डिजिटल सुरक्षा की मूल बातें

CII
Confederation of Indian Industry
Digital Saksham

अनुक्रमणिका

अनुक्रमणिका

अनुक्रमणिका

पाठ योजना

यह मॉड्यूल प्रतिभागियों को डिजिटल सुरक्षा की मूल बातें और इसके घटकों से परिचित कराता है जो व्यवसाय के लिए डिजिटल सुरक्षा उपायों को अपनाने के महत्व को समझने के लिए आवश्यक हैं। इस मॉड्यूल में शुरू की गई अवधारणाओं और प्रक्रियाओं का उद्देश्य प्रतिभागियों को डिजिटल सुरक्षा के साथ सहज बनाने के लिए एक प्राइमर के रूप में कार्य करना है।

CII
Confederation of Indian Industry
Digital Saksham

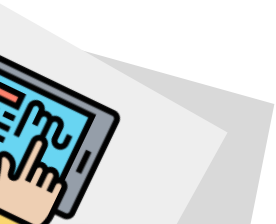
उद्देश्य/उम्मीदें

- डिजिटल सुरक्षा की मूल बातें और इससे जुड़ी शर्तों से अवगत कराना।
- प्रतिभागियों को सबसे सामान्य साइबर खतरों और उनसे निपटने के तरीकों और साधनों से अवगत कराया जाता है।
- प्रतिभागियों को डिजिटल सुरक्षा की समझ हासिल करने में मदद करना।

CII
Confederation of Indian Industry
Digital Saksham

आवश्यक सामग्री

- डिजिटल सुरक्षा की मूल बातों की सॉफ्ट और हार्ड कॉपी
- खाली A4 साइज की शीट
- प्रोजेक्टर
- लैपटॉप
- व्हाइटबोर्ड
- डस्टर
- कलम (व्हाइटबोर्ड के लिए)



Confederation of Indian Industry
Digital Saksham

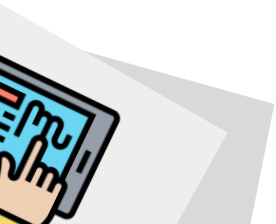
पासवर्ड

01

Confederation of Indian Industry
Digital Saksham

काम के ईमेल एक्सेस करते समय, श्रेड हार्ड ड्राइव से सामग्री एक्सेस करते समय या ऑनलाइन सेवाओं का उपयोग करते समय, पासवर्ड महत्वपूर्ण होता है।

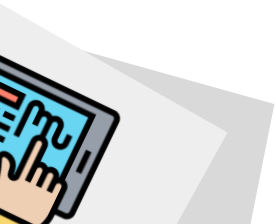
व्यवसायिक प्रणालियों और खातों को सुरक्षित करने के लिए मजबूत पासवर्ड आवश्यक हैं।



Confederation of Indian Industry
Digital Saksham

पासवर्ड के लिए दिशानिर्देश

- मजबूत पासवर्ड वाक्यांश होते हैं – यादृच्छिक विचार और लंबाई में 15 वर्ण होने चाहिए।
- व्यक्तिगत और कार्य खातों के लिए कभी भी समान पासफ्रेज़ का उपयोग न करें, और अपने उपयोगकर्ता नाम और पासवर्ड टीम के सदस्यों सहित किसी के साथ साझा न करें।
- किसी भी समय दो-कारक प्रमाणीकरण का उपयोग करें, यह उपलब्ध है।



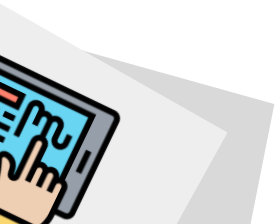
Confederation of Indian Industry
Digital Saksham

सॉफ्टवेयर अपडेट

02

Confederation of Indian Industry
Digital Saksham

सभी सॉफ्टवेयर और सिस्टम को अपडेट रखना महत्वपूर्ण है क्योंकि इनमें फिक्सेस और पैच होते हैं जो सॉफ्टवेयर और सिस्टम को हमले से बचाते हैं।



