साईबर सुरक्षा के संबंध में एडवायरी जारी

जयपुर, 14 अगस्त। मुख्य सचिवों के तृतीय राष्ट्रीय सम्मेलन में ''साइबर सुरक्षा: उभरती चुनौतियाँ'' से संबंधित बिन्दुओं के संदर्भ में संवाद किश गया था। इस बारे में सूचना प्रौद्योगिकी एवं संचार विभाग ने साईबर सुरक्षा पर जमीनी स्तर पर साइबर सुरक्षा के प्रति जागरूकता को बढावा देने के लिए फिशिंग मेल और मजबूत पासवर्ड के उपयोग के संबंध में एडवायरी गृह विभाग में प्रषित की है।

साईबर सुरक्षा पर जमीनी स्तर पर साइबर स्वच्छता के प्रति जागरूकता को बढावा देने के लिए फिशिंग मेल और मजबूत पासवर्ड के उपयोग के संबंध में जारी एडवायजरी में का सोशल मीडिया एवं अन्य माध्यमों से व्यापक प्रचार-प्रसार कर आमजन को जागरूक बनाने की आवश्यकता बताई गई है।

एडवाइजरी के अनुसार सावधान और संशयी रहें, ईमेल को हमेशा सावधानी से देखें, खासकर अज्ञात या संदिग्ध स्रोतों से। प्रेषक को सत्यापित करें, प्रेषक के ईमेल पते की जाँच करें और सुनिश्चित करें कि यह उस संगठन की आधिकारिक संपर्क जानकारी से मेल खाता है जिसका वे प्रतिनिधित्व करने का दावा करते हैं।

वर्तनी और व्याकरण की त्रुटियों की जाँच करें, फिशिंग ईमेल में अक्सर टाइपिंग, व्याकरण संबंधी गलतियों या अजीब भाषा होती है। अनजान लिंक को न खोलें।

क्लिक करने से पहले होवर करें: वास्तविक URL को प्रकट करने के लिए ईमेल सुनिश्चित करें कि URL ईमेल में प्रदर्शित किए गए URL से मेल खाता है और यह कोई भ्रामक लिंक नहीं है। सॉफ्टवेयर को अद्यतित रखें, ज्ञात कमजोरियों से बचाने के लिए अपने ईमेल क्लांइट, वेब ब्राउजर और ऑपरेटिंग सिस्टम को नियमित रूप से अपडेट करें। मजबूत, अद्वितीय पासवर्ड का उपयोग करें मज़बूत पासवर्ड बनाएं और उन्हें सुरक्षित रूप से संग्र हित करने के लिए पासवर्ड मैनेजर का उपयोग करें।

कारक प्रमाणीकरण सक्षम करें, अपने ईमेल खाते के लिए सुरक्षा की एक अतिरिक्त परत प्रदान करने के लिए जब भी संभव हो 2FA सक्षम करें। खुद को शिक्षित करें, नवीनतम फ़िशिंग तकनीकों और घोटालों के बारे में जानकारी रखें ताकि उन्हें बेहतर ढंग से पहचाना जा सके और उनसे बचा जा सके

संदिग्ध लिंक पर क्लिक न करें ईमेल में दिए गए लिंक पर क्लिक करने से बचें, जब तक कि आप उनकी प्रामाणिकता के बारे में आश्वस्त न हों। अज्ञात स्रोतों से अटैचमेंट डाउनलोड न करें: अटैचमेंट डाउनलोड करते समय सावधान रहें, खासकर अगर वे अप्रत्याशित हों या किसी अपरिचित प्रेषक से हों। व्यक्तिगत जानकारी न दें। वैध संगठन ईमेल के जरिए कभी भी व्यक्तिगत या वित्तीय जानकारी नहीं मांगेंगे। ईमेल के ज़रिए पासवर्ड, क्रेडिट कार्ड विवरण या सामाजिक सुरक्षा नंबर जैसी संवेदनशील जानकारी साझा करने से बचें। धमकी भरे संदेशों पर भरोसा न करें, फ़िशिंग ईमेल अक्सर पीड़ितों को गुमराह करने के लिए तत्काल या धमकी भरे शब्दों का इस्तेमाल करते हैं। ऐसे संदेशों पर संदेह करें और अन्य तरीकों से उनकी वैधता की पुष्टि करें।

एडवाइजरी के अनुसार मजबूत ईमेल फिल्टर का उपयोग करें। मजबूत स्पैम फ़िल्टर सक्षम करें और उन्हें संदिग्ध ईमेल को स्पैम फोल्डर में चिह्नित या डायवर्ट करने के लिए कॉन्फ़िगर करें। एंटीवायरस और एंटी-मैलवेयर सॉफ्टवेयर इंस्टॉल करें, फ़िशिंग प्रयासों का पता लगाने और उन्हें ब्लॉक करने के लिए अपने कंप्यूटर को अप-टू-डेट सुरक्षा सॉफ्टवेयर से सुरक्षित रखें। नियमित रूप से अपने डेटा का बैकअप लें। किसी भी संभावित फिशिंग हमलों के प्रभाव को कम करने के लिए महत्वपूर्ण फाइलों और डेटा का नियमित बैकअप बनाएँ।