ऑन लाइन खरीदारी में सुरक्षा हेतु अक्सर पूछे जाने वाले प्रश्न

1. ऑनलाइन खरीदारी करते हुए कैसे सुरक्षित रहें ?

आजकल ज़्यादा से ज़्यादा खरीदारी ऑनलाइन की जा रही है। बहुत सारे ऑन लाइन सौदे बिना परेशानियों के किये जाते हैं पर कुछ मामलों में जोखिम मौजूद होते हैं और इस लिए हमने इस पृष्ठ को बनाया है जिसमें उपयोगी सलाहें और टूल मौजूद है जिसका प्रयोग आप ऑनलाइन खरीदारी करते समय कर सकते हैं।

अविश्वसनीयता

यह अक्सर होता है। कहीं और बेचे जा रहे समान उत्पादों की कीमत के साथ तुलना करें। अगर कीमत में कुछ ज़्यादा ही अंतर है, सावधानी बरतें – यह सुनिश्चित करें कि आप बेचने वाले की अच्छे से शोध करें और उत्पाद की शर्तों के बारे में प्रश्न पूछें। जब एक साईट ऐसे उत्पाद प्रदान करती है जिसमें काफी ज़्यादा छूट शामिल होती है, उसमें बुरी ग्रैमर और गलत स्पेलिंग शामिल होते हैं, और अधिकारिक साईट के ब्रांड के मालिक की खराब गुणवत्ता वाली तस्वीरों का प्रयोग किया जाता है, हो सकता है वह नकली उत्पाद बेच रहे हों। इसलिए सावधान रहे, कई साइट जो नकली उत्पाद बेच रहे होते हैं वह ब्रांड के मालिक की साईट के डिजाइन कॉपी कर लेते हैं और समान तस्वीरें बना कर या डोमेन नाम का प्रयोग करके ब्रांड की नकल करते हैं।

अनजान बेचने वालों से सावधान रहें

अगर एक सौदागर से अपने पहले कुछ नहीं खरीदा है, पहले से यह जाँच कर लें कि वह वैध हैं। जैसे की, उनके व्यापारिक इतिहास के बारे में जानकारी प्राप्त कर लें और बाकी खरीदने वालों से बेचने वाले के साथ तजुरबे की समीक्षा के लिए वेब पर खोज कर लें। अगर आपको सौदे के साथ कोई परेशानी हो या कोई प्रश्न पूछना हो तो वैध सौदागर आपको संपर्क करने की जानकारी प्रदान करते हैं, जिसमें पता, फोन नंबर, या ई मेल ऐड्रेस शामिल होते हैं।

काफी साइट जो नकली उत्पाद बेचती हैं उनके यू आर एल सुनने में अधिकारिक लगते हैं, जिसमें वाक्यांश जैसे की [brand]onsale.com या official[brand].com शामिल होते हैं। साईट के पूरे रिकॉर्ड की जाँच करना एक तरीका है जिससे यह खुलासा हो सकता है की डोमेन का मालिक कौन है।

वह भुगतान करने का तरीका प्रयोग करें जिसमें खरीदार की सुरक्षा शामिल हो

कई मामलों में, क्रेडिट कार्ड कंपनियाँ धोखे के मामलों में ऑनलाइन खरीदारी के दायित्व की सीमा फिक्स कर देती है। कई ऑनलाइन भुगतान सिस्टम बेचने वाले के साथ पूरे क्रेडिट कार्ड नम्बर को शेयर नहीं करती ताकि आपको ज़्यादा सुरक्षा मिल सके।

सभी नियम व शर्तों पढ़ें

खरीदने से पहले, यह सुनिश्चित करें की आप बेचने वाले की शिपिंग, वारंटी और वापिस करने की नीति से वाकिफ हैं। कई स्टोर पूरा रिफंड प्रदान करते हैं, जबकि कई रीस्टॉकिंग फीस चार्ज करते हैं और सिर्फ स्टोर क्रेडिट प्रदान करते हैं।

सौदे का रिकॉर्ड बचा कर रखें

डिजिटल या कागज की कॉपी रखना उस समय आपकी मदद कर सकता है अगर आपको कोई रिटर्न करना हो या अपने अकाउंट के साथ हुए अनाधिकृत चार्ज के खिलाफ संघर्ष करना हो।

