पं.क्र. (04/21/05/207665/19)

अन्तरा शब्दशक्ति
प्रकाशन एवं बहुउद्देशीय संस्था
www.antrashabdshakti.com

शब्द
से संवेदना तक...
लेखन से
परिवर्तन तक...

हिन्दी
हमारी पहचान
हमारी शक्ति

'समसामयिक प्रश्नों पर आपकी कलम'

(लेख प्रतियोगिता)

विचार...
चिंतन...
संवाद...
और
एक बेहतर
कल की ओर...

रचनाकार :-
हर्ष धीरेन्द्रकुमार सोनी

आयोजक:-
अन्तरा शब्दशक्ति प्रकाशन
वारासिवनी (म.प्र.)

पं.क्र. (04/21/05/207665/19)

अन्तरा शब्दशक्ति

प्रकाशन एवं बहुददेशीय संस्था
www.antrashabdshakti.com

कलम की शक्ति, समाज की दिशा

हिन्दी हमारी पहचान हमारी शक्ति

शब्द से संवेदन तक...
लेखन से परिवर्तन तक...

संपादक : डॉ. प्रीति समकित सुराना
तकनीकी संपादक : Webcoodee.com
मुख्य कार्यालय : 15 नेहरू चौक, वारासिवनी, जिला बालाघाट (म.प्र.) 481331

Antrashabdshaktiprakashan

संपर्क : 9009423393
ईमेल : antrashabdshakti@gmail.com
वेबसाइट : www.antrashabdshakti.com

वैधानिक सूचना

पुस्तक में प्रकाशित सभी रचनाएँ संबंधित रचनाकारों की मौलिक अभिव्यक्तियाँ हैं। प्रत्येक रचना में व्यक्त विचार, कथ्य एवं अभिमत के लिए संबंधित रचनाकार स्वयं उतरदायी हैं। रचनाओं के चयन एवं प्रकाशन का उद्देश्य साहित्यिक अभिव्यक्ति को मंच प्रदान करना एवं हिन्दी लेखन को प्रोत्साहित करना हैं।

पं.क्र. (04/21/05/207665/19)
अन्तरा शब्दशक्ति
www.antrashabdshakti.com
प्रकाशन एवं बहुद्देशीय संस्था

लेख प्रतियोगिता

लेखक/लेखिका - हर्ष धीरेन्द्रकुमार सोनी

साइबर सुरक्षा : वर्तमान समस्याएँ और उनके समाधान

साइबर सुरक्षा :
वर्तमान समस्याएँ और उनके समाधान

“ज्ञान शक्ति है, लेकिन डिजिटल युग में साइबर जागरूकता ही सुरक्षित शक्ति है।”

प्रस्तावना ----------

आज का युग विज्ञान और प्रौद्योगिकी का युग है। एक समय था जब दूर रहने वाले रिश्तेदारों से बात करने के लिए पत्र लिखना पड़ता था, पैसे भेजने के लिए बैंक की लंबी कतार में खड़ा होना पड़ता था और किसी जानकारी के लिए पुस्तकों या पुस्तकालय का सहारा लेना पड़ता था। आज केवल एक स्मार्टफोन के माध्यम से दुनिया के किसी भी कोने में बैठे व्यक्ति से कुछ ही क्षणों में बात की जा सकती है, कुछ सेकंड में पैसे भेजे जा सकते हैं, घर बैठे शिक्षा प्राप्त की जा सकती है, ऑनलाइन खरीदारी की जा सकती है और असंख्य जानकारियाँ प्राप्त की जा सकती हैं।

इंटरनेट ने वास्तव में पूरी दुनिया को एक “वैश्विक गाँव” में बदल दिया है। कंप्यूटर, स्मार्टफोन, इंटरनेट, क्लाउड कंप्यूटिंग, डिजिटल भुगतान, कृत्रिम बुद्धिमत्ता अर्थात Artificial Intelligence (AI), सोशल मीडिया और Internet of Things (IoT) जैसी तकनीकों ने मानव जीवन को अधिक सरल, तेज और सुविधाजनक बनाया है।

लेकिन सिक्के का दूसरा पहलू भी है।

जो तकनीक मानव जीवन को सरल बनाती है, उसका दुरुपयोग करके अपराधी व्यक्ति, संस्था और देश को नुकसान पहुँचा सकते हैं। किसी व्यक्ति का पासवर्ड चुराया जा सकता है, बैंक खाते से पैसे निकाले जा सकते हैं, नकली पहचान बनाई जा सकती है, व्यक्तिगत जानकारी का दुरुपयोग किया जा सकता है, सोशल मीडिया अकाउंट हैक किया जा सकता है, महत्वपूर्ण कंप्यूटर प्रणाली को बंद किया जा सकता है और फिरौती माँगी जा सकती है। आज कृत्रिम बुद्धिमत्ता की सहायता से नकली आवाज, नकली तस्वीर और नकली वीडियो भी बनाए जा सकते हैं।

इसलिए आज के डिजिटल युग में केवल साक्षर होना पर्याप्त नहीं है; डिजिटल रूप से साक्षर और साइबर जागरूक होना भी उतना ही आवश्यक है।

साइबर सुरक्षा का अर्थ कंप्यूटर, मोबाइल, नेटवर्क, सॉफ्टवेयर, डिजिटल जानकारी और ऑनलाइन सेवाओं को अनधिकृत प्रवेश, चोरी, धोखाधड़ी, नुकसान और दुरुपयोग से सुरक्षित रखने की प्रक्रिया है।

साइबर सुरक्षा अब केवल कंप्यूटर विशेषज्ञों का विषय नहीं है। यह प्रत्येक नागरिक का विषय है। विद्यार्थी से लेकर शिक्षक तक, अभिभावक से लेकर व्यापारी तक, छोटे व्यवसाय से लेकर बड़ी कंपनी तक और सामान्य नागरिक से लेकर सरकार तक—सभी की इसमें जिम्मेदारी है।

कहा जाता है:

"सावधानी हटी, दुर्घटना घटी।"

डिजिटल दुनिया में यह कहावत और भी प्रासंगिक हो गई है। यहाँ छोटी-सी लापरवाही भी बड़ी आर्थिक, सामाजिक या मानसिक समस्या उत्पन्न कर सकती है।

1. साइबर सुरक्षा क्या है?

