.64 | |
| | Median | | 222.00 | |
| | Variance | | 1473.444 | |
| | Std. Deviation | | 38.385 | |
| | Minimum | | 177 | |
| | Maximum | | 285 | |
| | Range | | 108 | |
| | Interquartile Range | | 72 | |
| | Skewness | | .184 | .717 |
| | Kurtosis | | -1.214 | 1.400 |

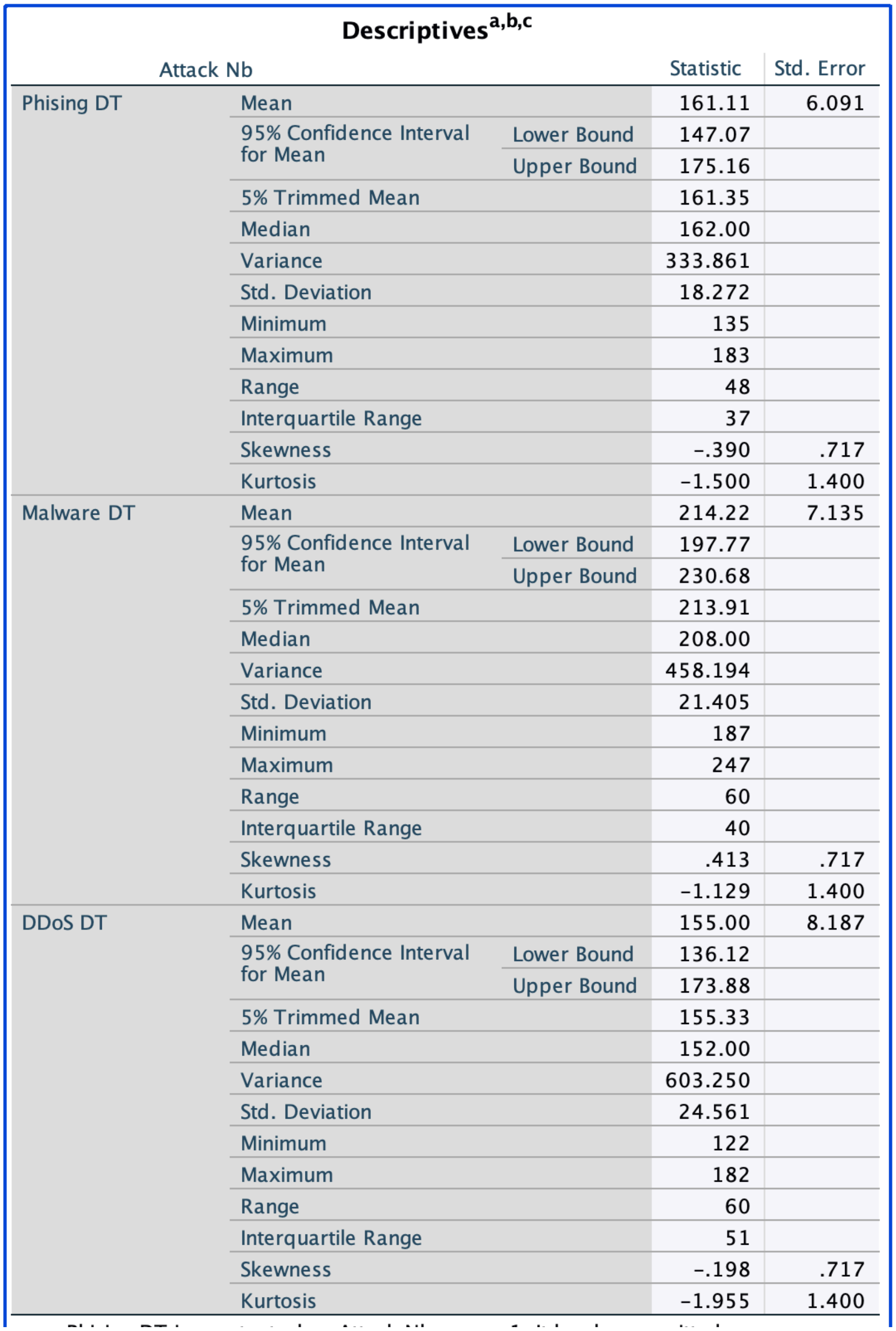
Appendix 2



**Percentiles**[a,b,c]

| | Attack Nb | Percentiles | | |
|---|---|---|---|---|
| | | 25 | 50 | 75 |
| Weighted Average (Definition 1) | Phising RT | 441.50 | 498.00 | 541.00 |
| | Malware RT | 304.00 | 327.00 | 338.50 |
| | DDoS RT | 194.00 | 222.00 | 265.50 |
| Tukey's Hinges | Phising RT | 448.00 | 498.00 | 537.00 |
| | Malware RT | 308.00 | 327.00 | 337.00 |
| | DDoS RT | 198.00 | 222.00 | 251.00 |

