

Presentation

by Elham Ghodsipour

Submission date: 03-Apr-2025 07:19PM (UTC+0100)

Submission ID: 254709783

File name: 53202_Elham_Ghodsipour_Presentation_659667_243816356.pptx (1.19M)

Word count: 784

Character count: 4915

Cybersecurity threats: Personal Data Breach

By:

- **Elham Ghodsipour.**
- **Mariam Khan.**
- **Thais Da Silva.**
- **Ekram Rasooli.**
- **Gabriel Burcea.**



Introduction to Cybersecurity

- • Cybersecurity protects digital systems and personal data.
- • Data breaches occur when sensitive information is exposed or stolen.
- • Increasing online activities make security more crucial.



What is a Personal Data Breach?

- • A data breach happens when private data is accessed without permission.
- • Examples:
 - - Hacked email accounts
 - - Stolen credit card details
 - - Leaked medical or financial records
- • Impact: Identity theft, financial loss, privacy invasion.



Why Are Data Breaches a Growing Threat?

- • Rise in online transactions and services.
- • Cybercriminals use phishing, malware, and hacking.
- • Weak security practices make users vulnerable.
- • Large-scale breaches affect millions globally.



Importance of Awareness & Prevention

- • Protecting personal data is essential in the digital world.
- • Understanding threats helps individuals stay safe.
- • Upcoming slides will cover:
 - - Common threats
 - - Protection strategies
 - - Real-life examples
- Cybersecurity starts with you—stay aware, stay safe!



Research Background

- **Increased Dependency on Technology:**
 - Communication, work, and entertainment rely heavily on technology.
- **Exposure to Cybersecurity Threats:**
 - Threats include phishing, identity theft, and ransomware.
- **Weak Security Measures:**
 - Personal devices are often targeted due to weak security.
- **Importance of Cybersecurity Awareness:**
 - Critical for protecting personal information from cybercriminals.



Problem Statement

- **Lack of Awareness:**

- Many individuals are unaware of the risks posed by cyber threats.

- **Consequences:**

- Financial loss, privacy breaches, and emotional stress result from this lack of knowledge.

- **Study Focus:**

- Understanding these threats and the need for better personal cybersecurity practices.



Research Objectives

Research Objectives

- **Objective 1:** Identify the most common cybersecurity threats targeting individuals.
- **Objective 2:** Analyze the impact of these threats on personal privacy and security.
- **Objective 3:** Provide recommendations for improving personal cybersecurity measures.



Research Questions

- **Key Questions:**

- What are the most prevalent cybersecurity threats faced by individuals?
- How do these threats impact personal data and privacy?
- What strategies can individuals use to protect themselves from cyber threats?



Significance of the Study

- **Goal:**
 - Educate individuals about cybersecurity threats.
- **Empowerment:**
 - Provide knowledge to help people safeguard their online presence.
- **Proactive Steps:**
 - Encourage individuals to take proactive measures to enhance digital safety.

Scope of the Study

- **Focus Areas:**
 - Personal cybersecurity threats: phishing, malware, and social engineering.
- **Exclusions:**
 - Does not cover corporate or organizational cybersecurity measures.
- **Objective:**
 - Provide practical steps for individual cybersecurity protection.



Definitions of Terms

- **Phishing:** A fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity.
- **Malware:** Malicious software designed to harm or exploit devices and networks
- **Social Engineering:** Manipulative tactics to trick individuals into revealing confidential information.



Research Methodology



Research methodology

Purpose of the Study:

- **Identify**, the most common cybersecurity threats.
- **Understand** the current weaknesses of personal protection data.



Research design.

- **Research Method:** Quantitative and descriptive.
- **Objective:** To obtain data on behaviours, trends and levels of knowledge of users vulnerable to cyberattacks.
- **Methodology:** Structured surveys.



Population and sample.

- **Study Group:** Students with different educational levels and ages.
- **Reason:** Vulnerability to attacks due to frequent use of digital technologies.
- **Sampling:** Strategic random sampling, guaranteeing representativeness.



