प्रथम अंक –जनवरी 2013

सुरक्षित –केन्द्रीय उत्पाद एवं सीमा शुल्क बोर्ड की सूचना सुरक्षा विज्ञप्ति

केन्द्रीय उत्पाद एंव सीमा शुल्क बोर्ड के अर्धवार्षिक सूचना सुरक्षा विज्ञप्ति के प्रथम अंक में आपका स्वागत है। इस विज्ञप्ति का लक्ष्य आपको सूचना सुरक्षा जगत के उभरते मुद्दों– जैसे सुरक्षा युक्तियां, सूचना सांख्यिकी समाचार और आंकडों से अवगत कराना है।

अध्यक्षा (सी.बी.ई.सी.) का संदेश

"सी.बी.ई.सी. सूचना प्रौद्योगिकी समेकन कार्यक्रम का आई.एस.ओ.27001 मानक से प्रमाणित होना एक गर्व पूर्ण उपलब्धि है। एक केन्द्रीयकृत आई.टी. पर्यावरण के लिए सूचना सुरक्षा जागरूकता की आवश्यकता सर्वोपरि है। इस दिशा मे यह विज्ञप्ति एक योग्य कदम है।"

सदस्य (कम्प्यूटराइज़ेशन) कहतीं हैं –

"प्रौद्योगिकी एक प्रमुख प्रदायक है, लेकिन उस अपना 'बॉस' न बनने दें। किसी जानकारी के प्रयोग के साथ साथ उसको सुरक्षित रखने की जानकारी भी रखिये। यह केवल कुछ बुनियादी सावधानियां बरतने से सम्भव हो सकता है।"

महानिदेशक (प्रणाली) का संदेश–

"आई.एस.ओ. प्रमाणीकरण एक सुरक्षित सूचना प्रणाली सुविधा की तरफ प्रारम्भिक कदम है। इस यात्रा में प्रणाली निदेशालय के सभी कर्मियों के सहयोग और योगदान की आवश्यकता है। एक सामूहिक प्रयास और सतत सतर्कता ही सुरक्षित व्यवस्था की कुंजी है।"

प्रमुख सूचना सुरक्षा अधिकारी की कलम से–

"सुरक्षा, प्रौद्योगिकी से अधिक हमारी मानसिकता पर निर्भर करती है। अरस्तू के शब्दो में– ' जो हम बार बार करते हैं, हम वही बन जातें हैं। अतः उत्कृष्टता क्रिया नहीं, आदत की बात है।' सी.बी.ई.सी. मे हमें सुरक्षा को अपनी आदत बनाने की आवश्यकता है।

आज प्रौद्योगिकी हमारे सामान्य जीवन के सभी क्षेत्रो का मुख्य अंग है– चाहे वह ई–मेल और फोन जैसे आधुनिक संचार माध्यम हों, इन्टरनेट द्वारा घर बैठे खरीददारी करना या जी.पी.एस. यंत्रो से दिशा निर्देश लेना– प्रौद्योगिकी ने हमारी जीवन शैली को पूरी तरह से बदल दिया है। 'गूगल' जैसे खोज इंजनों से किसी भी प्रकार की सूचना बस एक बटन दबाते ही प्राप्त की जा सकती है। इसी के साथ प्रौद्योगिकी के दुरूपयोग का खतरा भी बढ़ता जा रहा है और इसलिए जरूरत है कि हम सूचना सुरक्षा संबंधी कुछ रक्षोंपायों का ख्याल रखें और उन्हे प्रयोग मे लाऐं।

सी.बी.ई.सी. करदाता की सेवा में सूचना प्रौद्योगिकी को अपनाने में अग्रणी रहा है। 'आई.सी.ई.एस.', 'आईसगेट' से 'ऐ.सी.ई.एस.' तक के सफर में दो चीज़ें उल्लेखनीय रहीं हैं–अप्रत्यक्ष कर प्रशासन में बढ़ता स्वचालन और उपयोग कर्ता के लिए अदृश्य होता आई.टी. प्रबंधन।

सी.बी.ई.सी. देश के केन्द्रीय अप्रत्यक्ष कर डाटा का अभिरक्षक है। अतः इस डाटा की गोपनीयता, सत्यनिष्ठा एवं उपलब्धता का दायित्व हम पर है।