"साइबर" शब्द डिजिटल तकनीक, कंप्यूटर प्रणाली, नेटवर्क और इंटरनेट से संबंधित है। "सुरक्षा" का अर्थ है जोखिम से संरक्षण।

अर्थात साइबर सुरक्षा वह व्यवस्था है जिसके माध्यम से डिजिटल उपकरणों, नेटवर्क, प्रणालियों और सूचनाओं को साइबर हमलों तथा अनधिकृत उपयोग से सुरक्षित रखा जाता है।

साइबर सुरक्षा के तीन प्रमुख आधार हैं:

1. **गोपनीयता** – Confidentiality

जानकारी केवल अधिकृत व्यक्ति तक पहुँचे, यह सुनिश्चित करना।

2. **अखंडता** – Integrity

जानकारी में कोई अनधिकृत परिवर्तन न हो और वह सही बनी रहे, यह सुनिश्चित करना।

3. **उपलब्धता** – Availability

जब अधिकृत व्यक्ति को जानकारी या प्रणाली की आवश्यकता हो, तब वह उपलब्ध रहे, यह सुनिश्चित करना।

ये तीनों मिलकर सुरक्षित डिजिटल व्यवस्था का निर्माण करते हैं।

इसलिए डिजिटल माध्यमों के सकारात्मक पक्ष से इनकार नहीं किया जा सकता।
समस्या तब उत्पन्न होती है जब आभासी संबंध वास्तविक संबंधों का विकल्प बनने लगते हैं। हम किसी की तस्वीर देखकर समझ लेते हैं कि हमें उसके जीवन का पता है। किसी की मुस्कुराती हुई पोस्ट देखकर मान लेते हैं कि वह सुखी है। किसी के उपलब्धि-संदेश देखकर हम उसके संघर्ष का अनुमान लगा लेते हैं।
परंतु स्क्रीन केवल दृश्य दिखाती है, जीवन नहीं। सोशल मीडिया पर दिखाई देने वाली मुस्कान के पीछे छिपे आँसू कैमरे में नहीं आते। सफलता की तस्वीर के पीछे की असफलताएँ दिखाई नहीं देतीं। सजे हुए घर के पीछे का तनाव दिखाई नहीं देता। उत्सव की तस्वीरों के पीछे छिपी थकान दिखाई नहीं देती।
हम दूसरों के जीवन का संपादित संस्करण देखते हैं और फिर अपने जीवन की अनसंपादित वास्तविकता से उसकी तुलना करने लगते हैं। यहीं से जन्म लेती है—हीनता, असंतोष और मानसिक बेचैनी।

2. डिजिटल क्रांति और साइबर जोखिम

भारत में डिजिटल क्रांति ने सामान्य नागरिक के जीवन में व्यापक परिवर्तन किया है। ऑनलाइन बैंकिंग, UPI, डिजिटल भुगतान, ऑनलाइन शिक्षा, ई-कॉमर्स, डिजिटल सरकारी सेवाएँ और सोशल मीडिया अब दैनिक जीवन का हिस्सा बन चुके हैं।
इन सुविधाओं का उपयोग जितना बढ़ा है, साइबर अपराधों की संभावनाएँ भी उतनी ही बढ़ी हैं।
आज कोई व्यक्ति अपना मोबाइल नंबर सार्वजनिक कर दे, सोशल मीडिया पर अत्यधिक व्यक्तिगत जानकारी साझा करे, कमजोर पासवर्ड रखे या किसी अनजान लिंक पर क्लिक कर दे, तो वह अनजाने में साइबर अपराधी के लिए रास्ता खोल सकता है।
यह समझना आवश्यक है कि साइबर अपराधी हमेशा कंप्यूटर प्रणाली को ही निशाना नहीं बनाता; कई बार वह मनुष्य की भावनाओं, विश्वास, जल्दबाजी और अज्ञानता को निशाना बनाता है।
इसीलिए साइबर सुरक्षा में तकनीक जितनी महत्वपूर्ण है, मानव व्यवहार भी उतना ही महत्वपूर्ण है।

3. फिशिंग : विश्वास का डिजिटल शिकार

फिशिंग साइबर अपराध का एक अत्यंत सामान्य प्रकार है। इसमें अपराधी बैंक, सरकारी विभाग, कंपनी, स्कूल, मित्र या किसी विश्वसनीय संस्था का प्रतिनिधि बनकर नकली ई-मेल, SMS, WhatsApp संदेश या अन्य संचार भेजता है।

उदाहरण के लिए किसी व्यक्ति को संदेश मिलता है:

"आपका बैंक खाता बंद होने वाला है। तुरंत नीचे दिए गए लिंक पर क्लिक करके KYC अपडेट करें।"

व्यक्ति घबराकर लिंक खोलता है। नकली वेबसाइट पर बैंक संबंधी विवरण, पासवर्ड या अन्य जानकारी दर्ज करता है। यह जानकारी सीधे साइबर अपराधी तक पहुँच सकती है। ऐसी धोखाधड़ी में डर और जल्दबाजी का उपयोग किया जाता है।

समाधान:

• अनजान लिंक पर क्लिक न करें।

• संदेश में दी गई लिंक के बजाय संस्था की आधिकारिक वेबसाइट या ऐप का उपयोग करें।

• OTP, PIN और पासवर्ड किसी को न दें।

• "तुरंत करें", "खाता बंद हो जाएगा", "आपने इनाम जीता है" जैसे संदेशों से सावधान रहें।

• संदिग्ध संदेश की आधिकारिक माध्यम से पुष्टि करें।

4. स्मिशिंग और WhatsApp आधारित धोखाधड़ी

SMS के माध्यम से की जाने वाली फिशिंग को सामान्यतः "स्मिशिंग" कहा जाता है। आज WhatsApp और अन्य मैसेजिंग प्लेटफॉर्म के माध्यम से भी ऐसी धोखाधड़ी की जाती है।

नकली नौकरी, ऋण, इनाम, डिलीवरी, KYC, बिजली बिल, सरकारी सहायता और बैंकिंग सेवा के नाम पर लोगों से जानकारी या पैसे प्राप्त करने का प्रयास किया जाता है। कभी-कभी अपराधी किसी परिचित व्यक्ति का फोटो लगाकर नकली प्रोफाइल बनाता है और संदेश भेजता है, "मुझे तुरंत पैसे की जरूरत है।"

