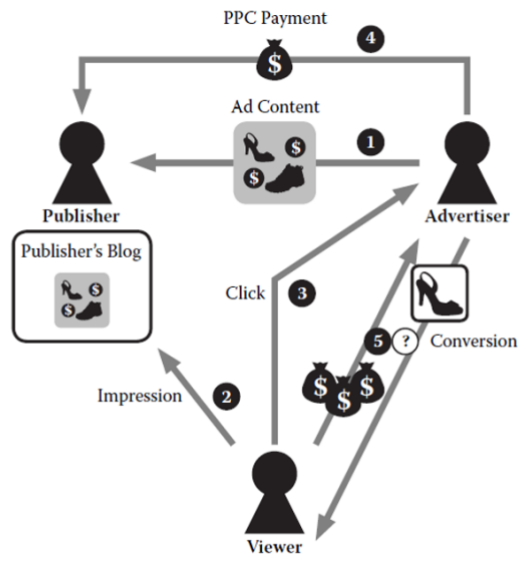
	RV College of Engineering® Department of Computer Science and Engineering		
Course & Code	INTRODUCTION TO CYBER SECURITY (CS114BT)		Semester: I
Date : Dec 2023	Duration: 90 minutes	Max Marks: 50 Marks	Staff :MH/ARA/TP
USN :	Name :		

CIE 2 Scheme and Solution

Sl.no.	Questions
1.a	<p>Passive attack involves gathering information about the target without his/her (individual or Company) knowledge. Few ways of doing are</p> <ul style="list-style-type: none"> • Googling • Surfing online community groups • Looking into organization website • Blogs, news papers and press releases • From job sites finding requirements for job profiles. <p><i>passive attack - 2 marks Any 4 tools with brief explanation – 4 marks</i></p>
1.b	<ol style="list-style-type: none"> 1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks. 2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities. 3. Launching an attack (gaining and maintaining the system access). <p><i>Listing of all three phases – 1 mark, Brief explanation to each phase – 3 marks</i></p>
2.a	<p>Shoulder surfing: Shoulder surfing is a social engineering technique that is conducted by observing what someone is doing by looking over their shoulders. As a shoulder surfer (with malicious intent), it's relatively easy to watch someone fill out a form, use an ATM or pay using a credit card when they are in a crowded place since it's fairly easy to stand next to them. Shoulder surfing can also happen electronically, as attackers try to steal sensitive information from mobile devices. To prevent shoulder surfing, it is best practice to use a privacy screen protector on your electronic device and to be aware of your surroundings when inputting sensitive information.</p> <p>Dumpster driving: A dumpster diving attack is a cyber attack that entails threat actors to search through a victim's trash. Dumpster drivers can get the phone numbers of your family members, friends, customers, and business associates from your trash. They can also gain access to codes and passwords written on notepads.</p> <p><i>03 marks each</i></p>

2.b	<p>Precautions:</p> <ul style="list-style-type: none"> • Do not do online transactions. • Never save password. • Avoid shoulder surfing. • Never leave your System • Use Virtual Keyboard • Clear logs <p><i>4 Marks</i></p>
3.a	<p>Fraudsters abuse ad networks by generating invalid traffic for profit, competitive advantage, or even retribution. - 1 Marks</p> <p>This direct relationship between the number of clicks and the amount of money earned by the publisher has resulted in a form of fraud best known as click fraud.</p> <p>Click fraud occurs when an ad network charges an advertiser for a click when there was no opportunity for a legitimate conversion. - 1 Marks</p> <p>Different ways of doing</p> <ol style="list-style-type: none"> 1) publisher can click his or her own ad, he or she could just as easily ask friends to click the ads. 2) An advertiser's competitor might also be inclined to commit click fraud. 3) Nonfinancial motivations might also cause a person to commit click fraud. If a person disagrees with how any company treats its workers, they might click that company to cost the company additional money. - 2 Marks <p>How to mitigate</p> <p>Behavior patterns after the fraudster clicks an ad are another way in which ad networks and advertisers can detect potential click fraud. In the PPC industry, an ad click that does not result in any additional clicks on the website is a bounce, and the percentage of visitors who exhibit that behavior is the bounce rate. While a poor-quality website might have a high bounce rate because visitors do not find it interesting, if clicks from a particular publisher have a much higher bounce rate than others, it may indicate click fraud. - 2 Marks</p>
3.b	<p>Proxies' definition with brief explanation – <i>2 marks</i></p> <p>How and why attackers use proxies – <i>2 marks</i></p>
4.a	<p>Social Network: This is a type of social network where people stay in touch with friends, family members, acquaintances or brands through online profiles and updates, or find new friends through similar interests. Some examples are Facebook, Myspace and Instagram.</p> <p>Advantages:</p> <ul style="list-style-type: none"> • Global Connections Are Made Possible Through Social Networking. ... • Quick and Simple Communication Methods. ... • Social Networking Helps Businesses Advertise Their Brands. ... • Reduces the Price Of Marketing. ... • An Excellent Educational Tool. ... • Shares Large Amount of Information Daily

4.b	<p>Pay-per-Click (PPC) fraud, also known as click fraud, is a type of online fraud that specifically targets pay-per-click advertising models. In PPC advertising, advertisers pay a fee each time their ad is clicked. Click fraud occurs when clicks on these ads are generated fraudulently, either by automated scripts, bots, or individuals with the intention of depleting the advertiser's budget, sabotaging competitors, or creating false metrics.</p>  <p style="text-align: center;">Exhibit 2-11 Pay-per-click business model.</p> <p><i>Block diagram - 2 marks explanation - 2 marks</i></p>
5.a	<p>Explanation of credit card fraud in detail – 3 marks</p> <p>Explanation of the risks involved in it – 3 marks</p>
5.b	<div style="border: 1px solid black; padding: 10px;"> <p>Yes 2 mark</p> <p>Oversharing Creates Risks for Curated Phishing</p> <p>Everyone knows someone within their social media circle who overshares – that virtual social butterfly with way too many “friends” who offer a running commentary on everything they are doing, everywhere they are going, every personal problem they’re having. that this kind of oversharing can open a person up to the risk of spear phishing</p> <p>Bad Actors Can Aggregate Data Across Forums</p> <p>Every bit of information you put on your social media accounts is a potential data point, but it’s not only about the content you share. Bad actors can gather information from the memes and quizzes you fill out. It’s a seemingly harmless diversion to respond to memes like “Your secret agent name is your mother’s maiden name plus your favorite color.” It’s been shown that some of these quizzes are created by malicious actors to gain access to your online accounts</p> <p>Disinformation on Social Media Leads to Business Risk</p> <p>Attackers are taking advantage of disinformation and misinformation. For instance, malicious actors could take advantage of a recent data breach by sending an email like, “Your account has been compromised” or “You’re locked out of your account. Click here to change your password.”</p> <p>These attackers are taking advantage of the individual’s decision cycle to get access to corporate computer systems, sensitive information, bank accounts and more</p> </div> <p><i>Explanation – 2 marks</i></p>

