| | | | |
|---|---|---|---|
| | **RV College of Engineering®**<br>**Department of Computer Science and Engineering**<br>**CIE - III** | | |
| **Course & Code** | **INTRODUCTION TO CYBER SECURITY (22EM106)** | | **Semester: I** |
| **Date : FEB 2023** | **Duration:**120 minutes | **Max.Marks**:(10+50)=60 Marks | **Staff :** MH |
| | | | **Section : Physics cycle** |

## Scheme and Solution

| Sl.no | PART - A | Marks |
|---|---|---|
| 1 | Man-in-the-Middle Attack | 1 |
| 2 | Social Engineering | 1 |
| 3 | Nessus | 1 |
| 4 | Ping | 1 |
| 5 | Ransomware | 1 |
| 6 | Authorization | 1 |
| 7 | Firewalls | 1 |
| 8 | Pharming | 1 |
| 9 | Zombie<br>“Zombie” is the term used when an attacker takes control of your computer without your knowledge. A zombie attack aimed either to steal your sensitive information or to make your computer do things that it normally shouldn't. | 1 |
| 10 | Spoofing:<br>Spoofing happens when cybercriminals use deception to appear as another person or source of information. | 1 |

| Sl.no. | PART - B | Marks |
|---|---|---|
| 1.a | E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction.<br>Ecommerce security refers to the measures taken to protect your business and your customers against cyber threats.<br>**Types of E-Commerce Models**<br>Electronic commerce can be classified into four main categories. The basis for this simple classification is the parties that are involved in the transactions. So the four basic electronic commerce models are as follows,<br>**1. Business to Business**<br>This is Business to Business transactions. Here the companies are doing business with each other. The final consumer is not involved. So the online transactions only involve the manufacturers, wholesalers, retailers etc.<br>**2. Business to Consumer**<br>Business to Consumer. Here the company will sell their goods and/or services directly to the consumer. The consumer can browse their websites and look at products, pictures, read reviews. Then they place their order and the company ships the goods directly to them. Popular examples are Amazon, Flipkart, Jabong etc.<br>**3. Consumer to Consumer**<br>Consumer to consumer, where the consumers are in direct contact with each other. No company is involved. It helps people sell their personal goods and assets directly to an interested party. Usually, goods traded are cars, bikes, electronics etc. OLX, Quikr etc follow this model.<br>**4. Consumer to Business**<br>This is the reverse of B2C, it is a consumer to business. So the consumer provides a good or some service to the company. Say for example an IT freelancer who demos and sells his software to a company. This would be a C2B transaction.<br>What is m-Commerce?<br>**Examples of E-Commerce**<br>• Amazon<br>• Flipkart<br>• eBay<br>• Fiverr<br>• Upwork<br>• Olx<br>• Quikr<br><br>*E-commerce Security and different types – 3 marks*<br>*Threats and issues in E-Commerce- 3 marks* | 06 |

