अपने ईमेल की सुरक्षा

हम इंटरनेट के ज़रिये पहले से कहीं ज़्यादा जुड़ने लगे हैं। हम 140 कैरेक्टर के सन्देश भेज सकते हैं (ट्विटर पर), ऑनलाइन बातें कर सकते हैं (गूगल टॉक पर), फ़ोन कॉल कर सकते हैं (स्काइप पर) या फ़ोटोज़ और वीडियोज़ भी साझा कर सकते हैं।

फिर भी ईमेल, इंटरनेट पर हमारे संचार का मुख्य माध्यम बना हुआ है, बहुत ही बड़े पैमाने पर निजी और/या ऑफिस के काम के सिलसिले में इस्तेमाल किया जाता है। क्योंकि यह यहाँ रहने ही वाला है, चलिए इसकी सुरक्षा (या इसकी कमी) और हमारी जानकारियों की रक्षा के बारे में पता करते हैं, क्योंकि यह इंटरनेट के ज़रिये एक जगह से दूसरी जगह पहुंचती है। जब आप एक शहर से दूसरे शहर जाते हैं, आपकी सुरक्षा इस तरह से बाँटी जा सकती है, शुरुआत की जगह, आपके लक्ष्य स्थान, रोड पर सुरक्षा, और आपकी यानि कि मुसाफ़िर की। वेब आधारित ईमेल के लिए भी यह इसी तरह काम करता है, ईमेल प्रदाता के अनुरूप (स्त्रोत), आपका ईमेल इंटरफ़ेस (लक्ष्य), इंटरनेट संचरण (रोड), और विषय (मुसाफ़िर)।

प्रदाता/प्रोवाइडर: आपकी जानकारियों को रखने वाला

2007 तक "फ्री" ईमेल सर्विसेज़ में बढ़ोतरी हुई और यह सिलसिला अब तक जारी है। इसका मतलब है अपनी ईमेल तक आसानी से पहुँच, (उन लोगों के लिए भी जिनके पास अपने कंप्यूटर या नियमित इंटरनेट नही है) और ऑनलाइन लगातार बढ़ती हुई भंडार करने की जगह। इसका यहाँ एक मतलब यह भी है कि आसान पहुँच मिलने के एवज में अपने डाटा पर नियंत्रण का बढ़ता हुआ खतरा। जब भी आप फ्री ईमेल प्रदाता के द्वारा दी जाने वाली ईमेल सर्विस का उपयोग करें तब नीचे दी गई बातों के बारे में सोचें:

आपकी जानकारियाँ (इमेल्स, अटैचमेंट्स, आदि) आपके प्रदाता के सर्वर में स्थित हैं। यह कैसे संचालित होती हैं इस पर आपका बहुत ही कम कहना है, अपनी जानकारियों को और दूसरे लोग जो आपसे संचार करते हैं उनकी जानकारियों को लेकर आपको उनपर विश्वास करना पड़ता है।

इस बात को समझने की कोशिश करें कि यदि प्रदाता आपकी जानकारियों का इस्तेमाल करना चाहता है और कैसे करना चाहता है (किसी भी 'आई अग्री/सहमती' बटन पर क्लिक करने से पहले पढ़ें)।

ज़्यादा संवेदनशील ईमेल और सम्प्रेषण के लिए कृपया दूसरी ऐसी फ्री ईमेल सर्विसेज़ का उपयोग करने के बारे में सोचें जो स्पष्ट रूप से यह कहती हों कि वे आपकी जानकारियों का उपयोग या उनका प्रकाशन नही करेंगी (उदाहरण के लिए पढ़ें http://security.ngoinabox.org/en/riseup_main)

सम्प्रेषण एक दो तरफ़ा प्रक्रिया है। यह सुनिश्चित करें कि आप जिस व्यक्ति के साथ संचार कर रहे हैं वह भी सुरक्षित सर्विस का उपयोग करते हों। अगर केवल एक ही पार्टी सुरक्षित सर्विस का उपयोग कर रही है तो यह आपके ईमेल को सुरक्षित नही बनाता।

इंटरफ़ेस: आप कैसे अपने ईमेल से जुड़ते हैं

अपने ईमेल से जुड़ने का सबसे आम तरीका वेब ब्राऊज़र के माध्यम से होता है। ऐसे व्यक्ति जिनके पास कंप्यूटर और नियमित इंटरनेट तक पहुँच नही होती वे वेब के माध्यम से आसानी से हमारे ईमेल तक पहुँच सकते हैं। इस तरह से ईमेल से जुड़ने का मतलब है सर्वर (जहाँ जानकारियाँ जमा होती हैं) से जानकारियों का यात्रा कर आप तक पहुँचना (ब्राऊज़र के माध्यम से)।

