Quadrant II - Notes

Paper Code : COG138

Module Name :Risks in E - Payment Systems

Risks in E - Payment Systems

1. **The Risk of Fraud**

   The system uses a particularly vulnerable protocol to establish the identity of the person authorizing a payment. Passwords and security questions aren't foolproof in determining the identity of a person. So long as the password and the answers to the security questions are correct, the system doesn't care who's on the other side. If someone gains access to your password or the answers to your security question, they will have gained access to your money and can steal it from you.

   E-commerce **fraud** is growing at 30% per year. If you follow the security rules, there shouldn't be such problems, but when a merchant chooses a payment system which is not highly secure, there is a risk of sensitive data breach which may cause identity theft.

2. **The need for internet access**

   There is need of 24x7 internet connection to facilitate online transactions. If the internet connection fails, it's impossible to complete a transaction.

3. **Risk of Being Hacked**

   When transacting online, your personal or account information and credit card number is exposed over the Internet. This leads to the risk of your account being hacked. Hackers may use your identity for fraudulent activities or make huge fund transfers from your account, which could mean financial losses for you.

4. **False Identity**

There are no means to verify if the person entering information online is the same person he claims to be. This is because unlike physical transactions, the individual is not present in person, and one's identity is not verified using a photograph or a physical signature

5. **Anonymity and Privacy Concerns**

The transaction and user details are recorded by the payment systems you are using, and stored in their database. This leads to lack of anonymity. Cases of identity theft have raised privacy concerns in electronic payments. If credit card details are not sent over a secure server, if online transactions are not carried out over a secure Internet connection, if virus protection software or firewalls are not in place, or if data encryption techniques are not used, there is a serious risk of privacy breach. In the absence of proper security measures, sensitive information may be exposed to hackers, leading to illegitimate use of your identity or money.

6. **Additional Cost and Effort**

Some electronic transaction services may require you to pay processing fees and the like, thus leading to increased costs. Electronic payment systems need Internet access, which may invite additional costs. Setting up the account, accessing the Internet, familiarizing oneself with the interface and operating it efficiently, involves additional effort, and may be cumbersome for some.

7. **Loss of Smart Cards**

Electronic payments involve the use of smart cards (credit and debit cards, ATM cards, identity cards, etc.) And this involves the risk of their theft or loss. In case a lost smart card falls in the wrong hands or if it is stolen, your identity is at the risk of theft and the money in the account that the card is linked to, may be spent by fraudulent users. There are measures to inform the bank about the loss of your card and get it blocked. But the time between losing the card and blocking it, is critical. Unauthorized users may carry out transactions in your name during that period.

8. **Disputed transactions**

Disputed transactions are another area of concern when it comes to electronic payment systems.Say, for example, that someone else used your card to make a purchase without your knowledge or permission. In this case, it would be difficult for you to prove that you weren't the original purchaser, and it might be difficult to reclaim your funds or get a refund.

9. **Security risks**

As with any piece of technology out on the market these days, all technological solutions are prone to some security risks and breaches.This is why it's crucial to protect your private information as much as you can.Once again, inform your bank or financial institution if you suspect anything out of the ordinary.Servers may fail to work for temporary periods of time, transactions may bounce back, a payment might not be cleared, you might get double charged – all of these factors are security risks that you need to be aware of.

10. **Technical Problems**

There are a number of technical issues that could prevent your e-payment from being successful. Internet and server problems such as poor signal connection can disable online payment methods. In addition to this, some banks block international transactions for security reasons. While this can be solved by contacting your bank directly, it can often result in them blocking your card – which is slightly annoying.

And then there are technical glitches, which can sometimes take days to resolve. Popular payment gateways such as PayPal will undergo regular upgrades and changes to improve its service. In some situations, the upgrades may not go to plan, which disrupts the service and can result in the platform's server being down.

11. **Impulse Buying.**

Impulse buying means sudden buying. E-payment systems encourage impulse buying , especially online. Impulse buying leads to disorganized budgets.

12. **Dishonest merchants**

Sometimes, some ecommerce website are fake and if the customers does any transaction from that website then it becomes a fraudulent activity for that customer.There are fake merchants who provoke the customers to buy the goods.