HindiTech
A Blind Double Peer Reviewed Bilingual Web-Research Journal

आनलाइन शॉपिंग में सावधानियाँ

अंजनी राय

anjani.ray@gmail.com

सॉफ्टवेयर विशेषज्ञ एवं एसोसिएट संपादक, हिंदीटेक

भारत में इंटरनेट का आगमन 15 अगस्त 1995 में VSNL के गेटवे के माध्यम से हुआ। इंटरनेट और वेब की दुनिया में इ-कॉमर्स का आगमन वर्ष 2000 था. इस समय तक भारत इंटरनेट प्रयोगकर्ता की संख्या के आधार पर बहुत तेजी से उपर चढ़कर 12 स्थान पर पहुँच गया था. इंटरनेट प्रयोगकर्ता सूचकांक में चीन, यूनाइटेड स्टेट के बाद तीसरे स्थान पर है. इंटरनेट प्रयोगकर्ता संख्या में प्रति वर्ष 14 प्रतिशत के दर से इजाफा हो रहा है. इस तेजी का एक कारण यह हो सकता है की वेब पर बहुत तरह के नए-नए उत्पाद एवं सुविधाओं का विकास हो रहा है. इ-कॉमर्स का एक महत्त्वपूर्ण घटक आनलाइन शॉपिंग है. इंटरनेट आपको एक सुविधा से भरपूर शॉपिंग का आमंत्रण देता है, जो कि आप किसी भी शॉपिंग आऊटलेट में नहीं पा सकते हैं। आप शॉपिंग अपने घर से कर सकते हैं। आप बिना लाइन में खड़े हुए बहुत सारी सामग्री खरीद सकते हैं। इंटरनेट से आप शॉपिंग करते समय बहुत सारे आइटम को खोज सकते हैं, उन आइटमों का ऑनलाइन वर्चुअल ट्रायल भी ले सकते है। विभिन्न ब्रांडों के बीच मूल्य एवं विशेषता के आधार पर तुलना करके देख सकते हैं। ये सभी कार्य आप बिना लाइन में लगे माउस के कुछ क्लिक से कर सकते है।

इंटरनेट से शॉपिंग करना जितना आसान एवं सुविधाजनक है, उतना ही साइबर हमलावरों के लिए भी आप को शिकार बनाना भी आसान है. साइबर हमलावरों के लिए ऑनलाइन शॉपिंग करने वालों के व्यक्तिगत और वित्तीय सूचना को चुराने के बहुत सारे मौके होते हैं। साइबर हमलावर इन सूचनाओं का उपयोग कर आपके धन की भी चोरी कर सकते है जैसे कि साइबर हमलावर इन सूचनाओं के द्वारा अधिक

से अधिक खरीदी कर सकता है या इन सूचनाओं को किसी अन्य को बेच सकता है। हमलावर ऑनलाइन खरीदार पर हमला करने के लिए निम्नलिखित तीन रास्ते अपनाते हैं-

1. दूषित कम्प्यूटर को लक्ष्य बनाकर

यदि आपका कम्प्यूटर अपने आप को वयारस से सुरक्षित रखने में असमर्थ है या आपने अपने कम्प्यूटर को वायरस से सुरक्षित रखने के लिए किसी प्रकार का एँटीवायरस का प्रोग्राम नहीं डाला है तो हमलावर इस अवसर का फायदा उठाकर आपके कम्प्यूटर तक अपनी पहुँच बनाता है और आपके कम्प्यूटर में से सारी सूचनाओं को ले जा सकता है। यदि आपने अपनी व्यक्तिगत एवं वित्तीय सूचनाओं को किसी विक्रेता के साइट पर रखा है और हमलावर उस विक्रेता के साइट से जुड़े कंप्यूटर पर हमला करने में सफलता हासिल कर लेता है तो इस स्थिती में आपकी भी सूचनाओं को भी चुरा सकता है। हम कह सकते है कि हमलावर दूषित कम्प्यूटर को लक्ष्य बनाकर हमला को अंजाम देता है.