हैक की गयी साइट का प्रयोग ना करें और ब्राउजर के एड्रेस बार पर नजर रखें

अगर आप किसी लिंक पर क्लिक करते हैं और तुरंत रीडाइरैक्ट हो जाते हैं, वह साईट हैक हो सकती है और उसमें मैलवेयर हो सकता है। मैलवेयर, जैसे की वायरस, वर्म्स, और ट्रोजन हॉर्स, चुप चाप अनचाहे सॉफ्टवेयर को आपके कंप्यूटर में इंस्टॉल कर सकता है। कुछ हैक हुई साइट खुद ब खुद आपको अलग पृष्ठ पर रीडाइरैकट नहीं करती, पर उसमें अप्रासंगिक और स्पैम सामग्री मौजूद होती है। जागरूक रहने के लिए एड्रेस बार पर नजर रखें ताकि आप यह सुनिश्चित कर सकें की जिस लिंक पर अपने क्लिक किया है उसी का पृष्ठ आपके सामने खुल रहा है।

संवेदनशील वेब ऐड्रेस को ब्राउजर के एड्रेस बार में टाइप करें

संवेदनशील अकाउंट को लिंक पर क्लिक करके, ऐड्रेस को कॉपी और पेस्ट करके नैविगेट ना करें। बल्कि, वेब ऐड्रेस को खुद टाइप करें। पर यह सुनिश्चित करें कि आप सही ऐड्रेस लिख रहे हों कुछ नकली साइट असली साइट जैसी ही लगती हैं, पर यह आपके अकाउंट की जानकारी को प्राप्त करने के लिए होती हैं।

संदेहजनक साइट पर निजी जानकारी ना डालें

अगर कोई साईट उत्पाद की खरीदारी या सेवा प्राप्त करने के लिए जरूरत से ज़्यादा आपकी निजी जानकारी की मांग कर रही है (जैसे कि बैंक अकाउंट की जानकारी, सुरक्षा प्रश्नों के जवाब, या पासवर्ड) सावधान रहे क्योंकि ऐसी पूछताछ फिशिंग की कोशिश का संकेत हो सकता है। कई साइट अधिकारिक साइट की नकल हो सकती है, जिसमें लोगो और लिखावट शामिल होते है, पर धोखेबाजों द्वारा सेट किये जाते हैं जिसका मूल उद्देश्य आपकी निजी जानकारी को हासिल करना होता है।

यहाँ कुछ चीजें है जिसको आपको नहीं करना चाहिए और फिशिंग साइट को रिपोर्ट करनी चाहिए :

यह सुनिश्चित करें की आपके पासवर्ड मजबूत हों

अलग अलग अकाउंट के लिए एक ही पासवर्ड का बार बार प्रयोग ना करें, और नियमित समय पर उसे बदलते रहें खास करके अगर आपको संदेह हो कि आपका अकाउंट जोखिम में है।

सुरक्षित कनेक्शन पर ही अपनी जानकारी को भेजें

जब कोई संवेदनशील जानकारी जैसे कि क्रेडिट कार्ड नम्बर या बैंक नम्बर को भेजना हो तो ऐड्रेस बार में https:// कनेक्शन के लिए देखें (और ऐड्रेस बार में पैडलॉक आइकन को देखें अगर आप गूगल क्रोम या इन्टरनेट एक्सप्लोरर का प्रयोग कर रहे हैं)। जब वित्तीय अकाउंट का प्रयोग कर रहे हों, यह जाँच करें कि वेब साईट के पास एक्सटेंडेड वैलिडेशन प्रमाणपत्र मौजूद हो – काफी आधुनिक ब्राउजरों में यू आर एल या वेब साईट का नाम यू आर एल बार में हरे रंग का दिखना चाहिए, जिसका मतलब होता है की जो संगठन इस वेब साईट को ऑपरेट कर रहा है वह मान्य है।

सार्वजनिक कंप्यूटर पर वित्तीय लेन देन ना करें

सार्वजानिक या शेयर किये जाने वाले कंप्यूटर पर संवेदनशील वित्तीय जानकारी वाले अकाउंट पर लॉग इन ना करें (जैसे कि बैंक अकाउंट या क्रेडिट कार्ड अकाउंट या ईकोम्मेर्स वेबसाइट)। अगर आप सार्वजनिक या शेयर किये जाने वाले कंप्यूटर पर ऐसी जानकारी का प्रयोग करते हैं, काम खत्म करने के बाद पूरी तरह से साइन आउट करने का और ब्राउजर की विंडो को बन्द करने का ध्यान रखें।

यह सुनिश्चित करें की जिसके लिए अपने पैसे दिए हैं वह आपको मिल गया है

एक बार आपको उत्पाद मिल जाए, तो तुरंत उसे देख लें और सुनिश्चित करें कि जैसा होना चाहिए वैसा वह है। जितनी जल्दी आप धोखे के मामले को पकड़ेंगे, उसको ठीक करने का आपको बेहतर मौका मिलेगा।