Confederation of Indian Industry
Digital Saksham

अपडेट के लिए दिशानिर्देश

- जब भी यह पेशकश की जाए, सभी डिवाइस और सॉफ्टवेयर पर ऑटो अपडेट सुविधा चालू करें।
- कंप्यूटर, फोन और टैबलेट के लिए सभी ऑपरेटिंग सिस्टम, सॉफ्टवेयर और प को नियमित रूप से अपडेट करें जैसे ही आपको एक नोटिफिकेशन मिलता है जो बताता है कि अपडेट तैयार है।
- सभी सॉफ्टवेयर और प्स को अपडेट करें - दोनों कंपनी द्वारा जारी किए गए और कर्मचारी द्वारा डाउनलोड किए गए।

CII
Confederation of Indian Industry
Digital Saksham

फायरवॉल

03

Confederation of Indian Industry
Digital Saksham

- फायरवॉल एक सुरक्षा उपकरण है जो ट्रैफिक को फिल्टर करके और बाहरी लोगों को व्यवसाय के कंप्यूटर पर निजी डेटा तक अनधिकृत पहुँच प्राप्त करने से रोककर व्यवसाय के नेटवर्क की सुरक्षा में मदद कर सकता है।
- यह आपके ऑपरेटिंग सिस्टम तक पहुंच प्राप्त करने के प्रयासों पर नजर रखता है और अवांछित ट्रैफिक या गैर-मान्यता प्राप्त स्रोतों को अवरुद्ध करता है।
- यह अवांछित आने वाले नेटवर्क ट्रैफिक को रोकता है और हैकर्स और मालवेयर जैसी किसी भी चीज के लिए नेटवर्क ट्रैफिक का आकलन करके एक्सेस को मान्य करता है।

इंटरनेट सुरक्षा

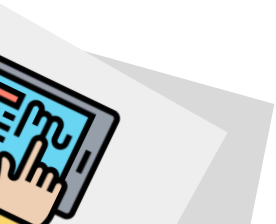
04

Confederation of Indian Industry
Digital Saksham

इंटरनेट सुरक्षा ऑनलाइन पहुंच और इंटरनेट के उपयोग के विशिष्ट खतरों और कमजोरियों पर केंद्रित है।

उपयोगकर्ताओं को इससे बचाता है:

- कंप्यूटर सिस्टम, ईमेल पते, या वेबसाइटों में हैकिंग
- दुर्भावनापूर्ण सॉफ्टवेयर जो सिस्टम को संक्रमित और क्षतिग्रस्त कर सकते हैं
- हैकर्स द्वारा पहचान की चोरी जो व्यक्तिगत डेटा जैसे बैंक खाते की जानकारी और क्रेडिट कार्ड नंबर चुराते हैं।



CII
Confederation of Indian Industry
Digital Saksham

कुछ सामान्य इंटरनेट सुरक्षा खतरे हैं:

- **मालवेयर**

"दुर्भाविनापूर्ण सॉफ्टवेयर" के लिए संक्षिप्त, मालवेयर कई रूपों में आता है, जिसमें कंप्यूटर वायरस, वर्म्स, ट्रोजन और बेईमान स्पाइवेयर शामिल हैं।

- **कंप्यूटर वर्म**

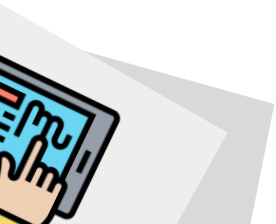
कंप्यूटर वर्म एक सा सॉफ्टवेयर प्रोग्राम है जो खुद को एक कंप्यूटर से दूसरे कंप्यूटर में कॉपी करता है। इन प्रतियों को बनाने के लिए मानवीय संपर्क की आवश्यकता नहीं होती है और यह तेजी से और बड़ी मात्रा में फैल सकता है।

CII Confederation of Indian Industry
Digital Saksham

कुछ सामान्य इंटरनेट सुरक्षा खतरे हैं:

- **स्पैम**

स्पैम आपके ईमेल इनबॉक्स में अवांछित संदेशों को संदर्भित करता है। कुछ मामलों में, स्पैम में केवल जंक मेल शामिल हो सकता है जो उन वस्तुओं या सेवाओं का विज्ञापन करता है जिनमें आपकी रुचि नहीं है। इन्हें आमतौर पर हानिरहित माना जाता है, लेकिन कुछ में से लिंक शामिल हो सकते हैं, जिन पर क्लिक करने पर आपके कंप्यूटर पर दुर्भावनापूर्ण सॉफ्टवेयर स्थापित हो जाएंगे।



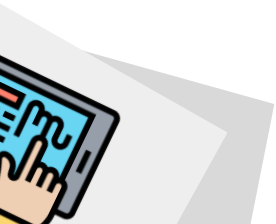
Confederation of Indian Industry

Digital Saksham

कुछ सामान्य इंटरनेट सुरक्षा खतरे हैं:

- **फिशिंग**

फिशिंग स्कैम साइबर अपराधियों द्वारा निजी या संवेदनशील जानकारी मांगने का प्रयास करके बनाए जाते हैं। वे आपके बैंक या वेब सेवा के रूप में सामने आ सकते हैं और आपको खाता जानकारी या पासवर्ड जैसे विवरणों को सत्यापित करने के लिए लिंक पर क्लिक करने का लालच दे सकते हैं।



Confederation of Indian Industry
Digital Saksham

कुछ सामान्य इंटरनेट सुरक्षा खतरे हैं:

- **बॉटनेट**

बॉटनेट निजी कंप्यूटरों का एक नेटवर्क है जिससे समझौता किया गया है। दुर्भावनापूर्ण सॉफ्टवेयर से संक्रमित, इन कंप्यूटरों को एक ही उपयोगकर्ता द्वारा नियंत्रित किया जाता है और अक्सर उन्हें नापाक गतिविधियों में शामिल होने के लिए प्रेरित किया जाता है, जैसे कि स्पैम संदेश भेजना या सेवा-से-इनकार (DoS) हमले।

इंटरनेट पर रहते हुए बरती जाने वाली सावधानियां:

- असुरक्षित वेबसाइटों पर जाने से बचें।
- अनजान ब्राउजर के इस्तेमाल से बचें।
- सार्वजनिक उपकरणों पर पासवर्ड सहेजने से बचें।
- अज्ञात वेबसाइटों पर सुरक्षित क्रेडेंशियल दर्ज करने से बचें।
- सोशल मीडिया पर अनजान लोगों से निजी जानकारी साझा न करें।
- यदि कोई ईमेल या SMS लिंक पुनर्निर्देशित किया जाता है, तो पृष्ठ की सुरक्षा को हमेशा सत्यापित करें।

Confederation of Indian Industry
Digital Saksham

डिवाइस/सिस्टम सुरक्षा

05

CII Confederation of Indian Industry
Digital Saksham

सुरक्षा उपाय जिसे पालन करना है:

- नियमित अंतराल पर पासवर्ड बदलें।
- डिवाइस पर एंटीवायरस इंस्टॉल करें और जब भी उपलब्ध हो अपडेट इंस्टॉल करें।
- उपयोग करने से पहले हमेशा अज्ञात USB ड्राइव/डिवाइस को स्कैन करें।
- अपने डिवाइस को खुला न छोड़ें।
- निर्दिष्ट समय के बाद डिवाइस के ऑटो लॉक को कॉन्फ़िगर करें।
- अज्ञात एप्लिकेशन या सॉफ्टवेयर स्थापित न करें।
- अज्ञात डिवाइस पर पासवर्ड या गोपनीय जानकारी संग्रहीत न करें।

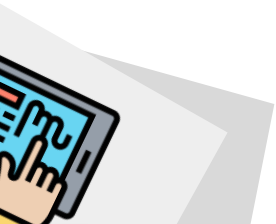
CII Confederation of Indian Industry
Digital Saksham

वित्तीय लेनदेन के लिए सामान्य सावधानियां

06

Confederation of Indian Industry
Digital Saksham

- आपके ब्राउज़िंग सत्र के दौरान दिखाई देने वाले संदिग्ध दिखने वाले पॉप अप से सावधान रहें।
- ऑनलाइन भुगतान करने से पहले हमेशा एक सुरक्षित भुगतान गेटवे (https:// - पैड लॉक प्रतीक के साथ URL) की जांच करें।
- अपना PIN (व्यक्तिगत पहचान संख्या), पासवर्ड और क्रेडिट या डेबिट कार्ड नंबर, CVV निजी रखें।



Confederation of Indian Industry

Digital Saksham

- वेबसाइट/डिवाइस/सार्वजनिक लैपटॉप/डेस्कटॉप पर कार्ड विवरण सहेजने से बचें।
- जहां सुविधा उपलब्ध हो वहां टू-फैक्टर ऑथेंटिकेशन ऑन करें।
- अज्ञात स्रोतों से आने वाले संदिग्ध अटैचमेंट या फिशिंग लिंक वाले कभी भी ईमेल न खोलें।
- चेक बुक, केवाईसी दस्तावेजों की प्रतियां अजनबियों के साथ साझा न करें।