2.धोखाधड़ी वाली साइटों और ई-मेल द्वारा

पारम्परिक शॉपिंग में हम दुकानों एवं दुकानदारों को हम जानते है कि वे किस प्रकार के समान रखते है, लेकिन ऑनलाइन शॉपिंग में हमलावरों द्वारा वैध साइट सा लगने वाला दुर्भावनापूर्ण बेवसाइट बनाया जाता है, या फिर हमलावर दुर्भावनापूर्ण ई-मेल बनाकर उसे लोगों को भेजते हैं जो किसी वैध स्थान से आया हुआ लगता है। लोग आनलाइन शॉपिंग करने के दौरान इन दुर्भावनापूर्ण बेवसाइट या दुर्भावनापूर्ण ई-मेल में शॉपिंग के लिए दिए गए लिंक पर चले जाते है जहाँ पर शॉपिंग करने वाले के द्वारा सभी प्रकार की सूचनाएं दी जाती है यह सभी सूचनाएं हमलावर के पास बड़े आसानी से पहुँच जाती है. कई ई-मेल दान, धर्म के नाम से बनाया जाता है. इस प्रकार के दुर्भावनापूर्ण ई-मेल या वेबसाइट बनाने की पीछे एक उद्देश्य निहित होता है कि आपको किसी प्रकार से विश्वास दिलाना जिससे आप आपनी व्यक्तिगत एवं वित्तीय जानकारी हमलावर को दे दें।

3.असुरक्षित लेन-देन

यदि जिस साइट से आप ऑनलाइन लेन-देन कर रहे हैं उसके ऑनलाइन विक्रेता द्वारा ऑनलाइन लेन-देन करने के दौरान सूचनाओ का किसी प्रकार से इन्क्रिपशन नहीं किया है तो ऐसी दशा में हमलावर आपकी वित्तीय लेन-देन से संबंधित जानकारी को आसानी से मालूम एवं दुरुपयोग कर सकता है।

आप कैसे अपने आपको सुरक्षित कर सकते हैं ?

आपके कम्प्यूटर में एंटीवायरस सॉफ्टवेयर इनस्टॉल होना चाहिए एवं उसे हर समय अपडेट रखें जिससे किसी प्रकार के नए वायरस और ट्रॉजन-हॉउस से आपके कम्प्यूटर को हानि नहीं पहुंच सकती हैं। वायरस आपके कम्प्यूटर के डेटा को परिर्वतित कर सकता है। जिससे आपका कम्प्यूटर भविष्य में शायद चालू ही न हो पाए, यदि चालू हो जाए तब भी वित्तीय लेन-देन करते वक्त आपकी सूचना को चुराया जा सके। इससे बचने के लिए आप अपने कम्प्यूटर पर फायरवाल भी लगा सकते है जो कि आपके कम्प्यूटर में आने वाले कनेक्शन एवं जाने वाले कनेक्शन पर नज़र रखता है यदि फायरवाल को किसी आने-जाने वाले पैकेट पर संदेह होता है तो उसे रोक देगा।

1. स्पाइवेयर

एड़वेयर या स्पाइवेयर प्रोग्राम का उपयोग कर हमलावर आपके कम्प्यूटर तक अपनी पहुँच बना सकता है आप अपने कम्प्यूटर में वैध स्पाइवेयर को हटने वाला सॉफ्टवेयर इंस्टाल करें और इस प्रकार के प्रोग्राम द्वारा एडवेयर या स्पाइवेयर फाइलों को हटा सकते हैं।

2. अद्यतनीकारण

अपने वेब ब्राउजर एवं सॉफ्टवेयर को अपडेट रखें सॉफ्टवेयर को अद्यतन करते रहें जिससे हमलावर आपके कम्प्यूटर में व्याप्त समस्याओं का फायदा न उठा सकें। आपरेटिंग सिस्टम में स्वत: अद्यतन करने की व्यवस्था होती है इसे लागू करें जब भी आपका कम्प्यूटर इंटरनेट से जुड़ेगा, आपरेटिंग सिस्टम स्वत: ही आपने को अद्यतन कर लेगा।

