มหาวิทยาลัยราชภัฏนครปฐม

Chapter 8

E-Commerce Security Systems

A.Pichaya Sookplung

Information Technology

pichaya@webmail.npru.ac.th

Introduction

- Security is crucial in E-Commerce to protect data and transactions.
- Cyber threats continue to evolve, requiring strong security measures.
- Businesses must ensure secure online environments for customers.

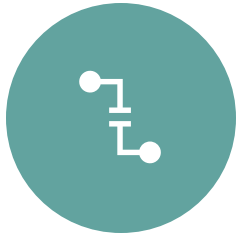
Common Security Threats

- PHISHING ATTACKS

- MALWARE AND RANSOMWARE

- DATA BREACHES

- IDENTITY THEFT



- MAN-IN-THE-MIDDLE (MITM) ATTACKS

SSL Certificates

• Secure Sockets Layer (SSL) ensures encrypted communication.

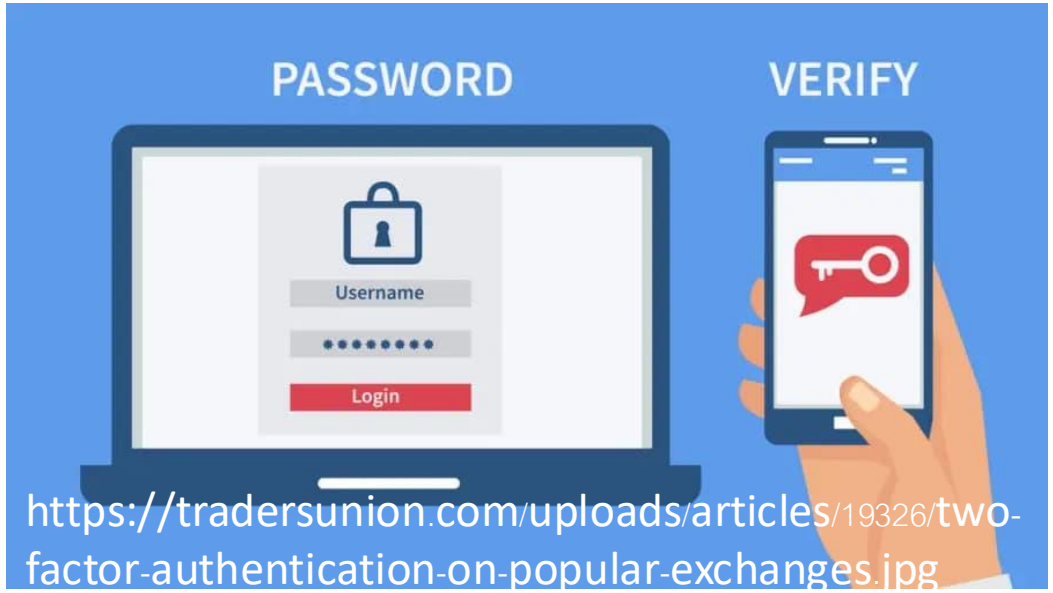
• Used to secure websites, especially for online transactions.

• Provides authentication and data integrity.

• Websites with SSL use HTTPS instead of HTTP.

Two-Factor Authentication (2FA)

- Adds an extra layer of security beyond passwords.
- Requires two forms of identification (e.g., password + OTP).
- Reduces risk of unauthorized access.
- Common methods: SMS OTP, Authenticator Apps, Biometric Authentication.



https://tradersunion.com/uploads/articles/19326/two-factor-authentication-on-popular-exchanges.jpg

Best Practices for E-Commerce Security

- Use strong and unique passwords.
- Implement regular software updates and patches.
- Encrypt sensitive customer data.
- Monitor and log activities for suspicious behavior.
- Educate users about cybersecurity threats.

Conclusion

- Security is a continuous process in E-Commerce.
- Businesses must implement strong security measures.
- Customers should be aware of online security threats.
- Staying updated with security trends is essential.

Summary

https://magnetoitsolutions.com/blog/top-ecommerce-business-models

มหาวิทยาลัยราชภัฏนครปฐม