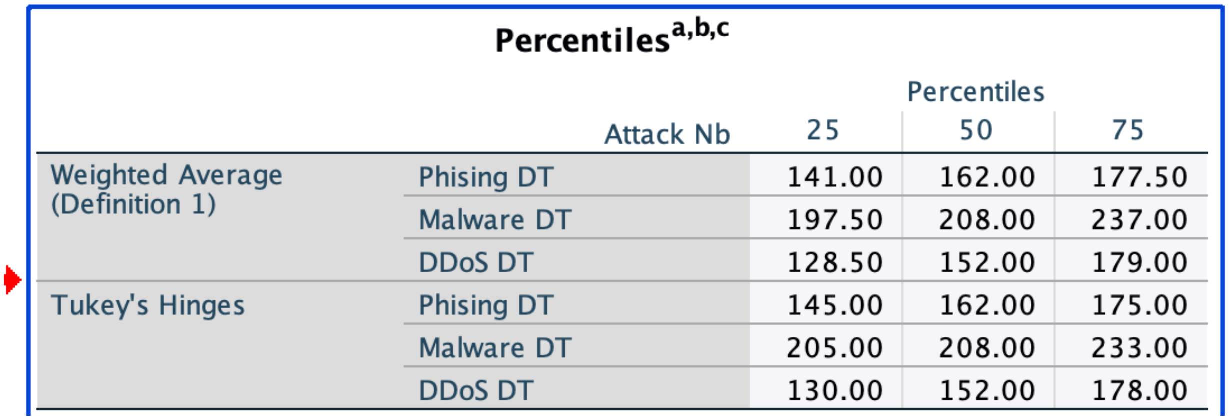
Appendix 3



**Descriptives**[a,b,c]

| Attack Nb | | | Statistic | Std. Error |
|---|---|---|---|---|
| Phising DT | Mean | | 161.11 | 6.091 |
| | 95% Confidence Interval for Mean | Lower Bound | 147.07 | |
| | | Upper Bound | 175.16 | |
| | 5% Trimmed Mean | | 161.35 | |
| | Median | | 162.00 | |
| | Variance | | 333.861 | |
| | Std. Deviation | | 18.272 | |
| | Minimum | | 135 | |
| | Maximum | | 183 | |
| | Range | | 48 | |
| | Interquartile Range | | 37 | |
| | Skewness | | -.390 | .717 |
| | Kurtosis | | -1.500 | 1.400 |
| Malware DT | Mean | | 214.22 | 7.135 |
| | 95% Confidence Interval for Mean | Lower Bound | 197.77 | |
| | | Upper Bound | 230.68 | |
| | 5% Trimmed Mean | | 213.91 | |
| | Median | | 208.00 | |
| | Variance | | 458.194 | |
| | Std. Deviation | | 21.405 | |
| | Minimum | | 187 | |
| | Maximum | | 247 | |
| | Range | | 60 | |
| | Interquartile Range | | 40 | |
| | Skewness | | .413 | .717 |
| | Kurtosis | | -1.129 | 1.400 |
| DDoS DT | Mean | | 155.00 | 8.187 |
| | 95% Confidence Interval for Mean | Lower Bound | 136.12 | |
| | | Upper Bound | 173.88 | |
| | 5% Trimmed Mean | | 155.33 | |
| | Median | | 152.00 | |
| | Variance | | 603.250 | |
| | Std. Deviation | | 24.561 | |
| | Minimum | | 122 | |
| | Maximum | | 182 | |
| | Range | | 60 | |
| | Interquartile Range | | 51 | |
| | Skewness | | -.198 | .717 |
| | Kurtosis | | -1.955 | 1.400 |

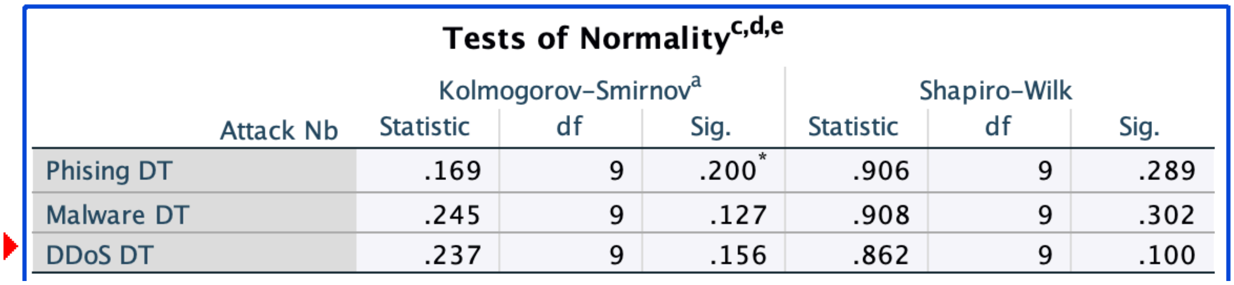
Appendix 4



### Percentiles[a,b,c]

| | | Percentiles | | |
|---|---|---|---|---|
| | Attack Nb | 25 | 50 | 75 |
| Weighted Average (Definition 1) | Phising DT | 141.00 | 162.00 | 177.50 |
| | Malware DT | 197.50 | 208.00 | 237.00 |
| | DDoS DT | 128.50 | 152.00 | 179.00 |
| Tukey's Hinges | Phising DT | 145.00 | 162.00 | 175.00 |
| | Malware DT | 205.00 | 208.00 | 233.00 |
| | DDoS DT | 130.00 | 152.00 | 178.00 |

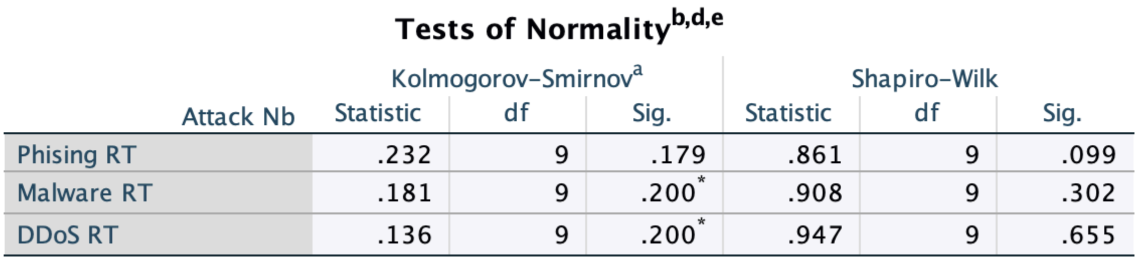
Appendix 5



### Tests of Normality[c,d,e]

| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|
| Attack Nb | Statistic | df | Sig. | Statistic | df | Sig. |
| Phising DT | .169 | 9 | .200* | .906 | 9 | .289 |
| Malware DT | .245 | 9 | .127 | .908 | 9 | .302 |
| DDoS DT | .237 | 9 | .156 | .862 | 9 | .100 |