| | | |
|---|---|---|
| 1.b | There is no cardinal difference between these payment methods (bank accounts and digital wallets) except for some points.<br>• When we make a payment on the Internet, for example, when we buy something in an online store, we enter our card details. It is not safe. The site may turn out to be fake, and then scammers can easily steal all the money from a bank account or even from deposits and piggy banks. It is much safer to keep a small amount in an electronic wallet to make mobile payments. In this case, even if the scammers steal money from it, they will not be able to get the rest of your funds.<br>• Easier to open. To do this, you do not need to interact with the bank and pay money. Get an e-wallet for free on the Internet and start using it right away.<br>• The e-wallet is convenient to use. Card data is not only dangerous to enter, but also long enough. And to take off some money from an electronic wallet, you only need a password and a mobile phone.<br>• Transactions through the e-wallet are instantaneous, regardless of the time of day, working days or holidays.<br>• Mobile wallets are not tied to a specific country and allow you to make payments and transfers regardless of location. For example, if you and the recipient are in different countries.<br>• An electronic wallet does not always mean an exclusively virtual look. Some operators issue cards for offline payment. In an ordinary store, in a market or in a cafe, you can pay with money from an electronic wallet and not endanger the funds in your bank account. | 04 |
| 2.a | • A hashtag is a word or keyword phrase preceded by a hash symbol (#).<br>• It's used within a post on social media to help those who may be interested in your topic to be able to find it when they search for a keyword or hashtag.<br>• It helps to draw attention to your posts and encourage interaction.<br><br>When it comes to promoting your brand on social media, hashtags are a great way to drive views, likes, and shares. Previously known as the pound sign (#), the hashtag is a way to make your content discoverable to a captive audience.<br><br>Hashtags were first widely used on Twitter, but they have become commonplace on other social media platforms including Facebook, Instagram, LinkedIn, Pinterest, and TikTok. Mastering the hashtag gives you a powerful way to engage your audience and increase your social impact at no cost other than the time it takes to do some research and pay attention to trends.<br><br>***Hashtags in social media – 2 marks***<br><br>***usage of hashtags effectively on social media – 4marks*** | 06 |
| 2.b | role and importance of cybersecurity in social media – 04 marks | 04 |
| 3.a | **The Pitfalls of Social Networking** | 06 |

- Bandwidth and storage consumption
- Potential legal liability
- Exposure to malware
- Decreased employee productivity.
- Disclosure of personal information
- Risk of leaking corporate secrets
- Limited executive use

The use of social networking is rising dramatically, and its scope has expanded far beyond the personal realm. Politically oriented videos and blogs are being posted to YouTube in an effort to influence primary elections.

Corporate and government entities are increasingly using social networking to facilitate communication and collaboration among individuals and groups, both internally and externally. While there are clear benefits to increasing communication, social networks also present a number of challenges, including the following:

**Bandwidth and storage consumption.** Many social network members post pictures, music, videos, high-definition movies and other large files. Downloading and storing these files can cripple your infrastructure and make capacity planning virtually impossible.

**Potential legal liability.** Students at Canterbury's University of Kent created a Facebook group named "For Those Who Hate the Little Fat Library Man," to harass a librarian they disliked. In the U.S., if employees were to use corporate IT resources for similar purposes, the company could be held responsible in any ensuing litigation.

**Exposure to malware.** Social networks are designed to be open, with few restrictions on content or links. In most cases, security was not a primary design criterion. Thus, these networks are potential vehicles for introducing viruses, worms and spyware.

**Decreased employee productivity.** Social networking for personal purposes can affect corporate productivity. A Goldman Sachs trader in the U.K. was spending four work hours a day on Facebook. When he was told to stop, he posted the warning e-mail and wrote, "It's a measure of how warped I've become that, not only am I surprisingly proud of this, but losing my job worries me far less than losing Facebook."

Even when networking is used for business purposes, corporations may want to limit the number of networks employees use. Monitoring many networks can become incredibly time-consuming. Moreover, interfaces among current networks don't support robust information-sharing. Unfortunately, unless all interested parties use the same network, many benefits are lost. Consider designating specific networks for companywide communications.

**Disclosure of personal information.** Companies regularly search MySpace, Classmates.com, LinkedIn and other social networking sites to glean information about

