



INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 6.078

(Volume 6, Issue 3)

Available online at: www.ijariit.com

Effective online transaction and data security in online transaction

Nefisath Mishriya
nefisath@gmail.com

Shaiju Joseph
Josephshaiju010@gmail.com

ABSTRACT

In a cashless trend and busy schedule life most of us expect things to be done faster. We book and buy almost everything online. Includes shopping, booking tickets, appointment etc. So, we need to ensure user data such as personal contact number, account details credit/debit card number, pin number, password is highly securable. This research paper gives insights on online transaction precaution to be taken care while doing online transaction.

Keywords— Electronic Fund Transfer (EFT), Two Factor Authentication(2FA), merchant, net banking, Credit card, Debit card, Unified Payment Interface (UPI), One-Time Password (OTP), Mobile wallet

1. INTRODUCTION

- Online transaction is a real time process, which involves transfer of data and money through Electronic Fund Transfer (EFT).
- It consists of buyer, seller and products.
- Main interface for online transaction is through website or application.
- Any form of online transaction requires internet connection.



Fig. 1: Sample Online transaction using mobile wallet

2. OBJECTIVE

- (a) To learn the process of online transaction
- (b) To understand the importance of online transaction
- (c) To understand the importance of security in online transaction.

3. LITERATURE REVIEW

There are different research papers which were developed for data security in online transaction.

Literature survey is presented starting with the paper [1] which provides the information about different protocols which helps to overcome the problem of security. Then coming to the paper [2] this paper presented with online transaction process. Paper [3] presented with different e-payment process, benefits, and security related issue of electronic payment system. Paper [4] presented the security threats in online payment and also addresses on PayPal system.

4. PURPOSE OF ONLINE TRANSACTION

- In a cashless trend and busy schedule life most of us expect things to be done faster.
- We book and buy almost everything online. Includes shopping, booking tickets, appointment etc. As it is more convenient rather than waiting in queues to accomplish the requirement. In short it is simpler, fast and less time consuming. For eg: If we go to a bank for money transfer will take more time compared to online. Due to the process such as waiting in queues, filling the slip etc.
- It also saves time and interchange fee. Since Booking agencies charge money for booking tickets which can be saved if we go for online booking.
- It also provides better customer experience, since the web site or app provides more insight on the product, including suggestions on the products, reviews, lists similar products which customer might be interested in and other products to attract customer.



Fig. 2: Shopping is an example of online transaction

5. ONLINE TRANSACTION PROCESS

1. User registration
User has to register first in merchant website/application. For example: Amazon.
2. Book/Order
Place an order in case of shopping, or booking tickets for Movie, or booking Cab/Flight/Train for travel.
3. Payment
 - Payment can be done through net banking/Credit card/Debit card/Unified Payment Interface (UPI), mobile wallet etc.
 - Once payment source is chosen, request will be sent to corresponding bank for verification. After successful verification One-Time Password (OTP) will be generated and sent to registered user. After providing OTP, can proceed to complete payment.
 - After completing the payment, mail and message will be sent to registered user on the successful order.

