SANS SECURITY AWARENESS

OUCH! نومبر ۲۰۱۷

تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

- جعلی آن لائن اسٹورز
- آپ کا کمپیوٹر/ موبائل آلہ
- آپ کا کریڈٹ کارڈ

محفوظ طریقے سے آن لائن خریداری کرنا

جائزہ

ہم میں سے کئی لوگوں کے لیئے چھٹیوں کا موسم آنے والا ہے اور عنقریب دنیا بھر سے لاکھوں لوگ بہترین تحائف کی تلاش میں ہوں گے- ہم میں سے کئی لوگ بہترین سودے کے لیئے آن لائن خریداری کریں گے تاکہ لمبی قطاروں اور بے صبر ہجوم سے بچ سکیں- بد قسمتی سے سال کا یہ وقت سائبر مجرمان کے لیئے جعلی آن لائن ویب سائٹس بنا کر جعلسازی کرنے اور دوسروں سے چوری کرنے کا بھی ہے- ہم نے نیچے آن لائن شاپنگ سے متعلق خطرات کو بیان کیا ہے اور یہ بھی بتایا ہے کہ آپ محفوظ طریقے سے کس طرح زبردست سودے خرید سکتے ہیں-

مہمان ایڈیٹر

لینی زیلٹسر مینروا لیبز میں سکیورٹی کی مصنوعات پر کام کرتے ہیں اور SANS انسٹیٹیوٹ میں میلویئر سے نمٹنے کے بارے میں پڑھاتے ہیں- لینی ٹوئیٹر پر **@lennyzeltser** کے ذریعے فعال ہیں اور **zeltser.com** پر سکیورٹی بلاگ لکھتے ہیں-

جعلی آن لائن اسٹورز

حالانکہ زیادہ تر آن لائن اسٹورز صحیح ہوتے ہیں لیکن سائبر مجرمان کچھ جعلی ویب سائٹس قائم کر دیتے ہیں- مجرمان ان جعلی ویب سائٹس کو بالکل اصل ویب سائٹ سے نقل کر کے بناتے ہیں یا پھر وہ مشہور اسٹورز یا برانڈز کے نام کو استعمال کرتے ہیں- پھر وہ ان جعلی ویب سائٹس کے ذریعے ان لوگوں کو نشانہ بناتے ہیں جو ممکنہ طور پر بہترین سودے کی تلاش میں ہوتے ہیں- جب آپ آن لائن سب سے سستی قیمت والی مصنوعات تلاش کرتے ہیں تو ہو سکتا ہے کہ آپ ان جعلی ویب سائٹس میں سے کسی پر چلے جائیں- جب آپ خریداری کے لیئے کسی ویب سائٹ کا انتخاب کرتے ہیں تو آپ ان ویب سائٹس سے ہوشیار رہیں جو ڈرامائی طور پر ملک میں بکنے والی باقی تمام ویب سائٹس پر موجود مصنوعات سے سستی قیمت فراہم کر رہی ہوتی ہیں- اتنی سستی قیمت کی وجہ یہ ہے کہ جو چیز آپ کو ملے گی وہ اصل نہیں ہوگی، شاید وہ جعلی یا چوری شدہ ہو یا کچھ صورتوں میں تو وہ کبھی آپ تک پہنچتی ہی نہیں ہے- آپ اپنے آپ کو مندرجہ ذیل اقدامات کے ذریعے محفوظ رکھ سکتے ہیں:

