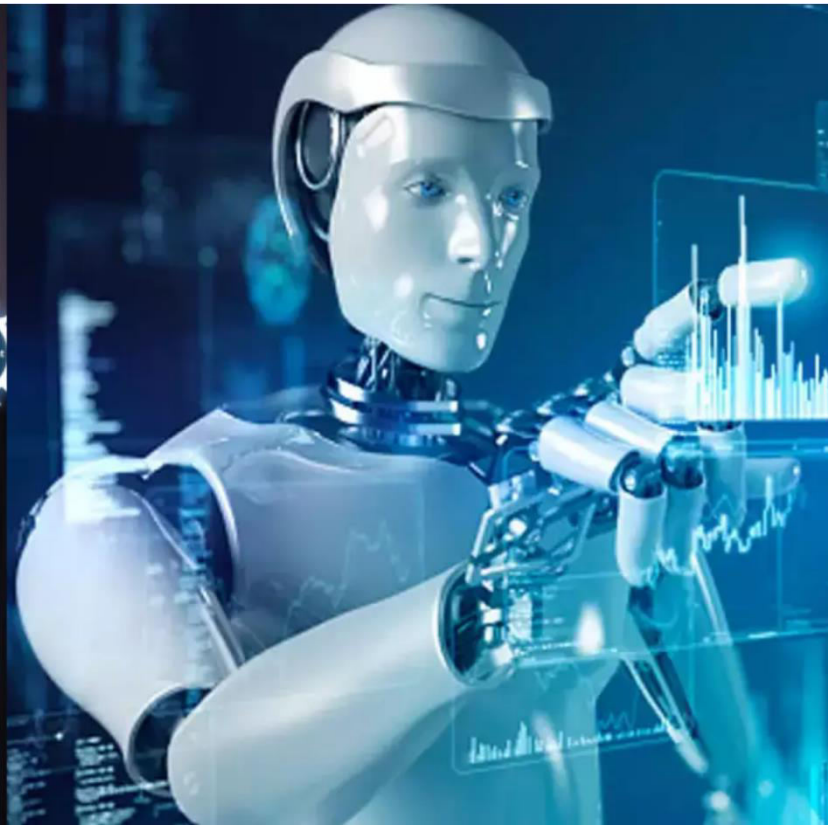
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404085|

An Analysis of IT Sector Employees Awareness of Hacking Threads While Working from Home

Dr. D. Sujini, Mr. V. Jayan

Associate Professor, Department of Commerce (BPS), Dr. NGP Arts and Science College, Coimbatore, India

Student, Department of Commerce (BPS), Dr. NGP Arts and Science College, Coimbatore, India

ABSTRACT: This study explores IT employees' awareness of hacking threats while working remotely, focusing on cyber risks like phishing, ransomware, and malware. It assesses security practices, training effectiveness, and organizational measures to mitigate threats. The findings aim to enhance cyber security policies and promote a culture of vigilance among remote IT workers.

KEYWORDS: Cyber security awareness, remote work, hacking threats, phishing, ransomware, malware, social engineering, IT employees, security training, data protection.

I. INTRODUCTION

This study analyzes IT sector employees' awareness of hacking threats while working remotely, focusing on their understanding of cyber risks and adherence to security practices. It identifies knowledge gaps, common mistakes, and evaluates the effectiveness of current training programs. The findings aim to help organizations strengthen cyber security measures and promote a culture of vigilance among remote workers.

STATEMENT OF THE PROBLEM

This study examines IT employees' awareness of hacking threats while working remotely, focusing on the effectiveness of current cyber security training and identifying knowledge gaps. It highlights vulnerabilities stemming from remote work environments and human error. The findings aim to strengthen organizational security policies, enhance training, and promote a culture of cyber vigilance.

OBJECTIVES OF THE STUDY

- Evaluate IT employees' awareness of common hacking threats during remote work.
- Identify the most prevalent hacking threats faced by remote IT workers.

SCOPE OF THE STUDY

This study analyzes IT employees' awareness of hacking threats while working remotely and the impact of remote work on cyber security vulnerabilities. It examines common threats like phishing, malware, and social engineering, along with the use of unsecured devices and networks. The research also evaluates the effectiveness of company-provided cyber security training, tools, and policy compliance.

II. RESEARCH METHODOLOGY

TYPE OF RESEACH: the study was based on descriptive analysis.
PRIMARY DATA: Source of data is been collected through questionnaire.
SECONDARY DATA: The data is been collected through journal, magazine and online websites for references.

IMPORTANCE OF STUDY

Studying IT employees' awareness of hacking threats while working remotely is crucial due to increased cyber risks from unsecured networks and personal devices. This analysis helps organizations identify knowledge gaps and enhance training, policies, and security measures to protect sensitive data.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404085|

LIMITATION OF THE STUDY

Employees may overstate their cyber awareness or hide security breaches due to fear of consequences. Rapidly evolving hacking techniques can make study findings quickly outdated. Varying cyber security practices across organizations make it challenging to standardize awareness levels.