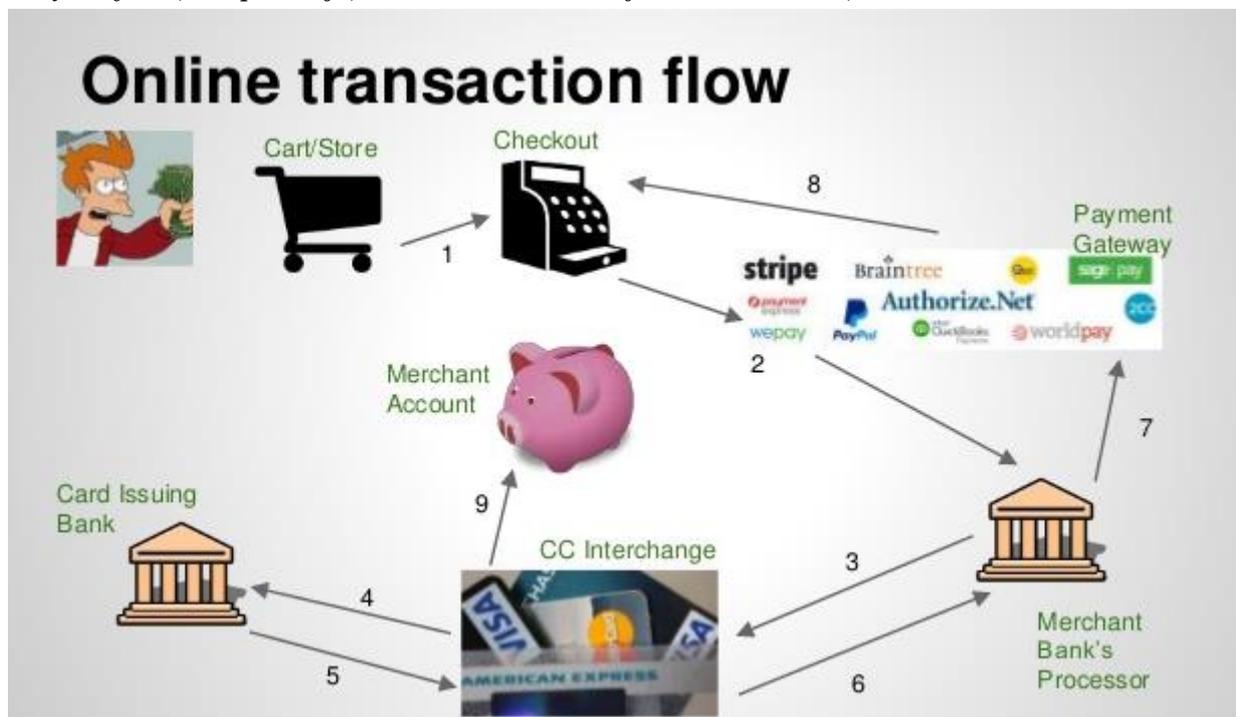


Fig. 3: Online transaction flow diagram

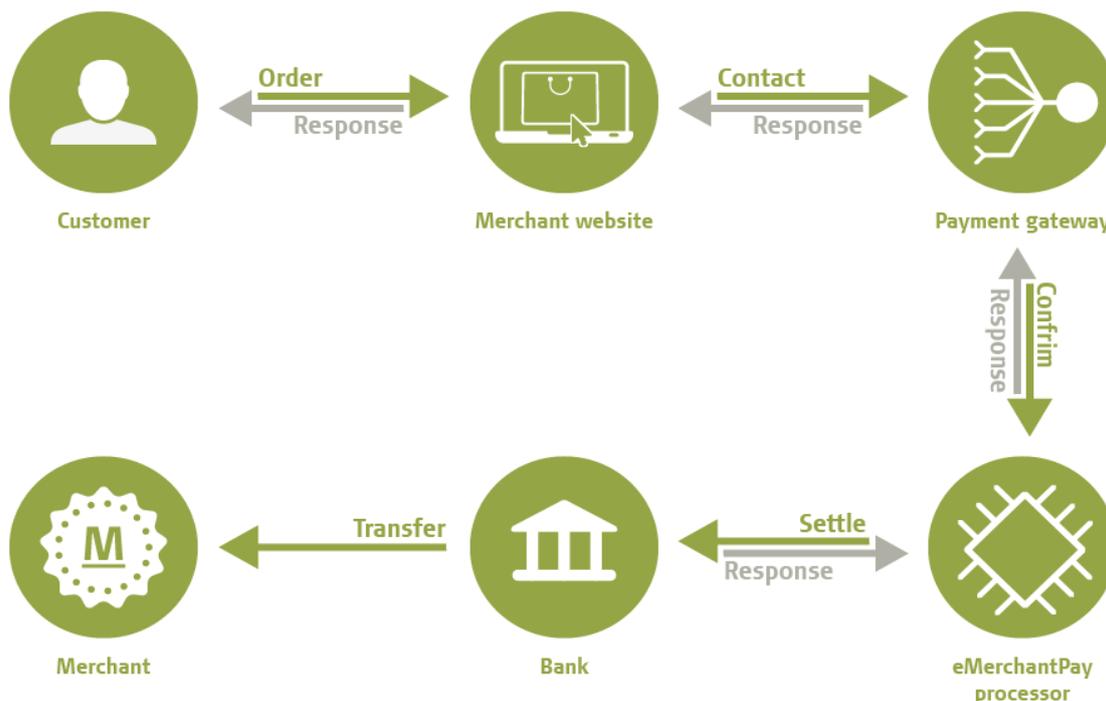


Fig. 4: Online transaction flow diagram

6. IMPORTANCE OF SECURITY IN ONLINE TRANSACTION

Security should be the main focus in online transaction as we know data can be steered by hackers, computer viruses such as malware, ransomware, phishing etc. So, we should pay more attention especially doing online payment.