- جب بھی ممکن ہو آپ صرف ان ویب سائٹس سے خریداری کریں جن کے بارے میں آپ کو معلوم ہے یا جن پر آپ کا بھروسہ ہے اور آپ پہلے وہاں سے خریداری کر چکے ہیں-
- آپ اس بات کی تصدیق کر لیں کہ اس ویب سائٹ پر ایک صحیح پتہ اور خرید و فروخت اور سپورٹ سے متعلق سوالات پوچھنے کے لیئے فون نمبر موجود ہیں- اگر یہ ویب سائٹ مشتبہ لگتی ہے تو آپ کال کر کے کسی شخص سے بات کریں- اگر آپ کی کسی شخص سے بات نہیں ہوتی ہے تو یہ اس ویب سائٹ کے جعلی ہونے کی سب سے بڑی علامت ہو سکتی ہے-
- آپ واضح انتباہ کی علامات کو ضرور دیکھیں جیسے کہ سودے کی ایسی پیشکش جو کہ غیر یقینی لگ رہی ہو یا پھر خراب گرائمر کا استعمال-
- اگر آپ کو کوئی ویب سائٹ ہُوبہُو کسی ایسی ویب سائٹ کی نقل لگ رہی ہو جسے آپ نے ماضی میں استعمال کیا ہو لیکن اس کا یو آر یل (URL) تھوڑا مختلف ہو تو آپ اس کے بارے میں مشکوک ہو جائیں- مثال کے طور پر آپ ایمیزون سے شاپنگ کرنے کے عادی ہوں جس کی ویب سائٹ ہے https://www.amazon.com لیکن اگر آپ کسی ایسی ویب سائٹ پر جاتے ہیں جو کہ ایمیزون ہونے کا دعوہ کر رہی ہو جیسے کہ http://store-amazoncom.com تو آپ بہت زیادہ ہوشیار ہو جائیں-

محفوظ طریقے سے آن لائن خریداری کرنا

آپ آن لائن شاپنگ صرف ایسی قابل بھروسہ ویب سائٹس کے ذریعے کریں جنہوں نے اپنی ساخ قائم کر رکھی ہو-

- آپ اسٹور کا نام یا یو آر ایل (URL) سرچ انجن میں لکھیں اور دیکھیں کہ لوگوں نے اس ویب سائٹ کے بارے میں ماضی میں کیا لکھا ہے- آپ «never again», «scam», «fraud» یا «fake» جیسی اصطلاحات ڈھونڈیں- اگر کسی ویب سائٹ کے بارے میں لوگوں کے تبصرے موجود نہیں ہیں تو یہ بھی ایک علامت ہے کہ یہ ویب سائٹ نئی ہے اور اس پر بھروسہ نہیں کیا جا سکتا ہے-
- کوئی بھی چیز آن لائن خریدنے سے پہلے آپ اس بات کو یقینی بنائیں کہ آپ کا اس ویب سائٹ تک کنیکشن انکرپٹڈ ہے- زیادہ تر ویب سائٹس آپ کو انکرپٹڈ کنیکشن کو ایک تالے کے ذریعے دکھاتی ہیں یا/اور ویب سائٹ کے نام سے پہلے HTTPS برے رنگ کا لکھا ہوا نظر آتا ہے-

یاد رکھیں کہ صرف اس وجہ سے کہ کوئی ویب سائٹ بہت پیشہ ورانہ لگ رہی ہے، یہ مطلب نہیں ہے کہ وہ مستند ہے- اگر آپ کسی ویب سائٹ سے مطمئن نہیں ہیں تو آپ اسے استعمال نہیں کریں- اس کے بجائے آپ کوئی ایسی ویب سائٹ ڈھونڈیں جس پر آپ بھروسہ کرتے ہوں یا آپ نے ماضی میں استعمال کی ہوئی ہو- ہو سکتا ہے کہ یہاں پر آپ کو کوئی بہت عمدہ سودا نہیں مل رہا ہو لیکن جو مصنوعات آپ خریدیں گے وہ بالکل مستند ہوں گی اور آپ کی ذاتی اور معاشی معلومات چوری ہونے سے بچ جائیں گی-

آپ کا کمپیوٹر/ موبائل آلہ

صحیح ویب سائٹ سے خریداری کرنے کے علاوہ آپ اس بات کو بھی یقینی بنائیں کہ آپ کا کمپیوٹر یا موبائل آلہ محفوظ ہے- سائبر مجرمان آپ کے آلات کو متاثر کرنے کی کوشش کرتے ہیں تاکہ آپ کے بینک اکاؤنٹ کی تفصیلات، کریڈٹ کارڈ کی معلومات اور پاس وورڈز حاصل کر سکیں- آپ مندرجہ ذیل اقدامات کے ذریعے اپنے آلات کو محفوظ رکھ سکتے ہیں-

