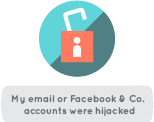
किट-१: मेरा ईमेल, फेसबुक या ट्विटर का खाता किसी ने चुरा लिया है.

मेरे अपने नाम से बनाये गए इ-मेल, फेसबुक और ट्विटर के खातों का मैं इस्तेमाल नहीं कर पा रहा हूँ. अगर किसी ने मेरे इन खातों को लागइन करने की सूचना ( यानि कि यूजर आईडी और पासवर्ड) चुरा लिया है और उसके पासवर्ड को बदल दिया है, जिसके कारण मैं इन खातों का इस्तेमाल नही कर पा रहा, तो ऐसी स्थिति में मुझे क्या करना चाहिए?

 मेरे ईमेल और फेसबुक और कंपनी का इ-मेल खाता किसी और ने चुरा लिया है.

एक दिन आपने अपना कंप्यूटर ऑन किया और पता चला कि न तो आप अपने इ-मेल, फेसबुक या ट्विटर, किसी भी अकाउंट का इस्तेमाल नही कर पा रहे. आप को पूरी तरह से यह विश्वास है कि आपने अपना पासवर्ड सही डाला है, पर किसी ने उसको बदल दिया है.

**तो ऐसी स्थिति में क्या करना चाहिए**

ऐसी स्थिति में सबसे पहले तो यह सुनिश्चित करें कि आप जो भी डाटा एनटर कर रहे हैं वो सही लाग-इन पेज के ऊपर कर रहे हैं ; यानि कि जो लिंक और इंटरफ़ेस आपके सामने कंप्यूटर के स्क्रीन पर आ रहा है वो वास्तविक है. ध्यान से देखिये कि यूआरएल कहीं थोडा बहुत बदला हुआ तो नहीं है. भलाई इस बात में है कि अपने आस पास किसी से यह सुनिश्चित कर लें कि आप जिस पेज को देखना चाहते हैं, वो मौजूद है और किन्ही तकनीकी कारणों से बंद तो नहीं है: ऐसी स्थिति कई बार बड़े से बड़े सर्विस प्रोवाइडर को भी झेलनी पडती है.

पासवर्ड पुनः सेट करिये. इसके बावजूद अगर लाग इन करने में असमर्थ हो रहे हैं तो आप वेब पेज पर यह एंट्री डालिए कि आप अपना पासवर्ड भूल गए हैं, और अब आप उसको फिर से सेट करना चाहते हैं. लगभग जितनी भी ऑनलाइन सेवाएं जो आज नेट के उपर उपलब्ध हैं , उनमें यह प्रावधान है कि आप किसी न किसी तरह से अपना पासवर्ड फिर से सेट कर सकते हैं और अपने अकाउंट को फिर से प्रयोग कर सकते हैं.

* इ-मेल : अधिकांश ईमेल की सेवाएं देने वाली साईट्स आपको अपने पासवर्ड को फिर से सेट करने के लिए अनुमति देने का विकल्प रखते हैं , और इसके लिए वे या तो आपके अन्य इ-मेल अकाउंट पर एक रिसेट लिंक भेजते हैं या आपके मोबाइल पर एक अस्थायी लॉग-इन कोड भेजते हैं या सुरक्षा प्रश्नों की एक श्रृंखला का जवाब देने के लिए कहते हैं । पासवर्ड को फिर से प्राप्त करने के प्रत्येक सर्विस प्रदाता के पास अलग-अलग विकल्प हैं, लेकिन इस दिशा में निर्देश प्राप्त करने की प्रक्रिया आमतौर पर आसान होनी चाहिए।
* फेसबुक: अगर फेसबुक अकाउंट में ऐसी स्थिति पैदा हो गयी है तो **'अपना पासवर्ड भूल गए? "** लिंक के उपर जायें और अपने अकाउंट की पहचान करें। फिर आपको फेसबुक पेज के माध्यम से अपने अकाउंट के फिर से प्रयोग करने की प्रक्रिया बताई जाएगी, जो कि या तो एक इ-मेल के रूप में होगी- वह इ-मेल जो कि आपके अकाउंट से जुडा हुआ है, या एक मोबाइल लिंक के माध्यम से आपके मोबाइल नंबर पर- अगर आपने अपने मोबाइल नंबर को भी अपने फेसबुक अकाउंट से जोड़ रखा है तो. (किट 3 # देखें) अगर आप इन दोनों में से किसी भी प्रक्रिया का प्रयोग करके अपने अकाउंट का प्रयोग नहीं कर पा रहे तो इसका मतलब है कि हैकर ने आपके अकाउंट से सम्बंधित जानकारी बदल दी है . ऐसी स्थिति में आपके पास विकल्प है कि आप एक नया ई-मेल या फोन नंबर प्रस्तुत कर सकते हैं, और इसी के साथ साथ अपने अकाउंट को फिर से चालु करने के लिए आपको अपने " भरोसेमंद संपर्क " की मदद भी लेनी होगी. अकाउंट को फिर से चालू करने के लिए। कभी-कभी आपको अपने अकाउंट का फिर से उपयोग करने के लिए 24 घंटे तक का इंतज़ार भी करना पड़ सकता है. इस प्रक्रिया को करने के बाद भी अगर आप अंततः अपने अकाउंट तक पहुंच हासिल नहीं कर सकते हैं, तो आपको फेसबुक को यह रिपोर्ट करना पड़ेगा कि आपके अकाउंट पर किसी और ने कब्जा कर लिया है.
* ट्विटर: यदि आप अपने अकाउंट में लाग-इन नहीं कर सकते हैं, तो आप एक अस्थायी लॉग-इन कोड का अनुरोध कर सकते हैं जो कि आपके ई मेल पते पर या मोबाइल फोन पर एसएम्एस के माध्यम से भेज दिया जाता है.। यह अस्थायी कोड सिर्फ एक बार ही इस्तेमाल हो सकता है । आप ट्विटर लॉग-इन पृष्ठ पर "पासवर्ड भूल गए?" लिंक के माध्यम से आपके ईमेल पते पर रीसेट लिंक भेजे जाने के लिए अनुरोध कर सकते हैं।
* अब जबकि आपके पास अपने अकाउंट से संपर्क टूट गया है, यह श्रेयस्कर होगा कि आप अपने किसी भरोसे वाले आदमी से यह अनुरोध करें कि वो आपकी तरफ से आपके घनिष्ट मित्रों को यह सूचित कर दे कि आपका अकाउंट हैक कर दिया गया है और जो सन्देश उन्हें आपके नाम से प्राप्त हो रहे हैं वो किसी छद्म व्यक्ति द्वारा भेजे जा रहे हैं.

## भविष्य में इस समस्या से कैसे निजात पाई जाए ?

जब आप फिर से अपने विभिन्न खातों का प्रयोग करने में सफल हो जायें तो निम्न तुरंत करें:

1. अपने अकाउंट की सेटिंग में जायें और वहां जाकर अपना पास फ्रेज बदल दें और इसके साथ ही साथ एक अन्य इ-मेल खाता भी अपने अकाउंट के साथ जोड़ दें.
2. अगर हो सके तो, अपना मोबाइल नंबर भी इस अकाउंट के साथ जोड़ दें, बशर्ते कि आपकी सरकार की यह ख्याति न हो कि वो मोबाइल सेवा प्रदाताओं के साथ मिल कर आपके मोबाइल के अकाउंट अपनी जांच के दायरे में रखती हो, अगर ऐसा है तो फिर अपना मोबाइल नंबर इस अकाउंट के साथ मत जोडें. अगर यह एक ऐसा मुद्दा नही है जो परेशान कर सकता है तो फिर अपने अकाउंट के साथ दो चरणीय या दो पद्धति सत्यापन प्रक्रिया जिसमे पासवर्ड और मोबाइल नंबर दोनों शामिल हैं (**२ ऍफ़ ए**) जरूर क्रियान्वित रखिए.
3. अपने अकाउंट की सिक्यूरिटी सेटिंग में जाईये और लाग-इन अलर्ट और लाग-इन सत्यापन को सक्रिय कीजिए. फेसबुक पर आप सक्रिय सत्रों यानि जितनी बार आपने अपने अकाउंट का इस्तेमाल किया है उसको देख सकते हैं , और किन किन जगहों से लाग –इन किया गया है उसका पुनरावलोकन कर सकते हैं. अगर आपको ऐसा लगता है कि किसी अनजाने उपकरण के माध्यम से या किसी अनजानी जगह से लाग-इन किया गया है तो “ गतिविधि समापन या एंड एक्टिविटी “ और क्लिक करके अपना सेशन खत्म कर सकते हैं.
4. आपके अकाउंट के संपर्क के माध्यम से चल रही विभिन्न थर्ड पार्टी एप्प्लिकेशंस जिनको आपने अनुमति प्रदान कर रखी है उनका पुनरवलोकन कर सकते हैं. फेसबुक पर आप “विश्वसनीय संपर्कों को फिर से निर्धारित कर सकते हैं जो कि भविष्य में अकाउंट के बंद हो जाने की स्थिति में आपकी मदद कर सकते हैं.
5. फेसबुक और ट्विटर पर जो भी लाग आपको फॉलो करते हैं उनके अकाउंट की एक बार फिर से जाँच करें ताकि यह निश्चित हो जाये कि हाल-फिलहाल में आपके संपर्क में आने वाले अकाउंट धारक संदेह के दायरे में रहने वाले तो नही हैं . फेसबुक के सम्बन्ध में यह और भी महत्वपूर्ण है क्योंकि आपकी प्राइवेसी सेटिंग के आलोक में आपके द्वारा किये गए सभी पोस्ट इनके फेसबुक अकाउंट में भी दिखाई देंगे.

## ध्यान दीजिये

आपके अकाउंट पर हमला करने वाले का हमेशा यह मकसद नहीं होता कि आपके पास फ्रेज को बदल कर आपको अपना ही खाता इस्तेमाल करने से रोक दे. एक हमलावर आपके अकाउंट पर इसलिए भी हमला कर सकता है ताकि आपकी गतिविधियों का सर्वेक्षण कर सके और आपके नाम का इस्तेमाल करके आप के चरित्र को भी नुक्सान पहुंचा सके. आपको यह पता भी नहीं चल पाएगा कि आप हैकिंग के शिकार हो गए हैं.

हर बार जब आप अपने अकाउंट का प्रयोग करते हैं तो एक नया सेशन बनाते हैं, और जब आप लाग आउट कर जाते हैं तो सत्र का समापन कर दीजिये. वेब ब्राउज़र से हर सत्र को लाग आउट कीजिये. सक्रिय सत्र और क्रियाकलाप जैसे कि संदेश, पोस्ट्स, थर्ड पार्टी अप्प्लिकेशन, और नए बनाये गए दोस्तों के क्रियाकलापों और उनके पोस्ट्स पर आपको विशेष ध्यान देने की जरूरत है.

यह देखा गया है कि फेसबुक के खातों पर जो सबसे खतरनाक हमले होते हैं वो उन दुर्भावनापूर्ण लिंक्स के द्वारा किये जाते हैं जो कि देखने में तो बहुत साधारण सी लगती हैं पर सबसे ज्यादा नुक्सान वही पहुँचाती हैं. ऐसे लिंक आपकी व्यक्तिगत जानकारी को जग जाहिर कर सकते हैं या आपके किसी प्रतिद्वंदी को यह अवसर प्रदान करते हैं कि आपका अकाउंट वो अपने नियंत्रण में कर ले. भलाई इसी में है कि अनजान व्यक्तियों द्वारा आपके इनबॉक्स में भेजे गए किसी भी लिंक या अटैचमेंट्स को क्लिक न करें और यहाँ तक कि विश्वशनीय मित्रों के द्वारा, जो कि आपके दोस्तों की सूचि में है, उसको भी क्लिक न करें.

यह सुनिश्चित करें कि जब भी आप अपने अकाउंट में लाग इन कर रहे हैं तो एड्रेस बार में https स्पष्ट दिख रहा हो. अगर आप अपने फोने का इस्तेमाल इन्टरनेट के प्रयोग के लिए कर रहे हैं तो कोशिश करें कि फोन की स्टैंड अलोन एप्लीकेशन का प्रयोग न हो, क्योंकि आप इस बात के लिए निश्चिन्त नहीं हो सकते कि आपका कनेक्शन सुरक्षित है. इसके बजाये आपके फोन के ब्राउज़र के माध्यम से सामाजिक नेटवर्क की साइट्स पर संपर्क उनके https यू आर एल से ही करें.

यह तो सही है कि अपने कार्यकलापों को एक सिलसिलेवार आयाम देने में फेसबुक महत्वपूर्ण भूमिका निभाता है पर यह हमेशा ध्यान रखना चाहिए कि फेसबुक एक सुरक्षित माध्यम नहीं है . आपके दोस्त और संपर्क आपकी सुरक्षा कवच में खामियों के कारण प्रतिकूल रूप से प्रभावित हो सकते हैं और यही उनके उपर भी लागू है. इसलिए ऑनलाइन मुहीम चलाने का बीड़ा उठाना एक बहुत ही जिम्मेदारी भरा हुआ काम है.

## कहाँ से मदद मिल सकती है

**नियंत्रित** करिए कि फेसबुक में कहाँ से लाग इन किया जा रहा है

* खोए हुए या भूल गए पासवर्ड को ट्विटर के माध्यम से फिर से प्राप्त कीजिये और पता लगाईये कि आपका ट्विटर खाता कही हैक तो नहीं हो गया है.
* सामाजिक नेटवर्किंग साईट्स के बारे में कुछ सुरक्षा सुझावों को पढ़िए
* पता करिए कि आपका जीमेल खाता हैक तो नहीं हो गया है

**किट # 2 अगर अपने कंप्यूटर की सामग्री को जब्त कर लिया जाता है, मुझे डर है कि इससे मेरी निजि सुरक्षा को नुक्सान पहुँच सकता है .**

# मेरा कंप्यूटर, खो सकता है, चोरी हो सकता है या जब्त कर लिया जा सकता है । ऐसी स्थिति मैं क्या कर सकता हूँ, जिसके कि मेरे कंप्यूटर में मौजूद डाटा मुझे या और किसी को एक प्रतिकूल परिस्थिति से बचा सके?

 मुझे इस बात का डर है कि अगर मेरे कंप्यूटर कही जब्त हो गया तो इससे मेरी सुरक्षा को नुक्सान पहुँच सकता है.

कंप्यूटर अक्सर खो जाते हैं, या चोरी हो सकते हैं या अधिकारियों, जो कि कंप्यूटर में मौजूद डाटा के पीछे पड़े हैं , द्वारा जब्त भी किये जा सकते हैं। आपका उपकरण एक तिजोरी की तरह है जिसमें संवेदनशील डाटा मौजूद रहता है. अगर यह डाटा किसी अविश्वस्त के हाथ लग जाये तो उसके अंदर यह क्षमता है कि आपको वो भारी चोट पहुंचा सके. उदाहरण के लिए, अगर आप थंडरबर्ड या आउटलुक ईमेल क्लाइंट प्रबंधन का उपयोग ईमेल भेजने के लिए कर रहे हैं तो, इस बात की पूरी सम्भावना है कि इस तरह के कार्यक्रम में आपके मित्रों के संपर्क से सम्बंधित सूचना और अन्य संवेदनशील निजी जानकारी, इस कार्यक्रम में शामिल हैं। अगर आपका कंप्यूटर खो जाता है, चोरी या जब्त कर लिया जाता है, तो नए मालिकों को आपकी यह सारी जानकारी प्राप्त हो जाती है । इसके साथ ही साथ और हानिकारक हो सकता है इन नए मालिकों द्वारा आपके पहचान को जामा पहन कर आपके जानकारों को संपर्क सन्देश के भेजे जाने की प्रक्रिया का शुरू कर देना, जो कि आपके लिए सबसे ज्यादा घातक हो सकता है.

