کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سیکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- جائزہ
- آپ کیوں ہدف بنتے ہیں
- اپنے آپ کو محفوظ رکھنا

جی، آپ ہی اصل ہدف ہیں

جائزہ

ایک عام غلط فہمی لوگوں کو یہ ہے کہ وہ سائبر حملے کا نشانہ نہیں ہیں، اور یہ کہ وہ یا انکے کمپیوٹر کی کوئی اہمیت نہیں ہے۔ اس میں سچائی نہیں ہے۔ اگر آپکے پاس کمپیوٹر، موبائل ڈیوائس، آن لائن اکاؤنٹ، ای میل ایڈریس، کریڈٹ کارڈ یا کوئی دوسری آن لائن سرگرمی میں مصروف ہونے کا ذریعہ ہے تو سائبر مجرمانکے نزدیک آپ کی اہمیت ہے۔ اس نیوز لیٹر میں ہمنے یہ بیان کیا ہے کہ آپ کیوں ہدف ہیں، آپ پر کس طرح حملہ ہوتا ہے اور آپ کن اقداماتکے ذریعے اپنے آپ کو محفوظ رکھ سکتے ہیں ۔

مہمان ایڈیٹر

ایریک کانریڈ بیک شور کمیونیکیشنزکے صدر اور سی ٹی او ہیں اور سی آئ ایس ایس پی اسٹڈی گائیڈ، دوسرا شمارہ اور ایلیونتھ آور سی آئ ایس ایس پی،دوسرا شمارہ،کے مرکزی مصنف ہیں- وہ SANS کے چھ روزہ کورس کنٹینیوس مانیٹرنگ اینڈ سیکیورٹی آپریشنز (SEC511)کے شریک مصنف بھی ہیں ۔

آپ کیوں ہدف بنتے ہیں

جرائم جیسے کہ فراڈ، شناخت کی چوری یا بھتہ خوری کا وجود تہذیبوںکے شروع ہونےسے ہے- یہ ہماری زندگی کا حصہ ہیں۔ ایک مجرم کا ہدف ہمیشہسے ایک ہی رہا ہے: کمسے کم ممکنہ خطرےکے ساتھ جتنے زیادہسے زیادہ پیسے کما سکتے ہیں کما لیں۔ روایتی طور پر یہ مشکل تھا کیونکہ مجرمان اپنی جگہ کی وجہسے محدود ہوتے تھے اور انہیں اپنے ممکنہ شکارسے خودہی ملنا پڑتا تھا- اسسے نہ صرف مجرمان کا لوگوں کو ہدف بنانے کا دائرہ کار محدود ہوتا تھا، بلکہ اسسےنقاب ہونے کا امکان کافی بڑھ جاتا تھا- تاہم انٹرنیٹ اور آن لائن ٹیکنالوجی کی آمدسے جرم یکثر تبدیل ہو گیا ہے- اب سائبر مجرم باآسانی دنیا بھر میں کسی کو بھی نشانہ بنا سکتے ہیں بہت کم یا بغیر کسی قیمتکے بدلے اور بہت کم خطرےکے ساتھ- اسکے علاوہ سائبر مجرمان انتہائی منظم اور فعال ہو چکے ہیں جس کی وجہسے وہ پہلےسے کہیں زیادہ مؤثر ہوگئے ہیں۔ بلآخر سائبر مجرمان یہ جانتے ہیں کہ وہ جتنے زیادہ کریڈٹ کارڈ چرائیںگے، جتنے زیادہ بینک اکاؤنٹس ہیک کرینگے، جتنے زیادہ پاس ورڈ حاصل کرینگے، اتنے ہی زیادہ پیسے کما سکتے ہیں۔ وہ انٹرنیٹسے منسلک کسی بھی شخص کو باضابطہ ہیک کرنے کی کوشش کرینگے جن میں آپ بھی شامل ہیں۔