3. सॉफ्टवेयर सेटिंग का मूल्यांकन करे

सभी सॉफ्टवयरों में डिफॉल्ट सेटिंग होता है, जो सभी प्रकार के उपलब्ध सुविधाओं को लागू कर देता है जबकी हमलावर इस अवसर का फायदा लेते हुए आपके कम्प्यूटर तक अपनी पहुँच बना सकता है। अत: यह बहुत आवश्यक है कि आप सॉफ्टवेयर सेटिंग की जाँच करें यदि आप इंटरनेट से जुड़ने वाले हैं। एक साधारण नियम यह अपना सकते हैं कि सभी प्रकार के सेटिंग को सुरक्षा पैमाने के आधार पर उसके उच्चतम स्तर पर रखें, इस स्तर का सुरक्षा मापदंड भी आपके कम्प्यूटर को सभी प्रकार का कार्य सुरक्षित रूप से करने की क्षमता प्रदान करता है।

4. खरीदारी केवल ख्याति प्राप्त विक्रेता से ही करें

जब आप अपनी व्यक्तिगत या वित्तीय लेन-देन संबंधित सूचनाओं को प्रदान कर रहे हैं तब आप इस बात से आस्वस्त हो जाएँ कि आप यह लेन-देन किसी ख्याति प्राप्त विक्रेता से कर रहे हैं या नहीं। ख्याति प्राप्त विक्रेता को ही अपनी व्यक्तिगत या वित्तीय जानकारी प्रदान करें। कुछ हमलावरों द्वारा दुर्भावपूर्ण वेबसाइट बनाकर जो कि वैध वेबसाइट की तरह दिखता है जानकारी प्राप्त करते हैं। अत: किसी साइट पर अपनी व्यक्तिगत या वित्तीय जानकारी देने के पहले उस वेबसाइट को वैधता को जाँच कर लें। तभी आप किसी प्रकार के सामाजिक ताने बाने या फिसिंग हमला से बच सकते हैं। इस तरह के हमलाओं में हमलावर आपके सामाजिक स्थति के अनुसार फिशिंग मेल भेजता है, जिसमें किसी सामाजिक या धार्मिक संगठन को दान-प्रदान करने को कहा जाता है। जब आप ख्याति प्राप्त सामाजिक एवं धार्मिक संगठनों को दान देने के लिए आपको भेजे गए मेल में दिए लिंक पर क्लिक करते हैं तो हमलावर आपको उन सामाजिक या धार्मिक संगठनों की वेबसाइट पर न ले जाकर उसी तरह का बनाया गया किसी और साइट पर ले जाता है यदि आपने दान देने के लिए वित्तीय लेन-देन वेबसाइट के माध्यम से करते है तो हमलावर आपकी सूचना को चुरा लेता है। चुरायी गई सूचना से वित्तीय गड़बड़ी कर सकता है। अत: इस तरह के लेन-देन में आप ख्याति प्राप्त विक्रेता समाजिक संगठन या धार्मिक संगठन की वैधता को जाँच कर ही वित्तीय लेन-देन करें।

5. सूचना भेजने का अनुरोध वाले ई-मेल से सावधान रहें

यदि खरीदी करने के बाद एक ई-मेल भेजा गया है, जिसमें आपसे अपनी व्यक्तिगत एवं वित्तीय सूचनाओं को भेजने को कहा जाएँ तो कोई भी जानकारी ना दें, क्योंकि वैध विक्रेता इस प्रकार के संदेश कभी नहीं भेजता है। आप किसी प्रकार के संवेदनशील सूचनाओं को ई-मेल के माध्यम से संप्रेषित न करें। और इस प्रकार के ई-मेल संदेश पर विकल्प न करें या सावधानियाँ बरतें। इस प्रकार के ई-मेल संदेश हमलावर द्वारा भेजा गया हो सकता है अत: इस प्रकार के ई-मेल का जवाब न दें।