समाधान:
पैसे भेजने से पहले उस व्यक्ति को फोन करके या किसी अन्य विश्वसनीय माध्यम से उसकी पहचान की पुष्टि करनी चाहिए।
“डिजिटल दुनिया में पहचान से अधिक महत्वपूर्ण सत्यापन है।”

5. OTP और UPI फ्रॉड

डिजिटल भुगतान ने भारत में आर्थिक लेन-देन को अत्यंत सरल बना दिया है। लेकिन इसके साथ डिजिटल वित्तीय धोखाधड़ी के नए तरीके भी सामने आए हैं।
एक सामान्य गलतफहमी है कि “पैसे प्राप्त करने के लिए UPI PIN डालना पड़ता है।”
सामान्यतः पैसे प्राप्त करने के लिए UPI PIN दर्ज करने की आवश्यकता नहीं होती।
साइबर अपराधी अक्सर “पैसे भेजने के लिए QR कोड स्कैन करें”, “रिफंड प्राप्त करने के लिए PIN डालें” या “KYC के लिए OTP दें” जैसे बहाने बनाते हैं।
समाधान:
• UPI PIN केवल अधिकृत भुगतान के लिए ही दर्ज करें।
• OTP किसी के साथ साझा न करें।
• अनजान QR कोड के संबंध में सावधान रहें।
• किसी अनजान व्यक्ति के कहने पर स्क्रीन-शेयरिंग या रिमोट-एक्सेस ऐप इंस्टॉल न करें।
• संदिग्ध लेन-देन होने पर तुरंत बैंक और संबंधित साइबर अपराध व्यवस्था को सूचित करें।

6. पहचान की चोरी – Identity Theft

डिजिटल भुगतान ने भारत में आर्थिक लेन-देन को अत्यंत सरल बना दिया है। लेकिन इसके साथ डिजिटल वित्तीय धोखाधड़ी के नए तरीके भी सामने आए हैं।
एक सामान्य गलतफहमी है कि “पैसे प्राप्त करने के लिए UPI PIN डालना पड़ता है।”
सामान्यतः पैसे प्राप्त करने के लिए UPI PIN दर्ज करने की आवश्यकता नहीं होती।
साइबर अपराधी अक्सर “पैसे भेजने के लिए QR कोड स्कैन करें”, “रिफंड प्राप्त करने के लिए PIN डालें” या “KYC के लिए OTP दें” जैसे बहाने बनाते हैं।

समाधान:

• UPI PIN केवल अधिकृत भुगतान के लिए ही दर्ज करें।

• OTP किसी के साथ साझा न करें।

• अनजान QR कोड के संबंध में सावधान रहें।

• किसी अनजान व्यक्ति के कहने पर स्क्रीन-शेयरिंग या रिमोट-एक्सेस ऐप इंस्टॉल न करें।

• संदिग्ध लेन-देन होने पर तुरंत बैंक और संबंधित साइबर अपराध व्यवस्था को सूचित करें।

7. पासवर्ड की कमजोरी

पासवर्ड साइबर सुरक्षा की पहली दीवार है। लेकिन लोग अक्सर "123456", जन्मतिथि, मोबाइल नंबर या अपने नाम जैसे सरल पासवर्ड रखते हैं।

दूसरी बड़ी गलती एक ही पासवर्ड को अनेक खातों में इस्तेमाल करना है।

यदि किसी एक वेबसाइट का पासवर्ड लीक हो जाए और वही पासवर्ड ई-मेल या अन्य खाते में भी इस्तेमाल हो रहा हो, तो दूसरे खाते भी जोखिम में आ सकते हैं।

समाधान:

• प्रत्येक महत्वपूर्ण खाते के लिए अलग पासवर्ड रखें।

• लंबा और अनुमान लगाना कठिन पासफ्रेज उपयोगी है।

• जहाँ संभव हो Multi-Factor Authentication (MFA) सक्रिय करें।

• पासवर्ड मैनेजर का उचित उपयोग किया जा सकता है।

• जहाँ उपलब्ध हो, Passkey जैसी आधुनिक प्रमाणीकरण पद्धति अपनाएँ।

मजबूत पासवर्ड, सुरक्षित डिजिटल जीवन की पहली सीमा है।"

8. रैनसमवेयर : डिजिटल फिरौती

रैनसमवेयर एक प्रकार का दुर्भावनापूर्ण सॉफ्टवेयर है जो कंप्यूटर प्रणाली या फाइलों को अनुपलब्ध कर सकता है और फिर हमलावर फिरौती की माँग करता है।

ऐसे हमले से व्यक्ति के अलावा स्कूल, अस्पताल, कंपनी और सरकारी संस्था भी प्रभावित हो सकती है।

रैनसमवेयर का खतरा इसलिए गंभीर है क्योंकि इसमें केवल जानकारी की चोरी ही नहीं, बल्कि कामकाज के रुक जाने का भी खतरा होता है।

समाधान:

- महत्वपूर्ण डेटा का नियमित बैकअप लें।
- बैकअप को अलग और सुरक्षित स्थान पर रखें।
- समय-समय पर जाँचें कि बैकअप से डेटा वापस प्राप्त किया जा सकता है या नहीं।
- सॉफ्टवेयर को समय पर अपडेट करें।
- अनधिकृत सॉफ्टवेयर इंस्टॉल न करें।
- कर्मचारियों को फिशिंग के संबंध में प्रशिक्षण दें।
- संस्था में Incident Response Plan तैयार रखें।

9. मालवेयर और स्पायवेयर

Malware अर्थात Malicious Software का उपयोग कंप्यूटर या मोबाइल को नुकसान पहुँचाने, जानकारी चुराने या अनधिकृत गतिविधि करने के लिए किया जा सकता है।

स्पायवेयर व्यक्ति की गतिविधियों पर नजर रख सकता है और संवेदनशील जानकारी चुरा सकता है।

समाधान:

अनजान स्रोत से एप्लिकेशन डाउनलोड न करें। मोबाइल और कंप्यूटर के ऑपरेटिंग सिस्टम तथा एप्लिकेशन को समय पर अपडेट करें। ऐप को दी जाने वाली अनुमतियों पर ध्यान दें।

यदि कोई साधारण या मुफ्त ऐप अनावश्यक रूप से संपर्कों, संदेशों, माइक्रोफोन, कैमरे या अन्य संवेदनशील जानकारी की अनुमति माँगता है, तो सावधान होना चाहिए।

