



कृषि में साइबर सुरक्षा का महत्व

हिमांशु*, विक्रम सिंह**, एन. पी. सिंह*** और एन. के. दहिया****

इलेक्ट्रॉनिक उपकरणों, नेटवर्क और संवेदनशील डेटा को अनधिकृत पहुंच, चोरी, क्षति या अन्य दुर्भावनापूर्ण हमलों से बचाने के अभ्यास को साइबर सुरक्षा अथवा सूचना सुरक्षा के रूप में भी जाना जाता है। इसमें हैकिंग, फिशिंग, वायरस और अन्य साइबर खतरों से सुरक्षा करना शामिल है। साइबर सुरक्षा उपायों में सिस्टम और डेटा को अनधिकृत पहुंच या क्षति को होने से रोकने के लिए फायरवॉल, एन्क्रिप्शन, पासवर्ड सुरक्षा और अन्य उपकरणों का उपयोग किया जाता है। संवेदनशील जानकारी की सुरक्षा एवं गोपनीयता बनाए रखने और वित्तीय नुकसान या अन्य नकारात्मक परिणामों को रोकने के लिए व्यक्तियों, व्यवसायों और सरकारों के लिए साइबर सुरक्षा बहुत महत्वपूर्ण है।

भारत की खाद्य आपूर्ति शृंखला की सुरक्षा और कृषि उत्पादों की सुरक्षा सुनिश्चित करने के लिए कृषि में साइबर सुरक्षा का अत्यधिक महत्व है। जैसे-जैसे कृषि तेजी से डिजिटल होती जा रही है, किसानों, पशुपालकों और अन्य कृषि व्यावसायिक के लिए साइबर सुरक्षा संबंधित जोखिमों से अवगत होना और संभावित साइबर खतरों से अपने उपक्रम को बचाने

*वरिष्ठ वैज्ञानिक; **वरिष्ठ वैज्ञानिक; ***मुख्य तकनीकी अधिकारी; ****सहायक मुख्य तकनीकी अधिकारी, भारतीय कृषि अनुसंधान परिषद, नई दिल्ली-110012

के लिए कदम उठाना जरूरी होता जा रहा है।

किसी संगठन में सूचना सुरक्षा, उनकी सूचना संपत्तियों की गोपनीयता, अखंडता और उपलब्धता की रक्षा के लिए डिजाइन की गई प्रथाओं, नीतियों और तकनीकों इत्यादि को संदर्भित करती है। इन सूचना संपत्तियों में संवेदनशील डेटा, जैसे-ग्राहकों की जानकारी, वित्तीय रिकॉर्ड और बौद्धिक संपदा, साथ ही साथ संगठन के हार्डवेयर, सॉफ्टवेयर और नेटवर्क आदि महत्वपूर्ण हैं। एक सुदृढ़ एवं प्रभावी सूचना सुरक्षा के संभावित जोखिमों और कमजोरियों की पहचान करना और

उनका आकलन करना, उचित सुरक्षा उपायों एवं नियंत्रणों को विकसित करना, लागू करना और उभरते खतरों के साथ सामंजस्य के लिए इन उपायों की लगातार निगरानी और अद्यतन करना भी बहुत जरूरी होता है।

कृषि में साइबर सुरक्षा उपायों में साइबर खतरों से बचाव के लिए फायरवॉल, घुसपैठ का पता लगाने वाली प्रणाली और अन्य नेटवर्क सुरक्षा उपायों को लागू करना सर्व प्रमुख है। इसमें कृषि प्रौद्योगिकी में कार्यरत कर्मचारियों को साइबर सुरक्षा की सर्वोत्तम प्रथाओं पर प्रशिक्षण देना भी शामिल है, जैसे कि संभावित खतरों की पहचान और रिपोर्ट कैसे करें।

कृषि को प्रतिकूल रूप से प्रभावित करने वाले कुछ विशिष्ट साइबर सुरक्षा खतरों में रैंसमवेयर हमले, जो कि महत्वपूर्ण कृषि डेटा को लॉक कर सकते हैं तथा संवेदी उपकरण या स्वचालित सिंचाई प्रणाली जैसे उपकरणों की हैकिंग और वित्तीय जानकारी या बौद्धिक संपदा जैसे संवेदनशील डेटा की चोरी आदि शामिल हैं। कृषि व्यवसायों में इलेक्ट्रॉनिक उपकरणों और डेटा को पर्याप्त रूप से सुरक्षित करने में विफलता के परिणामस्वरूप वित्तीय नुकसान, प्रतिष्ठा की क्षति और यहां तक कि उपभोक्ताओं के लिए सुरक्षा खतरे की आशंका भी हो सकती है। कृषि, प्रौद्योगिकी और डिजिटल प्रणालियों पर निर्भर होती जा रही है। इसमें निम्न क्षेत्र हैं, जो साइबर अपराध के प्रति संवेदनशील हैं:

- **स्मार्ट कृषि:** ये प्रणालियां खेती के तरीकों को अनुकूलित करने के लिए सेंसर, जीपीएस और अन्य तकनीकों का उपयोग करती हैं। वे साइबर हमले के प्रति संवेदनशील हैं और



भाकृअनुप में साइबर सुरक्षा पर सम्मेलन

कैसे करें साइबर सुरक्षा

कुछ प्रमुख साइबर सुरक्षा सर्वोत्तम प्रथाएं जिनका पालन करके, आप अपने डिवाइस, डेटा और नेटवर्क को साइबर खतरों से सुरक्षित रखने में सहायता कर सकते हैं, निम्नानुसार हैं:

- **मजबूत पासवर्ड:** मजबूत पासवर्ड, जिसका अनुमान लगाना मुश्किल हो और जिसमें अपरकेस और लोअरकेस अक्षरों, संख्याओं और विशेष वर्णों का मिश्रण हो, का उपयोग करें।
- जहां भी संभव हो मल्टी-फैक्टर ऑथेंटिकेशन (एमएफए) का इस्तेमाल करें।
- यह सुनिश्चित करने के लिए कि आपके पास नवीनतम सुरक्षा पैच और बग फिक्स हैं, अपने ऑपरेटिंग सिस्टम, एंटी-वायरस सॉफ्टवेयर और अन्य एप्लिकेशन सहित अपने सॉफ्टवेयर को नियमित रूप से अपडेट करें।
- हमले या सिस्टम की विफलता के कारण डेटा हानि को रोकने के लिए नियमित रूप से डेटा का बैकअप लें।
- संवेदनशील डेटा और सिस्टम तक पहुंच केवल उन्हीं तक सीमित करें, जिन्हें इसकी आवश्यकता है। उपयोगकर्ता भूमिकाओं, अनुमतियों और विभाजन जैसे अभिगम नियंत्रणों को लागू करें।
- कर्मचारियों को साइबर सुरक्षा की सर्वोत्तम प्रथाओं पर प्रशिक्षित करें और सुरक्षा जागरूकता की व्यवस्था बनाएं।
- संदिग्ध गतिविधि के लिए नियमित रूप से अपने नेटवर्क की निगरानी करें और किसी भी विसंगति की जांच करें।
- साइबर सुरक्षा की घटनाओं का जवाब देने के लिए एक योजना विकसित करें, जिसमें किससे संपर्क करना है, क्या कदम उठाने हैं और घटना से कैसे उबरना है, आदि जानकारी का समायोजन हो।

इन प्रणालियों को आधार देने वाले डेटा संग्रह और विश्लेषण को बाधित कर सकते हैं।

- **फार्म प्रबंधन सॉफ्टवेयर:** कई किसान वित्तीय लेनदेन, सूची प्रबंधन और कर्मचारी रिकॉर्ड सहित अपने कार्यों का प्रबंधन करने के लिए सॉफ्टवेयर का उपयोग करते हैं। इन प्रणालियों को साइबर अपराधियों द्वारा लक्षित किया जा सकता है, जो डेटा चोरी करने या इसे फिरौती के लिए रखने की मांग कर सकते हैं।
- **स्वायत्त वाहन:** कुछ फार्म स्वायत्त वाहनों का उपयोग फसलों के रोपण, कटाई और छिड़काव जैसे कार्यों के लिए कर रहे हैं। ये वाहन इंटरनेट से जुड़े होते हैं। साइबर हमलों के प्रति संवेदनशील हो सकते हैं और नियंत्रण प्रणाली से समझौता कर सकते हैं।
- **आपूर्ति शृंखला प्रबंधन:** कृषि आपूर्ति शृंखला जटिल होती है, जिसमें कई पार्टियां और प्रौद्योगिकियां शामिल होती हैं। ये सिस्टम साइबर हमले के प्रति संवेदनशील होती हैं, जो माल के प्रवाह को बाधित कर सकते हैं