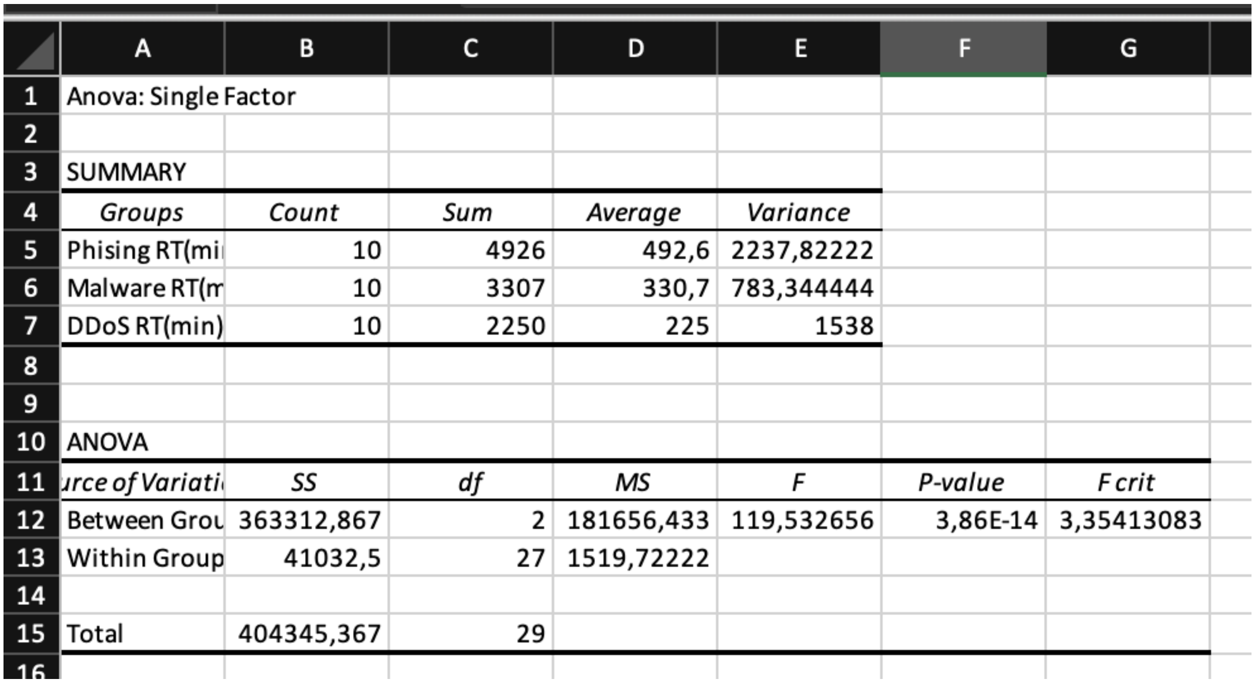
Appendix 6



### Tests of Normality[b,d,e]

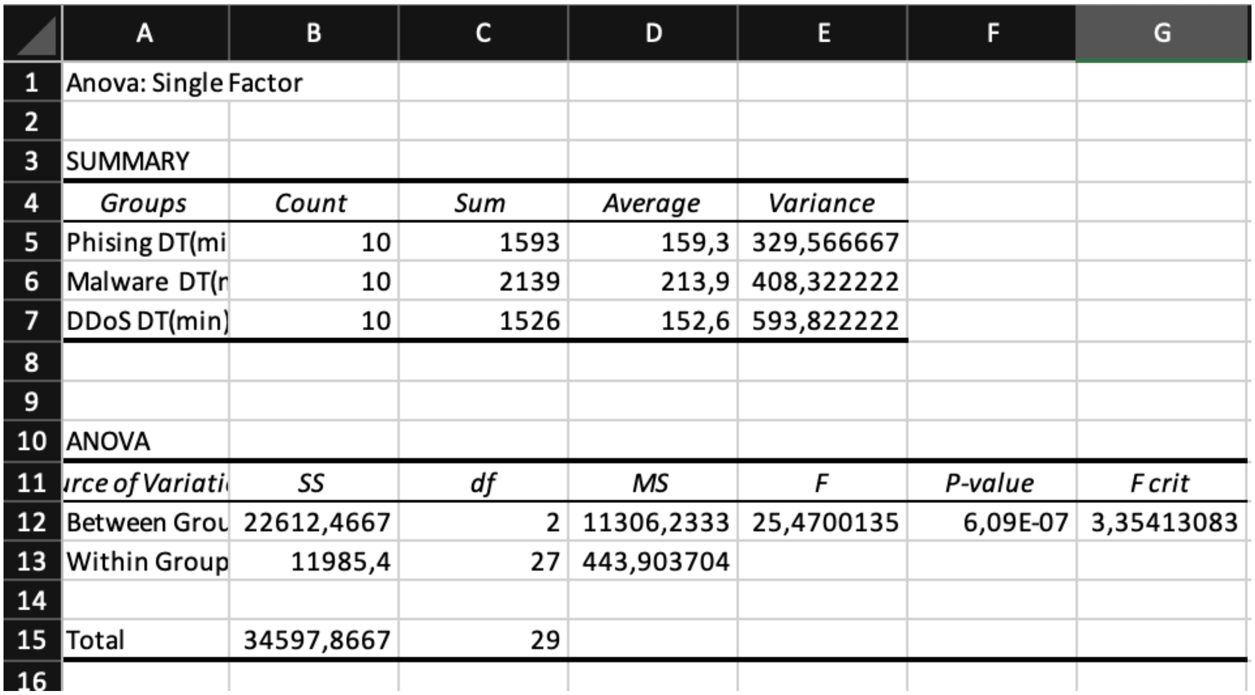
| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|
| Attack Nb | Statistic | df | Sig. | Statistic | df | Sig. |
| Phising RT | .232 | 9 | .179 | .861 | 9 | .099 |
| Malware RT | .181 | 9 | .200* | .908 | 9 | .302 |
| DDoS RT | .136 | 9 | .200* | .947 | 9 | .655 |