10. डेटा चोरी और गोपनीयता का उल्लंघन

डिजिटल युग में "जानकारी" अत्यंत मूल्यवान संपत्ति है।

व्यक्तिगत जानकारी, ग्राहकों का विवरण, कर्मचारियों के रिकॉर्ड, वित्तीय जानकारी, शैक्षणिक जानकारी और व्यावसायिक रहस्य चोरी हो सकते हैं।

डेटा चोरी से केवल आर्थिक नुकसान नहीं होता; व्यक्ति के निजता के अधिकार पर भी प्रभाव पड़ता है।

समाधान:

संस्थाओं को "जितना आवश्यक हो, उतना ही डेटा" एकत्र करने के सिद्धांत को अपनाना चाहिए।

संवेदनशील डेटा को उचित रूप से सुरक्षित रखना, जहाँ आवश्यक हो वहाँ एन्क्रिप्शन का उपयोग करना, पहुँच को नियंत्रित करना और पुराने या अनावश्यक डेटा का सुरक्षित निपटान करना आवश्यक है।

11. सोशल मीडिया : सुविधा या संकट?

Facebook, Instagram, YouTube, WhatsApp और अन्य सोशल मीडिया प्लेटफॉर्म ने संवाद और सूचना के आदान-प्रदान को सरल बनाया है। लेकिन अत्यधिक और लापरवाहीपूर्ण उपयोग जोखिमपूर्ण हो सकता है।

यदि कोई व्यक्ति अपनी हर गतिविधि सोशल मीडिया पर साझा करता है, तो अनजान लोग उसके बारे में बहुत कुछ जान सकते हैं।

इसके अलावा नकली प्रोफाइल, साइबर बुलिंग, फोटो का दुरुपयोग, अफवाह, धोखाधड़ी और गोपनीयता का उल्लंघन जैसी समस्याएँ उत्पन्न हो सकती हैं।

समाधान:

"पोस्ट करने से पहले सोचें" डिजिटल युग का महत्वपूर्ण नियम है।

किसी भी फोटो, वीडियो या व्यक्तिगत जानकारी को ऑनलाइन डालने से पहले सोचना चाहिए:

- क्या यह जानकारी सार्वजनिक करना वास्तव में आवश्यक है?
- क्या भविष्य में इसका दुरुपयोग हो सकता है?
- क्या इस पोस्ट से मेरी या किसी अन्य व्यक्ति की गोपनीयता प्रभावित होगी?

12. साइबर बुलिंग

साइबर बुलिंग का अर्थ डिजिटल माध्यम से किसी व्यक्ति को लगातार अपमानित करना, धमकी देना, परेशान करना, बदनाम करना या मानसिक रूप से प्रताड़ित करना है।

विद्यार्थियों में यह समस्या विशेष रूप से गंभीर हो सकती है। स्कूल में हुई घटना सोशल मीडिया के माध्यम से बहुत से लोगों तक पहुँच सकती है और पीड़ित विद्यार्थी पर लंबे समय तक मानसिक दबाव बना रह सकता है।

समाधान:

- साइबर बुलिंग को मजाक समझकर नजरअंदाज न करें।
- संदेश या स्क्रीनशॉट जैसे प्रमाण सुरक्षित रखें।
- माता-पिता या शिक्षक जैसे विश्वसनीय व्यक्ति को बताएँ।
- आवश्यकता होने पर संबंधित अधिकारियों को सूचित करें।
- स्कूलों में डिजिटल नागरिकता और साइबर अनुशासन की शिक्षा दें।

13. बच्चों और विद्यार्थियों के सामने साइबर जोखिम

आज के विद्यार्थी कम उम्र से ही स्मार्टफोन और इंटरनेट का उपयोग करते हैं। उन्हें ऑनलाइन गेमिंग, सोशल मीडिया, चैटिंग और वीडियो प्लेटफॉर्म में रुचि होती है।

बच्चे कभी-कभी अनजान व्यक्ति को मित्र समझ सकते हैं। वे अपनी व्यक्तिगत जानकारी, फोटो या अन्य विवरण साझा कर सकते हैं।

समाधान:

अभिभावकों को बच्चों की हर ऑनलाइन गतिविधि पर अविश्वास से निगरानी रखने के बजाय विश्वास और संवाद का वातावरण बनाना चाहिए।

बच्चों को समझाना चाहिए:

“ऑनलाइन अनजान व्यक्ति भी अनजान ही है, चाहे वह कितनी भी मीठी भाषा में बात करे।”

स्कूलों को भी साइबर सुरक्षा को जीवन-कौशल शिक्षा का हिस्सा बनाना चाहिए।

14. Deepfake और कृत्रिम बुद्धिमत्ता का खतरा

Artificial Intelligence मानवता के लिए क्रांतिकारी तकनीक है। यह शिक्षा, स्वास्थ्य, अनुसंधान, व्यवसाय और अनेक क्षेत्रों में उपयोगी है। लेकिन इसका दुरुपयोग भी संभव है।

Deepfake तकनीक के माध्यम से किसी व्यक्ति के चेहरे या आवाज को नकली रूप में प्रस्तुत किया जा सकता है।

कल्पना कीजिए कि किसी व्यक्ति को उसके परिचित की आवाज में फोन आता है:

"मुझे तुरंत पैसे चाहिए।"

आवाज वास्तविक लगने के कारण व्यक्ति धोखा खा सकता है।

समाधान:

AI के युग में "विश्वास करें, लेकिन सत्यापन अवश्य करें" का सिद्धांत अत्यंत महत्वपूर्ण है।

महत्वपूर्ण अनुरोध के लिए किसी दूसरे माध्यम से पुष्टि करनी चाहिए। केवल वीडियो देखकर यह मान लेना कि वह वास्तविक है या आवाज सुनकर यह मान लेना कि व्यक्ति वही है—जोखिमपूर्ण है।

15. नकली वेबसाइट और नकली एप्लिकेशन

साइबर अपराधी प्रसिद्ध कंपनियों या संस्थाओं जैसी दिखने वाली नकली वेबसाइट बना सकते हैं। नकली एप्लिकेशन के माध्यम से भी संवेदनशील जानकारी प्राप्त करने का प्रयास किया जा सकता है।

समाधान:

एप्लिकेशन केवल विश्वसनीय स्रोतों से ही इंस्टॉल करें। वेबसाइट का पता ध्यान से जाँचें। बहुत आकर्षक ऑफर, इनाम या छूट देखकर तुरंत विश्वास न करें।

