सायबर सुरक्षा आणि माहिती सुरक्षा व्याख्या माहिती सुरक्षा म्हणजे कायः अनधिकृत प्रवेश, वापर, प्रकटीकरण, व्यत्यय, बदल यापासून, त्याच्या स्वरूपाची पर्वा न करता, माहितीचे संरक्षण करणे.

कवि वनिाश. अधकि व्यापकः भौतकि आणि डिजिटिलसह सर्व प्रकारच्या माहितीचा समावेश करते. सायबर सुरक्षाः सायबर धोक्यांपासून प्रणाली, जाळे आणि डेटाचे संरक्षण करणे, तंत्रज्ञान आणि डिजिटिलवर लक्ष केंद्रति करणे

वातावरण. संकुचतिः वशिषतः डजिटिल प्रणाली, जाळे आणि डेटाचे संरक्षण करण्यावर लक्ष केंद्रति करते. सायबर सुरक्षेची तत्त्वे सायबर सुरक्षेमध्ये, सी. आय. ए. ट्रायड हे एक मूलभूत प्रतरिूप आहे जे डजिटिल प्रणाली, जाळे आणि डेटाचे प्रतनिधित्वि करते.

माहिती सुरक्षेची तीन मूलभूत तत्त्वे. ही तत्त्वे माहिती आणि प्रणालींचे प्रभावी संरक्षण सुनश्चिति करतात. गोपनीयताः माहिती केवळ अधकिारधारकांनाच उपलब्ध आहे याची खात्री करते.

त्यात प्रवेश करणे. सचोटीः साठवण कवि प्रसारणादरम्यान डेटा अचूक, पूर्ण आणि अपरविर्तनीय असल्याची खात्री करते. उपलब्धताः अधकिृत वापरकर्त्यांसाठी माहिती आणि संसाधने उपलब्ध असल्याची खात्री करते.

जेव्हा आवश्यक असेल तेव्हा. ववििधि प्रकारचे सायबर धोके सामाजकि अभयिांत्रकिी सामाजकि अभयिांत्रकिी हे एक हाताळणी तंत्र आहे जे खाजगी माहिती, प्रवेश कवि मौल्यवान वस्तू मळिवण्यिासाठी मानवी स्वभावाचा गैरवापर करते.

सायबर गुन्हे, या'मानवी हॅकगि'घोटाळ्यांचा कल संशयास्पद वापरकर्त्यांना डेटा उघड करण्यासाठी, मालवेअर संक्रमण पसरवण्यासाठी कवि प्रतबिंधति प्रणालींमध्ये प्रवेश देण्यासाठी आकर्षति करण्याचा असतो. हल्ले ऑनलाइन, वैयक्तकिरित्या होऊ शकतात,

आणि इतर परस्परसंवादांद्वारे. मालवेअर हानकिारक सॉफ्टवेअर जे प्रणालीच्या डेटामध्ये प्रवेश करू शकते, जसे की व्हायरस, स्पायवेअर, रॅन्समवेअर आणि वर्म्स फशिगि एक भ्रामक हल्ला जेथे सायबर गुन्हेगार स्वतःची वेशभूषा करतात

संवेदनशील माहिती उघड करण्यासाठी पीडतिांना फसवण्यासाठी कायदेशीर संस्था-सेवा नाकारण्याचा (डी. ओ. एस.) हल्ला-एक सायबर हल्ला जो प्रणालीच्या संसाधनांवर वर्चस्व गाजवतो, ज्यामुळे तो प्रतसिाद देण्यास असमर्थ ठरतो.

वैध सेवा वनिंत्या-डसि्ट्रबि्युटेड डनियल-ऑफ-सर्व्हसि (डी. डी. ओ. एस.) हल्ला हा डी. ओ. एस. हल्ल्यासारखाच हल्ला आहे, परंतु तो अनेक मालवेअर-संक्रमति यजमान यंत्रांद्वारे सुरू केला गेला

आहे-एस. क्यू. एल. इंजेक्शन-एक हल्ला जो शोषण करतो.