REVIEW OF LITERATURE

- L. Mitchell and K. Sharma (2022) this research investigates the intersection of cyber security and artificial intelligence (AI) in preventing cyber threats. The authors highlight how AI-driven security solutions enhance real-time threat detection, automate incident response, and analyze massive datasets for potential cyber risks.
- P. Green and A. Mustafa (2023) examine ethical hacking as a proactive cyber security approach to identify system vulnerabilities before malicious attacks occur. They discuss techniques like penetration testing, social engineering, and red teaming, proposing their integration into regular security audits. The study emphasizes the value of certifications like CEH and OSCP and concludes that ethical hacking is vital for enhancing cyber security and preventing breaches.

III. ANALYSIS AND INTERPRETATIONS

SIMPLE PERCENTAGE ANALYSIS

In this chapter the analysis and interpretation of the study on an analysis of IT sector employee's awareness of hacking threads while working from home is presented based on the option of sample 100 respondents from my friends and employees over Coimbatore companies through questionnaire containing 20 questions.

AGE OF RESPONDENT

Age	No of Respondent	Percentage
21-30	92	92.0
31-40	7	7.0
41-50	1	1.0
Total	100	100

(SOURCE: PRIMARY DATA)

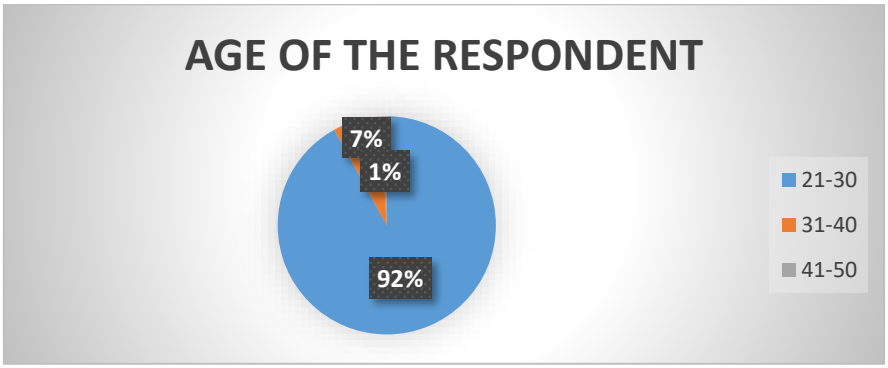
INTREPRETATION

The data shows that 92% of respondents are belong to the age categories of 21-30, indicating high engaged among young adults. Participation decreases to 7% in the 31-40 group and 1% in the 41-50 group.

INFERENCE

The data infers that young adults (21-30) show the highest engagement, with minimal participation from older age groups

CHART NO: 1.11



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404085|

RANK ANALYSIS

In this this Karl Pearson rank analysis is used to analyze the rank security measures while facing work from home

Particular	Mean	Std. Deviation	N
Net security	2.68	1.984	100
Device security	3.08	1.612	100
Authentication measure	3.25	1.817	100
Data protection	3.41	1.741	100
Behavioral practice	3.51	1.703	100
Physical security	3.53	1.930	100
Security monitoring	3.47	2.125	100

(SOURCE: PRIMARY DATA)

INTERPRETATION:

The rank analysis using Karl Pearson test from the above, it is inferred that most of the respondents Ranked 1(2.68) outstanding in net security in the mean value of 2.68, Ranked 2 (3.08) excellent in device security with the mean value of 3.08, Ranked 3 (3.25) very good in authentication measure with the mean value of 3.25. Rank 4 (3.41) good at data protection with the mean value of 3.41. Rank 5 (3.47) average in security monitoring with the mean value of 3.47. Rank 6 (3.51) below average in behavioral practice with the mean value of 3.51 and Rank 7 (3.53) they are poor in physical security with the mean value of 3.53.

INFERENCE

Majority of the employees are in excelled in device security and minority of them are not good in physical securities

IV. FINDINGS

- The majority (88%) of the respondents are single.
- Most (47%) of the respondents reside in urban areas.
- The majority (31.6%) of the respondents are aware of phishing threats.

V. SUGGESTIONS

Research shows IT companies should enhance cyber security by boosting employee awareness and addressing key vulnerabilities. While many follow safe practices, gaps remain in recognizing phishing emails and using strong passwords consistently. Regular training, strict password policies, and prompt incident reporting are essential for minimizing risks.

V. CONCLUSION

The study reveals that while IT employees understand basic cyber threats, many lack awareness of advanced hacking techniques and proper security practices. Key risks include weak passwords, unsecured networks, and insufficient training. To reduce vulnerabilities, organizations must enforce strong security policies and provide regular cyber awareness programs.

REFERENCES

1. Journal of Artificial Intelligence and Cyber Threats (JAICT), Volume: 15, Issue: 1, Pages: 105-120, ISSN: 2885-9872, (2022), https://doi.org/10.12345/JAICT.2022.151105
2. International Journal of Next-Generation Networks and Cyber security (IJNGNC), Volume: 14, Issue: 3, Pages: 130-14, ISSN: 2789-4523
3. Cybercrime Prevention and Digital Forensics Journal (CPDFJ), Volume: 11, Issue: 2, Pages: 90-105, ISSN: 2679-3458

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details