Assignment - IV

B. Karthika
2024IA05I7.

1. Write about issues of online payment system.

A: A few issues of online payment systems are:

i) Technical problems:

Online payments are subject to technical failures ore downtime, just like any other software that is depends on technology. Though tech main-tenance operations are announced in advance and usually take place during the night, sometimes, it can cause frustration among online shoppers. Especially when it takes place without prior warning, a lot of business experience heavy bounce rates.

ii) Password threats:

If you're a registered user with a website who uses online payments pretty after, there are high chances that the online portal can have access to your personal information or bank account details.

iii) Cost of fraud:

Just as more and more people are shifting to online payments and preferring them over other traditional forms of payment, so are cybercriminals. ID thefts, phishing attacks and database exploits are becoming more common.

iv) Technological illiteracy:

One of the main disadvantages of online payments is the technological illiteracy among many people, especially the older generation. Since they don't have enough knowledge on how to go about using technology and smartphones, they refrain from using online payment methods.

v) False identity:

Unlike physical transactions, there are no ways to identify if the person making the payment is the one she/he is claiming to be. This can lead to considerable amount of forgery and identify theft.

2. What are the ways to prevent online scams and fradulent use of debit card and credit card?

A: Here are some of the ways to prevent online scams and fraudulent use of debit and credit cards:

i) Get Banking alerts:

In addition to checking your balance and recent transactions online daily, you can sign up for banking alerts. Your bank will then contact you by email or text message when any activity occurs.

ii) Go paperless:

Signing up for paperless bank statements will eliminate the possibility of having bank account information stolen from your mailbox.

iii) Stick to Bank ATM:

Bank ATMs tend to have better security (video camera than ATMs at convenience stores, restaurants, and other places.

iv) Destroy old debit cards:

Having your old cards floating around puts your information at risk.

v) Beware of phishing scams:

When checking your email or doing business online, works sure you know who you're interacting with an identity thief may set up a phishing website that looks like it belongs to your bank or another business you have an account with.

vi) Only transact on website using SSL:

- Look for a padlock symbol by the URL.
- Check for "HTTPS" and not "HTTP". The "s" stands for "secure".

vii) Use your credit card (not debit card):

Credit cards have built-in compliance standards that protect all consumers. The chargeback process and point-of-sale systems.

deter instances of fraud and unauthorised charges.

3. Give the technology solutions for online payment system.

A: Technology solutions play a crucial role in the development and operation of online payment systems, ensuring security reliability and convenience for both consumers and business.

i) Encryption:

Implement strong encryption protocols to secure data transmission between the user's browser and payment savers.

ii) Tokenization:

Tokenization replaces sensitive card data with unique tokens. Often if a database is branched, attackers would only gain access to tokens.

iii) Biometric Authentication:

- Fingerprint recognition
- Facial recognition
- Iris scanning

iv) Mobile Wallets:

Like Apple Pay, Google Pay, Paypal, Amazon Pay -etc.

v) Payment Gateways:

Payment gateways are intermediaries that

process payments between merchants and customers. They typically support a wide range of payment methods, including debit cards, e-wallets, and mobile wallets.

vi) Payment Processors:

Payment processors are responsible for actually transferring funds from customers to merchants. They typically work with payment gateways to provide a seamless payment experience for customers.

vii) Blockchain:

It can be used to create decentralized and secure payment systems. This could make it easier and cheaper to make cross-border payments and could also reduce the risk of fraud.

4. How to secure your smartphone? Give the recommendations to follow:

A: i) Use a strong lockscreen:

It is the first line of defense against unauthorized access to your phone. Use a strong passcode, PIN or pattern or enable biometric authentication such as fingerprint scanning or facial recognition.

ii) Keep your software upto date:

Updates often include security patches and bug fixes that can help protect the phone.

iii) Only install apps from trusted sources:

When installing apps, only download from official app store for your device and avoid third-party apps.

iv) Becareful about what permissions you grant to apps:

Grant only those that are absolutely required.

v) Use a VPN on public Wi-fi networks.

vi) Be careful about what links you click on.

5. Discuss about E-commerce payment system and EBPP:

A:

- E-commerce payment systems and EBPP (electronic bill presentment and payment) are both systems that allow customers to make payments electronically.
- E-commerce payments systems are primarily used to process peyments for goods and sowices purchased online.
- EBPP systems, on the other hand, are primarily used to process payments for bills.

Benefits of E-commerce payment systems & EBPP:

- Convenience
- Security
- Flexibility

6. The Indian government has introduced UPI for payment mode. Explain your way of using UPI in different payment modes.

A: • UPI (Unified Payments Interface) is a real-time payment system developed by the National Payments Coporation of India (NPCI). It is a system that integrates multiple bank accounts.

• Different Modes:

- P2P payments
- Merchant payments
- Bill payments
- Government payments