Appendix 7



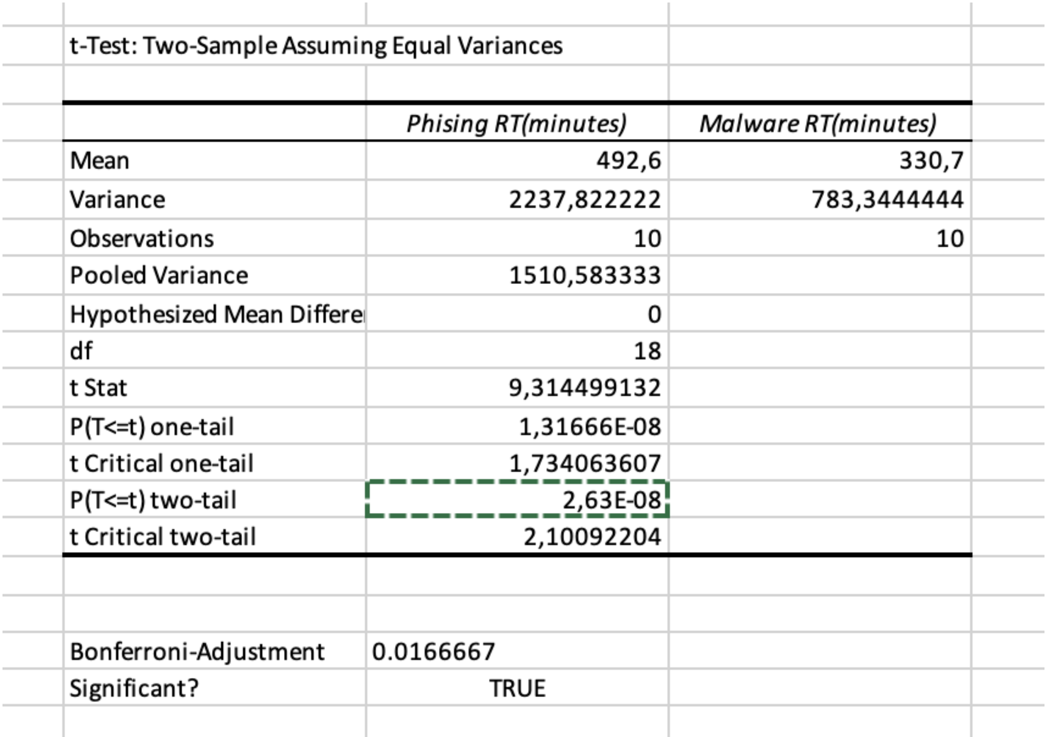
| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | Anova: Single Factor | | | | | | |
| 2 | | | | | | | |
| 3 | SUMMARY | | | | | | |
| 4 | *Groups* | *Count* | *Sum* | *Average* | *Variance* | | |
| 5 | Phising RT(mi | 10 | 4926 | 492,6 | 2237,82222 | | |
| 6 | Malware RT(m | 10 | 3307 | 330,7 | 783,344444 | | |
| 7 | DDoS RT(min) | 10 | 2250 | 225 | 1538 | | |
| 8 | | | | | | | |
| 9 | | | | | | | |
| 10 | ANOVA | | | | | | |
| 11 | *urce of Variati* | *SS* | *df* | *MS* | *F* | *P-value* | *F crit* |
| 12 | Between Grou | 363312,867 | 2 | 181656,433 | 119,532656 | 3,86E-14 | 3,35413083 |
| 13 | Within Group | 41032,5 | 27 | 1519,72222 | | | |
| 14 | | | | | | | |
| 15 | Total | 404345,367 | 29 | | | | |
| 16 | | | | | | | |

Appendix 8



| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | Anova: Single Factor | | | | | | |
| 2 | | | | | | | |
| 3 | SUMMARY | | | | | | |
| 4 | *Groups* | *Count* | *Sum* | *Average* | *Variance* | | |
| 5 | Phising DT(mi | 10 | 1593 | 159,3 | 329,566667 | | |
| 6 | Malware DT(r | 10 | 2139 | 213,9 | 408,322222 | | |
| 7 | DDoS DT(min) | 10 | 1526 | 152,6 | 593,822222 | | |
| 8 | | | | | | | |
| 9 | | | | | | | |
| 10 | ANOVA | | | | | | |
| 11 | *urce of Variati* | *SS* | *df* | *MS* | *F* | *P-value* | *F crit* |
| 12 | Between Grou | 22612,4667 | 2 | 11306,2333 | 25,4700135 | 6,09E-07 | 3,35413083 |
| 13 | Within Group | 11985,4 | 27 | 443,903704 | | | |
| 14 | | | | | | | |
| 15 | Total | 34597,8667 | 29 | | | | |
| 16 | | | | | | | |

Appendix 9

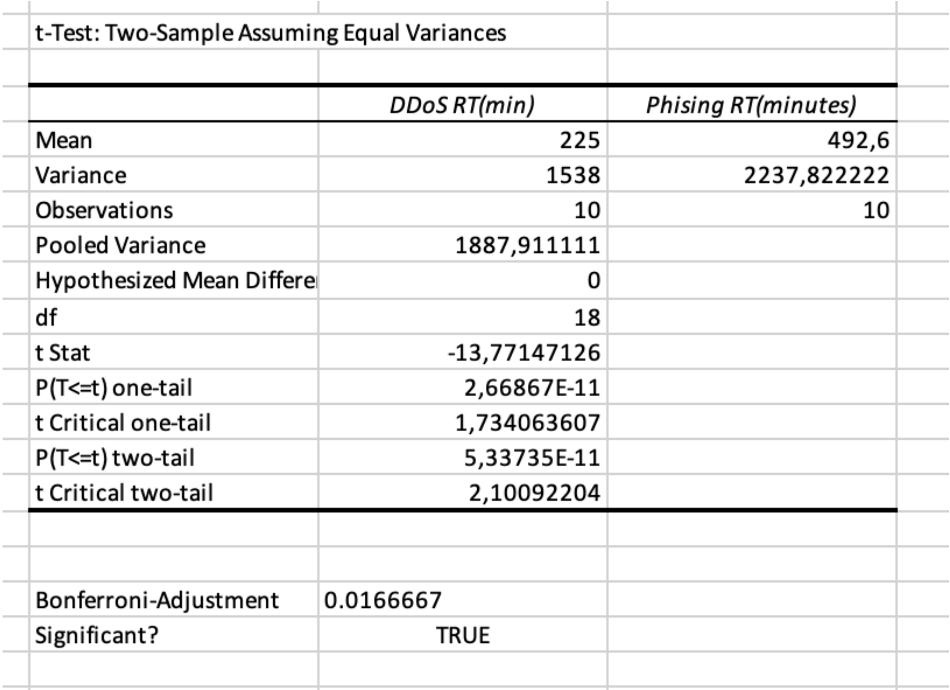


t-Test: Two-Sample Assuming Equal Variances

| | *Phising RT(minutes)* | *Malware RT(minutes)* |
|---|---|---|
| Mean | 492,6 | 330,7 |
| Variance | 2237,822222 | 783,3444444 |
| Observations | 10 | 10 |
| Pooled Variance | 1510,583333 | |
| Hypothesized Mean Differe | 0 | |
| df | 18 | |
| t Stat | 9,314499132 | |
| P(T<=t) one-tail | 1,31666E-08 | |
| t Critical one-tail | 1,734063607 | |
| P(T<=t) two-tail | 2,63E-08 | |
| t Critical two-tail | 2,10092204 | |

| | | |
|---|---|---|
| Bonferroni-Adjustment | 0.0166667 | |
| Significant? | TRUE | |