CII Confederation of Indian Industry
Digital Saksham

सुरक्षित इंटरनेट बैंकिंग के लिए सावधानियां

07

CII
Confederation of Indian Industry
Digital Saksham

- सार्वजनिक उपकरणों पर हमेशा वर्चुअल कीबोर्ड का उपयोग करें क्योंकि कीस्ट्रोक को छेड़छाड़ किए गए उपकरणों, कीबोर्ड आदि के माध्यम से भी कैप्चर किया जा सकता है।
- इंटरनेट बैंकिंग सत्र का उपयोग करने के तुरंत बाद लॉग आउट करें।
- पासवर्ड को समय-समय पर अपडेट करते रहें।
- ईमेल और इंटरनेट बैंकिंग के लिए समान पासवर्ड का प्रयोग न करें।
- वित्तीय लेनदेन के लिए सार्वजनिक टर्मिनलों (जैसे साइबर कैफे, आदि) का उपयोग करने से बचें।

भुगतान धोखाधड़ी और इसकी पहचान कैसे करें

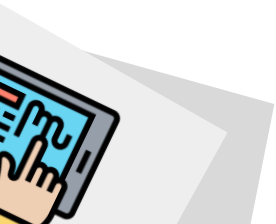
08

Confederation of Indian Industry

Digital Saksham

इन कोविड समय में, साइबर अपराधियों ने नए तौर-तरीके अपनाए हैं:

- टीके, दान और डिजिटल भुगतान के लिए धोखाधड़ी वाले कॉल और मेल।
- बैंक अधिकारियों के रूप में प्रस्तुत होने वाले साइबर अपराधी शुल्क के लिए ऋण पर स्थगन की पेशकश करते हैं।
- पीएम केयर्स फंड के लिए फर्जी UPI हैंडल।



CII Confederation of Indian Industry
Digital Saksham

इस्तेमाल की जाने वाली सावधानियां

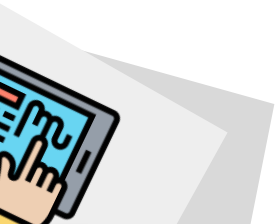
09

CII
Confederation of Indian Industry
Digital Saksham

इस्तेमाल की जाने वाली सावधानियां

ये कॉल घबराहट की भावना पैदा कर सकती हैं या कम कीमत पर कठिन परिस्थिति से बाहर निकलने का रास्ता पेश कर सकती हैं। जैसे - टीके, ऑक्सीजन सिलेंडर, वेंटिलेटर।

तात्कालिकता तेजी से कार्रवाई नहीं करने पर हारने के डर का आह्वान करेगी। इसलिए, अज्ञात नंबरों पर अग्रिम भुगतान करने से पहले ठीक से तथ्य जांच लें।



Confederation of Indian Industry
Digital Saksham

फिशिंग हमलों से सावधान रहें:

ये हमले फर्जी ईमेल भेजकर किए जाते हैं। इन ईमेल में से लिंक होते हैं जो आपकी जानकारी चुराने के लिए आपके सिस्टम में दुर्भावनापूर्ण सॉफ्टवेयर स्थापित कर सकते हैं।

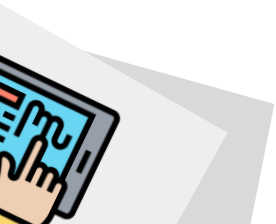
Confederation of Indian Industry

Digital Saksham

सुरक्षित रूप से खरीदारी करना

नकली ई-कॉमर्स साइटों से सावधान रहें, जो सच होने के लिए बहुत अच्छे हैं। इसलिए इन साइटों पर अपने कार्ड की जानकारी संग्रहीत करते समय सावधान रहें।

जांचें कि वेब पता https:// से शुरू होता है, जहां S सुरक्षित है।



Confederation of Indian Industry

Digital Saksham

OTP या व्यक्तिगत विवरण साझा न करें

डेबिट एवं क्रेडिट कार्ड नंबर, पिन, एक्सपायरी डेट, CVV नंबर, बैंक खाता विवरण, OTP आदि डिटेल्स किसी के साथ शेयर न करें।

यदि आप अपने बैंक खाते या डेबिट या क्रेडिट कार्ड या भुगतान के अन्य तरीकों से संबंधित कोई असामान्य गतिविधि देखते हैं तो तुरंत अपने बैंक से संपर्क करें।

