کمپیوٹر استعمال کرنے والوں کے لئے ماہانہ سکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- جعلی آن لائن اسٹور
- آپ کا کمپیوٹر، موبائل آلات
- آپ کا کریڈٹ کارڈ

بحفاظت آن لائن خریداری کرنا

یہ محتاط رہنے کا موسم ہے

چھٹیوں کا موسم آنے والا ہے اور عنقریب دنیا بھر میں لاکھوں لوگ بہترین تحائف خریدنے کی تلاش میں ہوں گے۔ ہم میں سے کئی لوگ بہترین سودے کی تلاش میں اور لمبی قطاروں اور بے صبر ہجوم سے بچنے کے لیئے آن لائن خریداری کا انتخاب کرتے ہیں- بدقسمتی سے سال کا یہ وقت مجرمان کے لیئے بھی آن لائن یا مالی دھوکہ دہی کے لیئے پسندیدہ وقت ہوتا ہے۔ اس مہینے ہم آپ کو آن لائن خریداری کے خطرات اور اس سے بچنے کے طریقے کے بارے میں بتائیں گے۔

مہمان ایڈیٹر

جاناتھن ہومر (@JonathanLHomer) سائبر تحفظ کی آگاہی کی صنعت کی معروف شخصیت ہیں اور وہ سرکاری اور نجی دونوں شعبوں میں فعال ہیں۔ جاناتھن لوگوں کو مشغول کرنے اور بہترین تربیت کی تکنیک کے ماہر ہیں-

جعلی آن لائن اسٹورز

جبکہ زیادہ تر آن لائن اسٹورز اصلی ہوتے ہیں، کچھ جعلی بھی ہوتے ہیں یعنی یہ جعلی ویب سائٹس ہوتی ہیں جنھیں مجرمان نے بنایا ہوتا ہے۔ مجرمان ان جعلی ویب سائٹس کو مشہور اصل اسٹور سے نقل کر کے یا ان کا نام استعمال کرتے ہوئے بناتے ہیں۔ وہ پھر ان ویب سائٹس کو استعمال کرتے ہوئے ان لوگوں کو شکار کرنے کی کوشش کرتے ہیں جو ممکنہ بہترین سودے کی تلاش میں ہوتے ہیں۔ جب آپ آن لائن خریداری کے لیئے کم ترین قیمت والی چیزیں تلاش کرتے ہیں تو ہو سکتا ہے کہ آپ ان جعلی ویب سائٹس میں سے کسی ایک کی طرف چلے جائیں۔

مصنوعات خریدنے کے لیئے جب آپ کسی ویب سائٹ کا انتخاب کرتے ہیں تو آپ ایسی ویب سائٹس سے ہوشیار رہیں جو حیرت انگیز طور پر کسی بھی جگہ سے بہت کم قیمت اشیاء کی تشہیر کر رہی ہوں یا ایسی مصنوعات فراہم کر رہی ہوں جو ملک بھر میں بک چکی ہوں۔ ان مصنوعات کے اتنے سستے یا غیر معمولی طور پر دستیاب ہونے کی وجہ یہ ہے کہ جو چیز آپ تک پہنچتی ہے وہ اصلی نہیں ہوتی ہے، یہ جعلی یا چوری شدہ مصنوعات ہوتی ہیں یا بعض صورتوں میں یہ آپ تک پہنچتی ہی نہیں ہیں۔ آپ اپنے آپ کو مندرجہ ذیل اقدامات کے ذریعے محفوظ رکھ سکتے ہیں۔

- آپ اس بات کی تصدیق کر لیں کہ اس ویب سائٹ پر فروخت یا سپورٹ سے متعلق سوالوں کے لیئے ایک صحیح ای میل ایڈریس اور فون نمبر موجود ہو۔ اگر ویب سائٹ آپ کو مشکوک لگ رہی ہو تو آپ وہاں کال کر کے کسی شخص سے بات کریں۔
- آپ واضح انتباہ کی علامات پر غور کریں جیسے کہ ناقص گرائمر یا ہجّے۔
- آپ ان ویب سائٹس سے بہت ہوشیار رہیں جو کہ کسی ایسی مشہور ویب سائٹ کی ہو بہو نقل ہوں جسے آپ ماضی میں استعمال کر چکے ہوں لیکن اس کا ڈومین نیم یا اسٹور کا نام اصل نام سے تھوڑا مختلف ہو۔ مثال کے طور پر ممکن ہے کہ آپ ایمازون کی تمام خریداری کے لیئے http://amazon.com پر جانے کے عادی ہوں لیکن ہو سکتا ہے کہ آپ بالکل اس جیسی کسی اور ویب سائٹ جیسے کہ http://store-amazon.com پر چلے جائیں، اس لیئے آپ بہت محتاط رہیں۔
- آپ اسٹور کا نام یا URL ایک سرچ انجن میں لکھیں اور دیکھیں کہ دوسرے لوگوں نے ماضی میں اس ویب سائٹ کے بارے میں کیا کہا