सी.बी.ई.सी. को जुलाई 2011 में आई.एस.ओ. 27001 मानक के लिए प्रमाणित किया गया है। किन्तु यह केवल एक प्रारंभिक कदम है। इसमे हमे सी.बी.ई.सी. के प्रत्येक व्यक्ति के योगदान की आवश्यकता है जिससे हम अपनी प्रणाली एवं डाटा को सुरक्षित रख सकें। इस विज्ञप्ति का लक्ष्य यही है।

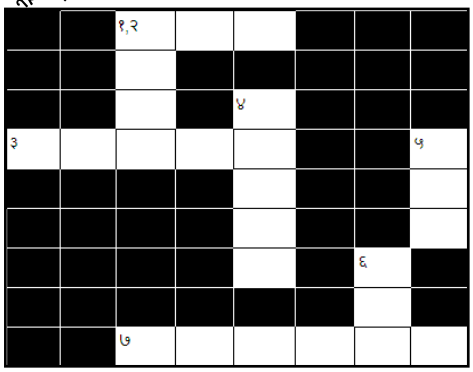
इन्टरनेट पर सावधान रहें

अपने फोन या ई–मेल पर कोई निजी जानकारी न दें

इन्टरनेट पर केवल कुछ देर की उपस्थिति भी आपकी पहचान एवं सुरक्षा को खतरे में डाल सकती है, यदि आप यथोचित रूप से सुरक्षित नही है। ऐसे किसी भी ई–मेल को न खोलें जो आपके जानकार से न आयी हो अथवा जो आपकी निजी सूचना मांगती हो, जैसे पासवर्ड, बैंक खाते सम्बंधित जानकारी, ए.टी.एम. के 'पिन' इत्यादि। सम्भवतः ऐसी ई–मेल एक तरह का 'फिशिंग' हमला हो सकता है।

फिशिंग एक ऐसा हमला है जिसक इस्तेमाल लोगों की संवेदनशील जानकारी (जैसे बैंकखाता या क्रेडिट कार्ड संबंधी जानकारी) प्राप्त करने के लिए किया जाता है ।

बूझो तो जानें-



आर-पार

१. अवांछित वाणिज्यिक ई-मेल (३)

३. प्रौघोगिक सुरक्षा उपकरण जो 'नेटवर्क' मे अनाधिकृत लोगों को प्रवेश न करने दे (५)

७. ऐसा 'सॉफ़्टवेयर' जो आपके कम्प्यूटर को, संक्रमणों का पता लगाने के लिए 'स्कैन' करे (६)

ऊपर से नीचे

२. यह कम्प्यूटर उपकरण या प्रोग्राम आपके 'डिजिटल नेटवर्क' मे गुजर रहे डाटा पर गुप्त रूप से निगरानी रखता है (४)

४. 'ट्रोजन', 'स्पाइवेयर', 'ऐडवेयर' के लिए एक शब्द (५)

५. आपकी संवेदनशील व्यक्तिगत जानकारी मांगने वाली ई-मेल (३)

६. जो आपके कम्प्यूटर की सुरक्षा प्रतिरोधक क्षमता को पार करने मे सक्षम हो (३)

प्रणाली एवं डाटा महानिदेशालय द्वारा प्रकाशित

आपकी सुरक्षा के लिए सुझाव

क्या करें

- ✓ सतर्क रहें और संदिग्ध गतिविधियों को रिपोर्ट करें।
- ✓ अपने कम्प्यूटर पर ऐंटीवायरस और फायरवॉल का प्रयोग करें।
- ✓ मोबाईल उपकरणों पर संवेदनशील डाटा को 'एन्क्रिप्शन' के प्रयोग से सुरक्षित रखें।
- ✓ पासवर्ड ऐसा रखें जिसका आसानी से अनुमान न लगाया जा सकें और नियमित रूप से अपना पासवर्ड बदलें।
- ✓ जब भी ऐसे कम्प्यूटर पर काम करें जिसे अन्य लोग भी प्रयोग करते हों तो काम के पश्चात् संवेदनशील फाईलें 'डीलीट' या नष्ट कर दें।
- ✓ ई–मेल मे आये दस्तावेजों को खोलनें से पहले उन्हे ऐन्टीवायरस की मदद से जांच (स्कैन) कर लें।
- ✓ आपकी व्यक्तिगत जानकारी मांगने वाले फोन या ई–मेल से सावधान रहें।
- ✓ आपने निजी सिस्टम और डाटा का नियमित रूप से 'बैकअप' लें और उसे सुरक्षित रूप से संग्रहित करें।
- ✓ आप अपनी प्रौद्योगिक परिसम्पत्ति के लिए उत्तरदायी हैं– उन्हे लावारिस न छोड़े।

