टेक सेवी सीनियर्स

साइबर सुरक्षा का परिचय: ऑनलाइन सुरक्षित कैसे रहें

इंटरनेट हमारे जीवन का एक अनिवार्य हिस्सा बन गया है और हम कई चीजें ऑनलाइन कर सकते हैं।

हम आपको यह बताना चाहते हैं कि इंटरनेट का सुरक्षित रूप से उपयोग कैसे करें और अपनी गोपनीयता की सुरक्षा के लिए सामान्य सावधानी ।

1. क्या मुझे इंटरनेट पर खुद को बचाने की ज़रूरत है?

इंटरनेट पर, कोई भी अपनी पहचान को गलत साबित कर सकता है, इसलिए आपको यह जानना होगा कि आपको किससे ईमेल स्वीकार करना चाहिए, जहां खरीदारी करना सुरक्षित है, और किसके लिए आपको अपना विवरण देना चाहिए।
साइबर क्राइम से आपको सुरक्षित रखने में इंटरनेट सुरक्षा सॉफ्टवेयर एक महत्वपूर्ण भूमिका निभाता है।
कुछ सामान्य ज्ञान कदम आपको स्कैमर से सुरक्षित रखेंगे :

- क्या आपके कंप्यूटर और वायरलेस नेटवर्क पासवर्ड-सुरक्षित हैं?
- ऑनलाइन अजनबियों को निजी, समझौता विवरण कभी न दें।
- एक सुरक्षा सॉफ्टवेयर स्थापित करें।

2. आप जिन खतरों का सामना कर सकते हैं

1) मैलवेयर

मैलवेयर (दुर्भावनापूर्ण सॉफ़्टवेयर) का आपके कंप्यूटर तक पहुंचने और जानकारी एकत्र करने के इरादे से बनाया जाता है, आमतौर पर अन्य इच्छुक पार्टियों को बेचने के उद्देश्य से। सबसे सामान्य रूप से
जाना हुआ मैलवेयर एक वायरस है।
आपको सावधान रहना होगा कि आप कौन से प्रोग्राम डाउनलोड करते हैं और अपने कंप्यूटर पर चलते हैं। यदि आप एक विवादित साधन से कोई प्रोग्राम डाउनलोड करते हैं, तो यह संक्रमित हो सकता है।

भले ही आप सुरक्षित रूप से ब्राउज़ करते हैं, आप दुर्भावनापूर्ण कोड को नवीनतम दुर्भावनापूर्ण कोड या उपयोगकर्ता की लापरवाही से १00% संक्रमित होने से नहीं रोक सकते हैं। इसलिए, आपको अपने पीसी पर एंटी-वायरस सॉफ़्टवेयर इंस्टॉल करना होगा और रीयल-टाइम सुरक्षा सक्षम करना होगा।
पीसी सुरक्षा के लिए वैक्सीन आवश्यक हो सकती है क्योंकि यह न केवल इंटरनेट पर निरीक्षण करता है, बल्कि यूएसबी और सीडी जैसे बाहरी उपकरणों का पता लगाया जाता है।

2) हैकर

हैकर (या बॉट): आपकी व्यक्तिगत फ़ाइलों तक पहुंचने के लिए आपके कंप्यूटर की सुरक्षा में भेद्यता का फायदा उठाने का प्रयास करता है।

उदाहरण के तौर पर, क्या आप विंडोज फ़ाइल साझाकरण के बारे में जानते हैं? यह एक कंप्यूटर को नेटवर्क पर किसी अन्य कंप्यूटर पर दस्तावेज़ भेजने की अनुमति देता है। लेकिन अगर यह पासवर्ड सुरक्षित नहीं है, तो एक हैकर इसका पता लगा सकता है और इसे अपने पीसी पर एक्सेस करने या
वायरस या अन्य प्रकार के मैलवेयर को आपके पीसी पर प्रत्यारोपित करने के लिए उपयोग कर सकता है।