بحفاظت آن لائن خریداری کرنا

ہے۔ آپ «never again»،«scam» اور «fake» جیسی اصطلاحات کو دیکھنے کی کوشش کریں۔ ویب سائٹ کے بارے میں کم لوگوں کے تبصرے بھی کوئی اچھی بات نہیں ہے کیونکہ اس سے یہ پتہ چلتا ہے کہ یہ نئی ویب سائٹ ہے۔

یاد رکھیں کہ صرف اس وجہ سے کہ کوئی ویب سائٹ بہت زیادہ پیشہ ورانہ لگ رہی ہے اس کا یہ مطلب ہرگز نہیں ہے کہ یہ صحیح ویب سائٹ ہے۔ اگر اس ویب سائٹ کی کوئی چیز آپ کو مشتبہ لگتی ہے تو آپ وقت نکال کر اس کی تفتیش کر لیں۔ اگر آپ اس ویب سائٹ کی وجہ سے آرامدہ محسوس نہیں کر رہے ہیں تو آپ اسے استعمال نہیں کریں۔ اس کے بجائے آپ ایسی معروف ویب سائٹ ڈھونڈیں جس پر آپ کو بھروسہ ہو یا آپ نے ماضی میں اسے محفوظ طریقے سے استعمال کیا ہو۔ ہو سکتا ہے کہ اس ویب سائٹ پہ آپ کو کوئی بہت اچھا سودا یا کوئی بہت اچھی چیز نہیں ملے لیکن اس بات کے کافی امکانات ہیں کہ آپ کو صحیح مصنوعات اور صحیح کریڈٹ رپورٹ ملے گی۔

اپنے آپ کو آن لائن خریداری کرتے وقت محفوظ رکھنے کے لیئے صرف ایسی قابل بھروسہ ویب سائٹس کا استعمال کریں جن کی ساکھ کافی اچّھی ہو۔

آپ کا کمپیوٹر / موبائل آلہ

صحیح ویب سائٹ سے خریداری کے علا وہ آپ کو اس بات کو بھی یقینی بنانا چاہیئے کہ آپ کا کمپیوٹر یا موبائل آلہ بھی محفوظ ہے۔ سائبر مجرمان آپ کے آلات کو متأثر کرنے کی کوشش کریں گے تاکہ وہ آپ کے بینک اکاؤنٹ، کریڈٹ کارڈ کی معلومات اور پاس ورڈز تک رسائی حاصل کر سکیں۔ آپ مندرجہ ذیل اقدامات اٹھا کر اپنے آلات کو محفوظ بنا سکتے ہیں۔

- اگر آپ کے گھر میں بچّے ہیں تو آپ دو آلات رکھنے پر غور کریں، ایک اپنے بچّوں کے لیئے اور دوسرا بڑوں کے لیئے- بچّے ٹیکنالوجی کے بارے میں تجسّس رکھتے ہیں اور اسے استعمال کرنا چاہتے ہیں- نتیجاً اُن کا اپنے آلہ کو متأثر کرنے کے امکانات بڑھ جاتے ہیں- علیحدہ کمپیوٹر یا ٹیبلیٹ کو آن لائن ٹرانزیکشن جیسے کہ آن لائن بینکنگ اور خریداری کے لیئے استعمال کرنے سے آپ کے متأثر ہونے کے امکانات کم ہو جاتے ہیں۔ اگر علیحدہ آلات استعمال کرنے کا اختیار موجود نہ ہو تو آپ مشترکہ کمپیوٹر پر علیحدہ اکاؤنٹس بنا دیں اور اس بات کی تأکید کر لیں کہ آپ کے بچّوں کے پاس ایڈمنسٹریشن اختیارات موجود نہ ہوں۔
- آپ صرف اُن وائرلیس نیٹ ورکس سے مُنسلک ہوں جن کے آپ منتظم ہوں جیسے کہ آپ کے گھر کا نیٹ ورک، یا مالی ٹرانزیکشن کرتے وقت ایسے نیٹ ورک سے منسلک ہوں جس پر آپ بھروسہ کرتے ہوں۔ عوامی وائی فائی نیٹ ورکس جیسے کہ کافی کی دُوکان، آپ کے لیئے خبریں پڑھنے کے لیئے تو بہترین جگہ ہو سکتی ہے لیکن اپنے بینک اکائنٹ تک رسائی حاصل کرنے کے لیئے نہیں۔
- آپ ہمیشہ جدید ترین اور موجودہ اینٹی وائریس سافٹ ویئر انسٹال کریں۔ اس طرح کسی بھی سائبر مجرم کے لیئے آپ کے آلہ کو متأثر کرنا بہت مشکل ہوجا ئے گا۔

