CYBER HYGIENE

Presented By: Balkrishna Kumar
Assistant Professor

"Cyber" शब्द की उत्पत्ति:

- यह शब्द "Cybernetics" से लिया गया है।
- Cybernetics शब्द की उत्पत्ति ग्रीक शब्द "κυβερνήτης" (kybernētēs) से हुई है, जिसका अर्थ होता है "**कप्तान**" या "**नियंत्रक**"।
- इसका प्रयोग सबसे पहले **Norbert Wiener** ने 1948 में किया था, जब उन्होंने अपनी पुस्तक *Cybernetics: Or Control and Communication in the Animal and the Machine* में इसका उपयोग किया।

हिंदी में "साइबर" शब्द:

- हिंदी में यह शब्द ज्यों का त्यों transliterate होकर "**साइबर**" बन गया है।
- इसका उपयोग कंप्यूटर नेटवर्क, इंटरनेट और डिजिटल दुनिया से संबंधित शब्दों में होता है, जैसे:
  - **साइबर सुरक्षा (Cyber Security)**
  - **साइबर क्राइम (Cyber Crime)**
  - **साइबर दुनिया (Cyber World)**

तो, संक्षेप में, "साइबर" शब्द हिंदी में एक **विदेशी (loan word)** है, जिसकी जड़ें ग्रीक भाषा में हैं और जो अंग्रेज़ी के माध्यम से तकनीकी शब्दावली का हिस्सा बना

साइबर हाइजीन (Cyber Hygiene) पर वर्णनात्मक टिप्पणी

परिचय:

आज के डिजिटल युग में, इंटरनेट और तकनीकी उपकरणों का उपयोग जीवन का अनिवार्य हिस्सा बन गया है। जैसे हम शारीरिक स्वास्थ्य बनाए रखने के लिए स्वच्छता (हाइजीन) का पालन करते हैं, वैसे ही **डिजिटल दुनिया में सुरक्षित रहने के लिए कुछ सावधानियाँ और आदतें अपनाना जरूरी है**, जिसे हम **साइबर हाइजीन** कहते हैं।

साइबर हाइजीन का अर्थ

साइबर हाइजीन का अर्थ है – **ऑनलाइन गतिविधियों और डिजिटल उपकरणों का सुरक्षित, सतर्क और जागरूकता के साथ उपयोग करना**, ताकि साइबर खतरों जैसे वायरस, हैकिंग, डेटा चोरी आदि से बचा जा सके

साइबर हाइजीन के मुख्य तत्व:

1. ☑ **मजबूत पासवर्ड का उपयोग:**
   - पासवर्ड लंबे और जटिल हों (अक्षर, अंक और विशेष चिन्हों के साथ)।
   - एक ही पासवर्ड कई जगहों पर न उपयोग करें।
2. ☑ **दो-चरणीय प्रमाणीकरण (2FA):**
   - लॉगिन सुरक्षा बढ़ाने के लिए 2FA का उपयोग करें, जैसे OTP या ऐप आधारित कोड।

3. ☑ **एंटीवायरस व फ़ायरवॉल सॉफ़्टवेयर:**
   - अपने उपकरणों में अपडेटेड एंटीवायरस और फ़ायरवॉल लगाएं।
4. ☑ **सॉफ़्टवेयर अपडेट करते रहें:**
   - ऑपरेटिंग सिस्टम, ऐप्स और ब्राउज़र को समय-समय पर अपडेट करें, ताकि सुरक्षा खामियाँ दूर की जा सकें।
5. ☑ **फिशिंग से सावधान रहें:**
   - अनजान ईमेल, लिंक या वेबसाइटों पर क्लिक न करें।
   - किसी भी संदिग्ध लिंक पर अपनी जानकारी साझा न करें।
6. ☑ **सार्वजनिक Wi-Fi से बचें:**
   - सार्वजनिक नेटवर्क पर संवेदनशील लेन-देन (जैसे बैंकिंग) न करें।
7. ☑ **डेटा बैकअप करें:**
   - महत्वपूर्ण फाइलों और डेटा का नियमित रूप से बैकअप लें।
8. ☑ **सोशल मीडिया पर सतर्कता:**
   - अपनी निजी जानकारी साझा करने में सावधानी रखें।

◆ महत्त्व और आवश्यकता:

- साइबर अपराधों में तेजी से वृद्धि हो रही है – जैसे कि पहचान की चोरी, ऑनलाइन धोखाधड़ी, रैंसमवेयर आदि।
- एक छोटी सी चूक भारी नुकसान का कारण बन सकती है – वित्तीय, सामाजिक और मानसिक रूप से।
- बच्चों और बुजुर्गों को भी साइबर हाइजीन की जानकारी देना जरूरी है।

दो-चरणीय प्रमाणीकरण (2FA) क्या है? – विस्तार से जानकारी (हिंदी में)

◆ परिभाषा:

दो-चरणीय प्रमाणीकरण (Two-Factor Authentication - 2FA) एक सुरक्षा प्रक्रिया है जिसमें उपयोगकर्ता को लॉगिन करने के लिए दो अलग-अलग प्रमाण (factors) प्रदान करने होते हैं। इसका उद्देश्य यह सुनिश्चित करना है कि केवल अधिकृत व्यक्ति ही किसी अकाउंट या सिस्टम तक पहुंच प्राप्त कर सके।

◆ 2FA के दो चरण क्या होते हैं?

1. ☑ **पहला चरण – कुछ जो आप जानते हैं (Something you know):**
   - पासवर्ड या पिन कोड
     उदाहरण: आपकी ईमेल का पासवर्ड
2. ☑ **दूसरा चरण – कुछ जो आप रखते हैं या प्राप्त करते हैं (Something you have):**
   - मोबाइल पर भेजा गया OTP

- प्रमाणीकरण ऐप (जैसे Google Authenticator, Microsoft Authenticator) से कोड
- हार्डवेयर टोकन या स्मार्ट कार्ड

2FA के उदाहरण:

- जब आप अपने बैंक अकाउंट में लॉगिन करते हैं:
  - पहले पासवर्ड डालते हैं
  - फिर मोबाइल पर आए OTP को डालते हैं
    - यही 2FA है।
- Gmail या Facebook में 2FA ऑन करने पर:
  - लॉगिन के बाद एक कोड आपके फ़ोन पर आता है।

2FA के फायदे:

1. **अधिक सुरक्षा**: केवल पासवर्ड चुराने से कोई आपके अकाउंट तक नहीं पहुंच सकता।
2. **फिशिंग से बचाव**: OTP या कोड की मांग से जालसाज़ों के लिए घुसपैठ कठिन हो जाती है।
3. **रियल-टाइम अलर्ट**: जब भी लॉगिन की कोशिश होती है, आपको तुरंत सूचना मिलती है।

2FA कैसे चालू करें? (सामान्य प्रक्रिया):

1. अपने अकाउंट (जैसे Google, Facebook, बैंक आदि) की **सिक्योरिटी सेटिंग्स** में जाएं।
2. **Two-Factor Authentication** या **2-Step Verification** विकल्प चुनें।
3. मोबाइल नंबर या प्रमाणीकरण ऐप से लिंक करें।
4. एक बार सेटअप होने के बाद हर लॉगिन पर कोड मांगा जाएगा।

निष्कर्ष:

2FA एक सरल लेकिन अत्यंत प्रभावी सुरक्षा तरीका है।
हर इंटरनेट उपयोगकर्ता को अपने महत्वपूर्ण अकाउंट्स (जैसे ईमेल, बैंक, सोशल मीडिया) में 2FA जरूर चालू करना चाहिए। यह एक अतिरिक्त ताला लगाने जैसा है — जिससे आपका डिजिटल जीवन सुरक्षित रहता है।

अगर आप चाहें, तो मैं आपको Google या Facebook में 2FA चालू करने की स्टेप-बाय-स्टेप प्रक्रिया भी भेज सकता हूँ। क्या आप किसी विशेष ऐप के लिए यह जानकारी चाहते हैं?

