InfoSec for WOMEN

NATIONAL CYBER SECURITY AWARENESS MONTH

October, 2020

USB स्टोरेज एिवाइस सिक्यॉंरिटी

विभिन्न कंप्यूटरों के बीच डेटा ट्रांसफर करने के लिए छच्ए (यूनिवर्सल सीरियल बस) स्टोरेज डिवाइस बहुत सुविधाजनक हैं। आप इसे एक झळ पोर्ट में प्लग कर सकते हैं, अपने डेटा को कॉपी कर सकते हैं, इसे निकाल सकते हैं और डेट ा अपने साथ कहीं भी ले जा सकते हैं। दुर्भाग्य से यह पोर्टेबिलिटी, सुविधा और लोकप्रियता आपकी जानकारी के लिए विभिन्न खतरे भी साथ लाती है।

डेटा की चोरी और डेटा का लीकेज अब रोज़मर्रा की खबर है! जानकारी को सुरक्षित करने के लिए इन सभी को नियंत्रित या कम किया जा सकता है अथवा देखभाल, जागरूकता के साथ उचित उपकरण का उपयोग करके नियंत्रित या कम से कम किया जा सकता है।

खतरे

- मैलवेयर छच्ए स्टोरेज उपकरणों के माध्यम से फैलता है। कोई व्यक्ति आपकी गतिविधियों, फ़ाइलों, प्रणालियों और नेटवर्क को ट्रैक करने के लिए जानबूझकर मैलवेयर के साथ छच्ए स्टोरेज डिवाइस आपको बेच सकता है।
- ध मैलवेयर झळ स्टोरेज डिवाइसेस के माध्यम से एक डिवाइस से दूसरे डिवाइस में चोंहि.टी, जो डिफ़ॉल्ट रूप से सक्षम होती है, का उपयोग करके फैल सकता है।

अनधिकृत उपयोग

कोई व्यक्ति आपके छच्ए उपकरण को डेटा के लिए चुरा सकता है।

बेटिंग/ ललचाना

कोई व्यक्ति जानबूझकर आपके डेस्क या कार्यस्थल पर मैलवेयर युक्त छच्ए डिवाइस छोड़ देता है

USB स्टोरेज के माध्यम से डेटा लीकेज को कैसे रोकें?

- USB स्टोरेज उपकरणों के उपयोग को सीमित करने के लिए एक अच्छी सुरक्षा नीति को डिज़ाइन करें और अपनाएं।
- कर्मचारियों की निगरानी करें कि वे क्या कॉपी कर रहे हैं।
- अपनी जानकारी को सुरक्षित करने के लिए प्रमाणीकरण, अनुमोदन और लेखाजोखा रखने की प्रणाली लागू करें।

डिवाइस खो जाने पर क्या करें?

- यदि आपने झळ ड्राइव के अंदर पासवर्ड आदि जैसी कोई भी व्यक्तिगत या संवेदनशील जानकारी संग्रहीत की है, तो कोइ भी अकाउंट बनाते समय प्रदान किए गए सुरक्षा प्रश्नों और उत्तरों के साथ सभी पासवर्ड तुरंत बदल दें हैकर द्वारा चोरी की गयी ड्राइव में मौजूद आपके डेटा का उपयोग कर उसके द्वारा आपके ऑनलाइन अकाउंट की लॉगऑन जानकारी प्राप्त करने की संभावना हो सकती है।
- यह सुनिश्चित करें कि खो गए डेटा की सुरक्षा के लिए सभी सुरक्षा उपाय किए गए हैं।

डिवाइस की चोरी को कैसे रोकें?

- ड्राइव को चाबी के गुच्छे में लगाकर हमेशा भौतिक रूप से सुरक्षित रखें।
- अपनी ड्राइव को कभी भी कहीं भी उपेक्षित अवस्था में या बगैर ध्यान दिए न रखें।
- संवेदनशील जानकारी को कभी भी एन्क्रिप्शन के बगैर न रखें।

USB के रूप में मोबाइल

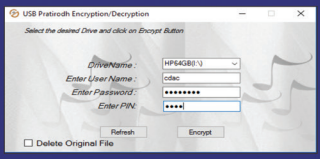
कंप्यूटर से कनेक्ट करने पर मोबाइल फोन को छच्ए मेमोरी डिवाइस के रूप में उपयोग किया जा सकता है। कंप्यूटर से कनेक्ट करने के लिए मोबाइल फोन के साथ एक झळ केबल दी जाती है।

- जब कोई मोबाइल फोन पर्सनल व्यक्तिगत कंप्यूटर से कनेक्ट किया जाता है, तो एक अपडेटेड एंटीवायरस का उपयोग करके उसकी एक्सटर्नल फोन मेमोरी तथा मेमोरी कार्ड को स्कैन करें।
- अपने फोन और एक्सटर्नल मेमोरी कार्ड का नियमित बैकअप लें क्योंकि यदि सिस्टम कैश या मैलवेयर प्रवेश जैसी कोई घटना होती है, तो कम से कम आपका डेटा सुरक्षित रहता है।
- कंप्यूटर से डेटा को मोबाइल में स्थानांतरित करने से पहले, डेटा को सभी अपडेट युक्त नवीनतम एंटीवायरस द्वारा स्कैन किया जाना चाहिए।
- कहीं जाने से पहले अपने कंप्यूटर से झळ (यूनिवर्सल सीरियल बस) कनेक्शन को निकालना याद रखें।
- वायरस से प्रभावित डेटा कभी किन्ही अन्य मोबाइल्स को फॉरवर्ड नहीं करें।

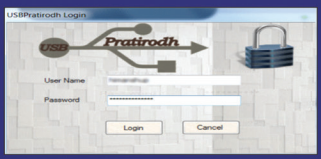
USB PRATIRODH

Standalone Version

USB Pratirodh is a software solution which controls unauthorized usage of portable USB mass storage devices



About USB Pratirodh :
USB Pratirodh controls the usage of removable storage media like pen drive, external hard drives, cell phones and other supported USB mass storage devices. Only authenticated users can access the removable storage media.



Benefits

- USB device control with password protection
- Data Encryption on USB devices
- Auto run protection and Malware Detection
- Configurable read/write privilege protection