آپ کا کریڈٹ کارڈ

آپ اپنے کریڈٹ کارڈ کی اسٹیٹمنٹ پر نظر رکھیں تاکہ آپ کسی بھی مشتبہ رقم کی کٹوتی کی شناخت کر سکیں، آپ کو اپنی اسٹیٹمنٹ کو باقاعدگی سے دیکھتے رہنا چاہیئے، کم از کم مہینے میں ایک مرتبہ ضرور۔ کچھ کریڈٹ کارڈ کمپنیز ہر دفعہ آپ کے کارڈ سے کٹنے والی رقم

بحفاظت آن لائن خریداری کرنا

یا کارڈ کی مختص کردہ رقم کی اطلاع کا اختیار آپ کو ای-میل یا ٹیکسٹ میسیجز کے ذریعے فراہم کرتی ہیں۔ ایک اور طریقہ یہ ہے کہ آپ آن لائن خریداری کے لیئے الگ الگ کریڈٹ کارڈ رکھیں، اس طرح اگر آپ کے کریڈٹ کارڈ کی معلومات افشاں ہو بھی جاتی ہے تو پھر بھی آپ اپنی بقیہ ادائیگی کی سرگرمیوں پر اثر انداز ہوئے بغیر باآسانی کارڈ تبدیل کر سکتے ہیں۔ اگر آپ کو لگتا ہے کہ آپ کے ساتھ دھوکہ ہوگیا ہے تو آپ فوراً اپنی کریڈٹ کارڈ کمپنی کو کال کر کے تمام صورت حال سے آگاہ کریں۔ اسی وجہ سے کریڈٹ کارڈز آن لائن خریداری کے لیئے ڈیبٹ کارڈز سے زیادہ بہتر ہیں۔ ڈیبٹ کارڈز آپ کے اکاؤنٹ سے براہ راست پیسے کاٹتے ہیں اور اگر آپ کے ساتھ کوئی دھوکہ ہو جائے تو آپ کے پیسے واپس ملنا کہیں زیادہ مشکل ہو جاتا ہے۔

آخر میں یہ کہ ایک نئی ٹیکنالوجی آئی ہے جس کے ذریعے آپ اپنے کریڈٹ کارڈ کو ظاہر کئے بغیر پیسے ادا کر سکتے ہیں- آپ ایسے کریڈٹ کارڈز پر غور کریں جو ہر آن لائن خریداری کے لیئے ایک منفرد کارڈ نمبر نکالے یا کوئی معرُوف ادائیگی کی کمپنی کی سروسز، جیسے کہ ‹پےپال›، کا استعمال کریں جس کے لیئے آپ کے کریڈٹ کارڈ نمبر کو کسی وینڈر کو ظاہر کرنے کی ضرورت نہیں پڑتی ہیں۔

مزید جانیئے

OUCH! کے ماہانہ سیکیورٹی تعلیم کے نیوز لیٹر کو سبسکرائب کریں،OUCH! archives تک رسائی حاصل کریں اورSANS سیکیورٹی سے مزیدآگاہی کے لئے اس ویب سائٹ کا دورہ کریں http://www.securingthehuman.org (انگریزی میں) ۔

اردو ایڈیشن

Rewterz پاکستان کی معروف انفارمیشن سکیورٹی کمپنی ہے جو پچھلے سات سالوں سے آئی ٹی سکیورٹی کے شعبے میں خدمات سرانجام دے رہی ہے - کمپنی کے بارے میں مزید معلومات کے لئے http://www.rewterz.com کا دورہ کریں یاہمارے فیس بک پیج https://www.facebook.com/Rewterz کو ‘لائک’ کریں یا ٹوئیٹر @Rewterz پر فالو کریں۔

وسائل:

محفوظ رہنے کے پانچ اقدمات: https://www.securingthehuman.org/ouch/2014#october2014

اپنے گھر کے نیٹ ورک کو محفوظ بنانا: https://www.securingthehuman.org/ouch/2014#january2014

ٹیبلیٹ کو محفوظ بنانا: https://www.securingthehuman.org/ouch/2013#december2013

SANS کی آج کی سکیورٹی تجویز: https://www.sans.org/tip_of_the_day.php

ایڈیٹوریل بورڈ: بل وے مین، والٹ اسکریونز، فل ہوفمن، لینس اسپٹزنر، کارمن رولی ہارڈی۔

ترجمہ: شعیب ہاشمی