Some scenarios where frauds try to trap us:

- You may get a call from unfamiliar agencies or site and they convince they will provide offer or loan etc. And to initiate the process we have to pay some money online. Never pay and do not provide sensitive information such as account details, Pin, personal contact etc. Unless we verify it is not fraud.
- You may get a message or call from known bank customers saying we have to share PIN to verify bank account details, or credit card etc. Never provide any sensitive details, because no one asks PIN. It is only for personal reference not to be shared with anyone. Never share your PIN with anyone, even closed ones unless you think trust worthy. Because PIN can be cloned and can be used for illegal transaction.
- Pay attention while doing transaction in ATM. There are frauds who try to steal sensitive data and money. Do not run in hurry while doing transaction in ATM. Attention is must.
- Online shopping in unfamiliar website, do not proceed with payment unless you verify the site such as, it should begin with https, domain name or company name should be active. Also, OTP message should be linked to the merchant site. Otherwise you may get trapped.

- (e) Do not use public Wi-Fi while doing online transactions. Frauds can easily hack data. Always use personal device and secured networks for online transaction.
- (f) Sometimes payment might not be successful, but money will be deducted from your account in these cases contact your bank immediately. Sometimes it could be due to network issues, or could be illegal transaction by frauds.

How stealing of data can be avoided?

- (a) Two factor authentication(2FA) – Along with password, we can also provide secret questions, biometric data -could be finger print or voice. Example: We have 2FA in Facebook, google etc.
- (b) Install anti-virus and anti-spyware software
- (c) If you are doing online transaction through mobile app, do not download the app from third party app stores.it may contain virus and cause malware on your device.
- (d) Also do not provide all permission when you download the app, read the reviews for the app, provide only required permission after reading the reviews.
- (e) Never leave phone or device unlocked.
- (f) Avoid public network or WI-FI.
- (g) Pay attention while doing transaction in ATM.

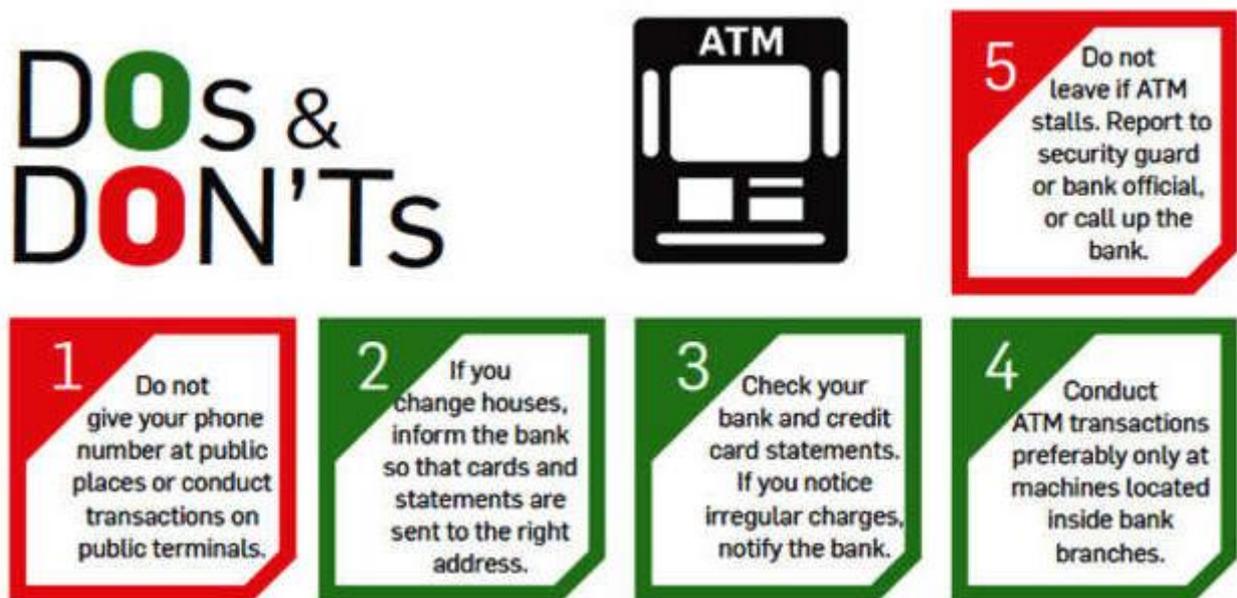


Fig. 5: Steps to follow in ATM

7. REFERENCES

- [1] Transaction Security for Internet E-commerce Application by Nikhil Khandare, Volume 5, Issue 2
- [2] Online Transaction processing by Jing Sun and Xingdi Tan
- [3] E-Commerce and Online Payment in the Modern Era by Momin Mukherjee and Sahadev Roy
- [4] To Study the Security Aspects in the Online Transactions Using PayPal by Dr. Ranjit D. Patil, Sujata P. Patil and Vidya H. Bankar.
- [5] <https://www.toppr.com/guides/business-studies/emerging-modes-of-business/online-transactions-and-security-of-e-transactions/>
- [6] <https://smartasset.com/personal-finance/10-tips-for-secure-online-transactions>