साइबर अपराध से बचाव

या संवेदनशील डेटा से समझौता कर सकते हैं।

- **जैव प्रौद्योगिकी:** कृषि में जैव प्रौद्योगिकी एक तेजी से उभरता हुआ महत्वपूर्ण उपकरण है, जिसमें आनुवंशिक रूप से संशोधित फसलों और जीन संपादन तकनीकों का उपयोग पैदावार में सुधार और पर्यावरणीय प्रभावों को कम करने के लिए किया जा रहा है। ये प्रौद्योगिकियां साइबर हमलों के प्रति संवेदनशील हैं, जो अनुसंधान डेटा या बौद्धिक संपदा को लीक कर सकते हैं।
- कृषि उद्योग में किसानों और अन्य हितधारकों के लिए यह महत्वपूर्ण है कि वे इन कमजोरियों से अवगत रहें और अपने सिस्टम और डेटा को साइबर अपराध से बचाने के लिए कदम उठाएं।
- कृषि व्यापार में वित्तीय लेन-देन को

सुरक्षित रखने के लिए कुछ अन्य प्रमुख सावधानियां इस प्रकार हैं:

- सुनिश्चित करें कि आप एक प्रतिष्ठित वित्तीय संस्थान का उपयोग करते हैं, जिसके पास आपके लेनदेन की सुरक्षा के लिए मजबूत सुरक्षा उपाय हैं।
- अपने ऑनलाइन खातों के लिए मजबूत पासवर्ड का इस्तेमाल करें और उन्हें नियमित रूप से बदलते रहें। अनुमान लगाने में आसान पासवर्ड का उपयोग करने से बचें।
- अपने सभी ऑनलाइन अकाउंट्स खासकर वित्तीय लेनदेन के लिए टू-फैक्टर ऑथेंटिकेशन को सक्षम करें।
- स्कैमर अक्सर फिशिंग ईमेल या संदेश भेजते हैं, जो आपको आपके लॉगिन क्रेडेंशियल देने के लिए बरगलाने की कोशिश करते हैं। किसी भी अवांछित

ईमेल या संदेशों से सावधान रहें और किसी भी संदिग्ध लिंक पर क्लिक न करें।

- सार्वजनिक वाई-फाई नेटवर्क अक्सर असुरक्षित होते हैं, जिससे हैकर्स के लिए आपके डेटा में संध लगाना आसान हो जाता है। वित्तीय लेनदेन के लिए सार्वजनिक वाई-फाई नेटवर्क का उपयोग करने से बचें।
- यह सुनिश्चित करने के लिए कि कोई अनधिकृत लेनदेन तो नहीं हो रहा है, अपने खातों की नियमित रूप से जांच करें। यदि आपको कोई संदिग्ध गतिविधि दिखाई देती है, तो इसकी सूचना तुरंत अपने वित्तीय संस्थान को दें।

इन सावधानियों को अपनाकर आप कृषि व्यवसाय में वित्तीय लेन-देन को सुरक्षित रखने में मदद कर सकते हैं और खुद को धोखाधड़ी और पहचान की चोरी से बचा सकते हैं। ■

साइबर सुरक्षा के मायने

सूचना सुरक्षा में सामान्यतः अभिगम नियंत्रण के उपायों का उपयोग किया जाता है, जिसमें पासवर्ड और बायोमीट्रिक प्रमाणीकरण, पारगमन में डेटा का एन्क्रिप्शन, फायरवॉल और घुसपैठ का पता लगाने वाली प्रणालियां, नियमित बैकअप एवं आपदा पुनर्प्राप्ति ढांचा और नियमित कर्मचारी प्रशिक्षण तथा जागरूकता कार्यक्रमों का बहुत महत्वपूर्ण योगदान होता है। संवेदनशील जानकारी को संभालने वाले प्रत्येक संगठन के लिए सूचना सुरक्षा एक महत्वपूर्ण आयाम है। कृषि में साइबर सुरक्षा का मुख्य लक्ष्य अनधिकृत पहुंच, चोरी, क्षति या अन्य दुर्भावनापूर्ण हमलों से कृषि कार्यों में उपयोग किए जाने वाले इलेक्ट्रॉनिक उपकरणों, नेटवर्क और डेटा की सुरक्षा करना है। आधुनिक कृषि पद्धतियों में इंटरनेट ऑफ थिंग्स (IoT) उपकरणों, ड्रोन और अन्य तकनीकों के उपयोग के साथ कृषि भी तेजी से प्रौद्योगिकी पर निर्भर हो गई है। प्रौद्योगिकी पर इस बढ़ती निर्भरता का अर्थ यह भी है कि कृषि साइबर खतरों के प्रति अधिक संवेदनशील होती जा रही है।

लेखकों से अनुरोध

आज सूचना प्रौद्योगिकी के बदले हुए कदमों को हमारे पाठक और लेखक दोनों ने पहचाना है। पाठकगण लेखकों से सीधी बात कर सकें। इसलिए हम चाहते हैं कि सभी लेखक अपने लेख के साथ अपना ई-मेल पता तथा मोबाइल नम्बर अवश्य दें।

—संपादक