फिशिंग

10

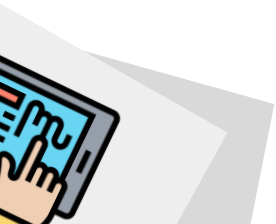
Confederation of Indian Industry
Digital Saksham

यह इस समय की सबसे आम साइबर समस्याओं में से एक है। साइबर खतरे का यह रूप एक हानिरहित दिखने वाले ईमेल के माध्यम से आता है जिसमें एक मालवेयर का लिंक होता है जिसे आपकी जानकारी चुराने के लिए प्रोग्राम किया जाता है।

Confederation of Indian Industry
Digital Saksham

फिशिंग हमलों के प्रकार

- उपयोगकर्ताओं को नकली ई-कॉमर्स या वित्तीय वेबसाइटों पर निर्देशित करके क्रेडेंशियल एकत्र करने के उद्देश्य से व्यापक गैर-लक्षित अभियान।
- स्पीयर-फिशिंग ईमेल विशिष्ट व्यक्तियों को उनके संगठन की सूचना प्रणाली में मालवेयर लगाने के लिए लक्षित करते हैं।



CII Confederation of Indian Industry
Digital Saksham

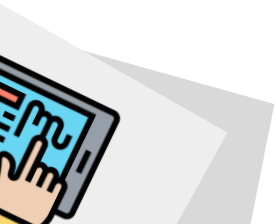
फिशिंग से बचाव के लिए अनुसरण करने की युक्तियां:

- प्रेषक के ईमेल पते और किसी भी अन्य पहचान की जानकारी, जैसे कि कंपनी का लोगो, सड़क का पता, और किसी भी विसंगति के लिए संपर्क विवरण, या संकेत यह नकली हो सकता है।
- यदि आप ईमेल भेजने वाले से परिचित नहीं हैं, तो किसी भी लिंक पर क्लिक न करें या ईमेल में कोई अटैचमेंट डाउनलोड न करें।
- किसी भी संदिग्ध ईमेल को हटा दें और तुरंत अपना ट्रैश खाली कर दें।

रैंसमवेयर

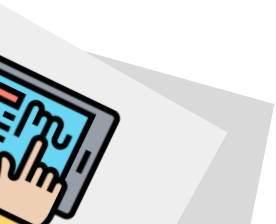
11

यह एक जबरन वसूली सॉफ्टवेयर है जो एक प्रकार का मालवेयर है जो आपके कंप्यूटर को लॉक कर सकता है और फिर इसे जारी करने के लिए फिरौती मांग सकता है।



कार्य-प्रणाली

मालवेयर पहले डिवाइस तक पहुंच प्राप्त करता है। रैंसमवेयर के प्रकार के आधार पर, या तो संपूर्ण ऑपरेटिंग सिस्टम या व्यक्तिगत फाइलें एन्क्रिप्ट की जाती हैं। इसके बाद पीड़ित से फिरौती की मांग की जाती है।



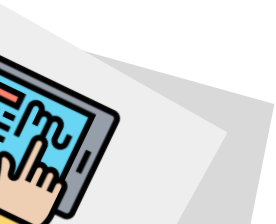
सुरक्षा कमजोरियां

- उपयोग किया गया उपकरण अब अत्याधुनिक नहीं है
- डिवाइस में पुराना सॉफ्टवेयर है
- ब्राउजर और/या ऑपरेटिंग सिस्टम अब पैच नहीं किए गए हैं
- कोई उचित बैकअप प्लान मौजूद नहीं है
- साइबर सुरक्षा पर अपर्याप्त ध्यान दिया गया है, और कोई ठोस योजना नहीं है।

CII Confederation of Indian Industry
Digital Saksham

रैंसमवेयर से बचाव

- असुरक्षित लिंक पर कभी भी क्लिक न करें
- व्यक्तिगत जानकारी का खुलासा करने से बचें
- संदिग्ध ईमेल अटैचमेंट न खोलें
- कभी भी अनजान USB डिवाइस का इस्तेमाल न करें
- प्रोग्राम अपडेट रखें



Confederation of Indian Industry

Digital Saksham

USB और हटाने योग्य मीडिया

12

Confederation of Indian Industry
Digital Saksham

USB डिवाइस हालांकि डेटा साझा करने के लिए अच्छे हैं, वायरस और मालवेयर पहुंचाने के लिए भी संवाहक हो सकते हैं।