| | | |
|---|---|---|
| | potential hires and competitors, but postings should always be taken with a grain of salt.<br><br>**Risk of leaking corporate secrets.** Companies often sanction social networking for the purpose of exchanging professional information. But take great care to protect corporate secrets. Definitions of secret may vary or be misunderstood, and critical information may inadvertently be revealed. Provide clear guidelines across the company, as well as to your suppliers and outsourcers.<br><br>**Limited executive use.** Many articles on social networking claim that it will facilitate sales. Executive use of social networking is not widespread, however. Many executives already have substantial personal networks and rely less on new technological platforms for interaction. (This will undoubtedly change in the future, but networks have limited selling power today.)<br><br>While social networking does offer many benefits, there are corporate costs and pitfalls to be considered. Organizations need to establish policies to address issues such as personal usage, business relevance, site restrictions and information confidentiality. Take time to thoroughly investigate and address these issues to maximize the effectiveness of social networking. | |
| 3.b | **Advantages:**<br><br>• With UPI, user's bank account can be used as a wallet with a simplified two-factor authentication which eliminates the need to store funds in any other wallet.<br>• Use of Virtual ID makes it more secure since there is no need to share credentials.<br>• UPI transaction can be made via IMPS in real time, which makes it available 24*7.<br>• Users can link multiple bank accounts to a single Smartphone. Hence sending or receiving money across banks is easier.<br>• For merchants, it is Suitable for electronic Commerce and a mobile Commerce transaction as well as it resolves the Cash on Delivery collection problem.<br>• Banks can create their own application interfaces as UPI provides flexibility and an open architecture.<br><br>**Security Measures:**<br><br>• Beware of Mobile phishing: always download legitimate UPI applications from bank's official website, and be cautious before you download it from App store.<br>• Keep strong passwords for your phone as well as for your UPI application.<br>• Do not share MPIN with anybody (not even with bank), and be suspicious of unknown callers claiming to be from your bank.<br>• Use biometric authentication if possible. | 04 |

| | | |
|---|---|---|
| | • Update your mobile OS and applications as often as possible to be secure from vulnerabilities.<br>• It is advisable for users to enable encryption, remote wipe abilities and anti-virus software on the phone.<br>• Keep your SIM card locked with a Pin to avoid misuse, in case of loss or theft of the mobile device, You can contact your subscriber to block the subscription of the SIM card.<br>• Avoid connecting phones to unsecured wireless networks that do not need passwords to access. | |
| 4 | Digital payment fraud is any form of the fake or fraudulent transaction completed by a hacker or cyber-criminal. With the advancement of technology, Cyber Crime is also increasing. Through the internet, the attacker robs the person of funds, private merchandise, interest, or confidential details. These activities can be classified as unauthorized transactions, loss of merchandise, false refunds, etc.<br>Internet fraud in e-commerce is popular ever since e-commerce sites were introduced. Since companies figured out a way that consumers could securely purchase goods from them without actually visiting the physical store, criminals also have done their best to access and profit from that data available on the internet.<br>How does it happen?<br>Scammers have become skilled in illegally collecting data online. Hackers often pretend as legitimate people and contact the card owners asking for sensitive details and information. They then use several ways, as mentioned below, to interact and steal crucial data.<br>• Email<br>• Messages<br>• Illegal websites<br>• Phone calls<br>• Sending malicious software to smartphones<br>Cybercriminals often operate in teams to breach data security systems. They check for bugs or fixes that have not been updated in quite some time. Such loopholes make it easy for hackers to gain access around the firewall and acquire confidential information.<br>Types of digital payment fraud<br>Identity theft – This is not a new thing, since it also happens outside cyberspace. Typically, this type of fraud entails a cybercriminal stealing your personal information by spoofing your system. In order to perform illegal online payment transactions, the hacker then uses your data. Since the cybercriminal has all the essential details, they can bypass restrictions and firewalls on fraud detection.<br>The merchant on the e-commerce website might not realize that it is the hacker who is doing the transaction instead of the real user, as all the details are being provided.<br>Phishing – You would have come across numerous email subscriptions and websites that persuade you to opt for updates and notifications. In most cases, these sources would ask you to provide certain personal information, including your credit card details. If the email is not from a reliable source, your data will be compromised and used to carry out fraud e-commerce transactions. This is known as a phishing attack. | 10 |

Merchant Identity Fraud – This involves a fraudster that builds a platform quite similar to that of the merchant account. The attacker then proceeds and imposes fake payments and fees on stolen credit cards. This whole operation is carried out in a quick way before the cardholders realize they are being cheated.

Pagejacking – At times, e-commerce websites are hacked by criminals who direct the customers to an unsecured network. This untrusted site can contain malware that can break webpage security systems and steal the customer's funds.

