**IT Security and Risk Management**

**June 2023 Examination**

**Question 1: Even in this age of Google Pay, Apple Pay and Samsung Pay, where you can use virtual payments to purchase items in real stores and restaurants with your Smartphone, the “old fashioned” credit card and debit card isn’t going away anytime soon. With that said, many people who use them are afraid that the payment information that’s on those cards could be lifted by hackers, even if they remain inside a wallet. That fear includes the newer credit and debit cards that have RFID chips inside. That’s why some folks who use those kinds of cards are buying RFID blocking wallets, which are supposed to keep hackers from taking your payment information. Explain RFID Hacking and ways to avoid it.**

**Ans:**

**Introduction**

Hacking, also known as radio frequency identity (RFID), is a form of robbery involving gaining unauthorized access to data stored on an RFID chip by employing a device that could intercept and decode the chip emitting the indicators. This may be performed using a radio frequency identity (RFID) device. Radiofrequency identification (sometimes known as hacking) is another call for this interest (RFID). The period "radio frequency identity" (RFID) is what the acronym "RFID" refers to. This technology allows hackers to get sensitive personal information, including credit card numbers and expiry dates. This eliminates the

It is only half solved

Buy Complete from our online store

<https://nmimsassignment.com/online-buy-2/>

NMIMS Fully solved assignment available for**session JUNE 2023,**

your**last date is 29th May 2023**.

Lowest price guarantee with quality.

Charges**INR 299 only per assignment.**For more information you can get via mail or Whats app also

Mail id is aapkieducation@gmail.com

Our website [www.aapkieducation.com](http://www.aapkieducation.com/)

After mail, we will reply you instant or maximum

1 hour.

Otherwise you can also contact on our

whatsapp no 8791490301.

Contact no is +91 87-55555-879

**Question 2: Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data. Most security professionals understand how critical access control is to their organization, which access control techniques would you want or expect your bank to employ to keep your bank account safe? Give detailed justifications for your recommendations**

**Ans:**

**Introduction**

In addition, the access management measures installed by my financial institution may be maintained up to date, and the effectiveness of these techniques could be tested frequently. That is something that I anticipate from my financial group. This would fall within the purview of my bank's duty. When protecting their networks, economic institutions want to undertake a proactive posture to stay one step ahead of the adverse actors, continuously developing new techniques for getting into

**Question 3. a :Explain the various types of malware and how is ransomware different from a virus/worm?**

**Ans:**

**Introduction**

Malware is a term used to describe malicious software designed to damage computer systems, and souse borrows facts or benefits from unauthorized access. There are several types of malware, including viruses, worms, and Trojans, ransomware, spyware, and root kits. Its miles essential to protect your computer system. You can do this to shield your laptop

**Question 3. b: What precautions should an employer of an SME take to prevent ransomware attacks on company resources?**

**Ans:**

**Introduction**

There are a variety of preventive moves that you, as a company of a small or medium-sized organization (SME), might also select to take to protect your organization's assets against ransomware assaults. This can assure that your company is prepared to respond to an attack