3) पहचान चोरी, फ़िशिंग और स्कैमर

इस बारे में कोई नियम नहीं है कि आप कह सकते हैं कि आप इंटरनेट पर कौन हैं, इसलिए लोग यह दिखाने का प्रयास कर सकते हैं कि वे कुछ हैं या कोई ऐसा व्यक्ति है जो आपको पैसे देने या क्रेडिट कार्ड नंबर और ऑनलाइन बैंकिंग लॉग इन जैसी व्यक्तिगत जानकारी प्रकट करने के लिए नहीं है।
अनिवार्य रूप से, जालसाज़ ने अपना व्यवसाय ऑनलाइन लिया है, और वे आपका लाभ लेने की कोशिश कर रहे हैं। एक आम घोटाला फिशिंग प्रयास है, जहां स्कैमर एक व्यक्ति या संगठन होने का नाटक करता है जिसके साथ आपका रिश्ता है, और आपको अपने बैंक खाते के विवरण जैसे निजी जानकारी छोड़ने का मौका मिलता है।

स्पैम और फ़िशिंग घोटालों की पहचान करने और इंटरनेट पर परेशानी से बचने में मदद करने के कुछ आसान तरीके हैं। यहां देखने के लिए कुछ चीज़ें दी गई हैं।

- ईमेल और प्रेषक के विषय की जांच करें। क्या यह किसी ऐसे व्यक्ति से है जिसे आप जानते हैं, और क्या यह उस चीज का वर्णन करता है जिसके लिए आपको साइन अप करना याद है? यदि नहीं, तो शायद यह स्पैम है।
- क्या आपकी व्यक्तिगत जानकारी के बदले में एक मुफ़्त पैसा है? क्या आप नकारात्मक परिणामों का वादा करते हैं यदि आप व्यक्तिगत जानकारी का जवाब नहीं देते हैं, या क्लिक करके या लिंक करते हैं? क्या आपके पास फ़ील्ड में आपका नाम है? ये फ़िशिंग घोटाले के सभी संकेत हैं।
- क्या ईमेल में वर्तनी और व्याकरण संबंधी त्रुटियां हैं, और क्या यह खराब रूप से प्रस्तुत की गई है? क्या एक 'मुफ़्त' ईमेल खाते से ईमेल है (outlook.com, yahoo.com, gmail.com)? यदि यह है, और प्रेषक आपको ज्ञात नहीं है, तो संदेह के साथ इसका इलाज करें।

'वैनिटी घोटाला' ईमेल बहुत आकर्षक हो सकता है, और कई प्रामाणिक दिखते हैं। यदि आप परीक्षा में हैं, तो सवाल करना सुनिश्चित करें कि आपको ऐसे ईमेल, जैसे नाम, पते और वेबसाइट क्यों प्राप्त होंगी।

3. सुरक्षा सॉफ्टवेयर क्या करता है?

<u>सुरक्षा सॉफ़्टवेयर के प्रकार</u>
अच्छी खबर यह है कि आप सुरक्षा सॉफ्टवेयर का उपयोग करके अधिकांश हमलों से खुद को बचा सकते हैं। आपका कंप्यूटर अंतर्निहित कुछ सुरक्षा सॉफ़्टवेयर के साथ आता है, लेकिन आपको इसके ऊपर अतिरिक्त सॉफ़्टवेयर जोड़ना चाहिए। विभिन्न प्रकार के सुरक्षा सॉफ़्टवेयर हैं जो आप प्राप्त कर सकते हैं:

1) **एंटीवायरस**: सॉफ़्टवेयर जो आपके कंप्यूटर को अधिकांश प्रकार के मैलवेयर से सुरक्षित करता है (और बाकी के लिए आपके कंप्यूटर के अंतर्निर्मित सुरक्षा पर निर्भर करता है)। आप एंटीवायरस सॉफ़्टवेयर को मुफ्त या छोटे शुल्क के लिए प्राप्त कर सकते हैं।
2) **इंटरनेट सुरक्षा सूट**: सॉफ़्टवेयर का एक पैकेज जो आपके कंप्यूटर को खतरे की पूरी श्रृंखला से बचाता है, जिसमें मैलवेयर, स्कैमर, जंक ईमेल, चाल वेबसाइट, हैकर्स और बहुत कुछ शामिल है। इंटरनेट सुरक्षा सूट का वार्षिक शुल्क होता है (आमतौर पर $ ६0 और $ 1६0 के बीच)।

