Assignment

Q1. What is Electronic Wallets ?

Ans: E-wallet is a type of electronic card which is used for transactions made online through a computer or a smartphone. Its utility is same as a credit or debit card. An E-wallet needs to be linked with the individual's bank account to make payments. It is a type of pre-paid account in which a user can store his/her money for any future online transaction. An E-wallet is protected with a password. With the help of an E-wallet, one can make payments for groceries, online purchases, and flight tickets, among others.

For setting up an E-wallet account, the user needs to install the software on his/her device, and enter the relevant information required. After shopping online, the E-wallet automatically fills in the user's information on the payment form. To activate the E-wallet, the user needs to enter his password. Once the online payment is made, the consumer is not required to fill the order form on any other website as the information gets stored in the database and is updated automatically.

Q2. What are threats to E-Wallets and countermeasures?

Ans: There are some threats which are given as:

1. Malware Attacks:

Malware attacks on apps have threatened the safety of user’s money. An attacker can inject a malware to attack the app and collect details from his phone to misuse it.

Counter Measures:

i) Use security software: Applications for detecting and removing threats, including firewalls, virus and malware detection and intrusion-detection systems, mobile security solutions should be installed and activated.

ii) Keep the wallet software up to date: Using the latest version of software allows receiving important stability and security fixes timely. Updates can prevent problems of various severities, include new useful features and help keep the wallet safe. Installing updates for all other software on the computer or mobile is also significant to keep the wallet environment safer.

2. Man-in-the-middle attack and Phishing:

These attacks intercept online transactions by reading payment data from the Internet browser while the user is typing his credit card or bank account details. Phishing attacks are used to steal users' login details and personal data, making e-wallet accounts susceptible to fraud.

Counter Measures:

The URL of the web-page should be verified, by establishing the authenticity of the website by validating its digital certificate. To do so, go to File > Properties > Certificates or double click on the Padlock symbol at the upper right or bottom corner of the browser window. Emails or text messages asking the user to confirm or provide personal information (Debit/Credit/ATM pin, CVV, expiry date, passwords, etc.) should be ignored.

3. Impersonation and SIM swapping:

i) Impersonation occurs when a fraudster steals information and then poses as a genuine user to do a transaction using the stolen e-wallet details and password.

ii) SIM swaps occurs when fraudsters first collect the user's information, and use it to get his / her mobile phone SIM card blocked, and obtain a duplicate one by visiting the mobile operator's retail outlet with fake identity proof. The mobile operator deactivates the genuine SIM card, which was blocked, and issues a new SIM to the fraudster who then generates one-time passwords using stolen information.

Counter Measures:

i) Financial service providers and support staff will never ask their customers for sharing their private information such as passwords or payment account numbers over e-mail requests or phone inquiries etc.

ii) Some Mobile network operators send an SMS to alert their customers of a SIM swap, the affected customer can act and stop this fraud in its tracks by contacting the mobile operator immediately.