फ़ायरवॉल सॉफ़्टवेयर (Firewall Software):

परिभाषा:

फ़ायरवॉल एक सुरक्षा प्रणाली है जो आपके कंप्यूटर या नेटवर्क और इंटरनेट के बीच एक **"डिजिटल दीवार"** की तरह काम करती है।
यह यह तय करता है कि कौन-सा डाटा अंदर आ सकता है और कौन-सा बाहर जा सकता है।

कैसे काम करता है:

- जब भी कोई डेटा इंटरनेट से आपके सिस्टम तक पहुँचता है, फ़ायरवॉल उसकी जाँच करता है।
- यदि वह सुरक्षित है तो ही अनुमति देता है।
- अनधिकृत या संदिग्ध कनेक्शन को यह **ब्लॉक** कर देता है।

प्रमुख कार्य:

- बाहरी हमलों से सुरक्षा
- इनबाउंड और आउटबाउंड ट्रैफ़िक को नियंत्रित करना
- नेटवर्क गतिविधियों की निगरानी
- पोर्ट ब्लॉकिंग और अलर्ट भेजना

प्रकार:

1. **सॉफ़्टवेयर फ़ायरवॉल** – जो आपके सिस्टम में इंस्टॉल होता है (जैसे Windows Firewall)
2. **हार्डवेयर फ़ायरवॉल** – बड़े नेटवर्क में प्रयोग होता है, जैसे ऑफिस या संस्था में

◇ एंटीवायरस और फ़ायरवॉल में अंतर:

विशेषता	एंटीवायरस	फ़ायरवॉल
उद्देश्य	वायरस हटाना और रोकना	अनधिकृत नेटवर्क एक्सेस को रोकना
स्कैन करता है	फाइलें, सॉफ़्टवेयर, मेल आदि	नेटवर्क ट्रैफ़िक
सुरक्षा	इंटरनल थ्रेट्स से	एक्सटर्नल थ्रेट्स से

◇ निष्कर्ष:

एंटीवायरस और फ़ायरवॉल दोनों की भूमिका अलग लेकिन बेहद ज़रूरी है।
एक वायरस से बचाता है और दूसरा बाहरी साइबर हमलों से।
अगर आप डिजिटल दुनिया में सुरक्षित रहना चाहते हैं, तो इन दोनों सॉफ़्टवेयर का उपयोग ज़रूर करें — खासकर तब, जब आप इंटरनेट का नियमित उपयोग करते हैं।

सॉफ़्टवेयर अपडेट करते रहें – विस्तृत जानकारी (हिंदी में)

📌 परिचय

डिजिटल दुनिया में सुरक्षित रहने के लिए **सॉफ़्टवेयर अपडेट** करना एक **जरूरी आदत** है।
यह केवल नए फीचर पाने के लिए नहीं होता, बल्कि **सुरक्षा की दृष्टि से भी अत्यंत महत्वपूर्ण** होता है।

🔧 सॉफ़्टवेयर अपडेट क्या होता है?

सॉफ़्टवेयर अपडेट का मतलब है –
किसी एप्लिकेशन, ऑपरेटिंग सिस्टम (जैसे Windows, Android, iOS), या प्रोग्राम का नया संस्करण इंस्टॉल करना, जिसमें:

- बग्स (खामियाँ) को ठीक किया गया होता है
- नई सुविधाएँ जोड़ी जाती हैं
- सुरक्षा संबंधी सुधार (security patches) शामिल होते हैं

🛡️ सुरक्षा के लिए क्यों जरूरी है?

1. 🔒 **साइबर हमलों से बचाव:**
   पुराने सॉफ़्टवेयर में अक्सर **सुरक्षा कमजोरियाँ (vulnerabilities)** होती हैं, जिनका फायदा उठाकर हैकर सिस्टम को नुकसान पहुँचा सकते हैं। अपडेट इन्हें ठीक करता है।
2. 🚫 **मैलवेयर और वायरस से सुरक्षा:**
   अपडेटेड एंटीवायरस और ऐप्स नई तरह के वायरस और खतरों से लड़ने में सक्षम होते हैं।
3. ⚙️ **सिस्टम की बेहतर परफॉर्मेंस:**
   अपडेट के साथ सॉफ़्टवेयर तेज़, स्थिर और अधिक विश्वसनीय बनता है।
4. 📱 **डिवाइस की उम्र बढ़ाना:**
   नियमित अपडेट डिवाइस को समय से पहले स्लो या बेकार होने से बचाते हैं।

☑️ कौन-कौन से सॉफ़्टवेयर अपडेट करना चाहिए?