Appendix 10

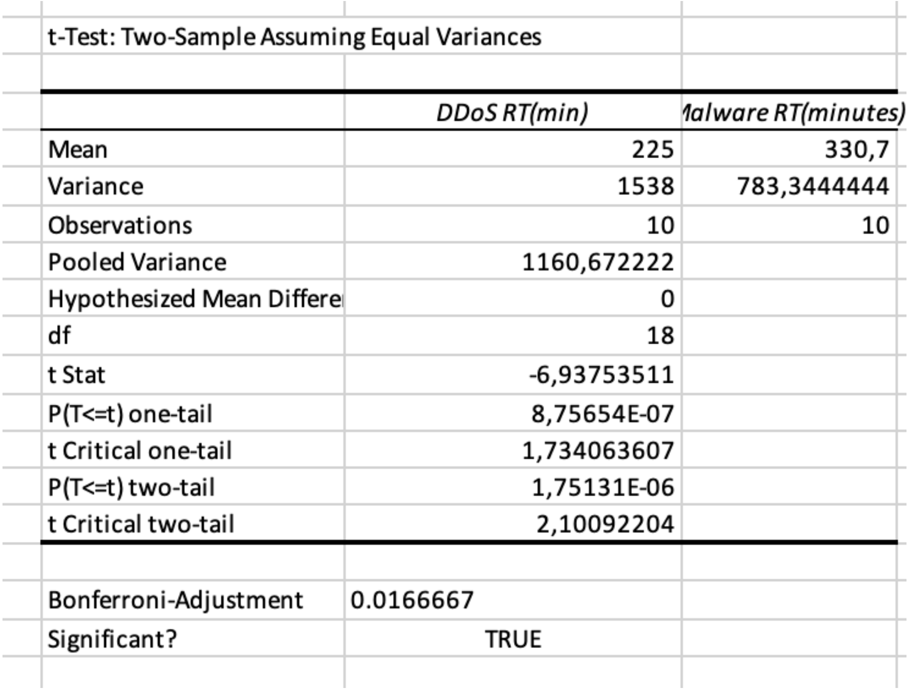


t-Test: Two-Sample Assuming Equal Variances

| | *DDoS RT(min)* | *Phising RT(minutes)* |
|---|---|---|
| Mean | 225 | 492,6 |
| Variance | 1538 | 2237,822222 |
| Observations | 10 | 10 |
| Pooled Variance | 1887,911111 | |
| Hypothesized Mean Differe | 0 | |
| df | 18 | |
| t Stat | -13,77147126 | |
| P(T<=t) one-tail | 2,66867E-11 | |
| t Critical one-tail | 1,734063607 | |
| P(T<=t) two-tail | 5,33735E-11 | |
| t Critical two-tail | 2,10092204 | |

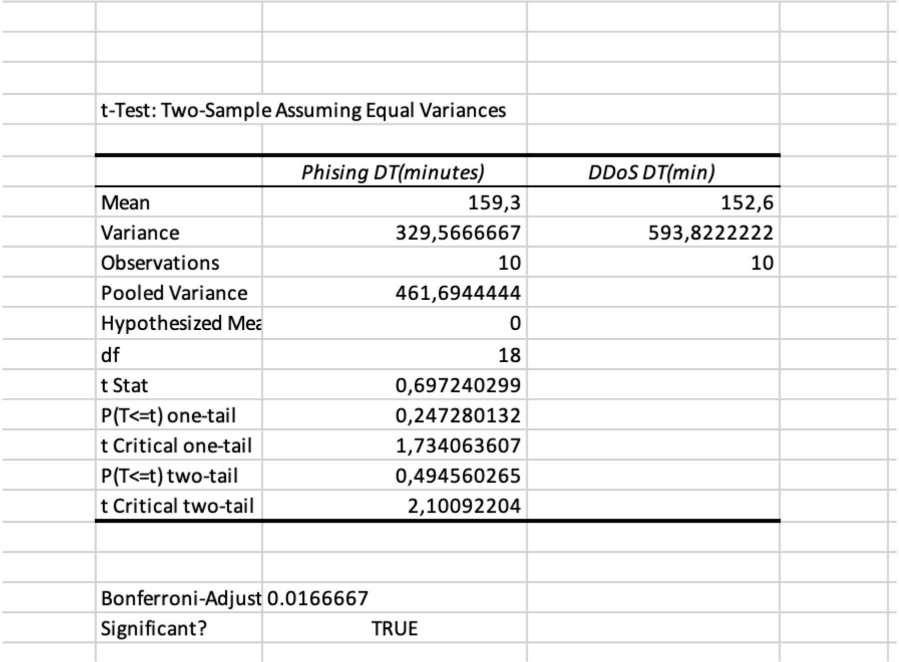
| | | |
|---|---|---|
| Bonferroni-Adjustment | 0.0166667 | |
| Significant? | TRUE | |