16. सार्वजनिक Wi-Fi और असुरक्षित नेटवर्क

कैफे, रेलवे स्टेशन, हवाई अड्डे या अन्य सार्वजनिक स्थानों पर मिलने वाला Wi-Fi सुविधाजनक है, लेकिन अनजान नेटवर्क का उपयोग करते समय सावधानी आवश्यक है।

समाधान:

संवेदनशील बैंकिंग या अन्य महत्वपूर्ण कार्यों के लिए विश्वसनीय नेटवर्क का उपयोग करें। डिवाइस में अनजान Wi-Fi से स्वतः जुड़ने की सुविधा बंद रखना बेहतर है।

17. क्लाउड सुरक्षा

आज डेटा केवल हमारे कंप्यूटर में नहीं रहता। Google Drive, OneDrive, iCloud और अन्य क्लाउड सेवाओं में भी महत्वपूर्ण जानकारी संग्रहित रहती है।

क्लाउड सेवा सुरक्षित होने के बावजूद उपयोगकर्ता का कमजोर पासवर्ड या गलत एक्सेस सेटिंग जोखिम पैदा कर सकती है।

समाधान:

- मजबूत प्रमाणीकरण।
- Multi-Factor Authentication।
- एक्सेस अधिकारों की नियमित समीक्षा।
- संवेदनशील फाइलों के लिए उचित सुरक्षा।
- अनावश्यक शेयरिंग बंद करना।

18. Insider Threat – आंतरिक खतरा

हर साइबर हमला बाहर से ही हो, ऐसा आवश्यक नहीं है।

कभी-कभी संस्था के कर्मचारी की लापरवाही से डेटा लीक हो सकता है या कोई अधिकृत व्यक्ति जानबूझकर जानकारी का दुरुपयोग कर सकता है।

समाधान:

हर कर्मचारी को उतनी ही पहुँच दी जानी चाहिए जितनी उसके कार्य के लिए आवश्यक हो। इस सिद्धांत को Least Privilege कहा जाता है।

कर्मचारियों को साइबर सुरक्षा का नियमित प्रशिक्षण देना और संवेदनशील गतिविधियों की उचित निगरानी करना आवश्यक है।

19. स्कूलों के लिए साइबर सुरक्षा

आधुनिक शिक्षा व्यवस्था में स्कूल भी डिजिटल हो रहे हैं। विद्यार्थियों के रिकॉर्ड, उपस्थिति, परीक्षा परिणाम, फीस, कर्मचारियों की जानकारी और शैक्षणिक सामग्री डिजिटल प्रणाली में संग्रहित हो सकती है।

इसलिए स्कूल भी साइबर हमले का लक्ष्य बन सकते हैं।

स्कूलों को:

• मजबूत पासवर्ड नीति बनानी चाहिए।

• कर्मचारियों के लिए MFA का उपयोग करना चाहिए।

• महत्वपूर्ण डेटा का बैकअप रखना चाहिए।

• सॉफ्टवेयर अपडेट रखना चाहिए।

• विद्यार्थियों को साइबर सुरक्षा की शिक्षा देनी चाहिए।

• संवेदनशील जानकारी केवल अधिकृत व्यक्ति तक सीमित रखनी चाहिए।

• साइबर घटना होने पर किसे सूचना देनी है, इसकी स्पष्ट प्रक्रिया रखनी चाहिए।

स्कूल के लिए एक प्रभावी संदेश हो सकता है:

“सुरक्षित विद्यार्थी – जागरूक शिक्षक – जिम्मेदार डिजिटल समाज।”

20. शिक्षकों की भूमिका

शिक्षक केवल विषय का ज्ञान देने वाला व्यक्ति नहीं है; वह विद्यार्थी के जीवन में मार्गदर्शक भी है।

आज के शिक्षक को विद्यार्थियों को केवल “इंटरनेट का उपयोग कैसे करें” नहीं, बल्कि “इंटरनेट का सुरक्षित और जिम्मेदार उपयोग कैसे करें” भी सिखाना चाहिए।

शिक्षक विद्यार्थियों को फिशिंग, पासवर्ड, गोपनीयता, साइबर बुलिंग, नकली जानकारी और डिजिटल फुटप्रिंट के बारे में समझा सकता है।

इस प्रकार शिक्षा संस्था साइबर सुरक्षा के मजबूत स्तंभ के रूप में कार्य कर सकती है।

21. अभिभावकों की जिम्मेदारी

बच्चे को मोबाइल देना आसान है; लेकिन उसे सुरक्षित डिजिटल नागरिक बनाना अधिक महत्वपूर्ण है।

अभिभावकों को बच्चों से नियमित बातचीत करनी चाहिए। केवल "मोबाइल बंद करो" कहने के बजाय "आप ऑनलाइन क्या करते हैं?" यह समझने का प्रयास करना चाहिए।

यदि किसी अनजान व्यक्ति ने बच्चे से संपर्क किया हो या उसे ऑनलाइन कोई समस्या हुई हो, तो उसे डराने के बजाय सहायता करनी चाहिए।

"भय से अधिक प्रभावी सुरक्षा संवाद है।"

22. सरकार की भूमिका

साइबर सुरक्षा में सरकार की भूमिका अत्यंत महत्वपूर्ण है।

सरकार को साइबर अपराधों के विरुद्ध कानूनी ढाँचा मजबूत करना, साइबर पुलिस और जाँच एजेंसियों को प्रशिक्षण देना, नागरिकों में जागरूकता फैलाना और अंतरराष्ट्रीय सहयोग बढ़ाना आवश्यक है।

भारत में साइबर अपराध की शिकायत के लिए उपलब्ध आधिकारिक व्यवस्था का नागरिकों को उचित उपयोग करना चाहिए। वित्तीय धोखाधड़ी होने पर विलंब नहीं करना चाहिए, क्योंकि प्रारंभिक स्तर पर शीघ्र सूचना जाँच और धन के प्रवाह को रोकने के प्रयासों में सहायक हो सकती है।

सरकार, बैंक, दूरसंचार कंपनियाँ, तकनीकी कंपनियाँ और नागरिकों के बीच समन्वय आवश्यक है।