वापरकर्त्याच्या इनपुटमध्ये दुर्भावनायुक्त कोड इंजेक्ट करून डेटाबेसमधील असुरक्षतिता क्रॉस-साइट स्क्रप्टिगि (एक्स. एस. एस.) एक हल्ला ज्यामध्ये वेबसाइटमध्ये दुर्भावनायुक्त कोड इंजेक्ट करणे समावष्टि असते, परंतु कोड केवळ वापरकर्त्याच्या इनपुटमध्ये चालतो.

वापरकर्त्याचा ब्राउझर रॅनसमवेअर हा सॉफ्टवेअरचा एक दुर्भावनायुक्त प्रकार आहे जो पीडति व्यक्तीच्या फायली एन्क्रप्टि करतो कवि त्यांना त्यांच्या संगणक प्रणालीतून लॉक करतो, सुरक्षति इंटरनेट आणि डिव्हाइसच्या बदल्यात खंडणीची मागणी करतो.

वापर संकेतस्थळाच्या सुरक्षतितेची पडताळणी करा यू. आर. एल. मध्ये एच. टी. टी. पी. एस. शोधा. मोफत उत्पादने कवि बक्षसिांचे आश्वासन देणाऱ्या पॉप-अप कवि जाहरितींवर क्लकि करणे टाळा. मजबूत संकेतशब्द वापरा. संकेतशब्द कमीतकमी 8 वर्ण लांब करा.

अक्षरे, संख्या आणि चिन्हांचे मश्रिण. सामान्य शब्द कवि वाक्ये वापरणे टाळा. सुरक्षति संकेतशब्द संचयति करण्यासाठी आणि तयार करण्यासाठी संकेतशब्द व्यवस्थापक वापरा. बहु-घटक प्रमाणीकरण (एम. एफ. ए.) सक्षम करा. अतरिक्ति शब्द जोडा

दुसऱ्या प्रकारची पडताळणी आवश्यक करून तुमच्या खात्यांसाठी संरक्षणाचा स्तर (उदाहरणार्थ, तुमच्या फोनवर पाठवलेला कोड). सुरक्षति ब्राउझगि-सॉफ्टवेअर अद्ययावत ठेवा-तुमचा ब्राउझर आणि प्लगइन पूर्ण क्षमतेचे असल्याची खात्री करा

असुरक्षतिता दूर करण्यासाठी तारीख. सुरक्षति ब्राउझर वापराः अंतर्नरि्मति सुरक्षा वैशष्ट्यांसह ब्राउझरचा वचिार करा. जाहरितींवर क्लकि करणे टाळाः जोखीम कमी करण्यासाठी पॉप-अप आणि जाहरिाती अवरोधति करा कवि त्याकडे दुर्लक्ष करा. खाजगी वापरा

ब्राउझगिः संवेदनशील क्रयिाकलापांसाठी गुप्त कवि खाजगी पद्धती वापरा. कुकीज मर्यादति कराः कुकीचा मागोवा कमी करण्यासाठी ब्राउझर सेटगि्ज व्यवस्थापति करा. सार्वजनकि वाय-फाय टाळाः असुरक्षति वर ब्राउझगि करताना व्हीपीएन वापरा

नेटवर्क. वापरानंतर लॉग आउट कराः खात्यांमधून नेहमी लॉग आउट करा, वशिेषतः सामायकि कवि सार्वजनकि उपकरणांवर. टायपोस्क्वेटगि डोमेनपासून सावध रहा (उदाहरणार्थ, सार्वजनकि वाय-फायसाठीच्या . टपिाऐवजी .)

वापरा-संवेदनशील व्यवहार टाळाः सार्वजनकि वाय-फायवर बँकगि कवि संवेदनशील खात्यांमध्ये प्रवेश करू नका. व्ही. पी. एन. वापराः संभाव्य गुप्तहेरांपासून तुमचा डेटा संरक्षति करण्यासाठी तुमचे इंटरनेट

कनेक्शन एन्क्रिप्ट करा.