## आपको क्या करना चाहिए

## अगर आपका कंप्यूटर गुम हो गया तो आप कुछ भी नहीं कर सकते. तो आप अपने सिस्टम को इस तरह से तैयार करें और अपने कंप्यूटर का उपयोग इस तरह से करें कि नुकसान की स्थिति में, संपर्क और अन्य संवेदनशील डाटा का रिसाव कम से कम हो सके.

* जानकारी के रिसाव के खिलाफ एक सबसे बुनियादी सुरक्षा के रूप में एक अवसरवादी (लक्षित नहीं) चोरी या नुकसान की वजह से, एक डेस्कटॉप आधारित पास फ्रेज का उपयोग करें। अपनी डिवाइस को इस तरह कॉन्फ़िगर करें को उसके चालू करने के बाद किसी भी प्रोग्राम का उपयोग करने से पहले एक पास फ्रेज की लक्ष्मण रेखा को लांघने की आवश्यकता हो , और एक पासवर्ड से सुरक्षित स्क्रीन सेवर या लॉक स्क्रीन सिस्टम में मौजूद हो जो कि स्वचालित रूप से कंप्यूटर या डिवाइस की निष्क्रियता के पांच मिनट के बाद सक्रिय हो जाए।
* यह बात ध्यान में रखें कि भले ही आपका कंप्यूटर किसी अन्य व्यक्ति द्वारा प्रयोग में लाया जा सकता है, पर आपके कंप्यूटर में मौजूद डाटा तक पहुँच पाना उतना आसांन नहीं होता, पर , पासवर्ड की दीवार को अनुभवी प्रौद्योगिकीविदों या कानून प्रवर्तन संस्थाओं द्वारा भेद पाना अपेक्षाकृत आसान है।
* अपने उपयोगकर्ता खातों को सुरक्षित रखें। आपके ब्राउज़र में अपने पासफ्रेज स्टोर मत रखें । उन्हें अपने डेस्कटॉप पर एक फ़ाइल में न रखें । उन्हें ईमेल या एसएमएस के द्वारा अपने आप को न भेजें। उन्हें अपनी मेज पर एक कागज के टुकड़े पर लिख कर न रखें । आपके ऑनलाइन उपयोगकर्ता खातों के लिए पासफ्रेज या तो अपने मस्तिष्क में या एक एन्क्रिप्टेड ढंग से जमा करके रखें . (देखें किट # 3)
* अपने ईमेल को सुरक्षित रखें। सुनिश्चित करें कि आपके ईमेल क्लाइंट आपको इस बात की इजाजत देते हैं कि आप अपनी प्रोफ़ाइल रक्षा के लिए उपयोग कूटशब्द- का प्रयोग क्र सकते हैं । जहाँ यह एक आम चोर के खिलाफ मदद करता है, वहीं वे कंप्यूटर विशेषज्ञ, जो आपके अपने डेटा में रुचि रखते हैं उनको रोकने में पूरी तरह सफल नहीं हो पाता । अगर आपको ऐसा लगता है कि आपके अपने ईमेल में मौजूद सामग्री के जग जाहिर होने से आपको एक वास्तविक खतरा बन सकता है, तो अपने ईमेल क्लाइंट से सम्बंधित सारी जानकारी का भंडारण ट्रूक्रिप्ट के द्वारा एन्क्रिप्ट करने पर विचार करें। [1] आप अपने मेल क्लाइंट को कॉन्फ़िगर कर सकते हैं ताकि जब पहली बार आपका क्लाइंट डाटा डाउनलोड करता है या सन्देश भेजता है तो उसको खोलने के लिए वो आपसे पासवर्ड का आग्रह करे. इसका फायदा यह होगा कि आपके नाम का कोइ गलत इस्तेमाल नहीं कर सकेगा.
* संवेदनशील फ़ाइलों को एनक्रिप्ट करें । यह अपनी आदत में शामिल कर लें कि कोई भी ऐसा डाटा जिसमें संवेदनशीलता है उसको आपके कंप्यूटर के अन्य डाटा से अलग रखना है, और इस इस संवेदनशील डेटा को एन्क्रिप्टेड करके रखने की आदत बना लें। डेटा को एन्क्रिप्टेड करके रखने के लिए एक विशिष्ट एन्क्रिप्शन सॉफ्टवेयर का प्रयोग करें जैसे कि फ्री / लिब्रे और "ट्रू क्रिप्ट " का प्रयोग करके अपने कंप्यूटर के हार्ड डिस्क में एक एन्क्रिप्टेड वॉल्यूम (डिस्क स्पेस) बनाएं. एन्क्रिप्टेड वॉल्यूम में अपनी संवेदनशील जानकारी रखें। एक एन्क्रिप्टेड वॉल्यूम एक तिजोरी है जो केवल आपके द्वारा ही खोला जा सकता है या जिसे आप पासवर्ड बता दें उसके द्वारा.

डिवाइस की ड्राइव एन्क्रिप्ट करना । डिस्क एन्क्रिप्शन का उपयोग करके आप इस बात को सुनिश्चित करते हैं कि केवल आप ही वो व्यक्ति होंगे जो पास फ्रेस का उपयोग करके कंप्यूटर में मौजूद सामग्री का उपयोग कर सकते हैं। ऑपरेटिंग सिस्टम के स्तर पर, आप पूरे कंप्यूटर को एन्क्रिप्ट कर सकते हैं, जो कंप्यूटर बंद हो जाने की स्थिति में उसमें मौजूद सारी सामग्री को सुरक्षित रखता है. ध्यान दें कि एक बार जब डिस्क डीक्रिप्ट हो गयी है और कंप्यूटर सुप्तावस्था में है, उसमें मौजूद डेटा आम तौर पर प्रयोग में लाया जा सकता है, और यह तब तक हो सकता है जब तक पूरी तरह से डिस्क फिर एन्क्रिप्टेड न हो जाये (आमतौर पर कंप्यूटर बंद करके)।

ट्रूक्रिप्ट विंडोज, मैक और जीएनयू / लिनक्स पर काम करता है। एंड्रॉयड और आईओएस डिवाइस पर एन्क्रिप्शन डिवाइस सेटिंग्स के तहत सक्रिय किया जा सकता है। अगर आप एक जीएनयू / लिनक्स के उपयोगकर्ता हैं तो आप इन्स्टालेशन प्रक्रिया के दौरान एन्क्रिप्ट कर सकते हैं । यह ध्यान रखें कि आपके एन्क्रिप्शन पास फ्रेस के बिना डेटा का उपयोग करना असंभव होगा. ( यह मुद्दा है ; हालांकि, अपने स्वयं के डेटा के नियंत्रण के इस संभावित नुकसान अपने आप में एक जोखिम है)

**कहां से और अधिक मदद मिल सकती है**  
• अपने कंप्यूटर पर संवेदनशील फाइलों को सुरक्षित रखें।  
• पासफ्रेज बनाएं और उन्हें सुरक्षित रखें।  
• अपने मोज़िला थंडरबर्ड ईमेल क्लाइंट की सामग्री को सुरक्षित रखें।  
• GNU / लिनक्स ऑपरेटिंग सिस्टम के बारे में जानें।  
• ट्रू क्रिप्ट के बारे में जानें।  
  
[1] नोट: सितंबर 2015 में, ट्रू क्रिप्ट- फ़ाइल और डिस्क एन्क्रिप्शन के लिए खुला स्रोत सॉफ्टवेयर- में महत्वपूर्ण सुरक्षा से सम्बंधित दोष पाए गए.परिणामस्वरुप, हम हमारे द्वारा दी गयी सलाह की समीक्षा कर रहे हैं और हम सुरक्षित फ़ाइल भंडारण के लिए इन वैकल्पिक उपकरणों का समर्थन करते हैं।

किट # 3। मैं अपने पासफ्रेज सुरक्षित रखना चाहता हूँ

# मैं अपने सभी महत्वपूर्ण पासफ्रेज कागज के एजेंडे में और अपने मोबाइल फोन में रखता हूँ, और इसके अलावा मेरा ब्राउज़र वे सभी पासफ्रेज जो मैं ऑनलाइन उपयोग करता हूँ याद रखता है। पर शायद यह सुरक्षित तरीका नहीं है। क्या कोई बेहतर समाधान है?

 मैं अपने पासफ्रेज सुरक्षित रखना चाहता हूँ

आप कई ऑनलाइन सेवाओं का उपयोग कर रहे हैं और प्रत्येक सेवा के लिए एक अलग पास फ्रेज का प्रयोग कर रहे हैं क्योंकि यह तरीका सुरक्षित है। आप उन सभी पास फ्रेज को तो याद नहीं कर सकते इसलिए आपने उन्हें याद करने की अनुमति अपने ब्राउज़र को दे रखी है । इसके अलावा आपको अन्य महत्वपूर्ण और संवेदनशील जानकारी याद रखनी होती है जैसे पिन, क्रेडिट कार्ड नंबर और महत्वपूर्ण फोन नंबर। क्योंकि इन सभी को याद रखना किसी के लिए असंभव है, आप इन सबके पासफ्रेज कागज पर और अपने डेस्कटॉप पर एक टेक्स्ट दस्तावेज़ में रखते हैं। लेकिन अगर वो कागज कही खो गया तो आप के जितने भी खातें है के उनका प्रवेश द्वार आपके लिए बंद हो जाएगा. अगर किसी अनजान आदमी के हाथ आपका कंप्यूटर या मोबाइल फोन लग गया, और उसने उस डॉक्यूमेंट को भी पा लिया तो उसके लिए आपके सारे खातों तक पहुँच जाना बच्चों का खेल हो जाता है.

**आपको क्या करना चाहिए**  
एक अच्छे पासफ्रेज प्रबंधन और ख़राब पासफ्रेज प्रबंधन के कुछ विकल्प हैं और कई तरीके भी हैं । यहाँ आपको क्या करना चाहिए और क्या नहीं करना चाहिए की एक सूची है।

* कभी भी अपने डेस्कटॉप पर या किसी अन्य तरह से जैसे कि एक टेक्स्ट फ़ाइल में पासफ्रेज या अन्य संवेदनशील जानकारी स्टोर न करें ताकि कभी कोई भी घुसपैठिया अगर आपके कंप्यूटर तक पहुँच भी जाता है तब भी आपके विभिन्न एकाउंट्स तक उसके लिए पहुंचना असंभव होगा.
* अपने ब्राउज़र के पासफ्रेज प्रबंधक में अपने विभिन्न खातों के पासफ्रेज को सहेज कर न रखें. अपने ब्राउज़र को ऑनलाइन सेवाओं जैसे आपका ईमेल या फेसबुक अकाउंट 'के पासफ्रेज याद रखने की अनुमति देने का मतलब है कि वह आपके पासफ्रेज एक एन्क्रिप्टेड फाइल में ही रखता है जिसको कोई भी व्यक्ति जो आपके कंप्यूटर का उपयोग कर रहा है, भौतिक रूप से या कही दूर से भी जान सकता है और आपके एकाउंट्स के साथ दुरूपयोग कर सकता है । उदाहरण के लिए, किसी एक मैलवेयर कार्यक्रम के माध्यम से दूरस्थ से आपके कंप्यूटर का उपयोग हो सकता है। यदि ऐसा होता है, तो कृप्या किट # 1 देखें- मेरा ईमेल, फेसबुक या ट्विटर खाते का अपहरण कर लिया गया । ब्राउज़र सेटिंग्स मेनू से, अपने पासफ्रेज के भंडारण को रोकने का निर्देश क्रियान्वित कर दें, जो पासफ्रेज संग्रहीत हैं उनको डिलीट कर दें, और भविष्य में आपसे अपने लॉग-इन जानकारी स्टोर करने के विकल्प को ही ब्राउज़र से नामंज़ूर कर दें ।
* स्टैंडअलोन आधार पर एक पासफ्रेज प्रबंधक एप्लीकेशन को स्थापित करें। यह आपको आसानी से ऑनलाइन फोर्मों में पासफ्रेज कॉपी और पेस्ट करने की अनुमति देता है। सॉफ्टवेयर इस तरह से बनाया गया है कि आपको कभी भी अपने स्क्रीन पर पासफ्रेज प्रदर्शित करने की जरूरत नहीं पड़ेगी । और क्योंकि आपको अब उन्हें टाइप करने की जरूरत नहीं है, यह आपको कुछ परिष्कृत तकनीक निगरानी से, विशेष रूप से शोल्डर सर्फिंग से बचाता है। अगर कोई आपके कंप्यूटर पर नियंत्रण कर भी लेता है, तो वे मास्टर पासफ्रेज के अभाव में किसी भी तरह की जानकारी के किसी भी तरह के उपयोग करने में सक्षम नहीं होगा।

एक पासफ्रेज प्रबंधक एप्लीकेशन जो विंडोज, मैक और जीएनयू / लिनक्स के लिए इस्तेमाल किया जा सकता है वो KeePassX है। KeePassX प्रयोग करने में आसान है, इसकी स्थापना की कोई जरूरत नहीं है और यूएसबी भंडारण के साथ कहीं भी ले जाया जा सकता है। KeePassX सहित अन्य ऐसे पासफ्रेज प्रबंधक, आपको न सिर्फ पासफ्रेज स्टोर करने की अनुमति देते हैं, बल्कि अन्य किसी तरह के टेक्स्ट या फाइल प्रकार को अटैचमेंट के रूप में मास्टर पासफ्रेज के माध्यम से सहेज के सखने में मदद करते हैं.

* ध्यान देने योग बात
* अपने सभी पासवर्ड की समीक्षा करें और उन्हें पासफ्रेज- जो अब और अधिक सुरक्षित हैं – में बदलने पर विचार करें।

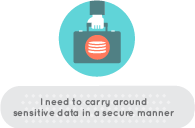
अपने सभी पासफ्रेज को सालाना बदलने पर विचार करें

* ध्यान रहे कि स्टैंडअलोन आधार पर पासवर्ड प्रबंधन का उपयोग भी 100% रूप से आपके पासवर्ड को चोरी होने से बचा नहीं सकता है, विशेष रूप से अगर आपका कंप्यूटर एक परिष्कृत मैलवेयर से संक्रमित है हालांकि, KeePassX जैसे पासवर्ड मैनेजर का उपयोग काफी हद तक ऐसी चोरी का खतरा कम कर सकता है।
* **और किन किन जगहों से मदद ली जा सकती है**
* Diceware का उपयोग कर सुरक्षित पासफ्रेज बनाएँ
* पासफ्रेज जिनको आप याद रख सकते हैं उनको बनाने के बारे में और अधिक जानकारी प्राप्त करें ।
* देखें किट # 4- मैं एक सुरक्षित तरीके से संवेदनशील डेटा कैसे लेके जा सकता हूँ ।
* सुरक्षित पासफ्रेज बनाए और उसका निरंतर रखरखाव करें ।
* सुरखित पासफ्रेज भण्डारण - KeePassX इस्तेमाल करना शुरू करें.