Appendix 11



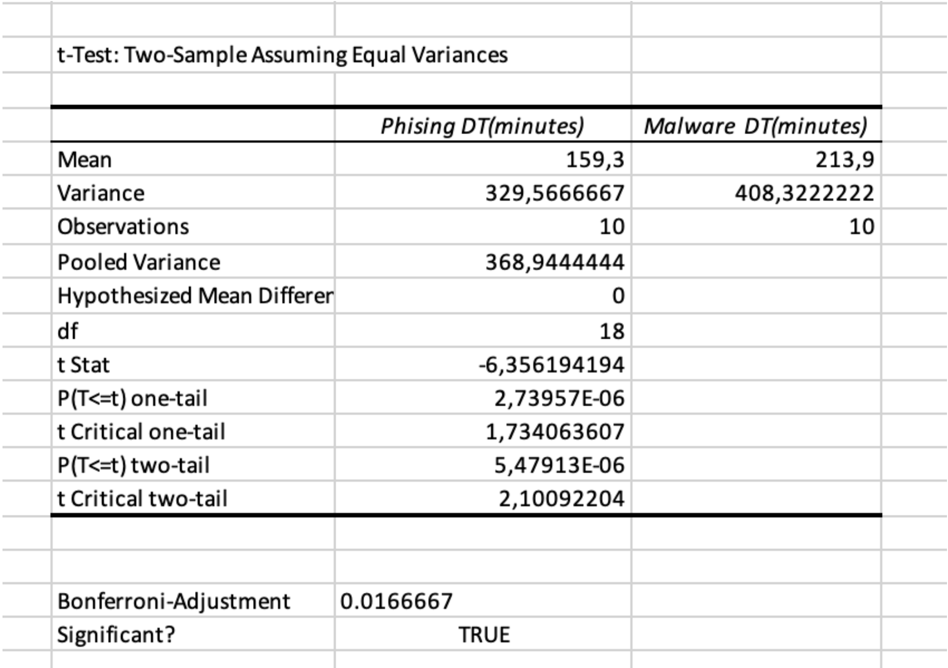
| t-Test: Two-Sample Assuming Equal Variances | | |
|---|---|---|
| | *DDoS RT(min)* | *lalware RT(minutes)* |
| Mean | 225 | 330,7 |
| Variance | 1538 | 783,3444444 |
| Observations | 10 | 10 |
| Pooled Variance | 1160,672222 | |
| Hypothesized Mean Differe | 0 | |
| df | 18 | |
| t Stat | -6,93753511 | |
| P(T<=t) one-tail | 8,75654E-07 | |
| t Critical one-tail | 1,734063607 | |
| P(T<=t) two-tail | 1,75131E-06 | |
| t Critical two-tail | 2,10092204 | |
| | | |
| Bonferroni-Adjustment | 0.0166667 | |
| Significant? | TRUE | |

Appendix 12



| t-Test: Two-Sample Assuming Equal Variances | | |
|---|---|---|
| | *Phising DT(minutes)* | *DDoS DT(min)* |
| Mean | 159,3 | 152,6 |
| Variance | 329,5666667 | 593,8222222 |
| Observations | 10 | 10 |
| Pooled Variance | 461,6944444 | |
| Hypothesized Mea | 0 | |
| df | 18 | |
| t Stat | 0,697240299 | |
| P(T<=t) one-tail | 0,247280132 | |
| t Critical one-tail | 1,734063607 | |
| P(T<=t) two-tail | 0,494560265 | |
| t Critical two-tail | 2,10092204 | |
| | | |
| Bonferroni-Adjust | 0.0166667 | |
| Significant? | TRUE | |

Appendix 13

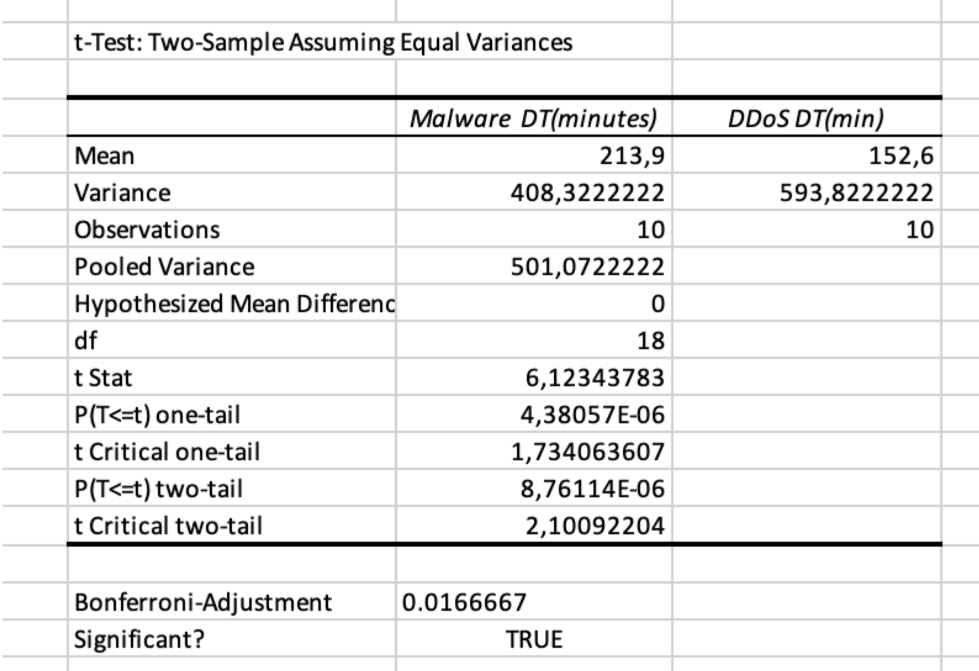


t-Test: Two-Sample Assuming Equal Variances

| | *Phising DT(minutes)* | *Malware DT(minutes)* |
|---|---|---|
| Mean | 159,3 | 213,9 |
| Variance | 329,5666667 | 408,3222222 |
| Observations | 10 | 10 |
| Pooled Variance | 368,9444444 | |
| Hypothesized Mean Differer | 0 | |
| df | 18 | |
| t Stat | -6,356194194 | |
| P(T<=t) one-tail | 2,73957E-06 | |
| t Critical one-tail | 1,734063607 | |
| P(T<=t) two-tail | 5,47913E-06 | |
| t Critical two-tail | 2,10092204 | |

| | | |
|---|---|---|
| Bonferroni-Adjustment | 0.0166667 | |
| Significant? | TRUE | |