دنیا بھرکے لاکھوں لوگوں کو ہیک کرنا بظاہر بہت زیادہ کام لگتا ہے لیکن حیران کن طور پر یہ بہت آسان ہوتا ہے کیونکہ ہیکرز خودکار ٹُولز کا استعمال کرتے ہیں جو انکے لئے سارے کام کرتا ہے۔ مثالکے طور پر وہ لاکھوں ای میل ایڈریسز کا ڈیٹا بیس بنا سکتے ہیں اور پھر خودکار ٹولز کا استعمال کرتے ہوئے ان میںسے ہر ایک کو فشنگ پیغام بھیج سکتے ہیں۔ مجرمان کو ای میل بھیجنے کی قیمت تقریباً کچھ بھی نہیں پڑتی ہے: وہ بس دوسرے ہیک شدہ کمپیوٹرز ،جس میں شاید آپ کا کمپیوٹر بھی شامل ہے، کا استعمال کرتے ہیں اپنے گندے کام کرنے کیلئے- یہ ایک اور مثال ہے آپ کی ڈیوائس کی اہمیت کی- اگر کچھ اور نہیں تو یہ دوسروں کو ہیک کرنے یا نقصان پہنچانے کیلئے استعمال کر سکتے ہیں۔ بلآخر یہ مجرمان یہ نہیں جانتے ہیں کہ انکے ای میلکے حملے کا نشانہ کون بنے گا لیکن وہ یہ جانتے ہیں کہ وہ جتنی زیادہ ای میلز بھیجینگے، اتنے ہی زیادہ لوگ ان کا شکار

جی، آپ ہی اصل ہدف ہیں

بنیں گے یا شاید مجرمان انٹرنیٹ پر موجود ہر کمپیوٹر کو باقاعدہ اسکین کریں گے (ایک بار پھر ہیک شدہ کمپیوٹر کو استعمال کرتے ہوئے)، ان کمپیوٹرز یا ڈیوائسز کی تلاش میں جنہیں وہ ہیک کرسکیں۔ یاد رکھیں کہ آپ کو صرف اس وجہ سے نشانہ نہیں بنایا جاتا کیونکہ آپ بہت خاص ہیں بلکہ یہ سائبر مجرمان جس کسی کو بھی نشانہ بنا سکتے ہوں، بناتے ہیں، بشمول آپ کے۔

اپنے آپ کو محفوظ رکھنا

جب سائبر مجرمان دنیا بھر کے لوگوں کو نشانہ بنانے کی کوشش کرتے ہیں تو وہ عام طور پر نسبتاً آسان طریقہ استعمال کرتے ہیں- خوش قسمتی سے آپ کچھ آسان اقدامات کو اپناکر اپنے آپ کو کافی حد تک محفوظ رکھ سکتے ہیں۔ ہم آپ کو چند مندرجہ ذیل اقدامات اپنانے کا مشورہ دیتے ہیں جن میں شامل ہیں:

آپ کو شاید اندازہ نہیں ہو لیکن آپ کی ڈیوائس اور آپ کی معلومات دنیا بھر کے سائبر مجرمان کیلئے بے انتہاءقیمتی ہے۔

- **آپ خود:** آخر کار آپ خودہی کسی بھی سائبر حملے کے دفاع کے خلاف پہلی کڑی ہوتے ہیں۔ بہت سارے حملے اس طرح شروع ہوتے ہیں کہ سائبر مجرمان آپ کو جھانسہ دینے یا بیوقوف بنانے کی کوشش کرتے ہیں جیسے کہ وہ دھوکہ دہی کے ذریعے آپ سے متاثرہ ای میل اٹیچمنٹ کھولنے کا کہتے ہیں یا آپ کو فون پر بیوقوف بنا کر اپنا پاس ورڈ دینے کے لیے اکساتے ہیں۔ آپ کی عقل آپ کا سب سے بہترین دفاع ہے- اگر آپ کو کچھ عجیب لگے، مشکوک لگے یا کچھ صحیح نہیں لگ رہا ہو تو اس بات کا قوی امکان ہے کہ یہ حملہ ہے۔

- **اپڈیٹ کرنا:** اس بات کی تاکید کرلیں کہ آپ کے زیراستعمال کمپیوٹر یا موبائل ڈیوائس مکمل اپڈیٹ ہے اور اس میں تمام تر تازہ ترین پیچز موجود ہیں۔ یہ نہ صرف آپ کے آپریٹنگ سسٹم بلکہ کسی بھی ایپلیکیشن یا پلگ-ان، جسے آپ استعمال کررہے ہوں، کے لئے ضروری ہے- اپنے سسٹم اور ایپلیکیشنز کو ہمیشہ اپڈیٹ رکھنے سے آپ سب سے عام حملوں کے خلاف اپنے آپ کی مدد کررہے ہوتے ہیں۔