अपने ब्राउज़र में, आपके कंप्यूटर के पार और अपने फोन पर KeePassX का प्रयोग शुरू करें

# Kit #4. मैं संवदनशील डाटा अपने साथ पूरी सुरक्षा के साथ लेकर चलना चाहता हूँ

# मेरे पास संवदनशील डाटा है जिसको मुझे भौतिक रूप से एक जगह से दूसरी जगह ले जाना है. मैं यह कैसे सुनिश्चित कर सकता हूँ कि मेरा डाटा सुरक्षित रहे?

 मैं संवदनशील डाटा अपने साथ पूरी सुरक्षा के साथ लेकर चलना चाहता हूँ

आपको अपने शहर के अन्दर एक जगह से दूसरे जगह या कई जगह एक महत्वपूर्ण मीटिंग के लिए जाना है, संभवतः बिना किसी इन्टरनेट की सुविधा का उपभोग करके. आपको अपने साथ एक संवेदनशील डाटा लाना है, जिसकी संवेदनशीलता के मद्देनज़र आप उसको किसी भी सर्वर पर लोड नहीं करना चाहते या और किसी ऑनलाइन प्लेटफार्म के माध्यम से.

## आपको क्या करना चाहिए

संवेदनशील डाटा के साथ अगर आपको एक स्थान से दुसरे स्थान पर जाना है तो आपको अपना डाटा एन्क्रिप्ट करने के साथ साथ उसके अस्तित्व को भी खत्म करना है.

भौतिक रूप से डाटा को अस्पष्ट कर दीजिये. अपने लैपटॉप के माध्यम से ले जाने के बजाये किसी छोटे उपकरण के माध्यम से फाइल को स्थानान्तरित करें. एसडी कार्ड और पेन ड्राइव्स के अन्दर काफी सारा डाटा रखा जा सकता है. यह उपकरण कही भी छुपाये जा सकते हैं और (कहीं भी गुम) हो सकते हैं. अगर आपको किसी मेटल डिटेक्टर या एक्स-रे के आर पार होकर गुजरना है तो आप एस डी कार्ड को किसी इलेक्ट्रॉनिक यंत्र के अन्दर डाल क्र ले जा सकते हैं, जैसे कि एक मोबाइल फोने या एक कैमरा.

* आपने जब एक बार यह टी क्र लिया है कि डाटा को किस तरह ले जाना है, तो उसके बाद डाटा को एन्क्रिप्ट कर दीजिये. ट्रू-क्रिप्ट या जीपी जी यंत्रों के माध्यम से किसी भी डायरेक्टरी या फाइल को एन्क्रिप्ट किया जा सकता है. ( कृपया किट २ देखिएं- अगर मेरे कंप्यूटर में मौजूद डाटा को जब्त कर लिया गया तो मुझे यह डॉ है इससे मेरी सुरक्षा पर भी असर पड सकता है.)
* या फिर पूरी ड्राइव को ही एन्क्रिप्ट कर दीजिये. आपके सम्वेदनशील डाटा का वॉल्यूम देखते हुए और किस प्रकार के उपकरण में इस डाटा को रखना है के मद्देनजर, सिर्फ संवेदनशील डाटा ही नहीं, जितना भी डाटा है उसको एन्क्रिप्ट करने के बारे में सोचा जा सकता है. पर अगर आप सारा ही डाटा एन्क्रिप्ट करने की सोच रहे हैं तो यह जरूर ध्यान में रखिएगा कि जाँच करने वाली संस्थाओं के संदेह के दायरे में आने की आपकी सम्भावना बढ़ जाएगी.
* डिजिटल रूप में डेटा को अस्पष्ट कर दें । अगर आप ट्रूक्रिप्ट का प्रयोग करते हुए एन्क्रिप्टेड मात्रा में अपने डेटा को सुरक्षित करने के लिए चुनते हैं, तो आप डाटा की मात्रा को भी छिपा सकते हैं, और ऐसा करके आप उस संभाव्यता को भी नकार सकते हैं जिसमें आपका कोई विरोधी आपको मजबूर करके या जबरन आपकी फाइल तक नहीं पहुँच पाएगा और आपसे डिक्रिप्शन पासफ्रेज बताने को भी मजबूर नहीं कर सकेगा। या, सबसे सरल तरीका यह है कि आप उस एन्क्रिप्टेड फाइल को "मेरा संगीत" नाम के साधारण से फाइल के रूप में सेव कर लें, और उसको ठेठ निर्देशिका संरचना के भीतर ही रख दें.।

## ध्यान देने योग्य बात

* जिस तरीके से यूएसबी ड्राइव और एसडी कार्ड में ठोस रूप में डाटा स्टोर किया जाता है वो उनकी विश्वसनीयता को रेखान्क्ति करता हैं, लेकिन साथ ही साथ उस डाटा को इन यंत्रों से मिटा पाना भी उतना ही मुश्किल काम होता है । कई बार डेटा को नष्ट करने का ज्यादा सुरक्षित तरीका, ताकि वो अंततोगत्वा किसी और के हाथ न पद जाये, उस उपकरण को तोड़ के नष्ट कर देना ही सही विकल्प है।
* गौर तलब है कि किसी भी डायरेक्टरी या फाइल का पास-फ्रेस के माध्यम से बचाव करना एन्क्रिप्शन नहीं है और इसको बड़ी आसानी से दरकिनार किया जा सकता है.
* अगर वो उपकरण जिसमें संवेदनशील डाटा मौजूद है किसी के हाथ लग गया और उसमें मौजूद डाटा का पता चल गया तो, एक असामान्य ऑपरेटिंग सिस्टम जैसे कि जी एन यु/ लिनक्स या इस बात का संकेत देना की पूरी डिस्क एन्क्रिप्टेड है, यह रेखान्क्ति करेगा की आप द्वारा कुछ न कुछ डाटा छुपाने का प्रयास किया गया है. इसलिए कई बार ज्यादा अच्छा यह होगा कि हाईड-इन-प्लेन-साईट तकनीकी का प्रयोग किया जाये.
* **मदद कहाँ से प्राप्त की जा सकती है**
* मात्रा को नियंत्रता के साथ प्रयोग करें।  
  • सीखें कि ट्रू क्रिप्ट का प्रयोग करके किस तरह हिडन वॉल्यूम बना सकते हैं

[1] नोट: सितंबर 2015 में, ट्रू क्रिप्ट- फ़ाइल और डिस्क एन्क्रिप्शन के लिए खुला स्रोत सॉफ्टवेयर- में महत्वपूर्ण सुरक्षा से सम्बंधित दोष पाए गए.परिणामस्वरुप, हम हमारे द्वारा दी गयी सलाह की समीक्षा कर रहे हैं और हम सुरक्षित फ़ाइल भंडारण के लिए इन वैकल्पिक उपकरणों का समर्थन करते हैं।

# Kit #5. मुझे अपना मोबाइल यंत्र और उस पर किये गए संपर्क को सुरक्षित करना है

# मुझे मेरे मोबाइल यंत्र से अपने दोस्तों, परिवार के सदस्यों और अपने सहकर्मियों से सहजता से बात करना बहुत अच्छा लगता है, पर मैं अपनी निजता को लेकर चिन्तित भी रहता हूँ. क्या कोई ऐसा तरीका है जिसके माध्यम से मैं अपने निजि मोबाईल के माध्यम से संवेदनशील संचार को सुरक्षित रख सकता हूँ.

मुझे अपने मोबाइल अंतर और उस पर किये जा रहे संवाद को सुरक्षित रखना है

आप सुरक्षा के प्रति जागरूक रहते हैं और अपने मोबाइल डिवाइस के साथ सुरक्षित रूप से संवाद करना चाहते हैं उसी तरह जिस तरह आप अपने लैपटॉप के साथ करते हैं। आप अपने मोबाइल पर अपने अधिकृत काम के ईमेल का उपयोग करना चाहते हैं , गुमनाम रूप से अपने फोन पर वेब ब्राउज़ करना चाहते हैं, या यहां तक कि अपने मोबाइल कनेक्शन के साथ सेंसरशिप को नाकाम करने में सक्षम होना चाहते है। लेकिन इन सबको करने का सुरक्षित तरीका क्या है या वो कौन सी चीज़े हैं जिनसे बचा जा सकता है?

मोबाइल स्मार्ट फोन हैं, छोटे हैं ,महंगे हैं और अपने अन्दर बड़ी मात्रा में जानकारी एकत्र करते हैं । मोबाइल का निर्माण सुरक्षा और गोपनीयता को ध्यान में रख कर नहीं बनाया जाता है। कॉल लॉग्स, संदेश और भौगोलिक स्थिति मोबाइल कंपनी के पास संगृहीत रहती हैं और उसको साझा भी करती हैं, जिन पर हमको भरोसा करना चाहिए ताकि व्यापक सुरक्षा प्रथाओं को लागू करने और आपकी गोपनीयता की रक्षा करते हुए स्थानीय कानूनों का पालन करते हुए आपको सहजता से डाटा प्रदान कराती हैं। अधिकांश देशों में, सरकार, एक संभाव्य विरोधी, आसानी से उस डेटा तक पहुँच सकते हैं। अक्सर सरकार के अनुरोध पर आपके मोबाइल प्रदाता भी सेवाओं को ब्लॉक या सामग्री को सेंसर कर सकते हैं।

## आपको क्या करना चाहिए

* . स्टैंडअलोन अप्प्लिकेश्न्स से बचें। फेसबुक और ट्विटर जैसी मोबाइल अप्प्लिकेश्न्स गोपनीयता के अनुकूल नहीं हैं। उन्हें स्थापित करने से पहले, आपको उन्हें उपयोग करने की अनुमति देनी चाहिए, और कुछ मामलों में अपने डिवाइस पर कई अन्य सेवाओं के प्रयोग में नियंत्रण रखना चाहिए, । आप कनेक्शन की प्रक्रिया को नियंत्रित नहीं कर सकते हैं और डिफ़ॉल्ट से कई अप्प्लिकेश्न्स असुरक्षित HTTP कनेक्शन का प्रयोग करते हैं, न कि HTTPS, इंटरनेट से कनेक्ट करने के लिए। श्रेयस्कर होगा कि आप अपने मोबाइल ब्राउज़र का उपयोग करें।
* अपने मीडिया को सुरक्षित रखें। उच्चस्तरीय सलाह दी जाती है कि प्राथमिक स्तर पर किसी भी संवेदनशील छवियों या वीडियो को अपने डिवाइस पर स्टोर न करें क्योंकि कई आम अप्प्लिकेश्न्स आपके मोबाइल की गैलरी का उपयोग करती है । ObscuraCam एक ऐसी मोबाइल अप्प्लिकेश्न्स है जिससे आप अपने चित्र और वीडियो एन्क्रिप्ट कर सकते हैं ।  
  • अपने डिवाइस और सिम लॉक करें। अपने डिवाइस पर सिम और स्क्रीन ताले सक्षम करें। ऐसा करने से, एक अवसरवादी चोर या औसत तकनीकी कौशल द्वारा सिम बदलने या आपकी अपनी सामग्री तक पहुंचने से रोका जा सकता है।
* अपने डिवाइस को एन्क्रिप्ट करें। अपने अपेक्षाकृत नए एंड्राइड या आई-फोन डिवाइस के प्रयोग से पहले अपने डेटा एन्क्रिप्ट करने की प्रक्रिया फोन में डाउनलोड करिए जिसको करना बहुत आसान है और यह एक आवश्यक कदम है, और इसको करने के बाद यह डेवईस के किसी तरह के भौतिक नुक्सान या किसी द्वारा उसको जब्ती किये जाने के मामले में डेटा की सुरक्षा करता है। आपको बस एन्क्रिप्शन को सक्षम करना है और एक अच्छा पास फ्रेस सेट करना होगा ताकि यह सुनिश्चित किया जा सके कि आपके डेटा निजी है और किसी भी अनधिकृत व्यक्ति द्वारा उस डाटा तक पहुँच पाना सुलभ नहीं है, यद्यपि उस अनधिकृत व्यक्ति को आपके उपकरण तक पहुँच सुलभ है. बनाने के लिए । ध्यान दें कि उपकरण पर किये गए एन्क्रिप्शन से आपका डेटा तभी तक सुरक्षित रहता है जब तक डिवाइस एन्क्रिप्टेड रहता है (आम तौर पर जब डिवाइस बंद रहता है) । एन्क्रिप्शन उन उपकरणों की रक्षा नहीं कर सकते हैं **that are on from data theft (this line is not clear)।**
* गुमनाम रूप से ब्राउज़ करें। आप Orweb के साथ वेब ब्राउज़िंग द्वारा अपने मोबाइल पर टोर का उपयोग कर सकते हैं। या फिर आप अपने डेवाईस को इस तरह कॉन्फ़िगर क्र सकते है ताकि सारा ट्रैफिक एक वीपीएन के माध्यम से ही हो. (किट # 12 देखें। मैं गुमनाम रूप से एक अवरुद्ध वेबसाइट का किस तरह उपयोग कर सकता हूँ )।
* सावधानी के साथ ईमेल करें । यह सलाह दी जाती है कि अपने मोबाइल डिवाइस से संवेदनशील ईमेल न भेजें और कभी भी अपने एन्क्रिप्शन कुंजी (जैसे OpenPGP ) स्टोर न करें । आप अपने मोबाइल पर उपयोग के लिए विशेष रूप से एक अलग ईमेल और सार्वजनिक / निजी OpenPGP कुंजी जोड़ी बना सकते हैं।
* सुरक्षित रूप से संदेश भेजें और प्राप्त करें । संदेश भेजने की प्रक्रिया में आपकी सुरक्षा आपके आप द्वारा प्रयोग किये जा रहे एप्लीकेशन से ही निर्देशित होती है. व्हात्सप्प, स्काइप या Viber के बजाय सिग्नल का उपयोग करें। सिग्नल आपको संदेश भेजने और एन्क्रिप्टेड आवाज कॉल करने के लिए अनुमति देता है।
* अत्यंत गोनियता से बात करें । यह ध्यान रखें कि मोबाइल के माइक्रोफोन अप्प्लिकेसंस से भी चालू किए जा सकते हैं । अगर आप यह सोचते हैं कि मोबाइल बंद क्र देने से सुरक्षा प्राप्त हो जाती है तो इस बात का ध्यान रखें कि मोबाइल फोन बंद करने के बाद भी मोबाइल फोन सेवा प्रदाता (या प्रदाता के माध्यम से सरकार) दूर से डिवाइस को सक्रिय कर सकते हैं । जब आप संवेदनशील मुद्दों के बारे में बात कर रहे हों , फोन की बैटरी बाहर निकाल ले या फोन अपने आपसे बहुत दूर रखें ।
* अपने डेटा बैकअप करने की आदत डालें । महत्वपूर्ण डेटा बार-बार डिवाइस पर बैकअप करें , जैसे कि आपकी संपर्क सूची.
* . अनुमति समाप्त करना। अगर आपका डिवाइस चोरी हो गया , खो गया या जब्त हो गया तो आप तुरंत एक वेब ब्राउज़र का उपयोग करते हुए आप अपने डिवाइस पर जिन खातों में लॉग इन थे उन सबके पासफ्रेज तुरंत बदल डालिए. उदाहरण के लिए आप फेसबुक, ट्विटर और जीमेल पर सभी सक्रिय सत्र से लॉग आउट कर सकते हैं .
* रिमोट से डाटा साफ़ करना . अगर आपका अपना डिवाइस चोरी हो गया , खो गया है या जब्त कर लिया गया है आप दूर से अपने मोबाइल डिवाइस को कुछ कमांड द्वारा नियंत्रित करने में सक्षम हो सकते हैं और अपना डाटा मिटा सकते हैं या उसकी स्थिति का पता भी लगा सकते है, लेकिन इस तरह के उपकरण हमेशा कामयब होने की गारंटी नहीं देते हैं, और उनकी सफलता कई कारकों पर निर्भर करती है जिनमें शामिल हैं मोबाइल पर डेटा कनेक्शन, जीपीएस, नेटवर्क की ताकत और क्या डिवाइस ऑन है? यह क्षमता आम तौर पर आपके डिवाइस के ऑपरेटिंग सिस्टम की एक विशेषता है इसलिए एंड्रॉयड या आईओएस के सेटअप और निष्पादन निर्देश में इसको ढूंढ क्र इसको क्रियान्वित कर लेने में ही भलाई है.

