साइबर सुरक्षा और सूचना सुरक्षा परभिाषा सूचना सुरक्षा क्या हैः सूचना की सुरक्षा, इसके प्रारूप की परवाह कएि बनिा, अनधकिृत पहुंच, उपयोग, प्रकटीकरण, व्यवधान, संशोधन से,

या वनिाश। व्यापकः भौतकि और डजिटिल सहति सभी प्रकार की सूचनाओं को शामलि करता है। साइबर सुरक्षाः प्रणालयिों, नेटवर्क और डेटा को साइबर खतरों से बचाना, प्रौद्योगकिी और डजिटिल पर ध्यान केंद्रति करना।

पर्यावरण. संकीर्णः वशिेष रूप से डजिटिल ससि्टम, नेटवर्क और डेटा की सुरक्षा पर ध्यान केंद्रति करता है। साइबर सुरक्षा के सद्धिांत साइबर सुरक्षा में, सी. आई. ए. ट्रायड एक मूलभूत मॉडल है जो साइबर सुरक्षा का प्रतनिधित्वि करता है।

सूचना सुरक्षा के तीन मुख्य सद्धिांत। ये सद्धिांत डेटा और प्रणालयिों की प्रभावी सुरक्षा सुनश्चिति करते हैं। गोपनीयताः यह सुनश्चिति करता है कि जानकारी केवल उन लोगों के लएि सुलभ है जो सूचना देने के लएि अधकिृत हैं।

इसे प्राप्त करें। सत्यनष्ठिा यह सुनश्चिति करती है कि भंडारण या संचरण के दौरान डेटा सटीक, पूर्ण और अपरविर्तति है। उपलब्धताः यह सुनश्चिति करता है कि जानकारी और संसाधन अधकिृत उपयोगकर्ताओं के लएि सुलभ हैं।

जब आवश्यकता हो। वभिन्नि प्रकार के साइबर खतरे। सोशल इंजीनयिरगि सोशल इंजीनयिरगि एक हेरफेर तकनीक है जो नजिी जानकारी, पहुंच या मूल्यवान वस्तुओं को प्राप्त करने के लएि मानव स्वभाव का शोषण करती है।

साइबर अपराध, ये "मानव हैकगि" घोटाले अनजान उपयोगकर्ताओं को डेटा को उजागर करने, मैलवेयर संक्रमण फैलाने या प्रतबिंधति प्रणालयिों तक पहुंच देने के लएि लुभाते हैं। हमले ऑनलाइन, व्यक्तगित रूप से हो सकते हैं,

और अन्य अंतःक्रयिाओं के माध्यम से। मैलवेयर हानकिारक सॉफ्टवेयर जो एक प्रणाली के डेटा तक पहुँच सकता है, जैसे कि वायरस, स्पाइवेयर, रैनसमवेयर और कीड़े फशिगि एक भ्रामक हमला जहां साइबर अपराधी प्रतरिूपण करते हैं।

पीड़तिों को संवेदनशील जानकारी का खुलासा करने के लएि धोखा देने के लएि वैध संस्थाएं-सेवा से इनकार (डी. ओ. एस.) हमला एक साइबर हमला जो एक प्रणाली के संसाधनों को अभभिूत कर देता है, जसिसे वह इसका जवाब देने में असमर्थ हो जाता है।

वैध सेवा अनुरोध-वतिरति सेवा-नषिेध (डी. डी. ओ. एस.) हमला डी. ओ. एस. हमले के समान हमला, लेकनि

कई मैलवेयर-संक्रमति मेजबान मशीनों द्वारा शुरू कयिा गया-एस. क्यू. एल. इंजेक्शन एक हमला जो शोषण करता है।

उपयोगकर्ता इनपुट में दुर्भावनापूर्ण कोड को इंजेक्ट करके डेटाबेस में कमजोरयिां-क्रॉस-साइट स्क्रप्टिगि (एक्सएसएस) एक हमला जसिमें एक वेबसाइट में दुर्भावनापूर्ण कोड को इंजेक्ट करना शामलि है, लेकनि कोड केवल वेबसाइट में चलता है।

उपयोगकर्ता का ब्राउज़र-रैनसमवेयर सॉफ्टवेयर का एक दुर्भावनापूर्ण रूप है जो पीड़ति की फ़ाइलों को एन्क्रप्टि करता है या उन्हें उनके कंप्यूटर ससि्टम से लॉक कर देता है, सुरक्षति इंटरनेट और डविाइस के बदले में फरिौती भुगतान की मांग करता है।

उपयोग वेबसाइट सुरक्षा सत्यापति करें यू. आर. एल. में एच. टी. टी. पी. एस. खोजें। मुफ्त उत्पादों या पुरस्कारों का वादा करने वाले पॉप-अप या वज्ञिापनों पर क्लकि करने से बचें। मजबूत पासवर्ड का उपयोग करें। कम से कम 8 वर्ण लंबे पासवर्ड बनाएँ।

