**IT Security and Risk Management**

# **June 2022 Examination**

##

## **Q1. Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for “malicious software.” Explain the various types of malware and how is ransomware different from a virus/worm? (10 Marks)**

## **Ans 1.**

## **Introduction**

Viruses and other forms of harmful software can be covered under the umbrella term "malware." Cybercriminals commonly utilize it to gain facts from their victims that they'll then exploit to make money. From financial records to healthcare statistics to personal emails and passwords, the breadth of data that can be hacked has grown exponentially. The phrase "malicious software program" or "malicious software" is an umbrella period for any malicious program or code damaging to a computer. Assailants and spies are malware targets to penetrate, harm, or ruin

Its Half solved only

Buy Complete from our online store

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

NMIMS Fully solved assignment available for**session June 2022,**

your**last date is 29th May 2022**.



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

**Q2. The estimated losses due to elder financial abuse range widely. The FBI’s Internet Crime Complaint Center (IC3) 2018 Internet Crime Report shows that people 60 and older submitted more than 62,000 fraud complaints in 2018 with losses totaling nearly $650 million. Some less conservative sources estimate that fraud against seniors, or what’s known as elder financial exploitation (EFE), costs families in the U.S. upwards of $36 billion per year. Research shows that as seniors age, they’re more likely to sustain higher average losses to senior financial scams.**

**Explain the most common types of attacks targeting senior citizens and suggest precautionary measures for them with reference to these attacks? (10 Marks)**

**Ans 2.**

## **Introduction**

The trouble of cyber fraudsters preying on the elderly affects many countries. The elderly may be more liable to -bit scams than different age businesses. This makes them easy prey for criminals, who prey on the elderly, widows, and lonely grandparents. Different concerns come into play. Many older people have been overdue adopters of technology, so they will have lousy behavior, which includes a reluctance to use complicated passwords or find out about new safety threats. As a whole, millennials are greater pleasant to strangers, which scammers benefit all the time.

agency offers a listing of resources to assist older adults in studying net safety.

**Q3. For a payment processing site , such as PayPal, security is of utmost important. In PayPal, more than 12 million payment transactions are processed on a daily basis, and this number rises to 15M million during peak days. Nowadays, PayPal has implemented a new and advanced approach to catching bugs and vulnerabilities in its website. This security feature was an add-on to a committed team of more than 2000 anti-fraud specialists who are responsible for taking care of the perimeter security. Each customer accountand payment transactions were monitored by the organisation 24/7 so that there is no fraudulent activity, email phishing and loss of identity.**

**Moreover, the security was also ensured by maintaining every communication between servers on SSL. However, in the case of any flaw in any of these security features, an alarm should be raised.**

**Now, PayPal has contacted and assigned members who can work on bonus basis for the website security. These security researchers who are paid for identifying the bugs and possible vulnerabilities in PayPal’s website are known as bounty hunters. “There are a lot of security researchers, there are a lot of other people out there who are experts on security. We have a very successful bug bounty program, where researchers will find a vulnerability on our sites that we’ve missed,” explains Shivananda.**

**Every bug spotter looks for his/her benefit in identifying bugs. Therefore, PayPal rewards these bounty hunters with the designation of a hero and their achievements portrayed on the ‘Wall of Fame’. In monetary terms, a huge amount is paid to them.**

**PayPal pays $10,000 (about `6.5 Lakh) to identify a remote code of execution. In this case, the spotter of an authentication bypass vulnerability will get $3000 and the one working on cross-site scripting error would get $750.**

**Many companies such as Facebook and eBay have involved the community for high- level security. Let’s understand the manner in which the bug bounty program introduced by PayPal works. First, a security researcher enters and submits a security bug on the PayPal portal. On its completion, the security professionals I working at PayPal test that vulnerability and checks whether or not it is a real issue. They also understand the fixes and communicates to the researcher saying “Yes, what you’ve submitted is a genuine issue. Thank you for that. We’re processing it, and as we process it, we’ll come back to you,” said Shivananda. After the bug is successfully closed, security researchers are entitled to compensation from PayPal.**

**The following vulnerabilities are out-of-scope for PayPal:**

**• Vulnerabilities based on social engineering techniques**

**• Vulnerabilities based on brute force**

**The main objective of a payment processing company is to serve customers innovatively in 200 markets taking care of the fact that the losses are a third of one percent. Along with this, a huge amount of creativity has to be brought in designing the fraud eco-system.**

## **PayPal invests a lot of resources in analysing the transactions, account details, and ensuring that no fraudulent transaction is completed on their website. In fact, it’s surprising that PayPal has the least loss in the payment industry that is one-third of one percent. The combination of machine learning and data sciences on the massive data sets helped PayPal to attain the position where it can assure the customers regarding the safety of their transactions.**

## **“A loss rate of one-third of one percent is something we can brag about in the industry,”**

## **beams Shivananda**

## **a. Why PayPal thought of hiring bounty hunters? (5 Marks)**

## **Ans 3a.**

## **Introduction**

Moral hackers who uncover vulnerabilities in PayPal's software program and services were rewarded handsomely in the latest media reviews. As of March 2018, PayPal's most worm bounty payout has been raised to $30,000, a significant reward for hackers. Due to the shift to HackerOne, PayPal's worm bounty program has become less noticeable, with ambiguous replies

**b. What type of issues can be faced by PayPal if there is some sort of security lapse in the customer payment transactions? (5 Marks)**

**Ans 3b.**

**Introduction**

PayPal payments private limited ("PayPal"), an Indian corporation, and you've entered into this agreement to govern your use of your PayPal account and the PayPal offerings. A character has to be a minimum of 18 years of age and a resident of India to establish a PayPal account and