

MODEL LESSON PLAN

NAME: SANDEEP KUMAR (213326)	SUBJECT: COMPUTER SCIENCE
DESIGNATION: PGT COMPUTER SCIENCE	TOPIC: CYBER CRIME & SAFETY
SCHOOL: GSSS DAMLA (178) YNR	CLASS: 11 th
CONTACT: +91 9991606900	DATE: 30.03.2023 Duration: 50 minutes.

1. Instructional Objectives:
(निर्देशात्मक उद्देश्य)

After completion of the topic, Students will be able to:

(टॉपिक पूरा होने के बाद, छात्र सक्षम होंगे):

1.1. Remembering (स्मरण):

- Recall basic facts and concepts related to cyber crime & safety. साइबर अपराध और सुरक्षा से संबंधित बुनियादी तथ्यों और अवधारणाओं को याद करें।
- Highlight different threats in cyber world. साइबर दुनिया में विभिन्न खतरों पर प्रकाश डालें।
- Bookmark the secure websites. सुरक्षित वेबसाइटों को बुकमार्क करें।
- Tabulate the various ways/types of cyber crime. साइबर अपराध के विभिन्न तरीकों/प्रकारों को सारणीबद्ध करें।
- Identify the steps that could lead to criminal activity online. उन कदमों की पहचान करें जो ऑनलाइन आपराधिक गतिविधियों को बढ़ावा दे सकते हैं।

1.2. Understanding (समझना):

- Predict various hazards to data protection in cyber world. साइबर दुनिया में डेटा सुरक्षा के लिए विभिन्न खतरों की भविष्यवाणी करें।
- Compare fraud and secure E- Mails/ websites. फ्रॉड और सुरक्षित ई-मेल/वेबसाइटों की तुलना करें।
- Interpret the concept of hacking and cracking. हैकिंग और क्रैकिंग की अवधारणा की व्याख्या करें।
- Exemplifying that cyber crime is not a victimless crime

उदाहरण देना कि साइबर अपराध पीड़ित रहित अपराध नहीं है

1.3. Applying(लागू करना):

- Determine the secure Antivirus/ software for our digital devices. हमारे डिजिटल उपकरणों के लिए सुरक्षित एंटीवायरस/सॉफ्टवेयर का निर्धारण करें।
- Articulate the Do's & Don'ts in respect of cyber safety. साइबर सुरक्षा के संदर्भ में क्या करें और क्या न करें स्पष्ट करें।
- Surfing the internet wisely with safety measures. सुरक्षा उपायों के साथ बुद्धिमानी से इंटरनेट पर सर्फिंग करें।
- Make a chart displaying the cyber safety Helpline no/ Emails/ websites. साइबर सुरक्षा हेल्पलाइन नंबर/ईमेल/वेबसाइट प्रदर्शित करते हुए एक चार्ट बनाएं।

1.4. Analyzing(विश्लेषण):

- Categorize the different forms of cyber attacks. साइबर हमलों के विभिन्न रूपों को वर्गीकृत करें।
- Correlate the various cyber threats by googling the cyber crime cases. साइबर अपराध मामलों को गूगल करके विभिन्न साइबर खतरों को सहसंबद्ध करें।
- Mind mapping the future opportunities with cyber skills. साइबर कौशल के साथ भविष्य के अवसरों का मानचित्रण करना।

1.5. Evaluating(मूल्यांकन):

- Detect the Ransomware, Phishing attack, identity theft. रैंसमवेयर, फिशिंग हमले, पहचान की चोरी का पता लगाएं।
- Posting the curated data on social media platforms. सोशल मीडिया प्लेटफॉर्म पर केवल क्यूरेटेड डेटा पोस्ट करना।
- Hypothesizing the intensity of cyber attack in financial aspect. वित्तीय पहलू में साइबर हमले की तीव्रता की परिकल्पना करना।