अक्षरों, संख्याओं और प्रतीकों का मश्रिण। सामान्य शब्दों या वाक्यांशों का उपयोग करने से बचें। सुरक्षति कूटशब्दों को संग्रहीत करने और उत्पन्न करने के लिए कूटशब्द प्रबंधक का उपयोग करें। बहु-कारक प्रमाणीकरण (एम. एफ. ए.) सक्षम करें।

सत्यापन के दूसरे रूप (जैसे, आपके फ़ोन पर भेजा गया एक कोड) की आवश्यकता के कारण आपके खातों में सुरक्षा की परत। सुरक्षति ब्राउज़गि-सॉफ़्टवेयर अद्यतन रखें: सुनश्चिति करें कि आपका ब्राउज़र और प्लगइन्स पूरी तरह से सुरक्षति हैं।

कमजोरयिों को ठीक करने की तारीख। सुरक्षति ब्राउज़र का उपयोग करें: अंतर्नहिति सुरक्षा सुवधिाओं वाले ब्राउज़रों पर वचिार करें। वज्ञिापनों पर क्लकि करने से बचें: जोखमि को कम करने के लिए पॉप-अप और वज्ञिापनों को अवरुद्ध या अनदेखा करें। नजिी का उपयोग करें।

ब्राउज़गि: संवेदनशील गतविधियिों के लिए गुप्त या नजिी मोड का उपयोग करें। कुकीज़ को सीमति करें: कुकी ट्रैकगि को कम करने के लिए ब्राउज़र सेटगि्स का प्रबंधन करें। सार्वजनकि वाई-फाई से बचें: असुरक्षति पर ब्राउज़गि करते समय वीपीएन का उपयोग करें।

नेटवर्क। उपयोग के बाद लॉग आउट: हमेशा खातों से लॉग आउट करें, वशिेष रूप से साझा या सार्वजनकि उपकरणों पर। टाइपोस्क्वैटगि डोमेन से सावधान रहें (जैसे, सार्वजनकि वाई-फाई के लिए .

युक्तयिों के बजाय .)

उपयोग करें-संवेदनशील लेन-देन से बचें: सार्वजनकि वाई-फाई पर बैंकगि या संवेदनशील खातों तक न जाएं।

वीपीएन का उपयोग करें-अपने डेटा को संभावति जासूसी करने वालों से बचाने के लिए अपने इंटरनेट कनेक्शन को एन्क्रप्टि करें।

साझा न करना: सार्वजनकि नेटवर्क से जुड़े रहने के दौरान फ़ाइल और प्रटिर साझा करने को अक्षम करें।

उपयोग के बाद नेटवर्क को भूल जाएं: सुनश्चिति करें कि आपका उपकरण स्वचालति रूप से सार्वजनकि वाई-फाई से फरि से कनेक्ट नहीं होता है।

प्रामाणकिता-नकली नेटवर्क से जुड़ने से बचने के लिए प्रदाता के साथ नेटवर्क नाम की पुष्टि करें।

सॉफ्टवेयर अद्यतन रखें: अपने उपकरण के ऑपरेटगि सस्टिम और सुरक्षा सॉफ्टवेयर को नयिमति रूप से अद्यतन करें। ईमेल करें

सुरक्षा युक्तयिाँ-क्लकि करने से पहले सोचें: ईमेल में संदग्धि लकि या संलग्नक पर क्लकि करने से बचें।

प्रेषकों को सत्यापति करें-स्पूफगि के संकेतों के लिए प्रेषक के ईमेल पते को ध्यान से देखें।

तात्कालकि भाषा: घोटालेबाज अक्सर आपको कार्रवाई करने के लिए धोखा देने के लिए तात्कालकिता का उपयोग करते हैं। स्पैम फ़लि्टर सक्षम करें: अवांछति ईमेल को कम करने के लिए अपने ईमेल प्रदाता की स्पैम फ़लि्टरगि सुवधिाओं का उपयोग करें।

संवेदनशील जानकारी: ईमेल के माध्यम से पासवर्ड, वत्तिीय ववरिण या व्यक्तगित जानकारी भेजने से बचें। एन्क्रप्शिन का उपयोग करें। अत्यधकि संवेदनशील संचार के लिए, ईमेल एन्क्रप्शिन टूल का उपयोग करें। ईमेल अपडेट करें।

नयिमति रूप से कूटशब्द: मजबूत, अद्वतिीय कूटशब्दों का उपयोग करें और उन्हें समय-समय पर बदलें।

संदग्धि ईमेल की सूचना दें: फ़शिगि प्रयासों के बारे में अपनी आईटी टीम या ईमेल प्रदाता को सूचति करें। क्या करें और क्या न करें

कसिी भी हार्डवेयर कॉन्फ़गिरेशन, ऑपरेटगि सस्टिम में सेटग्सि या उनके डेस्कटॉप पर इंस्टॉल कए गए कसिी भी एप्लकिेशन को बदलें। अपने डेस्कटॉप/लैपटॉप पर कोई भी सॉफ्टवेयर या एप्लकिेशन इंस्टॉल न करें।

