पर्यवेक्षण विभाग

साइबर सुरक्षा और सूचना प्रौद्योगिकी परीक्षा (CSITE)

"साइबर सुरक्षा जागरूकता माह - अक्टूबर 2024: ईमेल बुलेटिन भाग 2 "

"साइबर सुरक्षा: सुरक्षा की संस्कृति का विकास"

चूंकि हम साइबर सुरक्षा पर अपना ध्यान केंद्रित करना जारी रखते हैं, इसलिए यह पहचानना महत्वपूर्ण है कि हमारे डिजिटल वातावरण को सुरक्षित रखना एक सतत प्रतिबद्धता है। जिस तरह हम अपनी व्यक्तिगत सुरक्षा के प्रति सतर्क रहते हैं, उसी तरह हमें अपने ऑनलाइन इंटरैक्शन के लिए भी उतनी ही सावधानी बरतनी चाहिए। इस बुलेटिन में, हम अपने सामूहिक सुरक्षा प्रयासों को सुदृढ़ करने के लिए आठ आवश्यक साइबर सुरक्षा आदतें प्रस्तुत करते हैं।

कण्ट्रोल एक्सेस :

- आप यह सुनिश्चित करें कि,परिसर में प्रवेश करने के लिए अपने सुरक्षित प्रवेश क्रेडेंशियल का उपयोग करें और उन्हें दूसरों के साथ साझा न करें।

डेटा सुरक्षित रखें:

- संवेदनशील जानकारी की सुरक्षा और डेटा उल्लंघन को रोकने के लिए हमेशा एन्क्रिप्शन और मजबूत पासवर्ड का उपयोग करें।

सुरक्षित उपकरण:

- उपयोग में न होने पर अपने डिवाइस को लॉक करके तथा स्वीकृत सुरक्षा सॉफ्टवेयर का उपयोग करके सुरक्षित रखें।

नेटवर्क सुरक्षा:

- गोपनीय सिस्टम तक पहुँचते समय सुरक्षित नेटवर्क से कनेक्ट करें। दूरस्थ कार्य के लिए वीपीएन का उपयोग करें और संवेदनशील गतिविधियों के लिए सार्वजनिक वाई-फाई से बचें।

ईमेल सुरक्षा/सुरक्षित ब्राउज़िंग:

- अज्ञात लिंक या अटैचमेंट से बचें, जानकारी साझा करने से पहले प्रेषक को सत्यापित करें। सुरक्षित ब्राउज़िंग के लिए हमेशा HTTPS का उपयोग करें।

घटना की रिपोर्टिंग:

- संदिग्ध गतिविधि या उल्लंघनों की सूचना तुरंत अपने बैंक/आईटी विभाग को दें। शीघ्र रिपोर्टिंग क्षति को रोकती है और प्रतिक्रिया को गति देती है।

सोशल इंजीनियरिंग सतर्कता:

- जानकारी चुराने के उद्देश्य से impersonation जैसी चालों से सावधान रहें। गोपनीय जानकारी के लिए अनुरोधों की हमेशा पुष्टि करें ।

संसाधन:

- साइबर सुरक्षा प्रोटोकॉल पर नियमित प्रशिक्षण सत्रों में भाग लें और संभावित खतरों को पहचानना सीखें।