PHISHING ATTACKS IN CYBERSECURITY

Techniques, Detection, and Prevention

Submitted by: Sayooj Mohan

Internship: Digisuraksha Parhari Foundation

INTRODUCTION

- Phishing attacks use deception to trick individuals into sharing sensitive information. They are a major threat in the digital age, affecting businesses and individuals alike. This project explores how phishing works, how it can be detected, and how to prevent it.

PROBLEM STATEMENT

- Despite advancements in cybersecurity, phishing remains effective due to its reliance on human error. It can lead to credential theft, financial loss, and breaches of confidential data.

RESEARCH OBJECTIVES

- - Understand various phishing attack techniques

- - Analyze real-world phishing examples

- - Review effective detection and prevention strategies

- - Propose awareness and technology-based solutions

COMMON PHISHING TECHNIQUES

- - Email Phishing

- - Spear Phishing

- - Whaling

- - Vishing (Voice Calls)

- - Smishing (SMS)

- - Clone Phishing

DETECTION TECHNIQUES

- - AI-based spam filters

- - Suspicious URL detection

- - Email header analysis

- - Behavior-based anomaly detection

PREVENTION STRATEGIES

- - Multi-Factor Authentication (MFA)

- - Employee security awareness training

- - Browser/email security tools

- - Regular phishing simulations

REAL-WORLD USE CASES

- - 2020 Twitter spear-phishing attack on verified accounts

- - Google and Facebook losing $100M to a fake invoice scam

- - Constant phishing attempts on banks and financial institutions

ETHICAL AND SOCIAL IMPACT

- Phishing undermines trust in digital communication. Awareness and responsibility in technology use are crucial for mitigating its impact.

MARKET RELEVANCE

- Phishing attacks cause billions in losses annually.

- The cybersecurity market is investing heavily in email security, training platforms, and AI detection tools.

FUTURE ENHANCEMENTS

- - Gamified phishing awareness training

- - AI-powered real-time email scanning

- - Integration of decentralized identity management

- - Behavior-based phishing detection systems

CONCLUSION

- Phishing continues to evolve and adapt.

- Combining technical solutions with strong user awareness is essential to protect against such attacks.

THANK YOU