23. संस्थाओं के लिए Cyber Security Policy

किसी भी छोटी या बड़ी संस्था को साइबर सुरक्षा को केवल IT विभाग की जिम्मेदारी नहीं मानना चाहिए।

एक उचित Cyber Security Policy में निम्नलिखित बातें शामिल हो सकती हैं:

• पासवर्ड नीति
• MFA
• डेटा बैकअप
• एक्सेस नियंत्रण
• उपकरणों की सुरक्षा
• ई-मेल सुरक्षा
• सॉफ्टवेयर अपडेट
• कर्मचारी प्रशिक्षण
• Incident Response
• Disaster Recovery
• डेटा गोपनीयता

साइबर सुरक्षा में "आपदा के बाद उपाय" की अपेक्षा "आपदा से पहले तैयारी" अधिक प्रभावी है।

24. नियमित बैकअप का महत्व

डिजिटल डेटा नष्ट हो सकता है। कंप्यूटर खराब हो सकता है, मोबाइल खो सकता है, साइबर हमला हो सकता है या कोई कर्मचारी गलती से फाइल डिलीट कर सकता है।
इसलिए महत्वपूर्ण जानकारी का नियमित बैकअप रखना चाहिए।
लेकिन केवल बैकअप लेना पर्याप्त नहीं है। समय-समय पर यह जाँचना चाहिए कि बैकअप से जानकारी वापस प्राप्त की जा सकती है या नहीं।
"बैकअप डिजिटल दुनिया की बीमा पॉलिसी के समान है।"

25. Software Update क्यों आवश्यक है?

बहुत से लोग "Update Later" दबाकर सॉफ्टवेयर अपडेट को टाल देते हैं।
लेकिन सॉफ्टवेयर अपडेट में अक्सर सुरक्षा कमजोरियों के सुधार होते हैं। पुराना सॉफ्टवेयर हमलावर के लिए अवसर बन सकता है।
इसलिए ऑपरेटिंग सिस्टम, ब्राउज़र, एप्लिकेशन और सुरक्षा सॉफ्टवेयर को समय पर अपडेट करना चाहिए।

26. Cyber Hygiene – डिजिटल स्वच्छता

जैसे हम शरीर की स्वच्छता के लिए नियमित स्नान, हाथ धोना और साफ-सफाई रखते हैं, वैसे ही डिजिटल जीवन में भी “Cyber Hygiene” आवश्यक है।

डिजिटल स्वच्छता के कुछ नियम:

1. मजबूत और अलग पासवर्ड रखें।
2. MFA सक्रिय करें।
3. सॉफ्टवेयर अपडेट रखें।
4. संदिग्ध लिंक से बचें।
5. अनावश्यक एप्लिकेशन हटाएँ।
6. डेटा का बैकअप रखें।
7. गोपनीयता सेटिंग्स जाँचें।
8. अनजान डिवाइस से लॉगिन के प्रति सावधान रहें।
9. व्यक्तिगत जानकारी कम से कम सार्वजनिक करें।
10. संदिग्ध घटना तुरंत रिपोर्ट करें।

27. साइबर सुरक्षा में मानव जागरूकता का महत्व

तकनीक कितनी भी उन्नत क्यों न हो, यदि उपयोगकर्ता लापरवाह है तो सुरक्षा कमजोर हो सकती है।

एक कर्मचारी नकली ई-मेल पर क्लिक कर दे और पूरी संस्था की प्रणाली जोखिम में आ जाए—ऐसा संभव है।

इसलिए साइबर सुरक्षा का सबसे महत्वपूर्ण साधन केवल Firewall या Antivirus नहीं है; जागरूक मनुष्य भी उतना ही महत्वपूर्ण है।

“जागरूकता ही सुरक्षा की पहली कुंजी है।”

28. साइबर सुरक्षा और राष्ट्रीय सुरक्षा

साइबर हमला केवल व्यक्ति या कंपनी को नुकसान नहीं पहुँचाता। यदि किसी देश की बिजली, संचार, परिवहन, स्वास्थ्य या वित्तीय व्यवस्था को निशाना बनाया जाए तो उसका प्रभाव राष्ट्रीय स्तर पर हो सकता है।

इसलिए Cyber Security अब National Security का भी महत्वपूर्ण हिस्सा है। सरकार और महत्वपूर्ण संस्थाओं को Critical Infrastructure की सुरक्षा के लिए निरंतर निगरानी, बैकअप, वैकल्पिक व्यवस्था और Incident Response क्षमता विकसित करनी चाहिए।

29. क्या साइबर अपराधों के विरुद्ध कानून पर्याप्त है?

कानून आवश्यक है, लेकिन केवल कानून पर्याप्त नहीं है।

यदि नागरिक जागरूक न हो, संस्था सुरक्षा न बनाए रखे और कोई व्यक्ति स्वयं OTP दे दे, तो कानून बाद में अपराधी के विरुद्ध कार्रवाई कर सकता है; लेकिन नुकसान पहले ही हो सकता है।

इसलिए साइबर सुरक्षा में तीन बातों का संतुलन आवश्यक है:

कानून + तकनीक + जागरूकता

इन तीनों के साथ काम करने पर ही सुरक्षित डिजिटल समाज का निर्माण संभव है।

30. साइबर हमला होने पर क्या करें?

यदि किसी व्यक्ति को लगता है कि वह साइबर धोखाधड़ी का शिकार हुआ है, तो घबराना नहीं चाहिए।

सबसे पहले प्रभावित खाते या सेवा को सुरक्षित करें। आवश्यकता होने पर पासवर्ड बदलें, बैंक को तुरंत सूचित करें, कार्ड या संबंधित सेवा को ब्लॉक करवाएँ और संबंधित अधिकारियों के पास शिकायत करें।

महत्वपूर्ण प्रमाण—जैसे संदेश, फोन नंबर, ई-मेल, लेन-देन का विवरण और स्क्रीनशॉट—सुरक्षित रखें।

सबसे महत्वपूर्ण:

“साइबर अपराध की शिकायत करने में शर्म नहीं, सावधानी और साहस आवश्यक है।”

31. डिजिटल फुटप्रिंट

इंटरनेट पर हम जो कुछ भी करते हैं, उसका कोई न कोई डिजिटल निशान रह सकता है। पोस्ट, फोटो, कमेंट, लाइक, सर्च और ऑनलाइन अकाउंट हमारे डिजिटल व्यक्तित्व का निर्माण करते हैं।

विद्यार्थियों को विशेष रूप से समझना चाहिए कि आज मजाक में की गई पोस्ट भविष्य में भी प्रभाव डाल सकती है।

इसलिए पोस्ट करने से पहले सोचना चाहिए:

"क्या मैं यही बात पाँच वर्ष बाद भी सार्वजनिक रूप से देख सकूँगा?"

