SANS SECURITY AWARENESS

घर से सुरक्षित तरीके से काम करने के 5 सबसे अच्छे तरीके

हम जानते हैं कि घर से काम करना आप में से कुछ लोगों के लिए नई बात हो सकती है और शायद मुश्किल भी क्योंकि आपको नई परिस्थितियों के साथ तालमेल बैठाना होगा। हमारा उद्देश्य यह है कि आप घर से भी ज़्यादा से ज़्यादा सुरक्षा के साथ काम कर सकें। नीचे पाँच आसान तरीके दिए गए हैं जिनकी मदद से सुरक्षित तरीके से काम किया जा सकता है। इन तरीकों की सबसे अच्छी बात यह है कि इनकी मदद से न केवल आपका काम सुरक्षित रहता है बल्कि आप और आपके परिवार वालों की सुरक्षा भी पहले से कहीं ज़्यादा बढ़ जाती है क्योंकि आप अपने घर को साइबर हमलों से सुरक्षित कर लेते हैं।

1 You

आप: सबसे पहली और ज़रूरी बात, टेक्नोलॉजी अकेले आपको पूरी तरह से सुरक्षित नहीं रख सकती – सुरक्षा का सबसे मज़बूत हथियार आप ही हैं। हमलावर यह जान चुके हैं कि अपनी मर्ज़ी की चीज़ पाने का सबसे आसान रास्ता है, आपके कंप्यूटर या अन्य डिवाइस की जगह आपको निशाना बनाना। अगर उन्हें आपका पासवर्ड पता लगाना है, आपके काम से जुड़ा डेटा एक्सेस करना है या आपके कंप्यूटर का नियंत्रण पाना है, तो वे आपको चकमा देकर आपसे ये चीज़ें पाने की कोशिश करेंगे, अक्सर हड़बड़ी की स्थिति पैदा करके। उदाहरण के लिए, वे Microsoft की तकनीकी सहायता टीम से होने का दिखावा करके आपको कॉल कर सकते हैं और दावा कर सकते हैं कि आपका कंप्यूटर इन्फ़ेक्ट हो गया है। या फिर वे ईमेल से आपको यह चेतावनी भेज सकते हैं कि कोई पैकेट डिलीवर नहीं हो पाया और इस तरह बेवकूफ़ बनाकर आपसे किसी ख़तरनाक लिंक पर क्लिक करवा सकते हैं। किसी सोशल इंजीनियरिंग हमले के सबसे आम संकेतों में ये शामिल हैं:

- अगर कोई बहुत हड़बड़ी मचाए; ऐसा अक्सर डर, धमकी, किसी संकट या ज़रूरी डेडलाइन की बात करके किया जाता है। साइबर हमलावर ऐसे मैसेज बनाने में माहिर होते हैं जिन्हें देखकर लगे कि वे किसी भरोसेमंद संगठन ने भेजे हैं, जैसे कि बैंक, सरकार या कोई अंतरराष्ट्रीय संगठन।

- सुरक्षा नीतियों या प्रक्रियाओं को छोड़ने या उन्हें नज़रअंदाज़ करने के लिए दबाव, या कोई ऐसा ऑफ़र जो ज़रूरत से ज़्यादा अच्छा लग रहा हो (नहीं, आपने लॉटरी नहीं जीती!)
- जान-पहचान वाले किसी सहकर्मी या दोस्त का मैसेज मिलना, पर मैसेज के सिग्नेचर, उसकी टोन, शब्दों और लहज़े का उस परिचित व्यक्ति से मेल न खाना।

आखिरकार, इन हमलों के ख़िलाफ़ आप ही सबसे मज़बूत हथियार हैं।

घर कानेटवर्क: लगभग हर घर के नेटवर्क की शुरुआत वायरलेस (इसे आमतौर पर वाई-फ़ाई कहते हैं) नेटवर्क से ही होती है। इसी के ज़रिए आप अपने डिवाइस इंटरनेट से जोड़ पाते हैं। ज़्यादातर घरों के वायरलेस नेटवर्क आपके इंटरनेट राऊटर या अलग और ख़ास वायरलेस एक्सेस पॉइंट द्वारा नियंत्रित किए जाते हैं। दोनों एक ही तरह से काम करते हैं: ये वायरलेस सिग्नल प्रसारित करते हैं जिनसे घर के डिवाइस जुड़ते हैं। इसका मतलब है कि अपने घर को सुरक्षित रखने के लिए वायरलेस नेटवर्क को सुरक्षित रखना बहुत ज़रूरी है। हमारा सुझाव है कि वायरलेस नेटवर्क को सुरक्षित रखने के लिए, नीचे दिए गए तरीकों का पालन करें:

- आपके वायरलेस नेटवर्क को नियंत्रित करने वाले डिवाइस का डिफ़ॉल्ट एडमिन पासवर्ड बदलें। एडमिन अकाउंट से ही आप अपने वायरलेस नेटवर्क की सेटिंग कॉन्फ़िगर कर सकते हैं।
- पक्का करें कि सिर्फ़ आपके भरोसेमंद लोग ही आपके वायरलेस नेटवर्क से जुड़ सकें। ऐसा करने के लिए मज़बूत सुरक्षा चालू करें। मज़बूत सुरक्षा चालू करने का मतलब है कि आपके वायरलेस नेटवर्क से जुड़ने के लिए लोगों को पासवर्ड की ज़रूरत होगी और नेटवर्क से जुड़ने के बाद उनकी ऑनलाइन गतिविधियाँ एनक्रिप्ट की जाएँगी।
- पक्का करें कि आपके वायरलेस नेटवर्क से जुड़ने के लिए लोग जिस पासवर्ड का इस्तेमाल करते हैं, वह एक मज़बूत पासवर्ड हो और एडमिन पासवर्ड से अलग हो। याद रखें कि आपको अपने हर डिवाइस के लिए सिर्फ़ एक बार पासवर्ड डालने की ज़रूरत होती है क्योंकि ये डिवाइस पासवर्ड को सेव कर लेते हैं और उसे याद रखते हैं।