	<p>1.6. Creating (रचना):</p> <ul style="list-style-type: none"> Blogging / Podcasting on cyber crime & safety tips. साइबर अपराध और सुरक्षा युक्तियों पर ब्लॉगिंग/पॉडकास्टिंग। Building and update wiki pages for combating & preventing cyber crime. साइबर अपराध का मुकाबला करने और उसे रोकने के लिए विकी पृष्ठ बनाएँ और अपडेट करना । Facilitate the family as well as society to be safe from trending frauds. ट्रेडिंग फ्रॉड से परिवार के साथसाथ समाज को भी सुरक्षित करना। Programming to become a white hat hacker. व्हाइट हैट हैकर बनने के लिए प्रोग्रामिंग।
<p>2. Resources/ Teaching Aids संसाधन/शिक्षण सहायक सामग्री</p>	<p>Digital Board / Green Board, Related PPT, Key words display cards, Chalk, and Duster.</p> <p>डिजिटल बोर्ड/ग्रीन बोर्ड, संबंधित पीपीटी, की-वर्ड्स डिस्प्ले कार्ड, चॉक और डस्टर।</p>
<p>3. Key Competencies: प्रमुख दक्षताएँ</p>	<p>Digital literacy, social awareness, Think critically and responsible decision-making.</p> <p>डिजिटल साक्षरता, सामाजिक जागरूकता, आलोचनात्मक और जिम्मेदार निर्णय लेने पर विचार करें।</p>
<p>4. Teaching Methodology: शिक्षण पद्धति</p>	<p>Blended learning method involving Explanation, Demonstration visuals support, experiential learning, Encourage students and Interaction along with power-point presentation on digital smart board.</p> <p>मिश्रित शिक्षण पद्धति जिसमें स्पष्टीकरण, प्रदर्शन दृश्य समर्थन, अनुभवात्मक शिक्षा, छात्रों को प्रोत्साहित करना और डिजिटल स्मार्ट बोर्ड पर पावर-पॉइंट प्रस्तुति के साथ सहभागिता शामिल है।</p>
<p>5. Key Words महत्वपूर्ण शब्द</p>	<p>Hacking, Phishing, Identity theft, Ransomware हैकिंग, फिशिंग, आइडेंटिटी थेफ्ट, रैनसमवेयर।</p>
<p>6. Definition परिभाषा</p>	<p>Cyber crime is committed when digital devices are used illegally against other people and systems.</p> <p>साइबर अपराध तब होता है जब डिजिटल उपकरणों का अवैध रूप से अन्य लोगों और प्रणालियों के विरुद्ध उपयोग किया जाता है।</p>

7. Previous Knowledge Test (पूर्व ज्ञान परीक्षण):

Teachers Activity शिक्षक गतिविधि	Student's Responses छात्र की प्रतिक्रियाएँ																
How many students use digital devices? कितने छात्र डिजिटल उपकरणों का उपयोग करते हैं?	All students raise their hands. सभी छात्र हाथ उठाते हैं।																
How do you use internet in daily life? आप दैनिक जीवन में इंटरनेट का उपयोग कैसे करते हैं?	<table border="1"> <tr> <td>1. For communication</td> <td>1. संवाद के लिए</td> </tr> <tr> <td>2. For social media like facebook, whatsapp, twitter</td> <td>2. सोशल मीडिया जैसे फेसबुक, व्हाट्सएप, ट्विटर के लिए</td> </tr> <tr> <td>3. To play online games</td> <td>3. ऑनलाइन गेम खेलने के लिए</td> </tr> <tr> <td>4. We use email facility</td> <td>4. हम ईमेल सुविधा का उपयोग करते हैं</td> </tr> <tr> <td>5. For video calls</td> <td>5. वीडियो कॉल्स के लिए</td> </tr> <tr> <td>6. For online recharge</td> <td>6. ऑनलाइन रिचार्ज के लिए</td> </tr> <tr> <td>7. To download files</td> <td>7. फाइलें डाउनलोड करने के लिए</td> </tr> <tr> <td>8. For online classes</td> <td>8. ऑनलाइन कक्षाओं के लिए</td> </tr> </table>	1. For communication	1. संवाद के लिए	2. For social media like facebook, whatsapp, twitter	2. सोशल मीडिया जैसे फेसबुक, व्हाट्सएप, ट्विटर के लिए	3. To play online games	3. ऑनलाइन गेम खेलने के लिए	4. We use email facility	4. हम ईमेल सुविधा का उपयोग करते हैं	5. For video calls	5. वीडियो कॉल्स के लिए	6. For online recharge	6. ऑनलाइन रिचार्ज के लिए	7. To download files	7. फाइलें डाउनलोड करने के लिए	8. For online classes	8. ऑनलाइन कक्षाओं के लिए
1. For communication	1. संवाद के लिए																
2. For social media like facebook, whatsapp, twitter	2. सोशल मीडिया जैसे फेसबुक, व्हाट्सएप, ट्विटर के लिए																
3. To play online games	3. ऑनलाइन गेम खेलने के लिए																
4. We use email facility	4. हम ईमेल सुविधा का उपयोग करते हैं																
5. For video calls	5. वीडियो कॉल्स के लिए																
6. For online recharge	6. ऑनलाइन रिचार्ज के लिए																
7. To download files	7. फाइलें डाउनलोड करने के लिए																
8. For online classes	8. ऑनलाइन कक्षाओं के लिए																
Is it OK to share your password with close friends? क्या अपना पासवर्ड करीबी दोस्तों के साथ साझा करना ठीक है?	A big no from all students. सभी छात्रों की ओर से एक बड़ी नहीं।																
Is it good to guess someone else's password? क्या किसी और के पासवर्ड का अनुमान लगाना अच्छा है?	Some students say yes some says No. कुछ विद्यार्थी हाँ कहते हैं कुछ ना कहते हैं।																
Is it funny to post a status on friend's social media account without their permission? क्या किसी दोस्त की अनुमति के बिना उसके सोशल मीडिया अकाउंट पर स्टेटस पोस्ट करना मज़ेदार है?	Many students found it funny कई छात्रों को यह मजाकिया लगा																
What is crime? अपराध क्या है?	Crime is any illegal activity अपराध कोई भी गैरकानूनी गतिविधि है																
And what about cyber crime? और साइबर अपराध के बारे में क्या?	No response. कोई प्रतिक्रिया नहीं।																