सभी ब्राऊज़र (जैसे कि इंटरनेट एक्स्प्लोरर या फायरफ़ॉक्स) इंटरनेट पर बुरे हमलों से बचने के लिए असुरक्षित होते हैं। इसीलिए जब हम ब्राऊज़र का उपयोग अपने ईमेल पढ़ने या भेजने के लिए करते हैं तो, हम अपनी जानकारियों को दूसरों के सामने आ जाने के संभावित ख़तरे को बढ़ा देते हैं। ज़्यादा सुरक्षित ब्राऊज़र के इस्तेमाल के बारे में विचार कीजिए। फायरफ़ॉक्स एक अच्छा विकल्प है और यह और भी सुरक्षित बन सकता है जब आप सुरक्षा और गोपनीयता के अतिरिक्त उपायों या एडऑन्स शामिल कर लेते हैं। इसके बारे में और जाने: https://security.ngoinabox.org/en/firefox_main

ट्रांसमिशन: आपके ईमेल कैसे यात्रा करते हैं

दोनों तरफ़ से जानकारियों कि रक्षा करना थोड़ी सुरक्षा देता है। दोनो सिरों के बीच का रास्ता भी उतना ही ज़रूरी है। कंप्यूटर प्रोग्राम के द्वारा पहले से चुनी गई सेटिंग (डिफ़ॉल्ट), की वजह से ईमेल, ईमेल सर्वरों के बीच बहुत ही कम या बिना किसी सुरक्षा के यात्रा करते हैं। आपके ईमेल सामान्य रूप से पढ़ी जा सकने वाली भाषा में एक जगह से दूसरी जगह आते जाते हैं। इसका मतलब है ऐसा कोई भी व्यक्ति जिसके पास उस रास्ते तक की पहुँच है, वह आपके ईमेल पढ़ सकता है। नीचे दी गई बातों पर विचार करें:

जब भी आप कोई फ्री ईमेल सर्विस का उपयोग कर रहे हों अपने यूआरएल (ब्राऊज़र के एड्रेस बार पर) की जाँच करें। अगर एड्रेस एचटीटीपी से शुरू होता है, तो आपके ईमेल का आना जाना सुरक्षित नही है, और आपका ईमेल पढ़ी जा सकने वाली आम भाषा में यात्रा कर रहा है।

कुछ वेब आधारित ईमेल (उदाहरण के लिए याहू! मेल) आपको केवल आपके पासवर्ड (लॉग इन) का उपयोग करते समय तक के लिए ही सुरक्षित रखते हैं, जबकि दूसरे (जैसे कि गूगल मेल) आपको एचटीटीपीएस की सुविधा अपने पूरे ईमेल के लेन देन के दौरान सुरक्षित रखते हैं।

विषय वस्तु: वास्तविक सन्देश

आख़िरकार यह आपका वास्तविक सन्देश ही है जिसे आप सबके सामने आने से बचाना चाहते हैं। इसका मतलब है जब आपकी जानकारियाँ एक जगह से दूसरी जगह जा रही हों, या रास्ते में हों, तब कोई भी उसे अनुचित तरीके से देख या इस तक पहुँच न पाए। हालाँकि:

जब आप ईमेल भेज चुके होते हैं आपका उस ईमेल पर कोई भी नियंत्रण नही होता। जिन लोगों से आप संचार कर रहे हैं अगर वे सुरक्षा के प्रति सचेत नही हैं, तो आपका ईमेल और आपकी सुरक्षा भी खतरे में पड़ सकती है।

अगर आप अपने ईमेल अपने कंप्यूटर में जमा करके रखते हैं, और यदि दूसरों के पास उस तक पहुँच है तो वे भी आपका ईमेल पढ़ सकते हैं।

इसका एक उपाय है जिसे कूटलेखन या अंग्रेज़ी में एनक्रिप्शन कहा जाता है, यह आपके ईमेल की विषय वस्तु, फाइल्स, और दूसरी संवेदनशील जानकारियों को सुरक्षित रखने के सबसे अच्छे तरीकों में से एक है। जानकारियों का कूटलेखन या एनक्रिप्शन करने का मतलब है एक टूल (और एक एनकोड/डिकोड की) की मदद से आप उसे सांकेतिक शब्दों में बदल दें या उसे बिना क्रम के उलट पलट कर दें, और यह तभी पढ़ी जा सकने वाली बनेगी जब आप इसे फिर से पढ़े जा सकने वाली भाषा में बदलेंगे या इसे पढ़ी जा सकने वाली भाषा में बदलने के लिए कुंजी देंगे।

और पढ़ने के लिए देखें: *http://security.ngoinabox.org/en/chapter_7_4.*

हमारा टूलकिट देखें: **सिक्यूरिटी इन-ए-बॉक्स** - security.ngoinabox.org

विशेष आभार: टेक्टिकल टेक्नोलॉजी कलेक्टिव।
इस सामग्री का हिंदी रूपांतरण श्रद्धा माहिलकर के द्वारा इंटरनेट डेमोक्रेसी प्रोजेक्ट के लिए किया गया है।

सामग्री की मूल प्रति के लिए वेबसाइट https://tacticaltech.org/projects/flash-training-materials-2011 पर जाएँ।