- 💻 **ऑपरेटिंग सिस्टम** (जैसे Windows, macOS, Android, iOS)
- 🛡️ **एंटीवायरस सॉफ़्टवेयर**
- 🌐 **वेब ब्राउज़र** (Chrome, Firefox, Edge आदि)
- 📲 **मोबाइल ऐप्स**
- 🛠️ **अन्य सुरक्षा टूल्स और नेटवर्क सॉफ़्टवेयर**

🗓️ कैसे करें अपडेट?

1. **ऑटो-अपडेट चालू करें** – ज़्यादातर ऐप्स में यह विकल्प होता है।
2. **नियमित रूप से सेटिंग्स में जाकर जांचें** – जैसे "Check for Updates" बटन दबाना।
3. **संदिग्ध या अनौपचारिक स्रोतों से अपडेट न करें** – हमेशा आधिकारिक वेबसाइट या ऐप स्टोर से अपडेट करें।

⚠️ ध्यान देने योग्य बातें:

- अपडेट करते समय इंटरनेट कनेक्शन स्थिर रखें।
- कभी-कभी सिस्टम को रीस्टार्ट करना ज़रूरी हो सकता है।
- महत्वपूर्ण डेटा का बैकअप लेना फायदेमंद होता है (विशेषकर बड़े अपडेट से पहले)।

📝 निष्कर्ष:

"सॉफ़्टवेयर अपडेट" केवल सुविधा का मामला नहीं है, बल्कि यह एक साइबर सुरक्षा कवच है।
हर उपयोगकर्ता को चाहिए कि वह इसे गंभीरता से ले और नियमित रूप से अपने सभी डिजिटल उपकरणों को अपडेट करता रहे।

फिशिंग से सावधान रहें – विस्तृत जानकारी (हिंदी में)

📌 परिचय:

आजकल इंटरनेट उपयोगकर्ताओं को ठगने के लिए सबसे आम साइबर अपराधों में से एक है **फिशिंग (Phishing)**।
यह एक ऐसा तरीका है जिसमें **जालसाज़ (हैकर)** नकली ईमेल, वेबसाइट, या मैसेज भेजकर लोगों से **उनकी गोपनीय जानकारी (जैसे पासवर्ड, बैंक डिटेल, OTP)** चुरा लेते हैं।

🔍 फिशिंग क्या है?

फिशिंग एक धोखाधड़ी (fraud) तकनीक है जिसमें:

- उपयोगकर्ता को भ्रमित कर के
- नकली लिंक या वेबसाइट पर ले जाया जाता है
- और वहां उसकी निजी जानकारी चुराई जाती है

यह शब्द "**Fishing**" से लिया गया है – जैसे मछली को चारे से फंसाया जाता है, वैसे ही यूज़र को झूठे वादों या डर से फंसाया जाता है।

🎣 फिशिंग के सामान्य तरीके:

1. 📧 **ईमेल फिशिंग:**
   - नकली ईमेल जो असली बैंक, कंपनी, या सरकार की तरह दिखते हैं।
   - विषय (Subject) जैसे – *"आपका अकाउंट बंद होने वाला है"*, *"आपको इनाम मिला है"*, आदि।
2. 📱 **SMS फिशिंग (Smishing):**
   - फ़ोन पर भेजे गए फर्जी मैसेज जिनमें लिंक होते हैं।
3. 📞 **वॉइस कॉल फिशिंग (Vishing):**
   - कॉल पर खुद को बैंक अधिकारी या सरकारी एजेंट बताकर जानकारी मांगना।
4. 🌐 **फेक वेबसाइट:**
   - दिखने में असली वेबसाइट जैसी होती है, लेकिन उसका URL थोड़ा बदल होता है।
     उदाहरण: `www.paytm.in` की जगह `www.paytm-secure.in`

⚠️ फिशिंग से कैसे बचें?

सुझाव	विवरण
🔑 **कभी भी निजी जानकारी साझा न करें**	OTP, पासवर्ड, कार्ड नंबर आदि फ़ोन या ईमेल पर कभी न दें
🔗 **लिंक पर क्लिक करने से पहले जाँच करें**	URL को ध्यान से पढ़ें – स्पेलिंग में गड़बड़ी होती है
📧 **संदिग्ध ईमेल को न खोलें**	अज्ञात स्रोत से आया ईमेल, अटैचमेंट या लिंक न खोलें
🔒 **ब्राउज़र में "HTTPS" जरूर देखें**	सुरक्षित वेबसाइट का पता `https://` से शुरू होता है
🛠️ **एंटीवायरस और फ़ायरवॉल चालू रखें**	ये फर्जी वेबसाइटों और लिंक को ब्लॉक कर सकते हैं
📱 **OTP या बैंक डिटेल किसी से साझा न करें**	बैंक और सरकारी संस्थान कभी OTP नहीं मांगते

☑️ अगर गलती से जानकारी दे दी हो तो क्या करें?