सामायकिरण बंद करणेः सार्वजनकि जाळ्यांशी जोडले असताना फाइल आणि मुद्रक सामायकिरण अक्षम करा. वापरानंतर जाळ्यांना वसिरू नकाः तुमचे उपकरण स्वयंचलतिपणे सार्वजनकि वाय-फायशी पुन्हा जोडले जात नाही याची खात्री करा. जाळ्याची पडताळणी करा.

प्रामाणकिताः बनावट जाळ्यांशी जोडणी टाळण्यासाठी पुरवठादारासह जाळ्याच्या नावाची पुष्टी करा. सॉफ्टवेअर अद्ययावत ठेवा. तुमच्या उपकरणांची कार्यप्रणाली आणि सुरक्षा सॉफ्टवेअर नयिमतिपणे अद्ययावत करा. ईमेल करा.

सुरक्षा टपिा क्लकि करण्यापूर्वी वचिार कराः संशयास्पद दुव्यांवर कवि ईमेलमधील संलग्नकांवर क्लकि करणे टाळा. पाठवणाऱ्यांची पडताळणी कराः पाठवणाऱ्याचा ईमेल पत्ता फसवणुकीच्या चन्हिांसाठी काळजीपूर्वक तपासा.

तातडीची भाषाः फसवणूक करणारे अनेकदा तुम्हाला फसवून कारवाई करण्यासाठी तातडीचा वापर करतात. स्पॅम फल्टिर सक्षम कराः अवांछति ईमेल कमी करण्यासाठी तुमच्या ईमेल प्रदात्याच्या स्पॅम फल्टिरगि वैशष्ट्यांचा वापर करा.

संवेदनशील माहतीिः संकेतशब्द, आर्थकि तपशील कवि वैयक्तकि माहतीि ईमेलद्वारे पाठवणे टाळा. एन्क्रप्शिनचा वापर कराः अत्यंत संवेदनशील संवादांसाठी, ईमेल एन्क्रप्शिन साधने वापरा. ईमेल अद्ययावत करा.

संकेतशब्द नयिमतिपणेः मजबूत, अद्वतिीय संकेतशब्द वापरा आणि ते वेळोवेळी बदला. संशयास्पद ईमेलचा अहवाल द्याः फशिगि प्रयत्नांबद्दल तुमच्या आयटी कार्यसंघाला कवि ईमेल प्रदात्याला सूचति करा. काय करावे आणि काय करू नये

कोणतेही हार्डवेअर संरचना, ऑपरेटगि ससि्टममधील सेटगि्ज कवि त्यांच्या डेस्कटॉपवर स्थापति केलेले कोणतेही अनुप्रयोग बदला. तुमच्या डेस्कटॉपवर/लॅपटॉपवर कोणतेही सॉफ्टवेअर कवि अनुप्रयोग स्थापति करू नका.

सी. एम. ई. एस. च्या आय. टी. चमूने अधकिृत केलेले नाही कवि सी. एम. ई. एस. च्या व्यवसायासाठी आवश्यक नाही. यू. एस. बी. पोर्ट, कॉम्पॅक्ट डसि्क (सी. डी.)/डी. व्ही. डी., मेमरी कार्ड प्रवेश पूर्वनरि्धारतिपणे अक्षम केले आहेत. वापरकर्त्याला ते सक्षम करण्याची आवश्यकता असल्यास, मान्यता

वापरकर्त्याच्या व्यवस्थापकाकडून आणि आयटी चमूकडून आवश्यक असेल. सार्वजनकि ठकिाणी कवि

