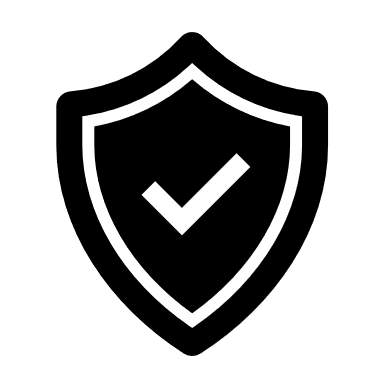
**Capstone Project**

**Incident Analysis Report**

**Project Title:  
Analysis of the Facebook and Google Phishing Scam (2013–2015)**

****

**Prepared By:  
Taniesha Stewart  
GitHub Username: Tanieshastewart@bellsouth.net**

**Submission Date:  
April 27, 2025**

**Institution/Organization:  
Capstone Project – Cybersecurity Analyst Program**

Table of Contents

[Summary 3](#_Toc196649641)

[Key Findings 3](#_Toc196649642)

[Recommendations 3](#_Toc196649643)

[Impact 3](#_Toc196649644)

[Conclusion 4](#_Toc196649645)

**Capstone Project Incident Analysis Report**

**Incident:**  
**Facebook and Google Phishing Scam (2013–2015)**

**Prepared By:**  
**Taniesha Stewart**

# Summary

Between 2013 and 2015, Facebook and Google were defrauded of over $100 million through an elaborate phishing scam involving a fake vendor and fraudulent invoices. The attacker impersonated Quanta Computer and used social engineering to trick employees into transferring large sums to his controlled accounts.

# Key Findings

* Lack of verification mechanisms contributed to the scam.
* Effective social engineering tactics exploited human vulnerabilities.
* Swift collaboration with law enforcement helped recover partial funds.

# Recommendations

* Implement multi-factor vendor verification processes.
* Conduct regular phishing awareness training sessions.
* Introduce stricter internal audit and transaction verification protocols.

# Impact

* Significant financial losses due to fraudulent transactions.
* Reputational damage and increased legal exposure.
* Reinforced need for enhanced internal controls and employee cybersecurity training.

# Conclusion

This case demonstrates that even the most technologically advanced companies are vulnerable to social engineering attacks if verification protocols are weak. It highlights the need for robust internal financial controls, continuous cybersecurity training, and proactive incident response planning to prevent similar breaches in the future.