

Research Issues

RSC811-Assignment 2

Prepared by
Abdulaziz Alarfaj



Part

1

Research Title : العنوان

Title: "A Descriptive Study on Cybersecurity Challenges of Working from Home during COVID-19 Pandemic and a Proposed 8-step WFH Cyber-attack Mitigation Plan"

Field of Study: The title covers an interesting and timely topic, especially in the context of the COVID-19 pandemic, which has brought about significant changes in work environments, including remote work. The topic addresses cybersecurity challenges faced by remote workers and proposes a plan to mitigate cyber-attacks.

Key Variables:

Independent Variable: Working from home during the COVID-19 pandemic.

Dependent Variable: Cybersecurity challenges and cyber-attacks.

Mediating/Moderating Variable: Security measures implemented (e.g., VPN, two-factor authentication, etc.).

Introduction : المقدمة

Clarity of Variables: The introduction clearly outlines the challenges organizations face in balancing flexibility and security during remote work. It mentions the increase in cyber-attacks and the exploitation of IT infrastructure vulnerabilities.

Problem Formulation: The problem is clearly identified by highlighting the increase in cyber-attacks due to remote work during the pandemic. Data from sources like the FBI and Interpol are used to confirm the rise in cyber-attack complaints.

Part

3

Problem Statement : مشكلة الدراسة

Problem Identification: The problem is clearly identified by pointing out the increase in cyber-attacks due to remote work during the pandemic. The study relies on data from sources like the FBI and Interpol to confirm the rise in cyber-attack complaints.

Main Questions: The study attempts to answer questions about employees' awareness of cyber-attacks and how to mitigate these attacks.

Part

4

Importance of the Study : أهمية الدراسة :

Theoretical Importance: The study adds to the existing literature on cybersecurity in the context of remote work, especially during the pandemic.

Practical Importance: The study provides a practical 8-step plan to mitigate cyber-attacks, which can be useful for organizations looking to improve their cybersecurity.

Part

5

أهداف الدراسة : Objectives of the Study

Objectives:

Measure employees' awareness of cyber-attacks.

Suggest effective methods for detecting and mitigating cyber risks.

Feasibility of Objectives: The objectives are realistic and achievable through the survey conducted.

Concepts and Definitions : مفاهيم وتعريفات الدراسة

Theoretical Framework: Key concepts such as social engineering, denial-of-service (DoS/DDoS) attacks, and ransomware are defined. The importance of employee security training is also highlighted.

Interrelation of Variables: The study explains how remote work increases exposure to cyber-attacks and how security measures can mitigate these risks.

Part

7

الدراسات السابقة - Previous Studies

Recent Studies: Recent studies (e.g., Das, 2019) on social engineering and phishing attacks are cited.

Agreements and Disagreements: Previous studies emphasize the importance of employee security training, but this study adds a new dimension related to remote work during the pandemic.

Part

8

Hypotheses : فرضيات الدراسة

Hypotheses: The study does not present explicit hypotheses but focuses on questions about employees' awareness and the effectiveness of security measures.

Relation to Title: The questions are directly related to the title and objectives of the study.

Part

9

Study Model : نموذج الدراسة

Study Framework: An 8-step framework for mitigating cyber-attacks is presented. This framework represents the relationships between remote work, cybersecurity challenges, and the measures needed to mitigate these challenges.

Methodology and Statistical Analysis: منهجية الدراسة و التحليل الاحصائي

Study Methodology: A survey was conducted using Google Forms, involving 109 participants who work from home.

Statistical Methods: Data were analyzed using percentages and proportions.

Discussion of Results and Recommendations : مناقشة النتائج والتوصيات

Interpretation of Results: The results showed that 62.4% of participants noticed an increase in fraudulent emails and phishing attempts since the start of the pandemic.

Achievement of Objectives: The study's objectives were achieved by identifying employees' awareness and suggesting effective security measures.

Recommendations: Practical recommendations such as using VPNs and two-factor authentication were provided, which can be applied in real-world settings.

Future Research: Future studies could focus on evaluating the effectiveness of the security measures proposed in this study.

Part

12

Summary

The study provides a comprehensive analysis of cybersecurity challenges in the context of remote work during the COVID-19 pandemic and offers a practical framework to mitigate these challenges. The recommendations provided can be beneficial for organizations seeking to enhance their cybersecurity in remote work environments.

Article link :

<https://ibimapublishing.com/articles/CIBIMA/2021/589235/589235.pdf>