सी. एम. ई. एस. की आई. टी. टीम द्वारा अधकिृत नहीं है या सी. एम. ई. एस. के व्यवसाय के लिए आवश्यक नहीं है। यू. एस. बी. पोर्ट, कॉम्पैक्ट डस्कि (सी. डी.)/डी. वी. डी., मेमोरी कार्ड का उपयोग डफ़िॉल्ट रूप से अक्षम है। यदि उपयोगकर्ता को उन्हें सक्षम करने की आवश्यकता है, तो अनुमोदन करें।

उपयोगकर्ता के प्रबंधक और आई. टी. दल से इसकी आवश्यकता होगी। लैपटॉप की भौतकि सुरक्षा के लिए उचति उपाय करें जैसे कि सार्वजनकि स्थानों पर या यात्रा करते समय लैपटॉप को बनिा देखे न छोड़ें।

हटाने योग्य मीडिया जैसे कि सी. डी./डी. वी. डी., यू. एस. बी. ड्राइव, और अन्य पोर्टेबल भंडारण मीडिया को किसी अज्ञात स्रोत से सी. एम. ई. एस. प्रणाली से न जोड़ें।

सीएमईएस अनुमोदित उपकरण का उपयोग करके एन्क्रिप्टेड प्रारूप में संग्रहीत किया जाएगा। संवेदनशील जानकारी वाले हटाने योग्य मीडिया को खुले में नहीं छोड़ा जाना चाहिए या अवसरवादी चोरी के लिए असुरक्षित होने की अनुमति नहीं दी जानी चाहिए।

साफ़ डेस्क और साफ़ स्क्रीन सुनिश्चित करें कि डेस्क और अन्य कार्य क्षेत्रों को कागज़ों और किसी भी भंडारण माध्यम से दूर रखा जाए जब उन पर ध्यान न दिया जाए। सभी वर्कस्टेशनों में पासवर्ड-लॉक स्क्रीन सेवर सक्षम होंगे।

5 मिनट की निष्क्रियता के बाद सक्रिय करने के लिए। एंटी-वायरस/एंटी-मैलवेयर-उपयोगकर्ता स्थापित एंटी-वायरस एजेंट को अक्षम नहीं करेंगे या स्थापना के दौरान परिभाषित इसकी सेटिंग्स को नहीं बदलेंगे।

अनपैच्ड सिस्टम या किसी भी वायरस के लिए आईटी टीम जो सिस्टम में पाई जाती है और एंटी-वायरस सॉफ्टवेयर द्वारा साफ नहीं की जाती है। यदि आपको किसी भी गैर-पालन या संदिग्ध गतिविधियों या ईमेल पर संदेह है, तो कृपया

दुर्भावनापूर्ण कोड की शुरुआत को रोकने और सीएमईएस परिसंपत्तियों की अखंडता की रक्षा के लिए, सभी हार्डवेयर और सॉफ़्टवेयर को . हार्डवेयर और सॉफ़्टवेयर पर

प्राप्त किया जाएगा

आई. टी. टीम के माध्यम से अनुरोध करना। सी. एम. ई. एस. की आई. टी. टीम यह सुनिश्चित करेगी कि अधिकृत सॉफ्टवेयर की एक अनुमोदित सूची बनी रहे। सभी कर्मचारी सॉफ्टवेयर कॉपीराइट कानून का पालन करेंगे और ऐसा नहीं करेंगे।

लाइसेंस समझौतों के तहत अनुमति के अलावा सॉफ़्टवेयर प्राप्त करना, स्थापित करना, दोहराना, स्थानांतरित करना या उपयोग करना। उपयोगकर्ता यह सुनिश्चित करेंगे कि व्यक्तिगत सॉफ़्टवेयर का उपयोग सीएमईएस के स्वामित्व वाली परिसंपत्तियों की सुरक्षा के लिए नहीं किया जाता है।

सी. एम. ई. एस. की परिसंपत्तियों और सूचनाओं की अखंडता। घटना की रिपोर्टिंग ब्लॉगिंग और सोशल मीडिया-सोशल मीडिया, ब्लॉगिंग/माइक्रो-ब्लॉगिंग और वीडियो साझा करने वाली वेबसाइटों जैसे फेसबुक, ट्विटर तक पहुंच।

कर्मचारियों की उत्पादकता सुनिश्चित करने के लिए लिंक्डइन, यूट्यूब आदि को प्रतिबंधित किया जाएगा। सीएमईएस के नाम को संरेखित करने वाले किसी भी आधिकारिक मामले, घटनाओं और घटनाओं पर सोशल

मीडयिा पर चर्चा/पोस्ट नहीं की जाएगी।

कर्मचारयिों द्वारा मीडयिा मंच। इस तरह की घटना की रपिोर्ट करने से कर्मचारयिों (कर्मचारयिों) के लएि गंभीर परणिाम हो सकते हैं।