8. Announcement of the Topic(विषय की घोषणा):

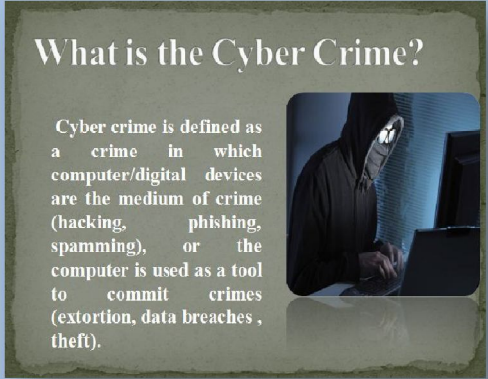

Finding that the students are unable to answer the last question the teacher will now announce the topic.

यह देखते हुए कि विद्यार्थी अंतिम प्रश्न का उत्तर देने में असमर्थ हैं, शिक्षक अब विषय की घोषणा करेंगे।


“CYBER CRIME & SAFETY”



"साइबर अपराध और सुरक्षा"


9. Content Elaboration (विषयवस्तु विस्तार):


Topic विषय	Teachers Activity शिक्षकों की गतिविधि	Student’s Activity छात्र की गतिविधि	Digital Smart Board Content डिजिटल स्मार्ट बोर्ड सामग्री
<p>9.1 Cyber Crime</p> <p>साइबर अपराध</p>	<p>Cyber crime is defined as a crime in which computer/digital devices are the medium of crime (hacking, phishing, spamming), or the computer is used as a tool to commit crimes (extortion, data breaches, theft).</p> <p>साइबर अपराध को ऐसे अपराध के रूप में परिभाषित किया जाता है जिसमें कंप्यूटर/डिजिटल उपकरण अपराध (हैकिंग, फिशिंग, स्पैमिंग) का माध्यम होते हैं, या कंप्यूटर का उपयोग अपराध (जबरन वसूली, डेटा उल्लंघन, चोरी) करने के लिए एक उपकरण के रूप में</p>	<p>Students Watch the power point slide carefully</p> <p>छात्र पावर प्वाइंट स्लाइड को ध्यान से देखें </p>	 