Securities fraud – Speed, fast access, and anonymous activity, all provide a suitable atmosphere for securities and stock market fraud. This can happen in several ways.

The most common of all involves providing misleading or fake information on a specific stock to shoot up its price. Investors treat this information as genuine and start buying the stock, resulting in a price increase. By the time they realize that the information is fake, the stock price falls, and the investors lose their money.

Another way is to offer stock that simply does not exist. Online investors, surfing the internet for information, invest in such stocks without realizing they are being the victim of a scam and eventually end up losing their money.

Stock market fraud–With the advancement in technology and everything at our fingertips, there has been a rise in stock market scams too. Unknowingly, the investors are exposed to the immense risk of a criminal who uses their personal data and investment for illegal trades, leaving investors at a loss.

Before the investor realizes that he/she has lost the money to a scam, the criminal would have shut this activity and moved to another fraud.

There is an increase in the number of victims of stock market scams in Dubai. The scammer deceives the victim by fraudulent means to persuade the investor to surrender their capital or property.

Foreign exchange fraud – This is a trading technique used to deceive investors by misleading them that by investing in the forex market, they can expect to make a high profit. Currency trading scams also lure customers through radio advertising, newspaper ads, or appealing internet pages.

There have been cases of forex trading frauds in Dubai, involving hundreds of victims. The scams involved transfers of foreign money meant to escape bank transaction charges and investments in different small businesses.

As part of forex investment scams in the UAE, multiple investors were persuaded into forex trading with a promise of making a high profit. The brokers refused to pay the investors at some point, customers then moved to the court in order to recover their capital.

Preventive measures

E-commerce firms have already begun to raise awareness regarding internet corrupt practices. Even though it is difficult to eradicate cybercriminals entirely, you can take certain measures to prevent internet fraud.

- Use a certified payment processor
- Be updated with recent trends in digital payment fraud
- Use tested antivirus software that runs regular checks
- Encrypt the transactions and emails containing confidential information
- Regularly change your login and passwords
- Regularly update network security systems

Depending on the severity of the case, you can also seek legal opinion for guidance and expert advice.

| | | |
|---|---|---|
| | ***Payment fraud-2 marks***<br>***How can it be prevented 3 marks***<br>***Explain different types of digital payments-5 marks*** | |
| 5 | **Social media addiction** is becoming common. People can begin to feel a sense of anxiety if they don't check their social media accounts, or they may compulsively refresh them. Social networking posts are also highly curated, people only post the good things that happen to them. This can cause a warped view of reality where the viewer thinks that others have better lives than they do. This leads to a fear of missing out (FOMO) on social events.<br><br>**Cyberbullying** is when someone makes social media posts with the intention to harm someone else. This can take the form of publicly posting the private information of someone or sending abusive messages. Tragically, cyberbullying has led to the suicide of some individuals. It is now a major concern in public schools. Doxing is when someone publicly posts the personally identifiable information, such as an address or phone number, of someone else.<br><br>SOCIAL MEDIA & DATA BREACHES<br><br>The massive stores of personal data that social media platforms collect and retain are vulnerable to hacking, scraping, and data breaches, particularly if platforms fail to institute critical security measures and access restrictions. Depending on the network, the data at risk can include location information, health information, religious identity, sexual orientation, facial recognition imagery, private messages, personal photos, and more. The consequences of exposing this information can be severe: from stalking to the forcible outing of LGBTQ individuals to the disclosure of one's religious practices and movements.<br>Without federal comprehensive privacy legislation, users often have little protection against data breaches. Although social media companies typically publish privacy policies, these policies are wholly inadequate to protect users' sensitive information. Privacy policies are disclaimers published by platforms and websites that purport to operate as waivers once users "consent" to them. But these policies are often vague, hard to interpret, full of loopholes, subject to unilateral changes by the platforms, and difficult or impossible for injured users to enforce.<br><br>*Social media addiction-3 marks*<br>*Cyberbullying-3 marks*<br>*Social media data breaches-4 marks* | 10 |