यदि उत्तर "नहीं" है, तो शायद उस पोस्ट को करने की आवश्यकता नहीं है।

32. Fake News और सूचना की जाँच

साइबर सुरक्षा केवल कंप्यूटर बचाने की बात नहीं है। गलत जानकारी से समाज में भय, अफवाह और विवाद भी उत्पन्न हो सकते हैं।

WhatsApp या सोशल मीडिया पर आया हर संदेश सत्य हो, यह आवश्यक नहीं है।

समाधान:

• समाचार का स्रोत जाँचें।

• आधिकारिक स्रोत से तुलना करें।

• तारीख जाँचें।

• देखें कि पुरानी तस्वीर को नई घटना के रूप में तो प्रस्तुत नहीं किया गया।

• भावनात्मक या भड़काऊ संदेश को तुरंत फॉरवर्ड न करें।

"बिना सोचे फॉरवर्ड करना भी डिजिटल लापरवाही है।"

33. भविष्य की साइबर चुनौतियाँ

आने वाले वर्षों में तकनीक और विकसित होगी। AI, Quantum Computing, IoT, Autonomous Systems और Cloud Technologies के विकास के साथ साइबर जोखिमों का स्वरूप भी बदलता जाएगा।

इसलिए भविष्य की साइबर सुरक्षा के लिए निरंतर अनुसंधान, प्रशिक्षण और नवाचार आवश्यक है।AI का उपयोग हमलावर भी कर सकते हैं और सुरक्षा विशेषज्ञ भी। इसलिए भविष्य में कई बार मुकाबला मनुष्य बनाम मनुष्य से आगे बढ़कर AI बनाम AI का भी हो सकता है।

34. साइबर सुरक्षा के लिए सामूहिक जिम्मेदारी

साइबर सुरक्षा केवल सरकार की जिम्मेदारी नहीं है।

इसमें सभी की भूमिका है:

नागरिक – जागरूक और जिम्मेदार डिजिटल व्यवहार करे।

विद्यार्थी – तकनीक का सुरक्षित और नैतिक उपयोग करे।

शिक्षक – डिजिटल जागरूकता फैलाए।

अभिभावक – बच्चों के साथ संवाद बनाए रखें।

कंपनी – ग्राहक और कर्मचारी के डेटा की सुरक्षा करे।

तकनीकी कंपनी – सुरक्षित उत्पाद बनाए।

सरकार – कानून, ढाँचा, प्रशिक्षण और क्रियान्वयन सुनिश्चित करे।

जब ये सभी मिलकर कार्य करेंगे तभी साइबर सुरक्षा मजबूत हो सकेगी।

35. साइबर सुरक्षा के दस स्वर्णिम नियम

प्रत्येक नागरिक को निम्नलिखित दस नियम याद रखने चाहिए:

1. OTP कभी किसी को न दें।
2. UPI PIN पैसे प्राप्त करने के लिए आवश्यक नहीं है।
3. अनजान लिंक पर क्लिक न करें।
4. प्रत्येक महत्वपूर्ण खाते के लिए अलग और मजबूत पासवर्ड रखें।
5. जहाँ संभव हो Multi-Factor Authentication चालू करें।
6. मोबाइल और कंप्यूटर को अपडेट रखें।
7. महत्वपूर्ण डेटा का बैकअप रखें।
8. सोशल मीडिया पर व्यक्तिगत जानकारी अत्यधिक साझा न करें।
9. नकली फोन, ई-मेल या AI-generated आवाज/वीडियो के प्रति सावधान रहें।
10. संदेह होने पर रुकें और स्वतंत्र रूप से सत्यापन करें।

ये तीन कदम अनेक ऑनलाइन धोखाधड़ियों को रोकने में सहायता कर सकते हैं।

36. “रुकें – सोचें – जाँचें” : सरल सुरक्षा मंत्र

साइबर धोखाधड़ी से बचने के लिए एक सरल मंत्र अपनाया जा सकता है:
रुकें।जल्दबाजी में कोई निर्णय न लें।सोचें।
क्या यह संदेश वास्तव में विश्वसनीय है?जाँचें।आधिकारिक माध्यम से इसकी पुष्टि करें।

37. तकनीक का विरोध नहीं, जिम्मेदार उपयोग

साइबर जोखिम के कारण हम तकनीक का उपयोग बंद नहीं कर सकते। तकनीक मानव प्रगति का शक्तिशाली साधन है।
प्रश्न यह नहीं है कि “तकनीक अच्छी है या बुरी?”
प्रश्न यह है:
“तकनीक का उपयोग कौन करता है, कैसे करता है और कितनी जिम्मेदारी से करता है?”
चाकू रसोई में भी उपयोगी है और नुकसान पहुँचाने के लिए भी इस्तेमाल किया जा सकता है। उसी प्रकार इंटरनेट ज्ञान और प्रगति का साधन भी है और अपराध का साधन भी बन सकता है।
इसलिए समाधान तकनीक से दूर जाना नहीं है; सुरक्षित और जिम्मेदार तकनीक उपयोग सीखना है।

38. साइबर सुरक्षा और नैतिकता

साइबर सुरक्षा का एक महत्वपूर्ण पहलू “Cyber Ethics” है।
किसी दूसरे का पासवर्ड जान लेना इसका अर्थ नहीं कि उसके खाते का उपयोग करने की अनुमति मिल गई। किसी की व्यक्तिगत तस्वीर बिना अनुमति साझा करना उचित नहीं है। नकली पहचान बनाकर किसी को धोखा देना अपराध है। किसी की प्रणाली में अनधिकृत रूप से प्रवेश करने का प्रयास भी अनैतिक और गैरकानूनी है।
इसलिए विद्यार्थियों को तकनीक का ज्ञान देने के साथ-साथ नैतिक जिम्मेदारी भी सिखानी चाहिए।

39. सुरक्षित डिजिटल भारत का सपना

भारत तेजी से डिजिटल हो रहा है। डिजिटल भुगतान, ऑनलाइन शिक्षा, ई-गवर्नेंस और डिजिटल सेवाओं का विस्तार देश के विकास के लिए महत्वपूर्ण है।