1. तुरंत संबंधित बैंक को सूचना दें और कार्ड या अकाउंट ब्लॉक करवाएं।
2. पासवर्ड तुरंत बदलें।
3. साइबर क्राइम की रिपोर्ट करें:
   - 🔗 www.cybercrime.gov.in
   - 📞 या पुलिस हेल्पलाइन 1930 पर कॉल करें।

📝 निष्कर्ष:

फिशिंग एक "डिजिटल जाल" है, जिसमें फँसने से आपके पैसे और पहचान दोनों खतरे में आ सकते हैं।
थोड़ी सी सतर्कता और जागरूकता से आप इस खतरे से पूरी तरह बच सकते हैं।
"सोच समझ कर क्लिक करें, फिशिंग से खुद को सुरक्षित रखें!"

सार्वजनिक Wi-Fi से बचें – विस्तृत जानकारी (हिंदी में)

📌 परिचय

जब हम कैफे, रेलवे स्टेशन, एयरपोर्ट या मॉल जैसी जगहों पर होते हैं, तो मुफ्त Wi-Fi बहुत आकर्षक लगता है। लेकिन यह **सुविधा जितनी आसान लगती है, उतनी ही खतरनाक भी हो सकती है।**
सार्वजनिक Wi-Fi नेटवर्क साइबर अपराधियों के लिए **आपकी निजी जानकारी चुराने का आसान जरिया** बन सकता है।

⚠️ सार्वजनिक Wi-Fi के खतरे

1. 🔓 **डेटा चोरी का खतरा:**
   - ये नेटवर्क **एन्क्रिप्टेड नहीं होते**, जिससे हैकर आपकी गतिविधियाँ देख सकते हैं।
2. 🕵️‍♂️ **"मैन-इन-द मिडल" हमला:**
   - हैकर आपके डिवाइस और इंटरनेट के बीच में बैठकर जानकारी चुरा सकते हैं (जैसे लॉगिन डिटेल्स, बैंक पासवर्ड)।
3. 📡 **फर्जी Wi-Fi हॉटस्पॉट:**
   - हैकर असली नाम जैसे "Free_Airport_Wifi" नाम से नकली नेटवर्क बनाते हैं।
   - यूज़र कनेक्ट होते ही सारा डेटा हैकर के पास पहुँच जाता है।
4. 🦠 **मैलवेयर इंस्टॉल होने का खतरा:**
   - फ्री Wi-Fi से जुड़ने पर हैकर आपके डिवाइस में **वायरस या ट्रोजन** भेज सकते हैं।

🛡️ सार्वजनिक Wi-Fi का उपयोग करते समय सावधानियाँ

सुझाव	विवरण
🔒 **VPN (Virtual Private Network) का उपयोग करें**	यह आपके डेटा को एन्क्रिप्ट करता है, जिससे हैकर उसे पढ़ नहीं सकते
💳 **बैंकिंग या खरीदारी न करें**	सार्वजनिक नेटवर्क पर कभी भी ऑनलाइन ट्रांज़ेक्शन से बचें
⚙️ **ऑटो-कनेक्ट बंद करें**	डिवाइस की सेटिंग्स में "Auto-connect to Wi-Fi" ऑप्शन को बंद करें
🔐 **2FA चालू रखें**	किसी भी अकाउंट में 2-चरणीय प्रमाणीकरण सुरक्षा बढ़ा देता है
🚫 **सार्वजनिक नेटवर्क पर फाइल शेयरिंग बंद करें**	"File Sharing" और "Bluetooth" बंद कर दें

सोशल मीडिया पर सतर्कता – विस्तृत जानकारी (हिंदी में)

📌 परिचय:

सोशल मीडिया आज हमारे जीवन का अभिन्न हिस्सा बन चुका है – जैसे Facebook, Instagram, WhatsApp, Twitter (X), YouTube आदि।
हालांकि यह प्लेटफ़ॉर्म्स हमें दुनिया से जोड़ते हैं, लेकिन **थोड़ी सी लापरवाही भारी नुकसान का कारण बन सकती है।**
इसलिए सोशल मीडिया पर **सतर्क रहना** बेहद जरूरी है।