<u>अपने कंप्यूटर की सुरक्षा करना</u>

1) फ़ायरवॉल इंटरनेट यातायात के लिए एक सुरक्षा चेकपॉइंट की तरह कार्य करता है - यह केवल अधिकृत यातायात के माध्यम से अनुमति देता है।
2) एंटीवायरस सॉफ़्टवेयर किसी भी मैलवेयर को ट्रैक करता है और हटा देता है - वायरस, स्पाइवेयर और एडवेयर सहित - जो आपके कंप्यूटर पर आता है। आपका कंप्यूटर एंटीवायरस सॉफ़्टवेयर के साथ नहीं आता है, और आपको इसे इंस्टॉल करना चाहिए।

4. सुरक्षा सॉफ्टवेयर का चयन करना

यह अनुशंसा की जाती है कि आप किसी भी डिवाइस को इंटरनेट से कनेक्ट करें - आपका पीसी, टैबलेट या स्मार्टफ़ोन - एंटीवायरस सॉफ़्टवेयर या आदर्श रूप से इंटरनेट सुरक्षा सूट से सुरक्षित रहें। यदि आप वार्षिक शुल्क का भुगतान करने में असमर्थ हैं, तो आप इसके बजाय एक मुफ्त एंटीवायरस एप्लिकेशन प्राप्त कर सकते हैं। यह आपके सिस्टम के साथ-साथ एक सुरक्षा सूट की रक्षा नहीं करेगा, लेकिन यह आपको सुरक्षा की बुनियादी पेशकश प्रदान करेगा।
नि: शुल्क एंटी-वायरस प्रोग्राम निम्नानुसार हैं:
माइक्रोसॉफ्ट: www.microsoft.com/securityessentials
एवीजी: www.avgfree.com.au
अवास्ट !: www.avast.com
कोमोडो : www.antivirus.comodo.com

5. अपने आप को सुरक्षित रखना (सुरक्षा सॉफ्टवेयर पर्याप्त नहीं है)

अपने कंप्यूटर पर सुरक्षा सॉफ्टवेयर स्थापित करना ऑनलाइन ख़ुद को सुरक्षित रखने में एक बड़ा और महत्वपूर्ण कदम है। लेकिन यह पूरा समाधान नहीं है: सुरक्षा सॉफ्टवेयर आपको जालसाज़ और साइबर अपराधियों से बचा नहीं सकता है। जो कुछ चीजें हम ऑनलाइन करते हैं वह उस जानकारी को शामिल करती है जो महत्वपूर्ण, निजी या प्राइवेट है। आपकी व्यक्तिगत जानकारी वह जानकारी है जो आपको पहचानती है। अपनी व्यक्तिगत जानकारी की सुरक्षा के लिए, आपको ऑनलाइन सार्वजनिक रूप से साझा करने के बारे में सावधान रहना चाहिए।

सामान्य ज्ञान और संदेह की एक स्वस्थ खुराक आपको घोटाले के लिए बहुत मुश्किल बना देगा!

वहाँ कुछ साधारण चीजें आप अपने आप को सुरक्षित रखने के लिए कर सकते हैं:

1) एक मजबूत और अद्वितीय पासवर्ड / पासफ़्रेज़ का उपयोग करें, और यह नियमित रूप से बदलने
2) सार्वजनिक साइटों पर व्यक्तिगत जानकारी पोस्ट न करें
3) मत खुला ईमेल अटैचमेंट्स जब तक आप कर रहे हैं वास्तव में यकीन है कि

4) बारे में सावधान रहें आप कौन से ईमेल का जवाब देते हैं
5) सावधान रहें, जो आप क्रेडिट कार्ड के विवरण देते
6) बेईमान स्रोतों से प्रोग्राम इंस्टॉल न करें