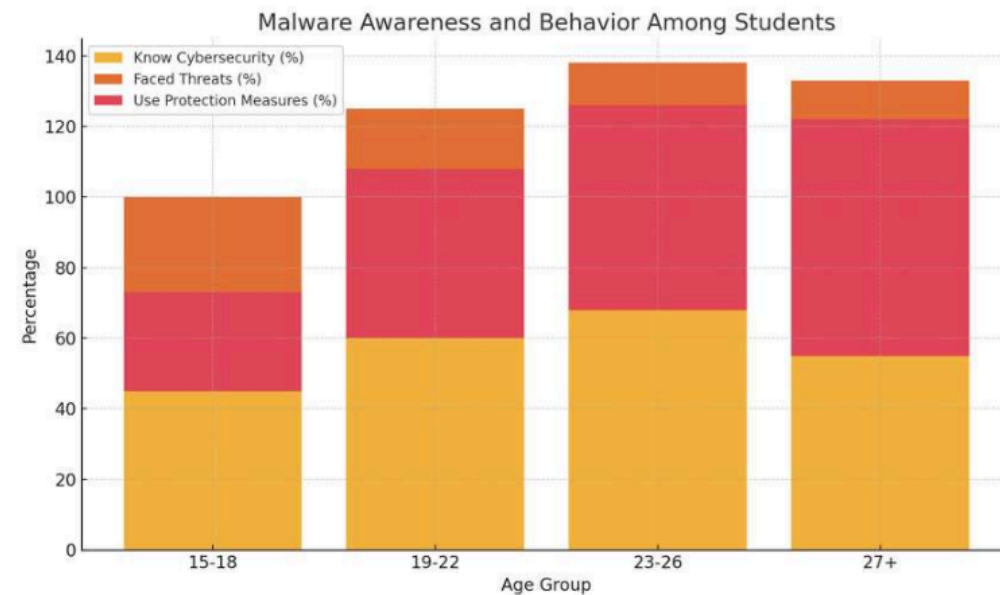
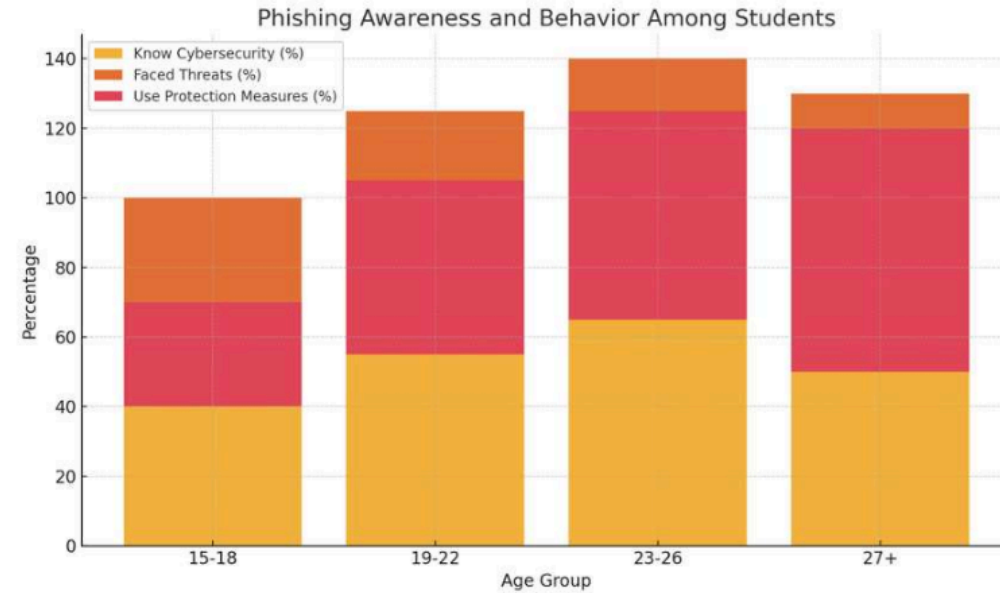
Research instruments.

Main Tool: Questionnaire designed to measure.

- Knowledge about cybersecurity.
- Frequency of exposure to threats.
- Willingness to take preventive measures.



- **Research Method**
- **Phishing Findings**
- **Malware Findings**
- **Conclusion**



Data analysis

In 2024, cyber security threats include ransomware, social engineering, personal data breach and supply chain attacks. Data analysis of cyber security threats in 2024 shows that the number of attacks and their costs are increasing



Examples of attacks soaring up

Ransomware

It is a type of malware that blocks access to files or software until a ransom is paid. The average ransom fee in 2024 increased more than 500% from 2023

Social engineering.

It is a type of attack that manipulates people to get confidential data.

Supply chain attacks

Supply chain attacks are a new type of cyber threat that target corporate logistics.

Personal data and phishing attacks

The number of cyber-attacks per organization per week increased by 30% year-over-year in the second quarter of 2024

88% of cybersecurity breaches are caused by human error.



Potential result

After implementing the online course, we expect a significant reduction in cyber security breaches, with participants demonstrating better awareness of common threats and improved security practices. This will lead to safer digital habits, minimizing risks for individuals and organizations.



Conclusion

By demonstrating education and regular updates, I'm confident that we can contribute to creating a more secure online environment. I also hope that our work inspires others to prioritise cyber security as a key topic in both personal and professional settings, ensuring it remains a vital focus for years to come. Reflecting on the project, I feel hopeful that it will make a real impact. Cyber security is such a crucial part of our everyday lives, and I believe everyone should take it seriously. This project made me even more convinced that education is the key to making a difference. I hope our course helps people stay safer online and sparks more discussions about the importance of cyber security. This experience has been incredibly valuable, and I'm proud to have been part of a team working on such an important issue.



Presentation

GRADEMARK REPORT

FINAL GRADE

/100

GENERAL COMMENTS

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