**कहां से और अधिक मदद मिल सकती है**

• अपने iPhone के एन्क्रिप्शन के बारे में जानें।

• एंड्रॉयड के बुनियादी सुरक्षा सेटअप गाइड को पढ़ें ।

• एंड्रॉयड सिग्नल्स जैसे कि सिग्नल, Orbot और Orweb के बारे में गार्जियन परियोजना से जानें

# किट # 6। आपके ब्लॉग या वेबसाइट पर हमला किया गया है या हैक कर दिया गया है

# मैं आज ऑनलाइन गया था और पता चला कि हमारी वेबसाइट से कोई संपर्क स्थापित नहीं किया जा सकता है ! मैं अपनी साइट फिर से कैसे वापस पा सकता हूँ और भविष्य के हमलों से इसे कैसे बचा सकते हैं?

मेरे ब्लॉग या वेबसाइट पर हमला किया गया है या हैक कर दिया गया है

आपके संगठन की वेबसाइट पर बर्बरता की गयी है और अब उससे संपर्क नहीं किया जा सकता है, या आप बस चिंतित है कि आगामी एक अभियान या कार्रवाई की वजह से , आपकी साइट प्रतिक्रियावादी ताकतों - या तो राज्य प्रायोजित या शौकिया -का लक्ष्य हो सकता है। इसे वापस पाने के लिए या अपने ब्लॉग या वेबसाइट और उसकी जानकारी पर नियंत्रण रखने की जरूरत है।

## हमें क्या करना चाहिये

जरुरत है कि आप अपने वेबसाइट डेवलपर से संपर्क करें या किसी तकनीकी विशेषज्ञ से, अगर आप यह नहीं समझ पा रहे कि आप की वेबसाइट से संपर्क क्यों नहीं स्थापित हो पा रहा है. इसकी शुरुआत हो सकती है एक सपोर्ट टिकेट के माध्यम से, जिसको आपको अपने होस्टिंग प्रोवाइडर को जारी करना है या फिर एपी सी जैसी संस्थाओं को एक इ-मेल भेज कर जो आपको यह बता पाएंगी कि आपकी वेबसाइट के साथ ऐसा क्यों हुआ. अगर आपको यह आशंका है कि आपकी वेबसाइट सेंसरशिप का शिकार हो रही है तो .तो वेब प्रॉक्सी या ग्रेट फायर जैसी सेवाओं का इस्तेमाल करें (अगर चीन में ऐसा हुआ है तो ) ताकि इस बाक का सत्यापन हो सके कि आपकी वेबसाइट से संपर्क हो सकता है या नहीं हो सकता है. एक बार जब समस्या पता च गयी फिर अनुगामी करवाई की जा सकती है

.

1. Restore the site with a recent backup.
2. Without a backup or tracked content revision of any kind, you may face data loss.

यदि आपकी साइट में तोड़फोड़ की गई थी, यह संभावना है कि किसी को आपकी साइट की सुरक्षा में एक कमजोरी के माध्यम से एक विशेषाधिकार प्राप्त उपयोगकर्ता के रूप में पहुँच प्राप्त हो गयी है। आपको निम्न करना करना चाहिए:  
1. लॉग इन करके और अविश्वसनीय उपयोगकर्ताओं से उपयोग रद्द।  
2. अगर आपका लॉग-इन काम नहीं कर रहा है और आपकी साइट पर एक थर्ड पार्टी को अपनी सेवा देने के साथ मेजबानी प्राप्त हो गयी है तो कृपया किट # 1 पढ़ें । मेरा ईमेल, फेसबुक या ट्विटर खाते का अपहरण कर लिया गया है , और इसी तरह के कदमों का अनुसरण करते हुए आपकी साइट के प्रशासन इंटरफ़ेस तक पहुँच हासिल करने की कोशिश करें।  
3. अगर आपका लॉग-इन अपनी खुद की मेजबानी की हुई साइट पर काम नहीं कर रहा है तो आप, आप अपनी साइट के मंच पर डेटाबेस / सर्वर स्तर पर पहुँच पाने में सक्षम होना चाहिए। चूँकि प्रत्येक मंच और सर्वर सेट-अप आपने आप में विशिष्ट हैं, आपको एक प्रौद्योगिकीविद् या मदद के लिए अपने वेब होस्ट पर किसी समर्थ व्यक्ति की सहायता की आवश्यकता हो सकती है।  
4. हाल ही में एक बैकअप के साथ साइट पुनर्स्थापित करें ।  
5. एक बैकअप या किसी भी प्रकार की नज़र रखी सामग्री संशोधन के बिना, आप डेटा हानि का सामना कर सकते।

* अगर आपकी अपनी साइट को आपके प्रदाता द्वारा ऑफ़लाइन कर दिया गया है, तो यह शायद इसलिए हुआ क्योंकि सरकार या अन्य कानूनी अनुरोधों ने ऐसा करने का अनुदेश किया । अक्सर ऐसी स्थितियां उत्पन्न होने पर आपके प्रदाता आपको इस आशय की सूचना प्रदान करेंगे. आपको निम्न करना चाहिए:

1. सामग्री हटाने के अनुरोध की अनुपालना करें ताकि अपनी पूरी साइट बहाल किया जा सके.
2. अपने प्रदाता से अपील करें , अपने काम के राजनीतिक संदर्भ को समझाएं और अपनी साइट को बहाल करने के लिए उन्हें निवेदन करें । अनुरोध की वैधता को चुनौती दें (यह आश्चर्य की बात है कि कितनी बार ऐसे अनुरोध गैर कानूनी होते हैं )। आप एक वकील की भी मदद ले सकते हैं ।
3. अपनी साइट को ऐसे प्रदाता के पास ले जायें जिसकी प्रतिबध्धता आपके संगठन के राजनीतिक विचारों से मेल खाती हो और जो इस तरह के अनुरोध की पालना नहीं करेंगे । अगर आप के पास अपनी साइट फ़ाइलों और डेटाबेस के हाल के एक बैकअप तक पहुँच नहीं है, तो आप को अपने मौजूदा प्रदाता के वापस जाकर एक प्रति के लिए अनुरोध कर सकते हैं।

* अगर आपके डोमेन नाम को एक हैक के माध्यम से अपहरण कर लिया गया था या आपका स्वामित्व खत्म हो गया था , तो आप तुरंत एक अपील प्रक्रिया डोमेन रजिस्ट्रार के साथ डाल सकते है जिससे उपयोग को बहाल करने की प्रक्रिया शुरू हो जाएगी । आईसीएएनएन विवाद समाधान की नीतियों के आलोक में इन अपीलों को डोमेन नाम शासन के आखिरी चरण तक लेके जाया जा सकता है.
* यदि आपकी साइट DDoS हमले का शिकार हो गयी है तो आप अपने प्रदाता से मदद मांग सकते है, जिसने हो सकता है इस दिशा में पहले से ही आपकी साइट पर आने वाले यातायात का भारी मात्रा कम करने के लिए कदम उठा लिए हैं । आपका प्रदाता आपको हमले के विवरण में मदद कर सकता है और एक प्रौद्योगिकीविद् कार्रवाई के माध्यम से सर्वोत्तम रास्ता सुझा सकता हैं। अगर आप इस बात का इंतज़ार नहीं कर रहे है कि हमले अपने आप कम हो जाएँगे ,तो आपको :

1. अपनी साइट को या तो एक नए सर्वर पर ले जायें या अपना नवीनतम बैकअप नए सर्वर पर अपलोड करें।
2. DNS टीटीएल की सेटिंग इस तरह से बदलें ("ऑनलाइन होने के लिए समय") कि वो इतना छोटा रहे कि जब आप वेबसाइट एक जगह से दूसरी जगह ले जायें तो , जोन रिकॉर्ड परिवर्तन तेजी से प्रचारित हो जाये ।
3. बहाल साइट को डीडीओएस संरक्षण के पीछे स्थापित करने के लिए वार्निश (सॉफ्टवेयर) या डीफ्लेक्ट की मदद प्राप्त करें।

* अगर आपकी वेबसाइट को सेंसर किया जा रहा है तो इसका कोइ त्वरित इलाज नहीं है जिसके द्वारा उन उपभोक्ताओं को फिर से इसकी सेवाओं का फायदा पहुचाया जा सके जो फ़ायरवॉल या फ़िल्टर के पीछे हैं. फिर भी आप निम्न कर सकते हैं:

1. प्रतिबिम्ब स्थापित करें : वेबसाइट का प्रतिबिम्ब स्तापित करने का मतलब होता है कि उसकी अलग अलग कापियां विभिन्न वेबसाईट पर उपलब्ध हैं. प्रतिबिम्ब स्थापन की भी वही प्रक्रिया है और एक बचाव का प्रयास होता है, अगर किसी तकनीकी समस्या का सामना करना पडे, सेंसरशिप या उसको टारगेटेड तरीके से हैक किया जाये.

* 2. सेंसरशिप के बारे में जागरूकता फैलाएं. सोशल मीडिया का प्रयोग कर अपने उपभोक्ताओं को जागरूक करें. इसके अलावा अभिव्यक्ति की स्वतंत्रता पर काम करने वाले एक्टिविस्ट्स को साईट की सेंसरशिप के बारे में जानकारी दें, और उन्हें एक नया यूआरएल दें जिससे वो साईट का फिर से उपयोग कर सकें.

3. सेंसरशिप उठाने के लिए प्रचार करें और नीतिगत पहल करके सेंसरशिप उठाने के बारे में जागरूकता पैदा करें.

4. सेंसरशिप से बचकर निकलने के बारे में अपने उपयोगकर्ताओं को शिक्षित करें. [Kit #12.](https://www.apc.org/en/irhr/digital-security-first-aid-kit-12)  मुझे एक ब्लाक वेबसाइट पर लाग इन करना है एक छद्म नाम से

* आप या एक तकनीकी विशेषज्ञ द्वारा सर्वर लॉग फाइल का निरीक्षण करके यह देखने की जरूरत है कि क्या हुआ है , अन्यथा आपके प्रतिद्वंदी ने आपकी वेबसाइट पर एक दुर्भावनापूर्ण "शैल " फ़ाइल अपलोड छिपा कर दिया हो सकता है, अपने डेटाबेस आपके वेबसाइट पर डंप कर दिया हो सकता है , या आपके सर्वर पर एक सिस्टम यूजर बना दिया हो सकता है । बस वेबसाइट को पुनः प्राप्त कर लेना ही समाधान नहीं है अगर सर्वर से छेड़छाड़ की गयी है तो.
* भविष्य की समस्याओ से कैसे निपटा जाये
* . साइट फ़ाइलों और डेटाबेस का बैकअप । लगातार बैकअप एक अनिवार्य प्रथा है। अगर आप वर्डप्रेस या ब्लॉगस्पॉट (ब्लॉगर) के रूप में एक तीसरी पार्टी के मंच पर एक ब्लॉग चला रहे हैं, तो आप किसी भी समय आपके कंप्यूटर पर पूरे ब्लॉग निर्यात कर सकते हैं। कम से कम हर महीने में यह करना चाहिए ।
* अगर आप अपनी खुद की साइट की मेजबानी करते हैं, तो अपने वेब होस्ट को यह निवेदन करें कि वो आपको अतिरेक और बैकअप विकल्प प्रदान करे। अगर उनका बुनियादी ढांचा विफल रहता है तो वो अपनी साइट कैसे बैकअप करते हैं? आप इन बैकअप की प्रक्रियाओं से कैसे लाभ ले सकते है? अगर एक स्वचालित बैकअप सुविधा का उपयोग करना है तो क्या उसका मासिक या वार्षिक सदस्यता पर अतिरिक्त लागत पड़ेगी?
* . • वेबसाइट के मंच को सुरक्षित करें । यदि आप अपनी वेबसाइट की मेजबानी कर रहे हैं, तो आप यह सुनिश्चित करें कि अपनी वेबसाइट के कोड नवीनतम सुरक्षा रिलीज के साथ अप टू डेट रहता है। एक बार जब सुरक्षा कमजोरियों का पता चल जाता है और अद्यतन उनके लिए जारी होते रहते हैं, तो हैकर्स भी इन कमजोरियों के बारे में जान जाते हैं और अपनी वेबसाइट के लिए पहुँच प्राप्त करने के लिए इसका फायदा उठा सकते हैं।
* अपने सर्वर को सुरक्षित करें । अगर आप एक सर्वर पर अपनी खुद की वेबसाइट की मेजबानी कर रहे हैं, तो यह महत्वपूर्ण है कि सुरक्षा सुविधाओं और होस्टिंग कंपनी की नीतियों को पढ़ने के लिए कुछ समय बिताया जाए, खासकर जब टेक डाउन अनुरोध और डेटा भंडारण नीतियों का परिपेक्ष्य आता है। वहाँ कई एपीसी सदस्य संगठन है जो कार्यकर्ताओं के लिए तकनीकी सेवाएं प्रदान करने के लिए एक राजनीतिक दृष्टिकोण ले रहे हैं और उनमें शामिल हैं Colnodo (कोलम्बिया), GreenNet (यूके), Jinbonet (दक्षिण कोरिया), मई प्रथम (अमरीका), और Pangea (स्पेन).
* . अपने DNS को सुरक्षित रखें। डोमेन रजिस्ट्रार वाणिज्यिक प्रदाता हैं , जो उपयोगकर्ता की गोपनीयता और डेटा नियंत्रण करने की अपनी प्रतिबद्धता के मद्देनजर अपने बुनियादी ढांचे में एक कमजोर बिंदु हो सकता है। सरकार या कोइ अन्य विरोधी आपका DNS बंद कर सकता है। या आप के अपने डोमेन नाम के स्वयं का नियंत्रण हैकर्स के लिए एक लक्ष्य हो सकता है। अपने खाते को सुरक्षित रखने के लिए EasyDNS की तरह एक विश्वसनीय रजिस्ट्रार का उपयोग करें और हमेशा समय पर खाते को नवीनीकृत करना सुनिश्चित करें।
* साइट के लिए सुरक्षित ट्रैफिक । यह अत्यंत महत्वपूर्ण है कि अपनी साइट के लिए HTTPS पहुँच सक्षम क्रियान्वित हो, कम से कम तब जब आप एक व्यवस्थापक के रूप में साइट में लॉग इन करें और साथ ही साथ उपयोगकर्ताओं की गोपनीयता के लिए भी । टीएसएल एक एन्क्रिप्शन प्रोटोकॉल है जो कि आपके कंप्यूटर और सर्वर, आपके ईमेल या जा रही वेबसाइट होस्टिंग के बीच एक सुरक्षित चैनल स्थापित करता है। सुरक्षित चैनल की आवश्यकता है कि उसे एक टीएसएल प्रमाण पत्र से प्रमाणित किया जाये जिसे आपने ने एक प्रमाणपत्र प्राधिकारी से खरीडा हो और जिसका उद्येश्य साइट की विश्वसनीयता को मान्य करने की। कई प्रमाण पत्र अधिकरण जैसे कि StartSSL.com जैसे गैर लाभ वाली संस्थाओं के लिए निशुल्क प्रमाण पत्र जारी करते हैं।
* सुरक्षित लॉग-इन। व्यवस्थापक या आपकी साइट के लिए उपयोगकर्ता की पहुँच के लिए दो कदम सत्यापन सक्षम करें। साइट को इस तरह से कॉन्फ़िगर करें कि उपयोगकर्ता द्वारा खातों में असामान्य गतिविधि के लिए लॉग रखें और उन पर नजर रखे। , या वो उपयोगकर्ता या आईपी पते जिन पर आपको भरोसा नहीं है, उनको ब्लॉक करें, उनके खातों को हटाएँ और प्रतिबंध लगा दें ।
* सक्षम लॉग-इन चालू करें. सभी पुनर्प्राप्ति विकल्प खुद के लिए सेट करें जैसे कि एक अन्य ईमेल पता । के रूप में एक कॉर्पोरेट ब्लॉगिंग प्लेटफार्म की तुलना में अगर आप अपनी स्वयं की वेबसाइट की मेजबानी कर रहे हैं तो आपके पास अपना मोबाइल नंबर, वसूली प्रश्न या एक विशेष पिन कोड जोड़ने के रूप में अतिरिक्त विकल्प होगा।
* • DDoS हमलों को रोकें । सबसे अच्छा तरीका जिससे यह सुनिश्चित हो जाये कि एक DDoS हमला अपनी वेबसाइट और संभवतः अपने अन्य वेब सेवाओं जैसे कि ईमेल को बंद कर देने की स्थिति न आये उसके लिए रोकथाम एक संभाव्य विकल्प है। डिफ्लेक्ट एक मुक्त / मुफ्त और खुला स्रोत सॉफ्टवेयर उपकरण और प्रगतिशील समूहों और संगठनों के लिए मुफ्त सेवा है। आप आसानी से इसकी सेवाएं प्राप्त करने के लिए साइन अप कर सकते हैं और यह निःशुल्क है, साथ ही साथ ये आपके लिए वेब आँकड़े का नियंत्रण और उपयोग को बनाए रखने में मदद कर सकते हैं।