लेकिन डिजिटल भारत तभी सफल माना जाएगा जब वह सुरक्षित डिजिटल भारत भी बने।

डिजिटल विकास के साथ साइबर जागरूकता, डेटा सुरक्षा, डिजिटल साक्षरता और साइबर रक्षा को मजबूत करना आवश्यक है।

हर गाँव, स्कूल, कॉलेज और शहर तक साइबर जागरूकता पहुँचनी चाहिए।

उपसंहार----------

साइबर सुरक्षा आज के युग की वैकल्पिक आवश्यकता नहीं है; यह मूलभूत आवश्यकता है।

जिस प्रकार हम अपने घर का ताला बंद करते हैं, वाहन चलाते समय हेलमेट या सीट बेल्ट का उपयोग करते हैं और अपने स्वास्थ्य की देखभाल करते हैं, उसी प्रकार डिजिटल जीवन की सुरक्षा करना भी आवश्यक है।

आज साइबर अपराधों का स्वरूप तेजी से बदल रहा है। फिशिंग, ऑनलाइन वित्तीय धोखाधड़ी, पहचान की चोरी, डेटा लीक, रैनसमवेयर, साइबर बुलिंग, नकली वेबसाइट, मालवेयर, सोशल मीडिया फ्रॉड और AI आधारित Deepfake जैसे खतरे हमारे सामने हैं।

लेकिन समस्या बड़ी है, इसलिए समाधान असंभव नहीं है।

मजबूत पासवर्ड, Multi-Factor Authentication, नियमित अपडेट, बैकअप, डेटा गोपनीयता, साइबर शिक्षा, कानूनी व्यवस्था, तकनीकी सुरक्षा और सबसे महत्वपूर्ण —मानवीय जागरूकता—के माध्यम से हम साइबर जोखिमों के विरुद्ध मजबूत बन सकते हैं।

हमें याद रखना चाहिए कि साइबर अपराधी अक्सर हमारे अज्ञान और जल्दबाजी का लाभ उठाता है। इसलिए हर संदेश पर तुरंत विश्वास नहीं करना चाहिए, हर लिंक नहीं खोलना चाहिए, हर फोन कॉल को वास्तविक नहीं मानना चाहिए और इंटरनेट पर दिखाई देने वाली हर चीज को सत्य नहीं मानना चाहिए।

डिजिटल युग का सबसे बड़ा सुरक्षा मंत्र शायद इतना सरल है:

“रुकें, सोचें, जाँचें और फिर ही क्लिक करें।”

हमें ऐसी पीढ़ी का निर्माण करना होगा जो केवल तकनीक का उपयोग करना न जानती हो, बल्कि उसका सुरक्षित, जिम्मेदार और नैतिक उपयोग भी जानती हो।

सरकार कानून बना सकती है, कंपनियाँ सुरक्षा प्रणालियाँ विकसित कर सकती हैं और विशेषज्ञ उन्नत तकनीक तैयार कर सकते हैं; लेकिन अंततः प्रत्येक नागरिक की एक छोटी-सी सावधानी पूरे समाज को बड़ी सुरक्षा प्रदान कर सकती है।

अंत में एक विचार अत्यंत उपयुक्त है:

“डिजिटल दुनिया में सुरक्षा किसी एक दिन का कार्य नहीं है; यह हर दिन की आदत है।”

इसलिए हमें तकनीक से डरना नहीं चाहिए, बल्कि उसे समझना चाहिए; इंटरनेट से दूर नहीं भागना चाहिए, बल्कि उसका जिम्मेदारी से उपयोग करना चाहिए; और साइबर जोखिम को केवल सरकार की समस्या न मानकर अपनी व्यक्तिगत जिम्मेदारी भी समझना चाहिए।

जागरूक नागरिक, सुरक्षित डिजिटल व्यवस्था और जिम्मेदार तकनीक—इन तीनों के समन्वय से ही सुरक्षित, सशक्त और प्रगतिशील डिजिटल भारत का निर्माण संभव है।

"साइबर सुरक्षा केवल कंप्यूटर की सुरक्षा नहीं है; यह हमारे विश्वास, पहचान, संपत्ति, निजता और पूरे डिजिटल भविष्य की सुरक्षा है।"

सुरक्षित रहें, सजग रहें और जिम्मेदार डिजिटल नागरिक बनें।

- हर्ष धीरेन्द्रकुमार सोनी

लेखक परिचय

नाम – हर्ष धीरेन्द्रकुमार सोनी
जीए-1 (भूतल), कल्प डिज़ायर फ्लैट,
सहयोग पेट्रोल पंप के सामने,
प्रमुख स्वामी महाराज सर्कल के पास,
मालपुर रोड, खालीकपुर,
मोडासा,
जिला अरावली, गुजरात

पं.क्र. (04/21/05/207665/19)

अन्तरा शब्दशक्ति

www.antrashabdshakti.com

प्रकाशन एवं बहुद्देशीय संस्था

अन्तरा शब्दशक्ति
प्रकाशन

कलम की शक्ति, समाज की दिशा

सम्मान-पत्र

यह प्रमाणित किया जाता है कि

आ.....**हर्ष धीरेन्द्रकुमार सोनी**.....जी

ने हिन्दी पखवाड़े के अवसर पर आयोजित "**एक लेख प्रतियोगिता**" में उत्साहपूर्वक सहभागिता करते हुए **समसामयिक विषय पर अपने विचारों को** प्रभावी एवं सार्थक ढंग से अभिव्यक्त किया।

उनकी साहित्यिक **अभिव्यक्ति** एवं रचनात्मक सहभागिता की सराहना करते हुए **अन्तरा शब्दशक्ति प्रकाशन** की ओर से यह **सम्मान-पत्र** सादर प्रदान किया जाता है।

आपकी सृजनशीलता एवं साहित्यिक यात्रा के उज्ज्वल भविष्य की हार्दिक शुभकामनाएँ।

हिन्दी विचारों को विस्तार देती है... समाज को जोड़ती है...

हिंदी
हमारी पहचान...
हमारी शक्ति...

प्रीति सुराना

समकित सुराना

अन्तरा शब्दशक्ति प्रकाशन एवं संस्था

डॉ. प्रीति समकित सुराना

शब्द से संवेदन तक... लेखन से परिवर्तन तक...