<p>9.2 Ways of Cyber Crime</p> <p>साइबर क्राइम के तरीके</p>	<p>किया जाता है।</p> <p>Hacking, phishing, fraud emails, identity theft, ransomware.</p> <p>हैकिंग, फिशिंग, धोखाधड़ी वाले ईमेल, पहचान की चोरी, रैनसमवेयर</p>	<p>Students Watch the power point slide carefully.</p> <p>छात्र पावर प्वाइंट स्लाइड को ध्यान से देखें</p>	
<p>9.3 Showing video on Smart board</p> <p>स्मार्ट बोर्ड पर वीडियो दिखाना</p>	<p>Watch video very sincerely.</p> <p>Cyber Security Awareness Program video</p> <p>https://youtu.be/8tR9P4QX82I</p> <p>वीडियो को बहुत ही ईमानदारी से देखें।</p> <p>साइबर सुरक्षा जागरूकता कार्यक्रम का वीडियो</p> <p>https://youtu.be/8tR9P4QX82I</p>	<p>Students watched the video carefully.</p> <p>इस वीडियो को स्टूडेंट्स ध्यान से देखें।</p>	
<p>9.4 Open Discussion in class</p> <p>कक्षा में खुली चर्चा</p>	<p>After the video allow the students to think about what they have seen. Open up the discussion by asking what measures alia took to remain safe in cyber world.</p> <p>वीडियो के बाद छात्रों को यह सोचने का मौका दें कि उन्होंने क्या देखा। चर्चा की शुरुआत यह पूछकर करें कि आलिया ने साइबर दुनिया में सुरक्षित रहने के लिए क्या उपाय किए।</p>	<p>All Students discuss the activities of Alia in the video with each other.</p> <p>सभी छात्र वीडियो में आलिया की गतिविधियों पर एक-दूसरे से चर्चा करते हैं।</p>	

<p>9.5 Hacking हैकिंग</p>	<p>Hacking is the act of unauthorized access to a computer, computer network or any digital system. Hackers usually have technical expertise of the hardware and software. They look for bugs to exploit and break into the system.</p> <p>Is hacking good or bad?</p> <p>हैकिंग एक कंप्यूटर, कंप्यूटर नेटवर्क या किसी डिजिटल सिस्टम तक अनधिकृत पहुंच का कार्य है। हैकर्स के पास आमतौर पर हार्डवेयर और सॉफ्टवेयर की तकनीकी विशेषज्ञता होती है। वे सिस्टम में शोषण और सेंध लगाने के लिए बग की तलाश करते हैं। हैकिंग अच्छी है या बुरी?</p>	<p>All Students confused some says it is good and some says not good.</p> <p>सभी छात्र असमंजस में पड़ गए, कोई कहता है अच्छा है तो कोई कहता है अच्छा नहीं।</p>	
	<p>Hacking, when done with a positive intent, is called ethical hacking. Such ethical hackers are known as white hat hackers.</p> <p>A non-ethical hacker is the one who tries to gain unauthorised access to computers or networks in order to steal sensitive data with the intent to damage or bring down systems.</p>	<p>Sir, White Hat Hackers.</p> <p>सर, व्हाइट हैट हैकर्स।</p>	

	<p>They are called black hat hackers or crackers.</p> <p>What type of hackers you want to be?</p> <p>हैकिंग जब सकारात्मक इरादे से की जाती है एथिकल हैकिंग कहलाती है। ऐसे एथिकल हैकर्स को व्हाइट हैट हैकर्स कहते हैं। एक गैर-नैतिक हैकर वह है जो सिस्टम को नुकसान पहुंचाने या नीचे लाने के इरादे से संवेदनशील डेटा चोरी करने के लिए कंप्यूटर या नेटवर्क पर अनधिकृत पहुंच प्राप्त करने का प्रयास करता है। इन्हें ब्लैक हैट हैकर्स या क्रैकर्स कहते हैं। आप किस प्रकार के हैकर बनना चाहते हैं?</p>		
<p>9.6 Phishing and Fraud Emails फिशिंग और फ़ॉड ईमेल</p>	<p>Students what comes in your mind on name of phishing?</p> <p>छात्रों फिशिंग के नाम पर आपके दिमाग में क्या आता है?</p>	<p>Sir it is like fishing.</p> <p>सर यह मछली पकड़ने जैसा है।</p>	
	<p>It is literally not the same but the concept is in similar way.</p> <p>Phishing is an unlawful activity where fake websites or emails that look original or authentic are</p>	<p>Yes sir my uncle also received the fraud call on the name of bank.</p> <p>But he didn't give the OTP & Card details.</p>	