**और मदद कैसे प्राप्त करें**

* बैक उप को मैनेज करें
* अपनी वर्डप्रेस साईट तो एक्सपोर्ट कर लें.
* परियोजना से मुफ्त में टी एस एल प्रमाणपत्र प्राप्त करें और टी एस एल परियोजना के बारे में जानकारी प्राप्त करें.
* [Deflect](https://deflect.ca/) के माध्यम से DDOS सुरक्षा के बारे में जानकारी प्राप्त करें

# Kit #7. मुझे बिना अपने आपको जाहिर किये हुए एक कंप्यूटर का प्रयोग करना है

# मेरे पास एक विशेष कार्य है जिसको करने के लिए मुझे गोपनीय रूप से ऑनलाइन जाने की आवशयकता है . मैं क्या क्र सकता हूँ जिससे मेरी गतिविधि और मेरी पहचान के बारे में किसी को पता न चल सके.

मैं कंप्यूटर का प्रयोग बिना किसी भी पदचिन्ह को चोदे हुए करना चाहता हूँ

आप कुछ वेबसाइटों को इस उद्येश्य से देखना चाहते होंगे ताकि कुछ अनुसंधान किया जाये , या ऑनलाइन कुछ जानकारी प्रकाशित या भेज सकते हैं। चाहे आप अपने स्वयं के या किसी और के कंप्यूटर का उपयोग करें, अपने कार्यों को जिस भी कंप्यूटर पर किया गया और जो ऑनलाइन यातायात आपने उत्पन्न किया है वो आपकी गतिविधि और आपकी पहचान को बेनकाब कर सकता है। आपको जरूरत है बिना कोई निशान छोड़े एक सुरक्षित तरीके से काम करने की।

## आपको क्या करना चाहिए

## यहां तक कि अगर आप अपने नाम न छापने के बारे में बहुत चिंतित हैं, कुछ मामलों में आपको लगता है कि एक कंप्यूटर का उपयोग करना पड सकता है जो आपका अपना नहीं है पर उस पर आप एक सुरक्षित माहौल में काम करना चाहते है ताकि काम करने के बाद आप किसी भी सबूत को छोड़े बिना एक सुरक्षित तरीके से काम समाप्त क्र देना चाहते हैं । आप चाहे अपना व्यक्तिगत लैपटॉप प्रयोग कर रहे हों, तभी भी आप अपनी गतिविधि के निशान छोड़ने से बचना पसंद करते हैं।

टेल्स एक लाइव ऑपरेटिंग सिस्टम (ओएस) है जो आप लगभग किसी भी कंप्यूटर पर एक डीवीडी, यूएसबी ड्राइव या एसडी कार्ड से बूट करके (कंप्यूटर शुरू करना ) उपयोग कर सकते है। एक जीवित ऑपरेटिंग सिस्टम के लिए एक पूर्ण ऑपरेटिंग सिस्टम कंप्यूटर के हार्डवेयर नहीं, बल्कि अपने सॉफ्टवेयर या ड्राइव भंडारण का उपयोग करता है। टेल्स एक विशेष लाइव ओएस है जिसका उद्येश्य आपकी गोपनीयता और गुमनामी की रक्षा करना है जो किसी भी प्रकार की आपकी गतिविधि के बारे में डेटा भंडारण नहीं करता है और टोर नेटवर्क के माध्यम से सभी इंटरनेट कनेक्शन को ऐसा ही करने के लिए मजबूर कर देता है । टेल, वेब ब्राउज़िंग, एन्क्रिप्शन के लिए कार्यक्रम, चैटिंग और संपादन दस्तावेजों का एक पूरा पैकेज है जो कि गोपनीयता का सम्मान करता हैं ।

टेल वेबसाइट में विस्तृत और सुलभ प्रलेखन शामिल है जिसके द्वारा टेल को डाउनलोड करके , सत्यापित करते हुए कैसे एक डीवीडी, यूएसबी ड्राइव या एसडी कार्ड पर स्थापित करने के बारे में जानकारी देता है जिसका उपयोग आप कहीं भी कर सकते हैं.

**ध्यान दें**

अगर आप एक संवेदनशील माहौल में काम कर रहे हैं, और आप एक सार्वजनिक स्थान में हैं, तो आपको अपने चारों ओर किसी भी सीसीटीवी / निगरानी के बारे में पता करने के लिए आवश्यकता हो सकती है। यही लागू होता है, उदाहरण के लिए, एक साइबर कैफे या एक पुस्तकालय में एक कंप्यूटर का उपयोग करने के दौरान भी ।  
टेल को हमेशा अप टू डेट रखें । अगर कोई नया अपडेट हो रहा है तो सिस्टम को आपको सूचित करना चाहिए, लेकिन ऐसी घोषणाओं के लिए अक्सर अपनी वेबसाइट की जाँच करने के लिए सलाह दी जाती है।  
**कहां से और अधिक मदद मिल सकती है**   
• टेल के साथ पहले कदम के बारे में जानें।  
• एक यूएसबी स्टिक पर टेल स्थापित करने के बारे में जानें।  
• टेल सुविधाओं जिसमे सॉफ्टवेयर भी शामिल है के बारे में जानें।  
• टोर के एक सिंहावलोकन को पढ़ें।

# Kit #8. कोई ऐसा है जो मेरे द्वारा कंप्यूटर पर की जा रही हर गतिविधि पर निगरानी रख रहा है

# मुझे ऐसा लगता है कि कोई है जिसको पता है मैं अपने कंप्यूटर पर क्या क्र रहा हूँ, पर मुझे यह समझ नहीं आता कि ऐसा संभव कैसे हो सकता है. मैं क्या करूं जिससे मेरी निजता बची रहे?

कोइ मेरी कंप्यूटर और की जा रही हर गतिविधि और निगरानी रख रहा है

आप को पता चला है कि आपके द्वारा किया जा रहा संचार उन लोगों को दिख रहा है जिन्हें उसे नहीं देखना चाहिए। आपने गौर किया है कि कुछ लोगों को आपके कंप्यूटर पर मौजुद निजी दस्तावेजों के बारे में पता है। आपको लगता है कि किसी को आपके कंप्यूटर की अन्दर की सामग्री के बारे में पता है पर आप आप यह नहीं जानते कि यह कैसे संभव है

शायद आपका कंप्यूटर किसी वायरस, ट्रोजन, स्पाईवेयर या आपके बिना जाने हुए उस पर कोई अन्य दुर्भावनापूर्ण सॉफ़्टवेयर (मैलवेयर) चल रहा है और इससे वो संक्रमित हो सकता है। आपने एक फाइल डाउनलोड की होगी, एक वेब पेज का दौरा किया होगा, एक लिंक पर क्लिक किया होगा, एक संक्रमित यूएसबी ड्राइव का इस्तेमाल किया, या एक ईमेल को क्लिक किया होगा जिससे कंप्यूटर के अन्दर मैलवेयर आ गया होगा। इस मैलवेयर के निर्माता को इस प्रक्रिया से आपने अपने कंप्यूटर पर नियंत्रण दिया हो सकता है। keylogger के जैसे हार्डवेयर आपके कंप्यूटर में छद्म रूप में प्रवेश कर गए हैं, और उसने किसी को आपकी गतिविधि की निगरानी करने की अनुमति दे दी है।

अलक्षित मैलवेयर विज्ञापन, चोरी, धोखाधड़ी, स्पैमिंग, "psiphing" कम्प्यूटेशनल शक्ति को खत्म करने , या व्यर्थ द्वेष के लिए इस्तेमाल किया जा सकता है। लेकिन, उदाहरण के लिए , आप को यह भी शक हो सकता है कि आप कानून प्रवर्तन के निशाने पर, अपने नियोक्ता, कोई आपके साथ रहता है उसके या अपने साथी के निशाने पर आ गए हैं,

**आपको क्या करना चाहिए**

1. सबसे पहले, सुनिश्चित करें कि यह एक मानवीय भूल है, जिसका अर्थ है कि कुछ लोग जिन पर आपको भरोसा है वे आपकी महत्वपूर्ण दस्तावेजों का खुलासा नहीं कर रहे है। अगर आप सकारात्मक हैं कि यह एक मानवीय त्रुटि नहीं है, तो:  
2. घर पर पता करें कि आपके पीछे से आपके डिवाइस का कोई उपयोग तो नहीं कर रहा है?" एक पासफ़्रेज़ से लॉग-इन स्क्रीन की रक्षा करें या अपना पास- फ्रेस बदल दें. ।  
3. इंटरनेट से कनेक्ट करने के लिए अगर आप वाई-फाई का उपयोग कर रहे हैं, तो, सुनिश्चित करें कि वाई-फाई कनेक्शन पास-फ्रेस से सुरक्षित है और किसी को भी जिस पर आप भरोसा नहीं करते इसका पता नहीं है।  
4. सुनिश्चित करें कि कोई भी, आपके ऑनलाइन खातों का उपयोग नही कर रहा । किट # 1 देखें। मेरा ईमेल, फेसबुक या ट्विटर खाते का अपहरण कर लिया गया था।  
5. सुनिश्चित करें कि आपने एंटी- वायरस सॉफ्टवेयर स्थापित किया गया है और वो नियमित रूप से अपडेट हो रहा है। अपने कंप्यूटर को पूरी तरह स्कैन करें ।  
6. सुनिश्चित करें कि आप के कंप्यूटर के चरों और एक फ़ायरवॉल है ।  
7. हमेशा HTTPS के साथ ब्राउज़िंग और अपने ईमेल के एन्क्रिप्शन के द्वारा अपने संचार को सुरक्षित रखने में तत्पर रहे ।  
8. यदि आपको संदेह है कि कोइ ऐसा दस्तावेज जो आपके कंप्यूटर पर है और आपने उसे इन्टरनेट या अन्य किसी माध्यम से नही भेजा है तो आपके कंप्यूटर का शायद “अपहरण कर लिया गया " या किसी को दुर्भावनापूर्ण माध्यम से आपके कंप्यूटर को कही दूर से बैठ कर चला रहा है और यह शायद की – लोगर जैसे सॉफ्टवेयर के द्वारा किया जाता है। अगर ऐसी चरम स्तर पर आपका कंप्यूटर पहुँच गया है, तो वह संक्रमित हो गया है और उसका उपयोग बंद कर दें और इंटरनेट और किसी भी मीडिया से डिस्कनेक्ट कर दें । ध्यान से एक नए ऑपरेटिंग सिस्टम के साथ एक नया डिवाइस पर अपनी सारी आवश्यक फ़ाइलें (अपना पूरा ड्राइव नहीं) पलायन करें ।

**कहां से और अधिक मदद मिल सकती है**

• अपने खुद के वाई-फाई नेटवर्क को सुरक्षित करें ।  
• एंटी-वायरस सॉफ्टवेयर का प्रयोग करें।  
• एंटी-स्पाईवेयर सॉफ्टवेयर का प्रयोग करें।  
• एक फ़ायरवॉल का उपयोग करें।  
• सुरक्षित रूप से HTTPS- पर हर जगह वेब ब्राउज़ करें।  
• अपने जीमेल खाते की सुरक्षा सेटिंग बदलें।

* .

# Kit #9. मैं एक सुरक्षित माहौल में चाट करना चाहता हूँ.

# मैं किसी से जब चैट करूँ , तो मैं यह चाहता हूँ कि हमारी बातचीत के बारे में न तो कोई सुने, और न ही उसकी निगरानी करें . मैं उनसे सूचना तभी बाटूंगा जब मुझे यह विश्वास हो जाएगा कि इसके बारे में किसे को भी पता नहीं चलेगा.

 मैं एक सुरक्षित तरीके से चाट करना चाहता हूँ.