नहीं जानते कि ये चरण कैसे पूरे करें? जो कंपनी आपको इंटरनेट सेवा देती है, उससे पूछें, उनकी वेबसाइट देखें, अपने वायरलेस एक्सेस पॉइंट के साथ आए दस्तावेज़ देखें या वेंडर की वेबसाइट पर जाएँ।

पासवर्ड: जब कोई साइट आपसे पासवर्ड बनाने के लिए कहे: एक मज़बूत पासवर्ड बनाएँ; पासवर्ड में जितने ज़्यादा वर्ण होंगे, वह उतना ही ज़्यादा मज़बूत होगा। मज़बूत पासवर्ड बनाने के सबसे आसान तरीकों में से एक है, पासफ़्रेज़ का उपयोग करना। पासफ़्रेज़ कई शब्दों से मिलकर बना पासवर्ड ही होता है, जैसे कि "*bee honey bourbon.*" एक ख़ास पासफ़्रेज़ इस्तेमाल करने का मतलब है, हर डिवाइस या ऑनलाइन अकाउंट के लिए अलग-अलग पासफ़्रेज़ इस्तेमाल करना। इस तरह, कोई एक पासफ़्रेज़ हैक हो जाने पर भी आपके अन्य अकाउंट और डिवाइस सुरक्षित रहेंगे। क्या आप इतने सारे पासफ़्रेज़ याद नहीं रख सकते?

पासवर्ड मैनेजर का इस्तेमाल करें जो कि एक ख़ास तरह का प्रोग्राम होता है। यह आपके सभी पासफ़्रेज़ को एनक्रिप्ट करके सुरक्षित रखता है (पासवर्ड मैनेजर में और बहुत सारी बढ़िया सुविधाएँ भी होती हैं!) अंत में, जब भी संभव हो, दो चरणों की पुष्टि (जिसे टू-फ़ैक्टर या मल्टी-फ़ैक्टर ऑथेंटिकेशन भी कहते हैं) चालू करें। यह सुविधा आपके पासवर्ड का इस्तेमाल करती है, लेकिन पुष्टि के लिए एक दूसरा चरण भी जोड़ देती है, जैसे कि आपके स्मार्टफ़ोन पर एक कोड भेजना या फिर कोई ऐप जो आपको कोड देता है। दो चरणों की पुष्टि संभवत: सबसे महत्वपूर्ण तरीका है जो आप अपने ऑनलाइन अकाउंट की सुरक्षा के लिए इस्तेमाल कर सकते हैं और यह बहुत आसान भी है।

अपडेट: पक्का करें कि आपके सभी कंप्यूटर, मोबाइल डिवाइस, प्रोग्राम और ऐप अपने सॉफ़्टवेयर के सबसे नए वर्शन पर चल रहे हों। साइबर हमलावर आपके डिवाइस के सॉफ़्टवेयर में लगातार नई-नई कमज़ोरियाँ ढूँढते रहते हैं। कमज़ोरियाँ मिलने पर, वे उनका फ़ायदा उठाने के लिए ख़ास तरह के प्रोग्राम इस्तेमाल करते हैं और आपके डिवाइस हैक कर लेते हैं। दूसरी तरफ़, इन डिवाइस के लिए सॉफ़्टवेयर बनाने वाली कंपनियाँ अपडेट रिलीज़ करके इन कमज़ोरियों को दूर करने के काम में जी-जान से लगी रहती हैं। पक्का करें कि आपके कंप्यूटर और मोबाइल डिवाइस पर नए अपडेट उपलब्ध होते ही इंस्टॉल कर लिए जाते हैं। ऐसा करके आप डिवाइस को हैक करना काफ़ी मुश्किल बना देते हैं। अपडेटेड रहने के लिए, जब भी संभव हो, बस ऑटोमैटिक अपडेट की सुविधा चालू करके रखें। यह नियम नेटवर्क से जुड़ी लगभग हर टेक्नोलॉजी पर लागू होता है। इसमें केवल आपके ऑफ़िस से जुड़े डिवाइस ही शामिल नहीं हैं बल्कि इंटरनेट से जुड़े टीवी, बेबी मॉनिटर, सुरक्षा कैमरे, घर के राऊटर, गेमिंग कंसोल और यहाँ तक कि आपकी कार भी शामिल है।

5 Kids & Guests

बच्चे / मेहमान: एक बात जिसकी आपको ऑफ़िस में रहते हुए बिल्कुल भी चिंता नहीं होती, वह है बच्चों, मेहमानों या परिवार के दूसरे सदस्यों द्वारा आपके ऑफ़िस का लैपटॉप या अन्य डिवाइस इस्तेमाल किया जाना। पक्का करें कि आपके परिवार वाले और दोस्त इस बात को समझें कि वे आपके ऑफ़िस के डिवाइस इस्तेमाल नहीं कर सकते क्योंकि ऐसा करने पर, वे ग़लती से कोई जानकारी मिटा या बदल सकते हैं, या फिर ग़लती से डिवाइस को इन्फ़ेक्ट कर सकते हैं, जो कि और भी बुरा होगा।