	<p>presented to the user to fraudulently collect sensitive and personal details, particularly usernames, passwords, banking and credit card details. Phishing attempts through phone calls or text messages are also common these days.</p>	<p>जी सर मेरे अंकल को भी बैंक के नाम से फ्रॉड कॉल आया। लेकिन उन्होंने ओटीपी और कार्ड की जानकारी नहीं दी।</p>	<div style="background-color: #0056b3; color: white; padding: 5px; text-align: center;"> BEWARE OF FAKE KYC LINKS! SBI NEVER SENDS ANY SUCH MESSAGES </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Dear customer Your SBI Bank Account has been Blocked Plz Update your Document visit SBI website Click here to Update by Net Banking https://sbikycupdate.online</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Dear customer Your SBI Bank Account has been Blocked Plz Update your Document visit SBI website Click here to Update by Net Banking https://sbikycupdate.online</p> </div> 
	<p>Right decision taken by your uncle. You all must do aware your family, friend and society about such frauds. आपके मामा जी ने सही फैसला लिया । आप सभी अपने परिवार, दोस्त और समाज को ऐसे फ्रॉड के बारे में अवश्य जागरूक करें।</p>	<p>Definitely sir, we will do it. बिल्कुल सर, हम करेंगे।</p>	
<p>9.7 Identity Theft आइडेंटिटी थेफ्ट</p>	<p>Identity thieves increasingly use personal information stolen from computers or computer networks, to commit fraud by using the data gained unlawfully. A user's identifiable personal data like demographic details, Email ID, banking credentials, passport, PAN, Aadhaar number and various such personal data are stolen and misused by the hacker on behalf of the victim. Do you have any experience of identity</p>	<p>Yes sir, previous days on facebook someone created the account on my name using my photos and contact details and started sending wrong messages and money demands to my friends. Then i reported that account online as a fake id and told my friends about the</p>	

	<p>theft? पहचान चोर अवैध रूप से प्राप्त डेटा का उपयोग करके धोखाधड़ी करने के लिए, कंप्यूटर या कंप्यूटर नेटवर्क से चुराई गई व्यक्तिगत जानकारी का तेजी से उपयोग करते हैं। एक उपयोगकर्ता की पहचान योग्य व्यक्तिगत डेटा जैसे जनसांख्यिकीय विवरण, ईमेल आईडी, बैंकिंग क्रेडेंशियल्स, पासपोर्ट, पैन, आधार संख्या और इस तरह के विभिन्न व्यक्तिगत डेटा को पीड़ित की ओर से हैकर द्वारा चुराया और दुरुपयोग किया जाता है। क्या आपके पास पहचान की चोरी का कोई अनुभव है?</p>	<p>fake id and asked them to unfriend that id and not to send any money on my name. हों सर, पिछले दिनों फेसबुक पर किसी ने मेरे फोटो और संपर्क विवरण का उपयोग करके मेरे नाम पर खाता बनाया और मेरे दोस्तों को गलत संदेश और पैसे की मांग भेजने लगा। फिर मैंने उस खाते को एक फर्जी आईडी के रूप में ऑनलाइन रिपोर्ट किया और अपने दोस्तों को फर्जी आईडी के बारे में बताया और उनसे उस आईडी को अनफ्रेंड करने और मेरे नाम पर कोई पैसा नहीं भेजने के लिए कहा।</p>	
<p>9.8 Ransom ware रैंसमवेयर</p>	<p>Any idea about the concept of ransomware! रैंसमवेयर की अवधारणा के बारे में कोई जानकारी!</p>	<p>No response कोई प्रतिक्रिया नहीं</p>	

Ransomware is another kind of cyber crime where the attacker gains access to the computer and blocks the user from accessing, usually by encrypting the data. The attacker blackmails the victim to pay for getting access to the data, or sometimes threaten to publish personal and sensitive information or photographs unless a ransom is paid.

रैंसमवेयर एक अन्य प्रकार का साइबर अपराध है जहां हमलावर कंप्यूटर तक पहुंच प्राप्त करता है और आमतौर पर डेटा को एन्क्रिप्ट करके उपयोगकर्ता को एक्सेस करने से रोकता है। हमलावर पीड़ित को डेटा तक पहुंच प्राप्त करने के लिए भुगतान करने के लिए ब्लैकमेल करता है, या कभी-कभी फिरौती का भुगतान न करने पर व्यक्तिगत और संवेदनशील जानकारी या तस्वीरों को प्रकाशित करने की धमकी देता है।

Sir it is like digital kidnapping.