Appendix 14

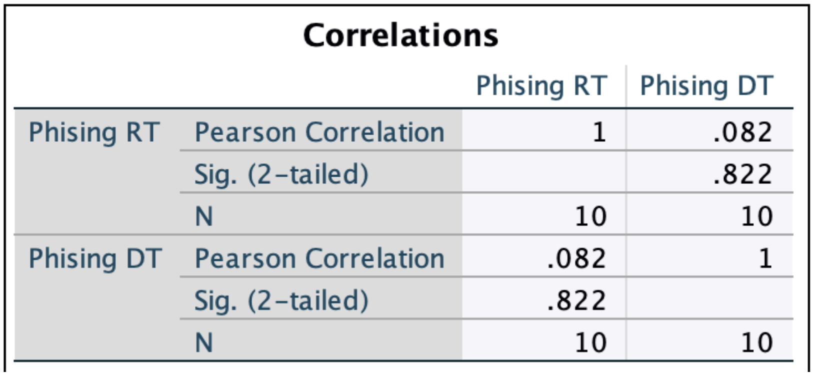


t-Test: Two-Sample Assuming Equal Variances

| | *Malware DT(minutes)* | *DDoS DT(min)* |
|---|---|---|
| Mean | 213,9 | 152,6 |
| Variance | 408,3222222 | 593,8222222 |
| Observations | 10 | 10 |
| Pooled Variance | 501,0722222 | |
| Hypothesized Mean Differenc | 0 | |
| df | 18 | |
| t Stat | 6,12343783 | |
| P(T<=t) one-tail | 4,38057E-06 | |
| t Critical one-tail | 1,734063607 | |
| P(T<=t) two-tail | 8,76114E-06 | |
| t Critical two-tail | 2,10092204 | |

| | | |
|---|---|---|
| Bonferroni-Adjustment | 0.0166667 | |
| Significant? | TRUE | |

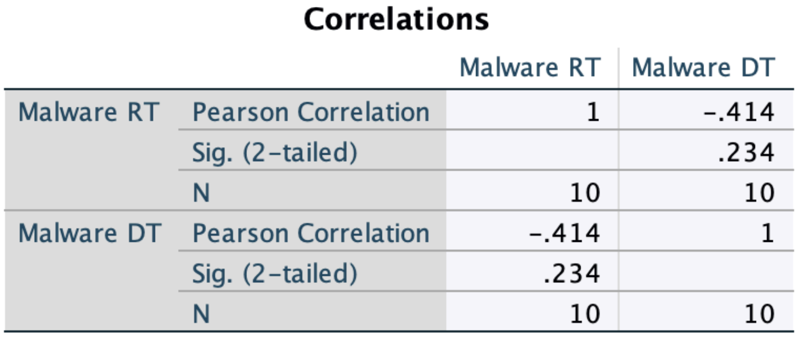
Appendix 15



**Correlations**

| | | Phising RT | Phising DT |
|---|---|---|---|
| Phising RT | Pearson Correlation | 1 | .082 |
| | Sig. (2-tailed) | | .822 |
| | N | 10 | 10 |
| Phising DT | Pearson Correlation | .082 | 1 |
| | Sig. (2-tailed) | .822 | |
| | N | 10 | 10 |

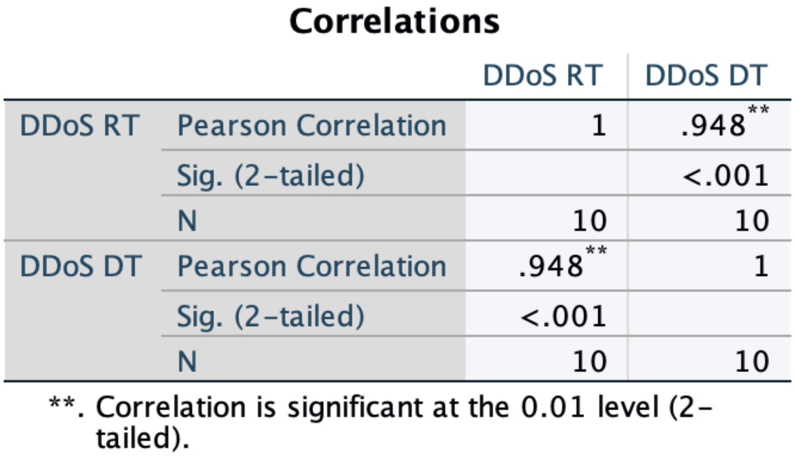
Appendix 16



**Correlations**

| | | Malware RT | Malware DT |
|---|---|---|---|
| Malware RT | Pearson Correlation | 1 | -.414 |
| | Sig. (2-tailed) | | .234 |
| | N | 10 | 10 |
| Malware DT | Pearson Correlation | -.414 | 1 |
| | Sig. (2-tailed) | .234 | |
| | N | 10 | 10 |