आप एक या अधिक सहयोगियों के साथ एक ऑनलाइन बैठक तैयारी कर रहे हैं और आपको उनके साथ गोपनीय जानकारी साझा करने की जरूरत है। आपको यह सुनिश्चित करना है कि कोई भी सक्रिय रूप से निगरानी या निष्क्रिय सामग्री या अपनी बातचीत से संबंधित किसी भी अन्य जानकारी को एकत्र नहीं कर रहा है ।

संचार के अन्य साधनों की तरह चैटिंग के उपकरण भी हम नित्य प्रतिदिन प्रयोग करते हैं.: उनकी भी निगरानी की जा सकती है और उनके प्रयोग में विभिन्न तरह के जोखिम मौजूद हैं . जब हम चैटिंग एप्लीकेशन इस्तेमाल कर रहे हैं तो यह सुनिश्चित करें :

वो एक सिरे से दुसरे सिरे तक एन्क्रिप्टेड हैं, जिसका मतलब यह है कि आप और उस सन्देश को प्राप्त करने वाला ही उस सन्देश को पढ़ सकता है और कोई नहीं

* सर्वर के साथ एन्क्रिप्टेड है, जिसका मतलब है कि सर्विस प्रोवाइडर के साथ तो आपका कनेक्शन सुरक्षित है पर आपको अपने सर्विस प्रोवाइडर पर भरोसा करना होगा (अगर स्काइप इस्तेमाल कर रहे हैं तो माइक्रोसॉफ्ट, हैंगआउट इस्तेमाल कर रहे हो तो गूगल )
* एन्क्रिप्टेड नहीं है, इसका मतलब यह है कि कोई भी जो आपके संचार की निगरानी कर रहा है आपके सारे सन्देश तो आराम से एक प्लेन टेक्स्ट ते रूप में देख सकता है

आपको एप्लीकेशन पर भरोसा करना चाहिए. किसी भी एप्लीकेशन की सुरक्षा को जांचने का और उसके निजता के दावों को चेक करने का सबसे सही तरीका है उसके कोड के पुनरवलोकन द्वारा जिसको खुले और पारदर्शी तरीके से किया जाये. एप्लीकेशन जो अपने कोड का पुनरवलोकन एक समुदाय द्वारा जांच के लिए तैयार रहती हैं , और बहुत सारे मानकों को पूरा करती हैं, को फ्री/ लिब्रे के नाम से जाना जाता है या फ्लॉस ( फ्री ओपन सोर्स सॉफ्टवेर) . फ्लॉस की सारी एप्लीकेशन भरोसेमंद होती हैं.

बहुत सारी लोकप्रिय एप्लीकेशन निजता और सुरक्षा के बीच में कोइ अन्तर्भेद नही रखती हैं. आपके संपर्क के लाग जहाँ इन एप्लीकेशन का प्रयोग करते होंगे, हमारी यह सिफारिश है कि आप वाएबेर, व्हात्सप्प , फेसबुक चैट, गूगल हंगआउट और टेलीग्राम जैसे एप्लीकेशन का प्रयोग बंद कर दें क्योंकि वो पारदर्शी रूप से सुरक्षा के मानकों को क्रियान्वित नहीं करते हैं.

## आपको क्या करना चाहिए

सुरक्षित चैट एप्लीकेशन के विभिन्न प्रकारों के बारे में जानकारी प्राप्त करें , जिनको नीचे स्त्रोतों की श्रेणी में शामिल किया गया है और उनमें से जो सबसे सही लगता है उसका प्रयोग करें. हम फ्लॉस एप्लीकेशन के प्रयोग की सिफारिश करते हैं क्योंकि वो एक सिरे से दुसरे सिरे तक पूर्णतया एन्क्रिप्टेड है.

**सिक्योर मेसजिंग स्कोरकार्ड** के माध्यम से सीखें कि किस एप्लीकेशन और उपकरण द्वारा सिक्यूरिटी के मानक लागू किया जाते हैं और किस के द्वारा नहीं

**और कहाँ से मदद मिल सकती है**

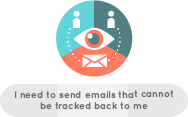
* एंड्राइड के लिए सिग्नल का प्रयोग करें
* आई – फोन के लिए सिग्नल का प्रयोग करें

जित्सी मीट के लिए जित्सी (xmpp) का प्रयोग करें

* वेब ब्राउज़र के लिए cryptocoat का प्रयोग करें ( डेवलपर द्वारा १९ फरवरी २०१६ का नोट: मैं अस्थाई रूप से cry ptocoat की सेवाएं बंद कर रहा हूँ जब तक मैं पूरा सॉफ्टवेर फिर से न लिख दूं, और फिर उसको मैं जारी करूंगा. मैं यह भरोसा दिलाता हूँ कि यह एक अस्थाई निलंबन है

# Kit #10. मैं ऐसे ईमेल भेजना चाहता हूँ जिनका स्त्रोत मुझ तक न खोजा जा सके

# मुझे ऐसे ईमेल भेजने हैं, जो अगर लीक हो गए, तो मुज्झे और मेरे सहभागियों के लिए खतरनाक हो सकते हैं. मैं ईमेल किस तरह भेज सकता हूँ, जो मुझ तक वापस न खोजे जा सकें.

. मैं ऐसे ईमेल भेजना चाहता हूँ जिनका स्त्रोत मुझ तक न खोजा जा सके

आप गुमनाम संदेश भेजना चाहते है, और येचाहते हैं कि कोई भी आपस उस मॉल का स्त्रोत आपतक ढूँढने में साक्षम न हो सके। आप को गुमनाम रूप से काम करने की जरूरत हो सकती है। आपको सावधानी बरतने की जरूरत है कि अगर कुछ संदेशों को बीच में रोका जा रहा है और पकड़ने की कोशिश की जा रही है तो ऐसी स्थिति में आपकी पहचान या अपने सहयोगियों की पहचान न हो सके और आपके सहयोगियों का कंप्यूटर न जब्त हो सके ।

**आपको क्या करना चाहिए**

आपके संदेश के रास्ते में कई ऐसे मकाम आते हैं प्राप्तकर्ता तक पहुचने तक जो आप की अपनी पहचान को बेनकाब कर सकते हैं। फिर भी, आप निम्नलिखित सावधानियां बरत सकते हैं, जिनसे भेजे गए सन्देश को आप तक वापस जोड़ने में काफी दिक्कत आएगी :

* ई-मेल खाता एक ऐसे सेवाप्रदाता के साथ बनाएं जो कि खुले तौर पर उपयोगकर्ता की गोपनीयता के लिए प्रतिबद्ध है और भडारण या उपयोगकर्ता या संदेश विवरण का खुलासा नहीं करता है। हर ईमेल संदेश प्राप्तकर्ता तक पहुंचना सुनिश्चित करने के लिए मेटाडाटा के साथ इंटरनेट के माध्यम से यात्रा करता है। सोचिये उन सभी डाकघरों के माध्यम से जो एक पैकेज यात्रा के टिकटों के माध्यम से अनपे गंतव्य तक पहुँचते हैं. कुछ ईमेल प्रदाताओं जानबूझकर पिछले सर्वर के माध्यम से जहाँ से ईमेल आया है के बारे में संदेश विवरण से हटा देते हैं । यही वह चीज़ है जिसकी आपको आवश्यकता है। अगर आपका ईमेल प्रदाता लंदन में स्थित है, तो आपके मेल की भौतिक उद्गम के के बारे में यही पता चलेगा कि आपका संदेश लंदन के मार्फत पहुँच है । ध्यान दें कि यह प्रभावी तभी होगा जब आपका ईमेल प्रदाता तक पहुंचता है और वहां पर उसको रोक दिया जाता है। Riseup.net इस तरह का एक ई-मेल प्रदाता है।
* अगर आपका उपयोग अस्थायी है, एक वेब आधारित यूजर रेमैलेर सेवा का उपयोग करें, लेकिन ध्यान दें कि आप इस अनाम रेमैलेर के माध्यम से पत्राचार ज्यादा नहीं बढाएं । वास्तव में, उन में से सभी आपके संदेशों को वापस आपको वितरित करेंगे। इसके अतिरिक्त ध्यान दें कि अगर आपको सेवा पर भरोसा भी हैं, तो रेमैलेर वेबसाइट का प्रयोग आप टो ब्राउज़र के साथ करें ताकि आपके आईपी पते का पता न चले।
* एक ईमेल पता जो कि इस तरह से कॉन्फ़िगर किया गया है कि वो एक ईमेल पते का इस्तेमाल कर सके, पर जिसको आपकी पहचान से जोड़ा नही जा सकता , के उपयोग करने के लिए ओनिओन रूटर (टीओआर) आवेदन का उपयोग करें। अगर ठीक से विन्यस्त है , तो आपका सन्देश एक श्रृंखलाबद्ध सर्वरों के माध्यम से आपके प्राप्तकर्ता तक ले के जाएगा, जिस पर आपका सन्देश रास्ते में अदृश्य हो जाएगा.

सार्वजनिक कंप्यूटर से इ-मेल भेजने और अपने ईमेल प्राप्त करने के लिए एक ईमेल क्लाइंट को एक पोर्टेबल आवेदन के रूप में उपयोग करें । उदाहरण के लिए, आप एक यूएसबी ड्राइव पर ईमेल क्लाइंट थंडरबर्ड स्थापित कर सकते है। तब आप अपने (या किसी भी अन्य) कंप्यूटर पर संदेश लिख सकते हैं, एक सार्वजनिक कंप्यूटर के माध्यम से , खुले थंडरबर्ड में अपने मेमोरी स्टिक प्लग कर , अपने संदेश भेज सकते हैं। एक सार्वजनिक कंप्यूटर से संदेश भेजे जाने का लाभ यह है कि कंप्यूटर और आईपी पते का आपस में सम्बन्ध नही होता और उसका लिंक आपसे नहीं जोड़ा जा सकता। यह सलाह दी जाती है कि सार्वजनिक कंप्यूटर का उपयोग कर के अपनी वेब गतिविधि और संचार शुरू करने से पहले वीपीएन या टोर का उपयोग करें. । इन सभी मामलों में एक सार्वजनिक कंप्यूटर के उपयोग करते समय भौतिक सुराग बन जाते है जैसे कि सीसीटीवी फुटेज या कंप्यूटर उपयोगकर्ता के लॉग के रूप में और इनसे आपकी पहचान की जा सकती है ।

## ध्यान रखिए

सार्वजनिक कंप्यूटर का उपयोग कर अपने आपको अज्ञात बनाए रखना उपयोगी हो सकता है, पर आपका आम तौर पर किस प्रकार का सोफ्टवेयर, मैलवेयर, keyloggers या दूरस्थ प्रशासन आवेदन उस कंप्यूटर पर चल रहा है उसका कोई नियंत्रण नहीं है। सार्वजनिक कंप्यूटर का उपयोग करते समय मन में इन संभावित खतरों का संज्ञान अवश्य रखें ।  
  
कहां और अधिक मदद मिल  
  
• Riseup'ssecure ईमेल और इंटरनेट सेवाओं के बारे में पढ़ें।  
• टो ब्राउज़र का उपयोग कर के बारे में जानें।  
• पोर्टेबल थंडरबर्ड के बारे में जानें  
• संदिग्ध ईमेल की निगरानी करने के लिए जवाब पर सुझाव

# Kit #11. मैं इ-मेल इस तरह से भेजना छटा हूम कि सिर्फ प्राप्तकर्ता ही उनको पढ़ सके

# मैं इस बात के लिए किस तरह निश्चिन्त हो सकता हूँ कि मेरे इ-मेल की सामग्री पूरी तरह गोपनीय रहे

 मैं इ-मेल इस तरह से भेजना चाहता हूँ कि सिर्फ प्राप्तकर्ता ही उनको पढ़ सके

आप अपने सहयोगियों या दोस्तों के लिए संवेदनशील जानकारी भेजना चाहते है, लेकिन आपने सुना है कि एक बार संदेश आपके कंप्यूटर से प्राप्तकर्ता तक जाने की यात्रा पर निकलता है तो उस पर से आपका नियंत्रण खतम हो जाता है । आपको एक संदेह है कि आपके सन्देश पर कोई निगरानी कर रहा है। यदि ऐसा होता है जब आप संवेदनशील जानकारी भेज रहे हैं, तो , आप और अन्य लोग भी गंभीर संकट में पड़ सकते है।

एक बार जब आपका ईमेल या चैट संदेश आपके कंप्यूटर को छोड़ देता है, तो वह रूटर, सर्वर और मिडिल बोक्सेस जैसे कई माध्यम से यात्रा करता है जहां उसे पकड़ा जा सकता है और पढ़ सकते हैं और भविष्य में उपयोग के लिए संग्रहीत भी किया जा सजता है । इंटरनेट का अंतर्निहित बुनियादी ढांचे खुलापन और एक माध्यम से दुसरे माध्यम के बीच बिना किसी रूकावट के स्थानानतरित करने के लिए बनाया गया था और इसलिए दुर्भाग्यवश इस माध्यम में गोपनीयता की गारंटी नहीं है।

**आपको क्या करना चाहिए**  
आपको अपने ईमेल प्रदाता और सॉफ्टवेयर जिसे आप प्रयोग कर रहे हैं के बारे में एकदम विवेकपूर्ण निर्णय करना चाहिए अगर आप यह चाहते है कि आपके संदेश इच्छित प्राप्तकर्ता के अलावा अन्य किसी के द्वारा नहीं पढ़ा जाना चाहिए ।  
अपने संचार को एन्क्रिप्ट कीजिये । इसका मतलब यह है कि एक अनधिकृत व्यक्ति अगर आपके संदेशों को रोकने या पढने की कोशिश करता है , तो उसे एक श्रृंखलाबद्ध तरीके में अक्षर और अंक ही दिखाई देंगे जिनका कोई मतलब नहीं होगा। ऐसा करने के लिए:

1. भेजने और ईमेल (तथाकथित वेबमेल का उपयोग) प्राप्त करने के लिए अपना ईमेल प्रदाता की वेबसाइट का उपयोग करने के बजाय, आप एक एन्क्रिप्शन सक्षम ईमेल क्लाइंट (आवेदन) का प्रयोग करना चाहिए अपने संदेशों प्रबंध करने के लिए। यह आपके कंप्यूटर पर आपके संदेशों को एकत्रित करके रखेगा , और यदि आप क्लाइंट कॉन्फ़िगर आईमैप के बजाय पॉप प्रोटोकॉल का उपयोग करते हैं तो उसे विशेष रूप से इसे करना होगा। एक संस्तुतित और अच्छी तरह से समर्थित ईमेल आवेदन मोज़िला थंडरबर्ड है।
2. यदि आप थंडरबर्ड स्थापित करते हैं, तो आपको Enigmail विस्तार जोड़ने की आवश्यकता होगी जो Open PGP का उपयोग करते हुए ईमेल एन्क्रिप्शन का प्रबंधन कर देगा .
3. . एक एन्क्रिप्शन कुंजी की स्थापना कीजिये, जो दोनों ही तरह से काम करते है , एक तो ये निजी कुंजी है जो आप किसी के साथ साझा नहीं करते हैं, और दुसरे यह एक सार्वजनिक कुंजी भी है जो आप अन्य लोगों को दे देंगे आप को संदेश भेजने के लिए। आप कई कारणों से और उपयोगों के लिए एक से अधिक कुंजी बना सकते हैं । एक बार जब आपने इसका प्रयोग शुरू कर दिया है और इस प्रक्रिया से परिचित हो गए तो इस पर काम करना आसान हो जायेगा। आपको सिर्फ एक छोटे से अभ्यास की जरूरत है. OpenPGP कैसे बना सकते हैं और उसको कैसे उपयोग कर सकते हैं उसके बारे में निर्देश के लिए नीचे दिए गए लिंक का पालन करें ..
4. आप के लिए सबसे सुविधाजनक है कि उपयोग करने में सक्षम होने के लिए अपने ईमेल क्लाइंट का इस तरह विन्यास करें कि ठीक से एन्क्रिप्ट और ईमेल संदेशों को डिक्रिप्ट कर अनुप्रयोग किया जा सके । नीचे दिए गए लिंक आपको एक निर्देश तक लेके जाएँगे जिसके द्वारा थंडरबर्ड ईमेल क्लाइंट में एन्क्रिप्शन का उपयोग करने को बढ़ावा मिलेगा।
5. अपने संवाददाताओं की सार्वजनिक कुंजी प्राप्त करें। एन्क्रिप्टेड संचार एक छोर से दुसरे छोर तक है, जिसका अर्थ प्रेषक और रिसीवर दोनों को ही एक तरह का एन्क्रिप्शन प्रोटोकॉल उपयोग करना है। आप OpenPGP का उपयोग थंडरबर्ड / Enigmail प्रबंधक के माध्यम से किसी और से संचार संवाद करने के लिए उपयोग कर सकते हैं जो OpenPGP का उपयोग किसी अन्य क्लाइंट जैसे कि क्लॉ मेल या या K9 + एजीपी मेल क्लाइंट और एंड्रॉयड पर OpenPGP प्रयोग करते हैं।