USB के संबंध में पालन करने के लिए दिशानिर्देश:

- USB ड्राइव के उपयोग में आसान विकल्प पेश करें, जैसे कि क्लाउड-आधारित फ़ाइल-साझाकरण सेवाएं ताकि USB ड्राइव कम आवश्यक हों।
- ऐसा कंप्यूटर सेट करें जो कंपनी नेटवर्क से कनेक्ट न हो, जिसका उपयोग USB ड्राइव के लिए मालवेयर स्कैनर के रूप में और USB से आवश्यक जानकारी निकालने के लिए किया जा सकता है।
- सबसे महत्वपूर्ण बात यह है कि अच्छे निर्णय का प्रयोग करें। यदि आप नहीं जानते कि ड्राइव कहां से आई है, तो इसे प्लग इन न करें।

घटना की प्रतिक्रिया

13

जब कोई साइबर घटना होती है, तो व्यवसाय का ध्यान निम्नलिखित पर होना चाहिए:

- तैयारी करना: सुनिश्चित करें कि सभी कर्मचारी अपने काम और डेटा का नियमित रूप से बैकअप ले।
- प्रतिक्रिया दें: यदि कोई हमला या समस्या होती है, तो कंपनी नेटवर्क से प्रभावित डिवाइस को तुरंत डिस्कनेक्ट कर दें। सभी कर्मचारियों को यह कदम उठाना चाहिए।
- पुनर्प्राप्ति करना: गायब हो गए डेटा को पुनर्स्थापित करें और साइबर सुरक्षा के लिए अच्छी प्रथाओं को विकसित करने के लिए घटना का उपयोग करें।

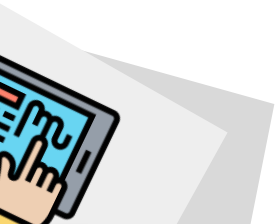
Confederation of Indian Industry
Digital Saksham

डेटा बैकअप और सुरक्षा

14

डेटा बेकअप

किसी डिवाइस पर महत्वपूर्ण जानकारी की एक कॉपी या संग्रह।



डेटा का बैकअप लेना

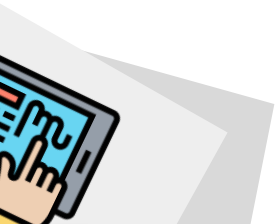
- अपनी महत्वपूर्ण जानकारी की एक कॉपी बनाएं
- इसे सुरक्षित, अलग स्थान पर स्टोर करें।
- बैकअप को अपने डिवाइस के लिए एक पुनर्स्थापना विधि के रूप में पहचानें।

Confederation of Indian Industry
Digital Saksham

डेटा बैकअप का महत्व

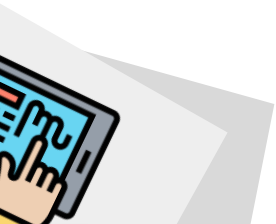
डेटा बैकअप कंपनी की महत्वपूर्ण जानकारी का एक सुरक्षित संग्रह है जो निम्नलिखित घटनाओं के होने की स्थिति में सुरक्षित रहता है -

- डिवाइस की चोरी
- रैंसमवेयर हमला
- डिवाइस वायरस से संक्रमित हो रहा है



डेटा जिसका व्यवसायों द्वारा बैकअप लिया जाना चाहिए:

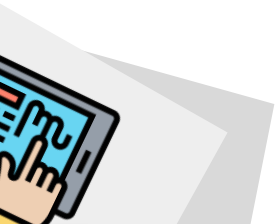
- ग्राहक डेटाबेस
- कॉन्फिगरेशन फाइलें
- मशीन इमेज
- ऑपरेटिंग सिस्टम
- रजिस्ट्री फाइलें
- दस्तावेज
- वित्तीय डेटाबेस
- स्प्रेडशीट्स
- ईमेल



CII Confederation of Indian Industry
Digital Saksham

डेटा बैकअप समाधान और विकल्प:

- रिमूवल मीडिया
- बाहरी हार्ड ड्राइव
- क्लाउड बैकअप
- बैकअप सेवाएं



Confederation of Indian Industry
Digital Saksham

सर्वोत्तम अभ्यास को पालन करना:

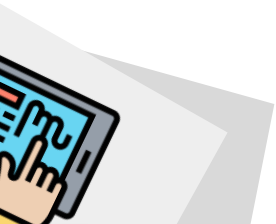
- नियमित रूप से बैकअप लें
- व्यवसायों को अधिक संग्रहण का विकल्प चुनना चाहिए
- भौतिक प्रतियों का उपयोग करें

अपनी खुद की डिवाइस नीति लाना (BYOD)

15

Confederation of Indian Industry
Digital Saksham

BYOD नीति कर्मचारियों को अपने निजी उपकरणों जैसे - लैपटॉप, स्मार्टफोन, टैबलेट का उपयोग कहीं से भी कंपनी डेटा तक पहुंचने में सक्षम बनाती है।



Confederation of Indian Industry

Digital Saksham

BYOD के लाभ

- **बढ़ी हुई उत्पादकता** – कर्मचारियों को डेटा एक्सेस करने और अपने निजी डिवाइस पर काम करने में एक स्तर का आराम मिलता है।
- **लागत में कटौती** - यह व्यवसाय को हार्डवेयर लागत बचाने में मदद करता है।
- **कर्मचारी विश्वास** – कर्मचारियों को यह समझने की जरूरत है कि कंपनी उपयोगकर्ता की गोपनीयता और व्यावसायिक डेटा की रक्षा कर रही है।

CII Confederation of Indian Industry
Digital Saksham

BYOD नीति बनाते समय ध्यान देने योग्य बातें:

कृपया विचार करने के लिए बिंदुओं की विस्तृत व्याख्या के लिए लिंक देखें - (https://www.ibm.com/downloads/cas/YK52D6GD)

- डिवाइस
- अनुपालन
- सुरक्षा
- ऐप्स
- समझौते
- कॉर्पोरेट एक्सेस
- उपयोगकर्ता गोपनीयता
- डेटा प्लान

CII Confederation of Indian Industry

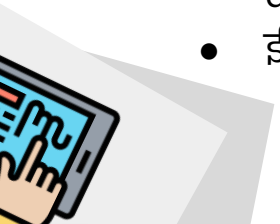
Digital Saksham

घर से काम करना – सर्वोत्तम अभ्यास

16

BYOD नीति बनाते समय ध्यान देने योग्य बातें:

- घर से एंटीवायरस और इंटरनेट सुरक्षा सॉफ्टवेयर का उपयोग करें
- परिवार के सदस्यों को काम के डिवाइस से दूर रखें
- स्लाइडिंग वेबकैम कवर में निवेश करें
- कर्मचारियों को एक्सेस करने के लिए कंपनियों को सुरक्षित VPN का उपयोग करने में निवेश करना चाहिए
- केंद्रीकृत भंडारण समाधान का उपयोग करें
- अपने घर को वाईफाई सुरक्षित करें
- अनधिकृत वीडियो कॉल प्लेटफॉर्म या प्स से संभावित जोखिमों से सावधान रहें
- मजबूत पासवर्ड बनाएं
- उपयुक्त सुरक्षा उपकरणों का उपयोग करके अपने ऑनलाइन बैंकिंग को सुरक्षित रखें
- ईमेल स्कैम से सावधान



CII Confederation of Indian Industry
Digital Saksham

प्रमुख निष्कर्ष

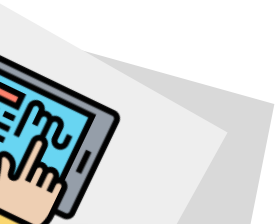
17

Confederation of Indian Industry

Digital Saksham

BYOD नीति बनाते समय ध्यान देने योग्य बातें:

- डिजिटल सुरक्षा आज के परिदृश्य में एक सफल व्यवसाय का एक महत्वपूर्ण निर्धारिक है जहां अधिक से अधिक व्यवसाय डिजिटल प्रक्रियाओं और उपकरणों को अपना रहे हैं।
- व्यवसाय अपने डेटा (व्यवसाय और ग्राहक) को डिजिटल सुरक्षा प्रोटोकॉल और उपकरणों को अपनाने की मदद से सुरक्षित कर सकते हैं जो ग्राहकों के बीच विश्वास को दोहराते हैं।
- डिजिटल सुरक्षा उपकरणों और प्रक्रियाओं के बारे में प्रशिक्षण से MSME मालिकों और कर्मियों का कौशल विकास होगा।



CII
Confederation of Indian Industry
Digital Saksham

धन्यवाद!!!