- **پاس ورڈ:** آپ اپنے ہر اکاؤنٹ کے لۓ مضبوط اور منفرد پاس ورڈ کا استعمال کریں- اس طرح اگر کوئی ویب سائٹ ہیک ہوتی ہے اور اس کے تمام پاس ورڈز (بشمول آپ کے) چوری ہو جاتے ہیں تو آپ کے دوسرے اکاؤنٹ محفوظ رہتے ہیں۔ اس لئے آپ اس بات کی بھی یقین دہانی کرلیں کہ آپ کی تمام مختلف ڈیوائسز مضبوط، منفرد پاسورڈ، پن یا کسی دوسرے سیکوریٹی طریقہ کار کے ذریعے محفوظ ہوں۔ اپنے تمام مختلف پاس ورڈز کو محفوظ طریقے سے منظم کرنے کے لئے ہمارا مشورہ ہے کہ آپ پاس ورڈ مینیجر استعمال کریں۔

- **کریڈٹ کارڈ:** آپ اپنی مالی تفصیلات کا اکثر جائزہ لیتے رہا کریں، ہمارا مشورہ ہے کہ کم از کم ہفتے میں ایک بار ضرور جائزہ لیں(ماہانہ جائزہ لینا کافی نہیں ہے)۔ جیسے ہی آپ اپنے کریڈٹ کارڈ پر معمولی ٹرانزیکشن دیکھیں تو آپ فوراً کریڈٹ کارڈ فراہم کرنے

جی، آپ ہی اصل ہدف ہیں

والی کمپنی کو مطلع کریں۔ اگر آپ کا بینک آپ کو غیر معمولی طور پر بڑی یا عجیب ٹرانزیکشن پر ای میل یا ٹیکسٹ میسج بھیجنے کی اجازت دیتا ہے تو آپ اس سہولت کو مشکوک سرگرمی کی تیز اطلاع کیلئے بھی استعمال کرسکتے ہیں۔

- **آپ کا نیٹ ورک:** آپ اپنے گھر کے وائی فائی نیٹ ورک ایکسس پوائنٹ کو مضبوط ایڈمنسٹریٹر پاسورڈ کے ذریعے محفوظ کریں اور اس بات کی تاکید کرلیں کہ آپ کے وائی فائی نیٹ ورک سے کسی کو بھی منسلک ہونے کیلئے پاسورڈ درکار ہو۔ اس کے علاوہ اس بات کی بھی تاکید کرلیں کہ آپ کو اس بات کا علم ہو کہ کون سی ڈیوائسز آپ نے اپنے گھر کے نیٹ ورک سے منسلک کی ہوئی ہیں اور یہ کہ وہ تمام ڈیوائیسز اپ ڈیٹ ہیں ۔

- **سوشل میڈیا:** آپ جتنی زیادہ معلومات آن لائن شائع کریں گے اتنا ہی زیادہ آپ اپنے آپ کو خطرے میں ڈالیں گے- نہ صرف یہ کہ آپ کی شائع کی ہوئی کوئی بھی معلومات سائبر مجرمان کیلئے آپ کو نشانہ اور بیوقوف بنانے کیلئے آسانی پیدا کر دے گی بلکہ وہ اصل میں آپ کو قیمتی ہدف کے طور پر شناخت کر دے گی۔

مزید جانئے:

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

اردو ایڈیشن

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

وسائل:

OUCH! پاس ورڈ مینیجرز:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! اپنے گھر کے نیٹ ورک کو محفوظ کرنا:	http://www.securingthehuman.org/ouch/2014#january2014
OUCH! فشنگ حملہ:	http://www.securingthehuman.org/ouch/2013#february2013
پوسٹر: آپ نشانہ ہیں:	http://www.securingthehuman.org/resources/posters

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

ترجمہ: شعیب ہاشمی