6. प्राइवेसी पॉलिशी की जाँच लें

किसी प्रकार के व्यक्तिगत एवं वित्तीय जानकारी प्रदान करने के पहले उस वेबसाइट के प्राइवेसी पॉलिसी की जाँच कर लें। इस बात को सही प्रकार से समझ लें कि आपके द्वारा दी गई जानकारी को कहीं वेबसाइट पर स्टोर तो नहीं हो रहा है यदि ऐसा है तो उस वेबसाइट के प्राइवेसी पॉलिसी में दिया होना चाहिए कहने का आशय यह है कि आप व्यक्तिगत एवं वित्तीय जानकारी उस वेबसाइट को बिना जाँच पड़ताल किये न प्रदान करें।

7. सूचनाओं का एन्क्रिप्शन किया जाना चाहिए

बहुत-सी वेब साइट्स एस. एस. एल. (सिक्योर सॉकेट लेयर) का इस्तेमाल सूचनाओ को एन्क्रिप्शन करने के लिए करती है. यदि कोई वेब साईट एस.एस.एल. का इस्तेमाल करती है तो उस वेब साईट की यूआरएल https से प्रारंभ होना चाहिए. जब हम इस वेब साइट्स को खोलते हैं तो ब्राऊज़र के पता पट्टी पर एक ताले का निशान दिखाई देगा. यह इस बात का संकेत है कि वेब साइट्स सूचना संचार के दौरान सूचना का एन्क्रिप्शन करेगा, जिससे संचार के दौरान आप के सूचनाओ की टैपिंग होना असंभव सा हो जाता है. यदि ब्रोऊज़र के पता पट्टी पर बंद ताले का निशान दिखाई देता है तो इसका मतलब है सूचना का एन्क्रिप्शन किया गया है. यह ताले का निशान सामान्यतः पता पट्टी के बाए तरफ होता है. हमलाबर कभी कभी जाली ताले का निशान बना सकता है जिसकी स्थिति उचित स्थान पर न होकर कही और हो सकती है. अतः जब भी कभी वित्तीय संबंधित आदान प्रदान किसी वेब साईट से करे तो ताले का निशान को पता पट्टी पर जरुर देख ले यदि ताले का निशान पता पट्टी पर दिखता है तो ही वित्तीय संचार करे अन्यथा नहीं करें.

8. क्रेडिट कार्ड का प्रयोग करें

वित्तीय लेन-देन के लिए क्रेडिट कार्ड का प्रयोग किया जाना चाहिए. क्रेडिट कार्ड से खरीद करने की सीमा को कम रखना चाहिए जिससे क्रेडिट कार्ड की धोखाधड़ी हो जाने के स्थिती मे नुक्सान कम से कम हो. इसी तरह की सेटिंग डेबिट कार्ड के लिए भी कर लें. ऑनलाइन खरीदारी में क्रेडिट कार्ड का ही प्रयोग किया जाना चाहिए, क्योंकि खरीदी करने की सीमा से अधिक की खरीदी करना हमलावर के लिए संभव नहीं होगा, जबकि डेबिट कार्ड की सूचनाओ की चोरी होने से हमलावर आपके खाते में उपलब्ध राशि तक की खरीदारी कर सकता है अतः डेबिट कार्ड से ऑनलाइन लेन-देन करने में खतरा क्रेडिट कार्ड की तुलना में ज्यादा हो सकता है. यदि आप को डेबिट कार्ड से ही ऑनलाइन लेन-देन करना है, तो ऑनलाइन लेन-देन के लिए एक बैंक खाता खोले जिसमे राशि सिमित मात्रा में रखें.

उपर्युक्त सुझाए गए सही उपायों का उपयोग करने पर भी धोखाधड़ी होने का खतरा हो सकता है, लेकिन सुझाव को अपनाने पर धोखाधड़ी खतरा को कम से कम हो जायेगा और आपको इस बात का मलाल भी नहीं होगा कि हमने किसी प्रकार के सुरक्षा पैमाना नहीं आपनाया था इसलिए मेरे साथ धोखाधड़ी हुआ है.

Reference:

http://www.internetlivestats.com/internet-users/india/

Citation: राय, अंजनी (2017). आनलाइन शॉपिंग में सावधानियाँ, HindiTech: A Blind Double Peer Reviewed Bilingual Web-Research Journal, 8 (4), 50-55. URL: https://hinditech.in/aanline-shopping-men-savdhaniyan/