क्या न करें

- X आसानी से अनुमान लगाये जाने वाले पासवर्ड जैसे जन्मतिथि, बच्चों के नाम, फोन नम्बर आदि का प्रयोग न करें।
- X अन्य लोगों के साथ अपना आई.डी. और पासवर्ड सांझा न करें।
- X आपने फोन, लैपटोप आदि उपकरणों को लावारिस न छोंड़े।
- X अज्ञात या अविश्वस्त स्रोतो से, या कॉपीराईट मालिक अनुमति के बिना कम्प्यूटर एवं सामग्री 'डाउनलोड' न करें।
- X 'ब्लूटूथ' आदि के माध्यम से अवांछित फाईल स्थानान्तरण स्वीकार न करें।
- X अति जिज्ञासु होकर अविश्वसनीय वेबसाईटों या यू.आर.एल. पर न जायें।
- X बिना लाईसेंस के अवैध सॉफ्टवेयर प्रोग्रामों का उपयोग न करें।
- X अनचाहे स्रोतों से आये ई–मेल संलग्न दस्तावेज न खोलें।
- X स्पैम ई–मेल मे अन्तरनिहित 'लिंक' पर क्लिक न करें।

हाल के सुरक्षा उल्लंघन

भारतीय कम्प्यूटर इमरजेंसी रिस्पॉंस टीम (CERT-In) की रिपोर्ट के अनुसार साल 2012 के पहले सात महिनों मे 273 वेबसाईटों को हैक किया गया था।

"29 अक्टूबर 2012 की रात को अलजीरियाई हैकरों द्वारा पांच वेबसाईटें हैक की गई थीं"। हैक हुई वेबसाईटों मे रक्षा अनुसंधान और विकास संगठन (डी.आर.डी.ओ.), भर्ती एवं मूल्यांकन परिषद् और सैम पिट्रोडा की वेबसाईटो के नाम शुमार हैं। –महानिदेशक (CERT-In)

CERT-In की रिपोर्ट के अनुसार पांच स्थानीय आयुक्तालयों की वेबसाईट 'डीफेस' करीं गई थीं। इनमें कोलकाता सीमा शुल्क, केन्द्रीय उत्पाद शुल्क मेरठ, केन्द्रीय उत्पाद शुल्क मुम्बई–5, सीमा शुल्क दिल्ली और आई.सी.डी. तुगलकाबाद की वेबसाईटें शामिल थी। इन वेबसाईटों को गृह मंत्रालय के दिशा निर्देशों के विरूद्ध विदेशी 'सरवर' पर 'होस्ट' किया गया था।

CERT-In के अनुसार 2009 से 2011 तक साईबर हमलों की संख्या मे तेजी से वृद्धि हुई है। 2009 मे 8266 की तुलना मे 2011 में इनकी संख्या 13000 थी।

"अधिकांश डाटा चोर पेशेवर अपराधी होते हैं जो जानबूझकर ऐसी जानकारी हासिल करते है जिसे वे बेचकर पैसे कमा सकें।"

–2012 वेराईज़न रिपोर्ट

छपते छपते

सी.बी.ई.सी. पुरस्कृत

भारतीय डाटा सिक्योरिटी कांऊसिल (डी.एस.सी.आई.) द्वारा ई–गर्वनेंस में सुरक्षा के लिए 2012 का उत्कृष्टता पुरस्कार सी.बी.ई. सी. को दिया गया है।

विस्तार @ http://www.dsci.in

१. स्पैम २. स्निफर ३. फ़ायरवॉल ४. मैलवेयर ५. फिशिंग ६. हैकर ७.ऐंटीवाइरस

आप अपने सूचना सुरक्षा संबंधी सुझाव हमें इस आई.डी. पर भेजें cbec.ciso@icegate.gov.in