🔍 सोशल मीडिया से जुड़े संभावित खतरे:

1. 🕵️ **पहचान की चोरी (Identity Theft):**
   - आपकी प्रोफ़ाइल से आपकी तस्वीर, नाम और जानकारी लेकर **फर्जी अकाउंट** बनाए जा सकते हैं।
2. **फिशिंग और धोखाधड़ी:**
   - फर्जी लिंक भेजकर आपकी गोपनीय जानकारी (पासवर्ड, बैंक डिटेल) चुराई जा सकती है।
3. 📲 **ओवरशेयरिंग (अत्यधिक जानकारी साझा करना):**
   - आपकी लोकेशन, यात्रा योजना, या व्यक्तिगत जीवन साझा करने से **चोर या साइबर अपराधी** फायदा उठा सकते हैं।
4. 🔺 **साइबर बुलिइंग और ट्रोलिंग:**
   - सोशल मीडिया पर गलत या भड़काऊ टिप्पणियाँ, धमकियाँ या मानसिक उत्पीड़न हो सकता है।
5. 🗞️ **फर्जी खबरें (Fake News):**
   - सोशल मीडिया फर्जी और भ्रामक जानकारी फैलाने का एक बड़ा माध्यम बन चुका है।

☑ सोशल मीडिया पर सतर्क रहने के उपाय:

उपाय	विवरण
🔒 **प्रोफ़ाइल प्राइवेसी सेट करें**	अपनी पोस्ट, फोटो और जानकारी को केवल "Friends" या "Private" रखें
❌ **अनजान लोगों को फ्रेंड न बनाएं**	हर रिक्वेस्ट को स्वीकार न करें, पहले प्रोफ़ाइल जांचें
🗞️ **गोपनीय जानकारी साझा न करें**	जैसे OTP, बैंक डिटेल, आधार नंबर, घर का पता आदि
🗺️ **लोकेशन शेयरिंग बंद करें**	लाइव लोकेशन शेयर करने से बचें, खासकर जब आप घर से बाहर हों
🕵️ **दो-चरणीय प्रमाणीकरण (2FA) चालू करें**	अपने अकाउंट को एक्स्ट्रा सुरक्षा दें
🚫 **फेक न्यूज़ को न फैलाएं**	किसी भी जानकारी को साझा करने से पहले उसकी सत्यता की पुष्टि करें

उपाय	विवरण
⚠️ **संदिग्ध लिंक या मैसेज पर क्लिक न करें**	ये लिंक आपकी जानकारी चुरा सकते हैं या वायरस डाल सकते हैं
🔒 **पब्लिक पोस्ट से बचें**	निजी जानकारी को "Public" पोस्ट करने से आपकी सुरक्षा खतरे में पड़ सकती है

📝 निष्कर्ष:

सोशल मीडिया का उपयोग करना आज की ज़रूरत है, लेकिन **स्मार्ट और सतर्क उपयोगकर्ता** ही इससे सुरक्षित रह सकते हैं।
"सोच समझकर पोस्ट करें, निजी जानकारी को निजी रखें, और सोशल मीडिया को अपने नियंत्रण में रखें – न कि इसके नियंत्रण में रहें।"

☑️ क्या करें यदि सार्वजनिक Wi-Fi का उपयोग करना जरूरी हो?

1. केवल HTTPS वेबसाइट का उपयोग करें
2. VPN सेवा का उपयोग करें (जैसे ProtonVPN, NordVPN आदि)
3. ब्राउज़र और सॉफ़्टवेयर को अपडेट रखें
4. उपयोग के बाद Wi-Fi को "Forget Network" कर दें

📝 निष्कर्ष:

सार्वजनिक Wi-Fi सुविधा जितनी मुफ्त होती है, खतरा भी उतना बड़ा होता है।
थोड़ी सी सावधानी आपको बड़ी हानि से बचा सकती है।
जहाँ तक हो सके, **मोबाइल डेटा का उपयोग करें**, और अगर Wi-Fi का उपयोग करना ही पड़े, तो **सुरक्षा नियमों का पालन करें।**