**ध्यान दें**

* एक इ-मेल का सन्देश और उसका अटैचमेंट तो एन्क्रिप्ट हो सकते हैं. पर उसके साथ जो एनी सूचना मेल के साथ चलती है ( जैसे कि विषय, प्राप्तकर्ता का नाम, भेजने वाले का नाम, और सर्वर जिसके माध्यम से सन्देश भेजा जा रहा है ) एनक्रिप्ट नही होता है.
* जो ईमेल आपने एनक्रिप्ट किया है उसे प्राप्तकर्ता के द्वारा तभी डिक्रिप्ट किया जा सकता है अगर उसकी खुद की निजी OpenPGP कुंजी है और उसे पासफ्रेस का पता है जो उसकी अनुमति देता है। नतीजतन, जिस किसी के पास भी अपना निजी OpenPGP कुंजी है, वो आप द्वारा भेजे गए किसी भी संदेश को पढ़ सकते हैं।
* एन्क्रिप्शन कुछ देशों में अवैध है। जाँच करें कि क्या आपके देश में ऐसी स्थितितो नहीं है , यह जागरूक होने के लिए है इससे पहले कि आप एन्क्रिप्शन का उपयोग शुरू करें ।

**कहां से और अधिक मदद मिल सकती है**

• सार्वजनिक कुंजी क्रिप्टोग्राफी के परिचय को पढ़ें और OpenPGP साथ एन्क्रिप्शन मेल करने के लिए मौजूद दस्तावेज का अध्ययन करें।  
• ईमेल एन्क्रिप्शन के बारे में और अधिक जानकरी प्राप्त करें ।  
• कैसे Enigmail साथ थंडरबर्ड में OpenPGP उपयोग कर सकते हैं उसके बारे में और अधिक जानें।  
• संदिग्ध ईमेल निगरानी का जवाब देने के सुझाव पर विशेष ध्यान दें ।  
• प्रत्येक देश में एन्क्रिप्शन से संबंधित कानूनों के बारे में जानें।

# Kit #12. मैं गोपनीय रूप से एक ब्लाक की गयी वेबसाइट पर जाना चाहता हूँ

# मैं एक अवरुद्ध वेबसाइट की जाँच करना चाहता हूँ जिसे ब्लाक क्र दिया गया है या जिसकी सामग्री का उपयोग अपने देश में गैरकानूनी है । अपने आप की ओर ध्यान खींचने के बिना ऐसा करने के लिए क्या कोई तरीका है?

मैं अज्ञात रूप से एक ब्लॉक्ड वेबसाइट का प्रयोग करना चाहता हूँ.

आप एक देश में रहते है जहाँ कुछ वेबसाइटों और ऑनलाइन सेवाओं को उन्हें पढ़ने से रोकने के लिए सेंसर किया हुआ है ,जब आप अपने ब्राउज़र में उनके यूआरएल टाइप में रहते हैं। इसके अलावा, आप जहां रहते हैं, अन्य मामलों में, ऐसी वेबसाइटों तक आप पहुंच तो पाते हैं, पर उनकी सामग्री अवैध है। इसके अलावा अगर आप इन वेबसाइटों तक पहुँच पाते हैं या आपने विशेष सामग्री डाउनलोड किया है आपको जुर्माना या कैद की सजा का सामना भी करना सकता है । या आप बिना कोई निशान छोडे या दूसरों के द्वारा "देखे " या जो इस ट्रैफिक को मॉनिटर करते हैं उन्हें बिना बताये एक वेबसाइट की यात्रा करना चाहते हैं ।

## आपको क्या करना चाहिए

वहाँ सामग्री जिसे सेंसर किया गया है, और जो आपके अपने स्थान में अनुपलब्ध या विवादास्पद श्रेणी में रखी गयी है का उपयोग करने के लिए तीन विकल्प हैं। वे सुरक्षा और गोपनीयता उपलब्ध कराने के मामले में, और उपयोग में आसानी के मामले में भिन्न होते हैं।

पहला तरीका है कि आप एक वर्चुअल प्राइवेट नेटवर्क (वीपीएन) का उपयोग करें। वीपीएन एक ठीक से विन्यस्त डिवाइस पर कंप्यूटर नेटवर्क के माध्यम से सभी डेटा भेजने और प्राप्त करने के लिए सक्षम करता है । उदाहरण के लिए, यदि आप https://apc.org का उपयोग कर रहे हैं तो आपका कंप्यूटर पहले वीपीएन को जोड़ता है और उसके बाद फिर https //apc.orgon को जोड़ता है और परिणाम वापस भेजता है। जब आप अपने सभी यातायात एक वीपीएन के माध्यम से इंटरनेट से कनेक्ट करते हैं तो आपकी सारी गतिविधियाँ एन्क्रिप्टेड चाहिए, अतः यह सुनिश्चित करें कि आपका वीपीएन प्रदाता ठीक से सुरक्षा लागू कर रहा है। यह एन्क्रिप्टेड "सुरंग" निगरानी से बचाता है और आपको सेंसरशिप को बायपास करने की अनुमति देता है।

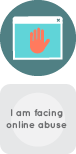
* एक ओनिओन राउटिंग नेटवर्क जैसे कि टोर के साथ, आपका इन्टरनेट यातायात आपके अनुरोध गंतव्य तक पहुँचने के लिए कम से कम तीन अन्य अज्ञात नोड्स या अंक के माध्यम से बाउंस और वापस आता है , और इस यात्रा के दौरान प्रभावी ढंग से अपनी पहचान को गुप्त रखने के लिए कई परतों का आवरण ओड़ लेता है जिससे आपकी पहचान एकदम अज्ञात हो जाती हैं । टोर ब्राउज़र एप्लीकेशन को आसानी से डाउनलोड किया जा सकता है और उसे स्थापित करना भी सरल है जिसमे ज्यादा विन्यास की आवश्यकता नहीं होती है। टो, हालांकि, सुरक्षित नहीं है। बशर्ते कि आप HTTPS का उपयोग करते हैं - और आपको हमेशा HTTPS का उपयोग करना चाहिए - और ईमेल एन्क्रिप्शन, टो नेटवर्क में किसी भी नोड या बिंदु पर सारी सूचना को देखा जा सकता है, उसे संगृहीत किया जा सकता है और आपके संचार की पूरी जानकारी का खुलासा भी हो सकता है । टोर की गति बेहद भी धीमी है।
* • एक वेब प्रॉक्सी शायद एक अवरुद्ध वेबसाइट तक त्वरित पहुँच के लिए सबसे आसान साधन है। एक वीपीएन के समानांतर , आप बस एक प्रॉक्सी वेबसाइट तक पहुँचते हैं और जो यूआरएल आप उपयोग करना चाहते हैं उसको टाइप करके उस तक पहुँच सकते हैं। प्रॉक्सी (एक मध्यस्थ सर्वर) आप के लिए वो साइट उपलब्ध तो करवा देता है , पर अक्सर विज्ञापन और अन्य अवांछित एम्बेडेड कोड भी साथ ले आता है । यह सिफारिश की जाती है कि नियमित रूप से वेबसाइटों के प्रयोग के लिए एक वेब प्रॉक्सी का उपयोग नहीं करना चाहिए । और अपने नियमित ब्राउज़र का इस्तेमान तो एक वेबसाईट उसकी प्रॉक्सी के साथ कभी नही करना चाहिए क्योंकि आपके वेब ब्राउज़र के अन्दर आपके बारे में पूरा ब्यौरा रखता है जिसे फिंगरप्रिंट कहते हैं और इसमें कूकीज और वेब ब्राउज़िंग के इतिहास की पूरी जानकारी होती है.
* • हालांकि आपका इन्टरनेट ट्रैफिक आप और आपके वीपीएन के बीच सुरक्षित है, वीपीएन प्रदाता पर भरोसा किया जाना चाहिए, क्योंकि वे देख सकते हैं, सहेज कर रखते हैं आपके द्वारा इन्टरनेट का पूरा इतिहास और आपके यातायात के विवरण का खुलासा भी कर सकते हैं ।
* टोर गुमनामी तो प्रदान करता है, यह आपकी संचार की सामग्री को टोह लेने वालों से बचाकर नहीं रख पाता है ।
* एक वीपीएन या अपने संचार के साथ टो नेटवर्क पर भरोसा न करें । हमेशा जब ब्राउज़िंग कर रहे हैं तो HTTPS का उपयोग करें और इ-मेल भेजते समय OpenPGP एन्क्रिप्शन का प्रयोग करें जब वो एक वीपीएन या टोर के साथ जुडा हुआ है। अगर आप HTTPS का उपयोग कुछ संवेदनशील वेबसाइटों तक पहुँचने के लिए नहीं कर सकते, या OpenPGP एन्क्रिप्शन ईमेल क्लाइंट के लिए सेट अप नहीं किया गया है , तो आपको टोर या अविश्वसनीय वीपीएन, का उपयोग नहीं करना चाहिए।
* जो भी सावधानियों आप गुमनाम रूप से अवरुद्ध या अवैध सामग्री को ब्राउज़ करने के लिए लेने के लिए करते हैं , आपका ब्राउज़र डिफ़ॉल्ट रूप से ऐसा कॉन्फ़िगर किया गया है कि वो आपके ब्राउज़िंग के इतिहास को याद रखता है । तो अगर आपके कंप्यूटर को जब्त कर लिया गया है या हैक कर दिया जाता है तो, घुसपैठिए उन सारी वेबसाइटों को आसानी से जांच सकते हैं जिनका आपने दौरा किया है। अगर यह आपके लिए एक चिंता का विषय है, तो में अपने ब्राउज़र को इस तरह से विन्यस्त कीजिए कि वो ब्राउज़िंग इतिहास का रिकॉर्ड ही नहीं रख पाए ।

## और मदद कहाँ से मिल सकती है ?

* . सेंसरशिप को बाई पास करने के तरीके जाने
* अपने फायरफोक्स ब्राउज़र की सुरक्षा बढ़ने के तरीका जाने
* टोर के बारे में जानकारी प्राप्त करें
* [HTTPS और टोर](https://www.eff.org/pages/tor-and-https) के एक इंटरैक्टिव उदाहरण को देखें जिसके आपको इस बात की जानकारी मिलेगे कि किस प्रकार आप इन्टरनेट के उपर सुरक्षित रह सकते हैं और गुमनाम भी
* [RiseupVPN](https://help.riseup.net/en/vpn) और [TunnelBearVPN](https://help.tunnelbear.com/customer/portal/topics/620889-getting-started/articles) के बारे में जाने .
* इस बात का जायजा लें कि VPN के प्रयोग से आपको वांछनीय सुरक्षा मिल जाएगी
* [Mozilla Firefox](http://www.blogtechnika.com/how-to-disable-browsing-history-feature-in-firefox/) से ब्राउज़िंग हिस्ट्री का विकल्प हटा दें .
* [Chrome](http://www.ehow.com/how_8156630_disable-browsing-history-google-chrome.html) से ब्राउज़िंग हिस्ट्री को अस्थायी रूप से हटा दें .

# Kit 13. मैं ऑनलाइन चरित्र हनन का शिकार हो रही हूँ

# किसी एक व्यक्ति द्वारा या बहुत सारे व्यक्ति मेरा पीछा क्र रहे हैं और मुझे ब्लैकमेल क्र रहे हैं, और मुझे बलात्कार और जान से मरने के धमके भी दे रहे हैं. मैं अपने आपको ऑन लाइन और ऑफलाइन एकदम असुरक्षित महसूस कर रही हूँ. कृपया मेरी मदद करें

 मैं ऑनलाइन चरित्र हनन का शिकार हो रही हूँ

ऑनलाइन हिंसा हिंसा का ही के प्रकार है और प्रौद्योगिकी सक्षम हिंसा से निपटने के तरीके बहुआयामी हैं और ऑनलाइन हिंसा को क्रियान्वित करने के तरीके जिनके माध्यम से आपको डराया और चुप कराया जा सकता है वो भी विविध प्रकार के हैं । अपने आप को और अपने सहयोगियों के खिलाफ ऑनलाइन दुरुपयोग से के साथ-साथ, कुछ मामलों में,ऑफ़लाइन खतरों पर रिपोर्ट करने के लिए स्थानीय समूहों या अधिकारियों के साथ काम करने की जरूरत है.