- اگر آپ کے گھر میں بچّے ہیں تو آپ دو آلات رکھنے پر غور کریں، ایک بچّوں کے لیۓ اور ایک بڑوں کے لیۓ- بچّے ٹیکنالوجی کے بارے میں کافی شوقین ہوتے ہیں اور اسے استعمال کرنا چاہتے ہیں، نتجتاً ان کے آلات کے متاثر ہونے کے امکانات زیادہ ہوتے ہیں- آن لائن ٹرانزیکشن جیسے کہ آن لائن بینکنگ یا آن لائن خریداری کے لیۓایک علیدہ کمپیوٹر یا ٹیبلٹ استعمال کرنے سے آپ کے دوسرے آلہ کے متاثر ہونے کے امکانات کم ہو جاتے ہیں-
- آپ ہمیشہ جدید ترین اپڈیٹس کو انسٹال کیا کریں اور اپنے اینٹی وائرس کو ہمیشہ تازہ ترین (اپڈیٹ) رکھا کریں- اس طرح سائبر مجرمان کے لیئے آپ کے آلہ کو متاثر کرنا بہت مشکل ہو جاۓ گا-

آپ کا کریڈٹ کارڈ

آپ باقاعدگی سے اپنے کریڈٹ کارڈ کی اسٹیٹمنٹس کا جائزہ لیتے رہیں تاکہ آپ کو کسی بھی مشکوک سرگرمی کا پتہ چلتا رہے خصوصاً اس وقت جب آپ نے کافی ساری آن لائن خریداری کی ہو یا کسی نئی ویب سائٹ سے خریداری کی ہو- کچھ کریڈٹ کارڈ آپریٹرز آپ کا کارڈ استعمال ہونے کی صورت میں یا

محفوظ طریقے سے آن لائن خریداری کرنا

ایک مخصوص رقم سے زیادہ استعمال ہونے کی صورت میں آپ کو ای میل یا ٹیکسٹ میسج کے ذریعے مطلع کرنے کی سہولت فراہم کرتے ہیں- ایک اور اختیار یہ ہو سکتا ہے کہ آپ کسی ایک کریڈٹ کارڈ کو صرف آن لائن خریداری کے لیئے استعمال کریں- اس طرح اگر اس کارڈ کے ذریعے کوئی غلط سرگرمی ہو بھی جاتی ہے تو آپ اس کارڈ کو دوسری کسی بھی ادائگی پر اثر انداز ہوئے بغیر با آسانی تبدیل کر سکتے ہیں- اگر آپ کو لگتا ہے کہ کوئی فراڈ ہو گیا ہے تو آپ اپنی کریڈٹ کارڈ کمپنی کو فوراً کال کریں- یہ ایک بڑی وجہ ہے کہ آپ کو آن لائن خریداری کے لیئے کریڈٹ کارڈز استعمال کرنے چاہیئے اور جتنا ممکن ہو ڈیبیٹ کارڈ سے اجتناب کرنا چاہیئے- ڈیبیٹ کارڈز سیدھا آپ کے بینک اکاؤنٹ سے پیسے نکالتے ہیں- اگر کوئی فراڈ ہو جائے تو آپ کو اپنے پیسے ملنا بہت مشکل ہو جاتا ہے- آخر میں یہ کہ آپ ان کریڈٹ کارڈز کو استعمال پر غور کریں جو ہر آن لائن خریداری یا گفت کارڈ کے استعمال پر ایک منفرد نمبر جاری کرتے ہیں یا پھر آپ کسی مشہور پیمینٹ سروس کا استعمال کریں جیسے کہ پےپال (PayPal)، جسے آپ کے کریڈٹ کارڈ نمبر کو آپ کے وینڈر کو دکھانے کی ضرورت نہیں پڑتی ہے-

مزید جانیئے

آخری بات یہ کہ آپ لوگوں کو !OUCH نیوز لیٹر جیسے وسائل کو سبسکرائب کرنے کی تجویز دیں تاکہ وہ اپنے طور پر چیزیں سیکھتے رہیں- یہ نیوز لیٹر ہر مہینے ۲۰ زبانوں میں شائع ہوتا ہے آپ securingthehuman.sans.org/ouch/archives کے ذریعے سائن اپ کر سکتے ہیں-

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:

سوشل انجینئرنگ: https://securingthehuman.sans.org/ouch/2017#january2017

محفوظ رہنے کے لیئے چار اقدامات: https://securingthehuman.sans.org/ouch/2016#october2016

اپنے گھر کے نیٹ ورک کو محفوظ بنانا: https://securingthehuman.sans.org/ouch/2016#february2016

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