Appendix 17

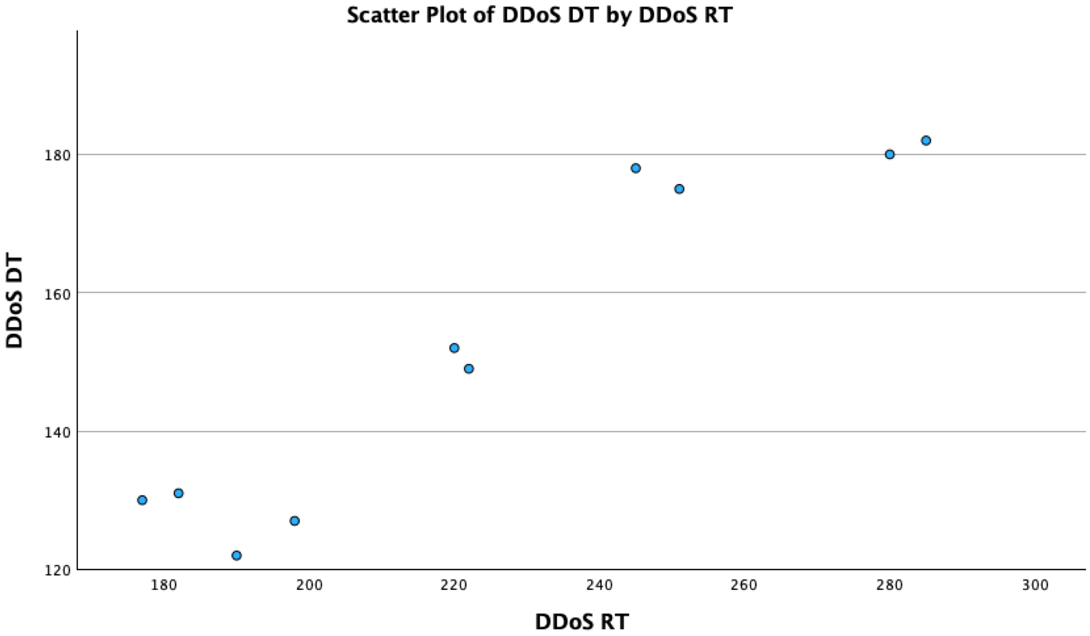


**Correlations**

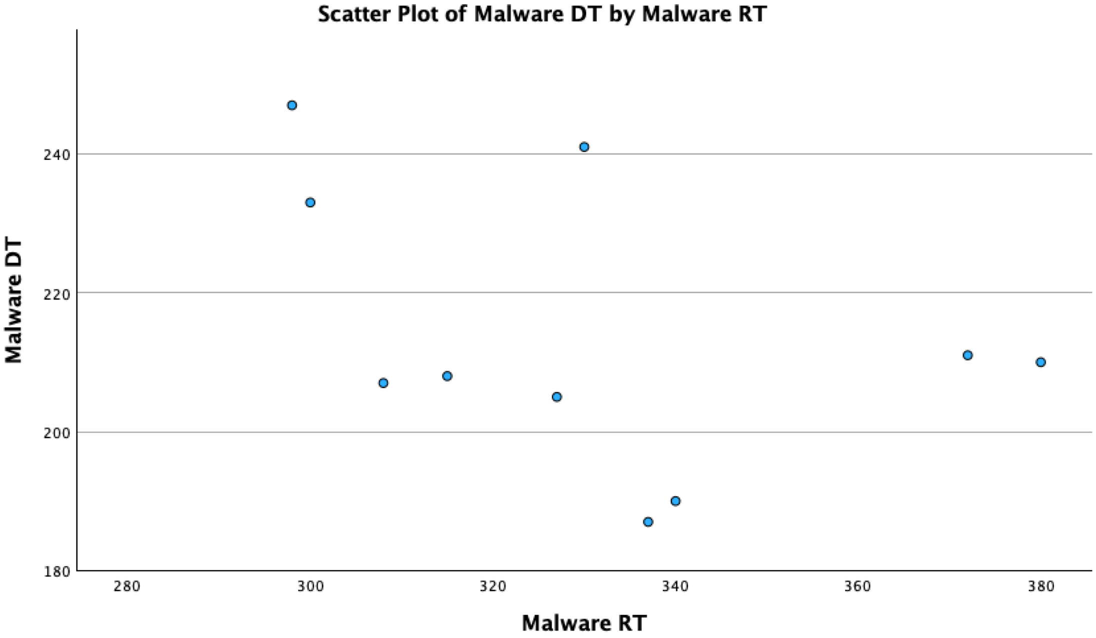
| | | DDoS RT | DDoS DT |
|---|---|---|---|
| DDoS RT | Pearson Correlation | 1 | .948** |
| | Sig. (2-tailed) | | <.001 |
| | N | 10 | 10 |
| DDoS DT | Pearson Correlation | .948** | 1 |
| | Sig. (2-tailed) | <.001 | |
| | N | 10 | 10 |

**. Correlation is significant at the 0.01 level (2-tailed).

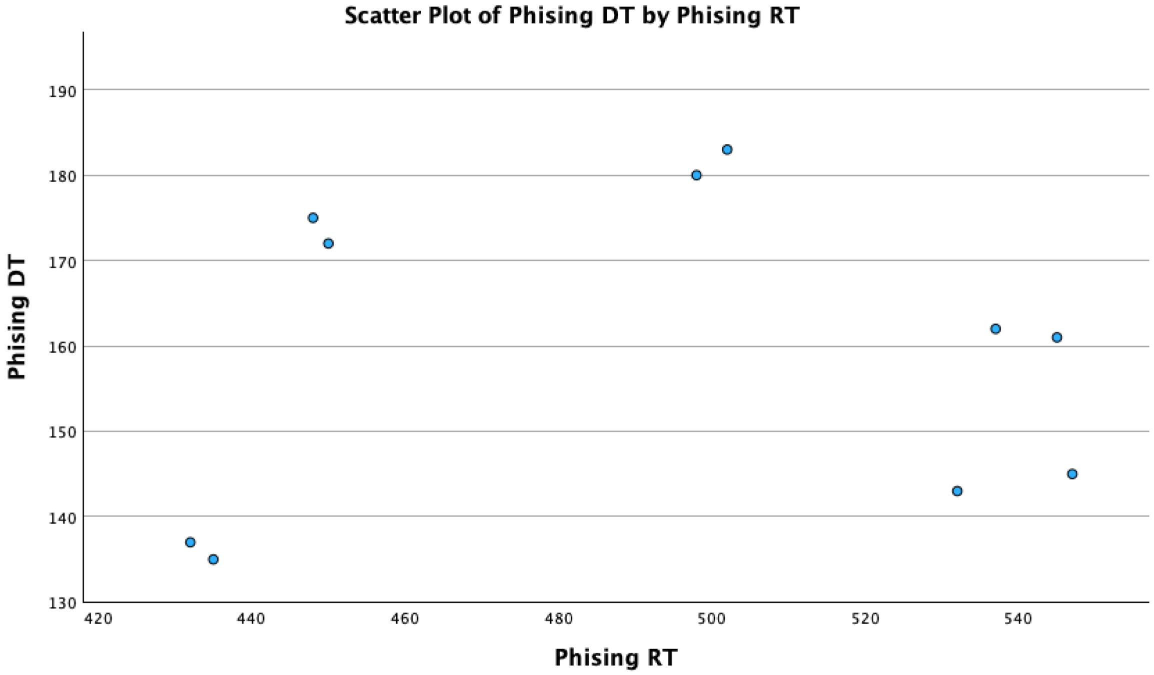
Appendix 18



Appendix 19



Appendix 20


Scatter Plot of Phising DT by Phising RT
Phising DT
190
180
170
160
150
140
130
420
440
460
480
500
520
540
Phising RT