सर यह डिजिटल किडनैपिंग जैसा है।



**9.9
Combating and Preventing Cyber Crime**

The challenges of cyber crime can be mitigated with the twin approach of being alert and taking legal help. Following points can be considered as safety measures to reduce the risk

Yes sir, it will be very helpful. We all will take care note of it.

हां सर, यह बहुत

साइबर अपराध का मुकाबला और रोकथाम

of cyber crime:

- Take regular backup of important data
- Use an antivirus software and keep it updated always
- Avoid installing pirated software. Always download software from known and secure (HTTPS) sites.
- Do not visit or download anything from untrusted websites.
- Use strong password for web login, and change it periodically.
- Don't share OTP & financial details with others.

सतर्क रहने और कानूनी मदद लेने के दोहरे दृष्टिकोण से साइबर अपराध की चुनौतियों को कम किया जा सकता है।

साइबर अपराध के जोखिम को कम करने के लिए निम्नलिखित बिंदुओं को सुरक्षा उपायों के रूप में माना जा सकता है:

- महत्वपूर्ण डेटा का नियमित बैकअप लें |
- एंटीवायरस सॉफ्टवेयर का उपयोग करें और इसे हमेशा अपडेट रखें |
- पायरेटेड सॉफ्टवेयर इंस्टॉल करने से बचें. हमेशा ज्ञात और सुरक्षित (HTTPS) साइटों से

मददगार होगा। हम सभी इसका ध्यान रखेंगे.

How to Secure Data?

- Keep your operating system and all system software updated regularly.
- Do proper password management
- keep antivirus software updated regularly
- Use firewall and other security software
- Avoid untrusted Wi-Fi connections
- Have data backup , update it regularly
- Avoid surfing untrusted websites.



सॉफ्टवेयर डाउनलोड करें।

- अविश्वसनीय वेबसाइटों से कुछ भी न देखें या डाउनलोड न करें।
- वेब लॉगिन के लिए मजबूत पासवर्ड का प्रयोग करें, और इसे समय-समय पर बदलते रहें।
- ओटीपी और वित्तीय विवरण दूसरों के साथ साझा न करें।

10. Recapitulation(सारकथन-):

Alright students let's recall what we have learnt so far :

ठीक है छात्रों आइए याद करें कि हमने अभी तक क्या सीखा है :

Cyber Crime, Ways of Cyber Crime. साइबर अपराध, साइबर अपराध के तरीके।

Hacking, Phishing and Fraud Emails. हैकिंग, फिशिंग और फ्रॉड ईमेल।

Identity Theft, Ransomware. आइडेंटिटी थेफ्ट, रैनसमवेयर।

What you have learned from video. आपने वीडियो से क्या सीखा।

Explore and find out how to file complaint with the cyber cell in your area.
अन्वेषण करें और जानें कि अपने क्षेत्र में साइबर सेल में शिकायत कैसे दर्ज करें।

11. Inspection (निरीक्षण):

Teacher will now inspect and check all the notebooks of the students so that he can make sure all students have written all the definitions and examples written/shown on digital/green board.

शिक्षक अब छात्रों की सभी नोटबुक का निरीक्षण और जांच करेगा ताकि वह सुनिश्चित कर सके कि सभी छात्रों ने डिजिटल/ग्रीन बोर्ड पर लिखी/दिखाई गई सभी परिभाषाएं और उदाहरण लिखे हैं।

12. HOME WORK/ ASSIGNMENT

गृह कार्य / असाइनमेंट

Home work is given to the students using online quiz on website:
<https://quizizz.com>

1. Link for homework is:
<https://quizizz.com/join?gc=12737495>
2. Prepare notes of the topic in final notebook.
3. List down the steps you need to take in order to ensure:
 - a) Your computer is in good working condition for a longer time.
 - b) Smart and safe Internet surfing.

वेबसाइट: <https://quizizz.com> पर ऑनलाइन क्विज का उपयोग कर छात्रों को गृह कार्य दिया जाता है

1. होमवर्क के लिए लिंक है:
<https://quizizz.com/join?gc=12737495>
2. फाइनल नोटबुक में टॉपिक के नोट्स तैयार करें।
3. निम्न को सुनिश्चित करने के लिए आपको जिन कदमों को उठाने की आवश्यकता है, उनकी सूची बनाएं:
 - क) आपका कंप्यूटर लंबे समय तक काम करने की अच्छी स्थिति में है।
 - ख) स्मार्ट और सुरक्षित इंटरनेट सर्फिंग