यौन हिंसा के रूप में महिलाओं (VAW) के खिलाफ हिंसा और यौन उत्पीड़न, घरेलू हिंसा के और विभिन्न तरीकों ने ऑनलाइन बढ़ावा दिया है , लेकिन आईसीटी के माध्यम से महिलाओं को मदद मिल सकती है , अन्य लोगों के साथ कनेक्ट और कार्रवाई करने के मौके उपलब्ध हो सकते हैं । महिलाओं के खिलाफ प्रौद्योगिकी से संबंधित हिंसा जिसमें शामिल है साइबर पीछा, ब्लैकमेल या अभद्र भाषा, हर एक की अपनी अलग स्थिति है। आप असहाय महसूस कर सकते हैं, लेकिन आप कार्रवाई कर सकते हैं।

साइबर क्षेत्र में पीछा करने की प्रक्रिया , एक व्यक्ति पर तकनीकी रूप से किया जाने वाला सक्षम हमला है जिसकी पृष्ठभूमि में होता है आक्रोश, बदले की भंवा या नियंत्रण की प्रवृति । इस बात की ज्यादा संभावना है कि महिलाओं को पुरुषों की तुलना में पीछा किये जाने का ज्यादा अनुभव होगा, और कई बार तो यह एक अंतरंग साथी के द्वारा किया जाता है। कभी कभी हिंसा के इस प्रकार में शारीरिक हमला भी शामिल हो सकता है।

साइबर पीछा उत्पीड़न, में शामिल है लक्षित व्यक्ति की अपमान और शर्मिंदगी ; परिवार, दोस्तों और नियोक्ताओं को परेशान किये जाने की प्रक्रिया ताकि लक्षित व्यक्ति को अलग-थलग किया जा सके ; लक्ष्य भयभीत बनाने के लिए रणनीति; दूसरे व्यक्ति की पहचान लेकर डराने की योजना ; निरंतर निगरानी और गतिविधियों और स्थान (उदाहरण के लिए फेसबुक का उपयोग कर सूचनाएं पता लगाने के लिए जहां व्यक्ति जा रहा है, स्पाईवेयर का उपयोग कर, जीपीएस सक्रिय) की निगरानी।

साइबर क्षेत्र में पीछा करने के मुद्दे की जड़ तक पहुंचना इसलिए भी कठिन हो जाता है क्योंकि पीछा करने वाले की पहचान गोपनीय है ; कानून प्रवर्तकों की यह धारणा है कि दूर स्थित एक शिकारी ऑनलाइन पीछा करने के बाद उसको और भयावह करने के लिए उस व्यक्ति विशेष के आवास तक भौतिक रूप से यात्रा नहीं करेगा ; बल्कि वह अपने और ऑनलाइन दोस्तों को उत्पीड़न में भाग लेने के लिए प्रोत्साहित करेगा , और इस तरह से उस व्यक्ति को, जिसका पीछा किया जा रहा हैं उसकी मुश्किलें और बाधा देगा। इसके अलावा, साइबर स्थल में पीछा करने वालों के खिलाफ कई देशों में कानूनन मान्यता प्राप्त नहीं है, जिसका अर्थ है साईबरस्टोकिंग से जो बच पाता है उसके पास कोई कानूनी सहारा नहीं है।

ब्लैकमेल एक धमकी का कार्य है जिसमें लिए एक व्यक्ति के बारे में हानिकारक जानकारी सार्वजनिक, परिवार या सहयोगियों के प्रकट करने का डर पैदा किया जाता है और कई बार ब्लैकमेलर की चुप्पी को खरीदना पड़ता है । ब्लैकमेल से प्रतिष्ठा को नुकसान, भलाई, रोजगार, या कुछ संदर्भों में, भौतिक सुरक्षा को भी नुकसान हो सकता है। ऑनलाइन सेक्स से ओतप्रोत छवियो के माध्यम से किया जाने वाला ब्लैकमेल वह प्रकार है जहां ब्लैकमेलर, अक्सर ऑनलाइन सेक्स से ओतप्रोत छवियों या पत्राचार को आपके चरित्र और छवि से जोड़ कर उसको बिना आपकी सहमति के प्रकाशित या वितरण के माध्यम से जगजाहिर कर सकते हैं । ब्लैकमेल से निजात की कीमत पैसे के रूप में या उस व्यक्ति की शारीरिक और भावनात्मक नियंत्रण की मांग के रूप में भी हो सकता है। जिसे प्रतिकार पोर्न “(जहां निजी सेक्सुअल छवियों या वीडियो को सहमति के बिना, लेकिन बिना वित्तीय मकसद के ऑनलाइन प्रकाशित कर दिया जाता है ) के रूप में जाना जाता है, के मामले में, उद्येश्य सिर्फ होता है शुद्ध अपमान और महिलाओं की सामाजिक रूप से नीचा दिखाने का प्रयास। यह कई प्रकार से हो सकता है और इसमें शामिल है , सत्ता के लिए सरकार की निगरानी से अपमानित करने की प्रक्रिया, फोटो के हेरफेर द्वारा अपमानित करना , वित्तीय लाभ के लिए छवियों की चोरी, बिना सहमति के लिया गया वीडियो, अपनी ही साथी द्वारा निगरानी करने की प्रक्रिया , हिंसात्मक गतिविधियों की छवि और किसी को नियंत्रित करने के लिए इन चित्रों के प्रयोग करने की प्रक्रिया

याद रखें कि ब्लैकमेल अस्वीकार्य है और आप को अधिकार प्राप्त है (पीडीएफ) : अभिव्यक्ति की स्वतंत्रता, गोपनीयता की स्वतंत्रता और मानहानि से आजादी , हिंसा से मुक्ति का अधिकार और अपनी कलात्मक काम की रक्षा का अधिकार .

**आपको क्या करना चाहिए**

यहाँ कुछ रणनीतियाँ है जिनका प्रयोग आप जवाब और अपने आप को बचाने के लिए कर सकते हैं। ध्यान देने वाली बात यह है कि , यह एक विस्तृत सूची नहीं है। याद रहे कि यह आपकी गलती नहीं है और हम यह सिफारिश करेंगे कि इस बारे में आप मदद के लिए अपने जीवन में विश्वस्त लोगों से बात करें.

* **एक फ़ायरवॉल स्थापित करें, अपने वाई-फाई को सुरक्षित करें और ब्लूटूथ बंद कर दे**। वाई-फाई हॉट स्पॉट्स और ब्लूटूथ कनेक्शन के द्वारा आपकी वास्तविक भौतिक स्थिति का पता चल जाता है और लोगों के लिए यह आसान हो जाता है कि वो आपके फोन को हैक कर सकते हैं। सार्वजनिक वाई-फाई का उपयोग करते समय फ़ायरवॉल आपका रक्षा कवच है। एक फ़ायरवॉल आपकी अविश्वस्त कनेक्शन -जो हैकर्स और वायरस के माध्यम से आपके कंप्यूटर पर हमले का एक खुला न्योता है – के उपयोग से इंटरनेट और स्थानीय नेटवर्क से रक्षा करता है। फ़ायरवॉल कंप्यूटर का पहला प्रोग्राम है जो कि इंटरनेट के माध्यम से आने वाले डाटा को देखता है और आखिरी कार्यक्रम है जो कंप्यूटर से बाहर जाने वाली जानकारी को अपनी देख-रेख में जाने देता है ।

1. अपने घर के कनेक्शन को सुरक्षित बनाने के लिए, सुनिश्चित करें कि आपका कनेक्शन WPA2 सुरक्षा द्वारा रक्षित हैं। WEP (एक और एन्क्रिप्शन मानक जो वाई-फाई नेटवर्क को हासिल करने के लिए प्रयोग किया जाता है ) को हैक करना हैकर्स के लिए बच्चों का खेल है।  
2. वाई-फाई कनेक्शन के लिए एक बहुत मजबूत पासवर्ड चुनें।  
3. एक फ़ायरवॉल स्थापित करें।  
4. अपने ब्लूटूथ कनेक्शन बंद कर दें।  
• एक वैकल्पिक सिम कार्ड प्राप्त करें। एक ऑनलाइन स्टाकर अगर आपका मोबाइल नंबर प्राप्त कर सकता है, तो वे आपको एसएमएस संदेश और फोन कॉल के माध्यम से परेशान भी कर सकते हैं। वे जीपीएस के साथ संयोजन में इसका इस्तेमाल करते हुए आपके स्थान को जान सकता है। प्राइवेट कॉल के लिए एक वैकल्पिक सिम कार्ड पर विचार करें।

* 1. अपने फोन को बंद कर दें, सिम कार्ड को बाहर निकल दें और अपने फोन को पुनः आरंभ करें।  
     2. काम समाप्त होने के बाद निजी कार्ड बाहर निकलना मत भूलें।  
     3. निजी सिम को एक सुरक्षित जगह में रखें।

**अपने फोन पर जीपीएस अक्षम** **करें** । जहाँ जीपीएस आपको बता सकता है कि कौन सी कॉफी की दुकानें आपके अगल बगल हैं,पर साथ ही साथ वह दूसरों को यह भी बता सकता है कि आप कहाँ हो सकते हैं। बहुमत स्मार्ट फोंस के जीपीएस चिप्स है जो कि सेकंड में फोन पृथ्वी पर कहाँ है चुटकी में बता सकते हैं।

1. जब आपको ज़रूरत है तभी केवल जीपीएस सेटिंग्स सक्षम करें।

2. सेटिंग> गोपनीयता> स्थान नेविगेट करके उन्हें बंद कर दें।

• **अपने मोबाइल कैमरे पर जीपीएस अक्षम करें**। मोबाइल के द्वारा खींचे गए फोटो में यह गुण है कि कब और कहाँ वो खींचे गए हैं इसकी जानकारी वो बता सकते हैं (अगर आपके कैमरे या फोन में जीपीएस है)। खींची गयी फोटो के अनुसार भी भौगोलिक स्थिति का पता लगाया जा सकता है .इस जानकारी के साथ फोटो को मिला के आपकी लोकेशन बताई जा सकती है । सामग्री के साथ, आप कहाँ रहते हैं, काम करते हैं या खेलते हैं उसका पता लगाना आसान हो जाता है।

1. आई –फोन पर, सेटिंग्स> गोपनीयता> स्थान के लिए जाकर और "कैमरा" के विकल्प को अक्षम करें।
2. एंड्रॉयड पर, कैमरा एप्लीकेशन पर जायें। सेटिंग्स के तहत, "स्थान टैग" "बंद" कर दें ।

* **एक पास फ्रेज के द्वारा अपने फोन को सुरक्षित रखें**। अगर आपका फोन पासवर्ड से सुरक्षित नहीं है, तो किसी के भी हाथ आने पर उसमें मौजूद आपकी जानकारी का उपयोग कर सकते हैं। पासवर्ड हैकिंग आम है, और जितना एक स्टाकर आप के बारे में जानता है, उतनी अधिक संभावना है कि वो आपके पासवर्ड का पता लगा लेगा । पासफ्रेस सुरक्षा के द्वारा अपना डेटा सुरक्षित रहता है, अगर आप अपने फोन खो जाता है या कोइ आपकी अनुमति के बिना उसका उपयोग करने की कोशिश करता है ।

1. अधिक जानकारी के लिए # किट 3 देखें: मैं अपना पासफ्रेज कैसे सुरक्षित रख सकता हूँ ।

* अपने पासफ्रेज नियमित रूप से रीसेट करें।
* **स्पाईवेयर और मैलवेयर से अपने कंप्यूटर और फोन को सुरक्षित रखें**। दुर्भावनापूर्ण एप्लिकेशन स्पायवेयर हो सकती है। जितना अधिक क्षमताओं वाला स्मार्टफोन आपके पास है, जैसे कि जीपीएस की तरह है, यही क्षमता आपके खिलाफ जासूसी करने के लिए इस्तेमाल की जा सकटी है। मैलवेयर और स्पाइवेयर आपकी निगरानी करते हैं, आप पर नजर रखते हैं और रिकॉर्ड करते हैं कि आप ऑनलाइन क्या कर रहे हैं ।
* विश्वसनीय मैलवेयर जैसे कि स्पाईबोट विरोधी ऐसे स्थापित करें।
* **सोशल मीडिया पर गोपनीयता बनाए रखें**। आप जहां रहते हैं, उन स्थानों का जहाँ आप नियमित रूप से दौरा करते हैं और वे लोग जिनके पोस्ट और चित्रों को आप पसंद करते हैं के माध्यम से आपके बारे में जानकारी बटोरना बहुत ही आसान है। आपके मित्रों के द्वारा भी अनजाने में आप के बारे में जानकारी का खुलासा हो सकता है।

1. साइट के पंजीकरण के लिए एक अलग ईमेल खाता बनाएँ। इससे स्पैम से बचाव हो सकेगा, और अगर ऑनलाइन सेवा के गोपनीयता से सम्बंधित अच्छे मानक नहीं है, तो आपके अपने व्यक्तिगत ईमेल का खुलासा भी नहीं किया जा सकेगा ।
2. वैकल्पिक क्षेत्रों को खाली छोड़ दें। जब ऑनलाइन पंजीयन कर रहे हों ,तो केवल आवश्यक क्षेत्रों में सूचना भरें और पहचान वाली सूचनाएं जैसे कि आपका जन्म दिन के बार एमें मांगी गयी जानकारी को खाली छोड़ दें ।
3. ऐसी प्रोफाइल फोटो का प्रयोग करें जो कि कि आप की पहचान नहीं करता । ऐसी फोटो चुने जिनसे आपकी भौगोलिक स्थिति का पता न चल सके और वो आपको पहचान न सकें और आपके खोज न सकें।
4. एक स्क्रीन नाम ऐसा चुने जो व्यक्तिगत नहीं हो। कई लोगों का स्क्रीन नाम ऐसे होते हैं जो उनको पहचानने में किसी प्रकार की मदद नहीं दे पाते । आप इस बारे में विचार कर सकते हैं कि एक ऐसा उपयोगकर्ता का नाम चुने जो कि लिंग तटस्थ है ।
5. अपनी गोपनीयता सेटिंग्स की जाँच करें। फेसबुक जैसे सर्विसेज उनकी गोपनीयता नीति हर समय बदलटी रहती हैं , और इसलिए नियमित रूप से इसकी जांच करते रहे ताकि यह सुनिश्चित हो जाये कि आपकी जानकारी आप केवल अपने विश्वसनीय लोगों के साथ साझा कर रहे हैं । कुछ साइटें आपको यह विकल्प प्रदान करती हैं कि आप देख लें कि आपका प्रोफाइल दूसरों के द्वारा किस रूप में देखा जा रहा है । सोशल नेटवर्किंग गोपनीयता सेटिंग्स के बारे में और अधिक जानकारी प्राप्त करें ।
6. किट # 1 का संदर्भ लें मेरा ईमेल, फेसबुक या ट्विटर खाते को हाई जैक कर लिया गया है।

* एक सुरक्षित चैट विकल्प जो सामाजिक नेटवर्किंग सेवाओं की मुख्यधारा में शामिल नहीं है, बेहतर हो कि ऐसा विकल्प जो बातचीत को एन्क्रिप्ट कर देता हो का प्रयोग करें। कई सामाजिक नेटवर्किंग साइटों चैट विकल्प प्रदान करते हैं। यह ऑनलाइन बातचीत करने के सबसे असुरक्षित तरीकों में से एक है। ऑनलाइन परिचित चैटरूम में आपको स्टाक कर सकते हैं।

1. स्काइप के बजाय जित्सी का उपयोग करें, क्योंकि यह अधिक भरोसेमंद है।
2. अपने मोबाइल फोन के लिए सिग्नल या टेलीग्राम के उपयोग पर विचार करें। गौरतलब है कि आप और दूसरा व्यक्ति जिससे आप बात करना चाह रहे हैं दोनों को ही एन्क्रिप्टेड सेवा का उपयोग करना चाहिए।
3. किट # 9 देखें। मैं एक सुरक्षित तरीके से बातचीत करना चाहता हूँ ।

* **अपना वेब कैमरा बंद कर दें** और अपने लैपटॉप या मोबाइल फोन पर कैमरे के लेंस पर एक स्टीकर या कागज का टुकड़ा लगा दें । स्टोकेर्स आपके ज्ञान या सहमति के बिना स्पायवेयर का उपयोग करते हुए वेबकैम से लोगों की फिल्म बना लेते हैं ।
* आप भी स्टोकर्स की निंदा और उनसे निवारण की संभाव्यता की तलाश कर सकते हैं। नीचे कुछ सुझाव दिए गए हैं जो आपको बताएँगे कि आप ऐसा कैसे कर सकते हैं।  
    
    
  **कहां से और अधिक मदद मिल सकती है ?**
* टेक बैक ड टेक (TBTT) सुरक्षा टूलकिट
* साईबर स्टोकिंग, ब्लैकमेल और नफरत भरे भाषण के बारे में जानें
* जीवित बचे लोगों से किस तरह बात करें
* गोपनीयता और गुमनामी के साथ तकनीक से संबंधित VAW का क्या सम्बन्ध है
* डेटा भंडारण के साथ तकनीक से संबंधित VAW का क्या सम्बन्ध है
* ज़ेन और आप के लिए तकनीक काम बनाने की कला