PROTECTING FROM ONLINE BANKING FRAUD: RISK AWARENESS AND PREVENTION STRATEGIES

Tony Griffiths, Griffith University

ABSTRACT

This research article focuses on the increasing risk of online banking fraud and the importance of awareness and prevention strategies. Online banking fraud is a type of cybercrime that involves unauthorized access to a customer's bank account and the theft of their funds or personal information. Various methods are used by fraudsters, such as phishing scams, malware attacks, and social engineering. To prevent online banking fraud, customers should never share their login credentials or other sensitive information, use strong passwords, keep their software and antivirus programs up to date, and regularly monitor their accounts for suspicious activity. The impact of online banking fraud can be significant, causing financial loss, identity theft, and reputational damage to customers and banks, and undermining trust in the banking system. Therefore, raising awareness about online banking fraud risk and encouraging everyone to adopt best practices to ensure the security of online banking transactions is essential.

Keywords: Online Banking Fraud, Cybercrime, Phishing Scams, Malware Attacks, Risk Awareness, Customer Protection, Bank Security, Financial Loss.

INTRODUCTION

The rise of digital banking has made it easier for customers to access their accounts and perform transactions from the comfort of their own homes. However, with the convenience of online banking comes the risk of fraud. Online banking fraud is a type of cybercrime that involves unauthorized access to a customer's bank account and the theft of their funds or personal information. This research article explores the risk of online banking fraud and the steps that can be taken to prevent it (Barker, 2020).

Overview of Online Banking Fraud

Online banking fraud is a growing problem, with fraudsters using various methods to gain access to a customer's bank account. These methods include phishing scams, malware attacks, and social engineering. Phishing scams involve tricking customers into providing their login credentials or other sensitive information. Malware attacks involve the installation of software that can capture login information or other sensitive data. Social engineering involves using psychological manipulation to convince customers to provide their information (Council, 2005; Tang, 2015).

Preventing Online Banking Fraud

There are several steps that customers can take to prevent online banking fraud. First, customers should never share their login credentials or other sensitive information with anyone. They should also use strong passwords that are difficult to guess and change them regularly. Secondly, customers should keep their software and antivirus programs up to date to prevent

Citation Information: Griffiths, T. (2023). Protecting from online banking fraud: risk awareness and prevention strategies. *Journal of the International Academy for Case Studies, 29*(S1), 1-2.

malware attacks. Thirdly, customers should be wary of emails or messages that ask them to click on links or download attachments, as these could be phishing scams. Lastly, customers should regularly monitor their accounts for any suspicious activity and report any unauthorized transactions to their bank immediately (Drew & Farrell, 2018; Lichtenstein & Williamson, 2006).

Impact of Online Banking Fraud

Online banking fraud can have a significant impact on customers, banks, and society as a whole. For customers, online banking fraud can result in financial loss, identity theft, and damage to their credit scores. For banks, online banking fraud can damage their reputation; result in financial losses, and lead to legal action. For society, online banking fraud can undermine trust in the banking system and lead to a decrease in economic activity (Youn, 2005).

CONCLUSION

Online banking fraud is a growing problem that requires attention from both customers and banks. By taking steps to prevent fraud and remaining vigilant, customers can protect themselves from financial loss and identity theft. Banks can also take steps to prevent online banking fraud by implementing advanced security measures and educating their customers on how to stay safe online. It is essential to raise awareness about online banking fraud risk and encourage everyone to adopt best practices to ensure the security of online banking transactions.

REFERENCES

Barker, R. (2020). The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention. *South African Journal of Business Management*, *51*(1), 1-10.

Council, F.F.I.E. (2005). Authentication in an internet banking environment. *Retrieved June*, *28*, 2006.

Drew, J.M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research*, *19*(6), 537-549.

Lichtenstein, S., & Williamson, K. (2006). Understanding consumer adoption of internet banking: an interpretive study in the Australian banking context. *Journal of Electronic Commerce Research*, *7*(2), 50.

Tang, S.L. (2015). Increasing the role of agency deference in curbing online banking fraud. *North Dakota Law Review*, *91*, 329.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, *49*(1), 86-110.

Received: 25-Jan-2023, Manuscript No. JIACS-23-13436; **Editor assigned:** 28-Jan-2023, PreQC No. JIACS-23-13436(PQ); **Reviewed:** 11-Feb-2023, QC No. JIACS-23-13436; **Revised:** 15-Feb-2023, Manuscript No. JIACS-23-13436(R); **Published:** 22-Feb-2023