प्रवास करताना लॅपटॉप न सोडणे यासारख्या लॅपटॉपच्या शारीरकि संरक्षणासाठी योग्य उपाययोजना करा.
काढून टाकण्यायोग्य माध्यम जसे की सी. डी./डी. व्ही. डी., यू. एस. बी. ड्राइव्ह आणि इतर पोर्टेबल स्टोरेज माध्यम अज्ञात स्त्रोताकडून सी. एम. ई. एस. प्रणालीशी जोडू नका. संवेदनशील कविा गोपनीय माहतिी असलेले काढून टाकण्यायोग्य माध्यम
सी. एम. ई. एस. मान्यताप्राप्त साधनाचा वापर करून एन्क्रप्टिेड स्वरूपात संग्रहति केले जाईल. संवेदनशील माहतिी असलेले काढून टाकण्यायोग्य माध्यम उघड्यावर सोडले जाऊ नये कविा संधीसाधू चोरीला बळी पडू दलि जाऊ नये.
मेजा साफ करा आणि पिडदा साफ करा-मेजा आणि कामाची इतर क्षेत्रे कागद आणि साठवण माध्यमांपासून दूर ठेवली आहेत याची खात्री करा. सर्व कार्यस्थानकांमध्ये पासवर्ड-लॉक केलेले स्क्रीन सेव्हर्स सक्षम असतील.
5 मनिटिांच्या नष्क्रियितेनंतर सक्रयि करण्यासाठी. अँटी-व्हायरस/अँटी-मालवेअर वापरकर्ते स्थापति अँटी-व्हायरस एजंट अक्षम करणार नाहीत कविा प्रतष्ठिापन दरम्यान परभिाषति केलेल्या सेटगि्जमध्ये बदल करणार नाहीत.
न जुळलेल्या प्रणालींसाठी कविा प्रणालीमध्ये सापडलेल्या आणि अँटी-व्हायरस सॉफ्टवेअरद्वारे साफ न झालेल्या कोणत्याही वषिाणूसाठी आय. टी. कार्यसंघ. तुम्हाला कोणत्याही गैर-पालन कविा संशयास्पद क्रयिाकलाप कविा ईमेलची शंका असल्यास, कृपया
दुर्भावनायुक्त कोडचा वापर रोखण्यासाठी आणि सीएमईएस मालमत्तांच्या अखंडतेचे संरक्षण करण्यासाठी, सर्व हार्डवेअर आणि सॉफ्टवेअरद्वारे प्राप्त केले जातील
आय. टी. चमूद्वारे वनिंती करणे. सी. एम. ई. एस. ची आय. टी. चमू हे सुनश्चिति करेल की अधकिृत सॉफ्टवेअरची मान्यताप्राप्त यादी ठेवली गेली आहे. सर्व कर्मचारी सॉफ्टवेअर कॉपीराइट कायद्याचे पालन करतील आणि करणार नाहीत.
परवाना करारांतर्गत परवानगी दल्याखेरीज सॉफ्टवेअर मळिवणे, स्थापति करणे, प्रतकिृती तयार करणे, हस्तांतरति करणे कविा वापरणे. वापरकर्ते हे सुनश्चिति करतील की सी. एम. ई. एस. च्या मालकीच्या मालमत्तेवर वैयक्तकि सॉफ्टवेअर वापरले जात नाही.
सी. एम. ई. एस. ची मालमत्ता आणि माहतिीची सचोटी. घटना अहवाल ब्लॉगगि आणि सोशल मीडयिा-सोशल मीडयिा, ब्लॉगगि/मायक्रो-ब्लॉगगि आणि फेसबुक, ट्वटिर सारख्या व्हडिओ सामायकिरण वेबसाइट्सवर प्रवेश,

कर्मचाऱ्यांची उत्पादकता सुनश्चिति करण्यासाठी लक्ड्इन, यूट्यूब इत्यादींवर नर्बिंध घालण्यात येतील. सी. एम. ई. एस. च्या नावाची सांगड घालू शकतील अशा कोणत्याही अधकृित बाबी, घटना आणि घटनांवर समाजमाध्यमांवर चर्चा/पोस्ट केली जाणार नाही.

कर्मचाऱ्यांद्वारे माध्यम मंच. अशा घटनेचा अहवाल दलि्यास कर्मचाऱ्यांसाठी गंभीर परणिाम होऊ शकतात.