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

OUCH!

اس شمارے میں شامل ہے:

- آپ کا وائرلیس نیٹ ورک
- آپ کے آلات

اپنے گھر کے نیٹ ورک کو محفوظ بنانا

جائزہ

کئی سال پہلے گھر کے نیٹ ورک نسبتاً سادہ ہوتے تھے، عام طور پر ایک وائرلیس ایکسس پوائنٹ اور ایک یا دو کمپیوٹر جو کہ انٹرنیٹ استعمال کرنے، آن لائن خریداری کرنے یا گیمینگ کے لیۓ استعمال ہوتے تھے- گھر کے نیٹ ورک اب کافی پیچیدہ ہوتے جا رہے ہیں- اب ہم ان نیٹ ورکس کے ساتھ پہلے سے کہیں زیادہ آلات مُنسلک کرتے ہیں اور اب انٹرنیٹ کا استعمال براؤزنگ سے کہیں زیادہ ہوتا ہے- اِس نیوز لیٹر میں ہم آپ کو بتائیں گے کہ آپ اپنے گھر میں اپنے اور اپنے خاندان کے لیۓ محفوظ نیٹ ورک کس طرح بنا سکتے ہیں-

مہمان ایڈیٹر

شیرل کانلے، ‹لاک ہیڈ مارٹن› میں سکیورٹی کی تعلیم اور آگاہی کی ٹیم کی سربراہی کرتی ہیں، جس کی مُہم ‹دی آئی کیمپین› کی رسائی ایک لاکھ سے زائد ملازمین تک ہے جن میں عالمی فشنگ پروگرام کے علاوہ تنظیم بھر سے مُختلف گرُوپس شرکت کرتے ہیں- آپ شیرل کو @conleychera کے ذریعے فالو کر سکتے ہیں-

آپ کا وائرلیس نیٹ ورک

تقریباً ہر گھر کا نیٹ ورک، وائرلیس نیٹ ورک (جو کہ وائی-فائی نیٹ ورک بھی کہلاتا ہے) سے شروع ہوتا ہے- وائرلیس نیٹ ورک کے ذریعے ہی آپ اپنے کسی بھی آلہ کو بغیر تار کے، انٹرنیٹ سے مُنسلک کرتے ہیں جن میں لیپ ٹاپس اور ٹیبلیٹس سے لے کر گیمینگ کنسولز اور ٹیلیویژنز شامل ہیں- زیادہ تر گھر کے وائرلیس نیٹ ورک آپ کے انٹرنیٹ راؤٹر کے ذریعے کنٹرول ہوتے ہیں، یہ ایک ایسا آلہ ہے جسے آپ کے انٹرنیٹ فراہم کرنے والی سروس آپ کے گھر میں انسٹال کرتی ہے تاکہ آپ انٹرنیٹ سےربط قائم کرسکیں- تاہم کچھ صورتوں میں آپ کا وائرلیس نیٹ ورک ایک علیدہ سسٹم، جوکہ وائر لیس ایکسس پوائنٹ کہلاتا ہے اور آپ کےانٹرنیٹ راؤٹر سے مُنسلک ہوتا ہے، کے ذریعے کنٹرول ہوسکتاہے- اِس بات سے قطع نظر کہ آپ کا وائرلیس نیٹ ورک کیا استعمال کر رہا ہے، یہ دونوں آلات ایک ہی طریقے سے کام کرتے ہیں یعنی وائرلیس سگنلز براڈکاسٹ کر کے- آپ کے گھر میں موجود مُختلف آلات ان سگنلز کے ذریعے آپ کے وائرلیس نیٹ ورک سے مُنسلک ہوتے ہیں- پھر یہ آلات انٹرنیٹ یا آپ کے گھر کے نیٹ ورک میں موجود دوسرے آلات سے مُنسلک ہو سکتے ہیں- اِس کا مطلب ہے کہ اپنے گھر کی حفاظت کا ایک اہم جُز وائرلیس نیٹ ورک کو محفوظ بنانا ہے- ہمارا مشورہ ہے کہ آپ مندرجہ ذیل اقدامات اپنا کر اپنے وائرلیس نیٹ ورک کو محفوظ بنائیں-

- اپنے انٹرنیٹ راؤٹر یا وائرلیس ایکسس پوائنٹ، جو بھی آپ کا وائرلیس نیٹ ورک کنٹرول کر رہا ہے، کے ڈیفالٹ ایڈمنسٹریٹر پاس ورڈ کو تبدیل کر دیں- ایڈمِن اکاؤنٹ کے ذریعے آپ اپنے وائرلیس نیٹ ورک کی سیٹنگز کنفیگر کر سکتے ہیں- آپ اِس بات کو یقینی بنائیں کہ آپ ایڈمنسٹریٹر کے پاس ورڈ کو ایسے مضبوط اور منفرد پاس ورڈ سے تبدیل کر رہے ہیں جو کہ صرف آپ کو معلوم ہو-
- اپنے وائرلیس نیٹ ورک (جو کہ SSID بھی کہلاتا ہے) کا ڈیفالٹ نام تبدیل کر دیں- یہ وہ نام ہے جسے آپ کے آلات، لوکل وائرلیس نیٹ ورک کو تلاش کرتے ہوئے دیکھتے ہیں- آپ اپنے نیٹ ورک کا نام منفرد رکھیں تاکہ اُس کی شناخت با آسانی ہو جائے لیکن اِس بات کو

اپنے گھر کے نیٹ ورک کو محفوظ بنانا

اپنے گھر کے نیٹ ورک کو محفوظ بنانے کے لیئے آپ اپنے وائرلیس نیٹ ورک کو محفوظ بنائیں، اسے اپڈیٹ کریں اور اپنے نیٹ ورک میں موجود تمام آلات کی پاس ورڈ کے ذریعے حفاظت کریں۔

یقینی بنائیں کہ اس میں کوئی ذاتی معلومات شامل نہیں ہیں- اپنے نیٹ ورک کو چھپانے (یا براڈکاسٹ نہ کرنے) کی زیادہ اہمیت نہیں ہے کیونکہ زیادہ تر وائرلیس اسکیننگ ٹُولز یا ہُنرمند حملہ آور، باآسانی چُھپے ہوئے نیٹ ورک کو دریافت کر سکتے ہیں-

- آپ اِس بات کو یقینی بنائیں کہ صرف وہ لوگ آپ کے وائرلیس نیٹ ورک سے مُنسلک ہو سکتے ہیں جن پر آپ کو بھروسہ ہے اور اِس بات کو بھی یقینی بنائیں کہ وہ تمام کنیکشنز انکرپٹڈ ہیں- آپ یہ سب کچھ مضبوط سکیورٹی کو فعال بنا کے کر سکتے ہیں- اِس وقت سب سے بہترین سکیورٹی طریقہ کار،WPA2، کا استعمال ہے- اسے فعّال کرنے کے بعد کسی کو بھی آپ کے گھر کے نیٹ ورک سے مُنسلک ہونے کے لیئے پاس ورڈ درکار ہو گا اور ایک بار جب وہ اس سے مُنسلک ہو جائیں تو اُن کی تمام آن لائن سَرگرمیاں انکرپٹ ہو جاتی ہیں- آپ اِس بات کو یقینی بنائیں کہ آپ کوئی پُرانا، متروکہ طریقہ، جیسے کہ WEP یا پھر سِرے سے کسی سکیورٹی کا استعمال، کر ہی نہیں رہے ہیں، جو کہ ایک کھلا نیٹ ورک ہوتا ہے- کُھلے نیٹ ورکس کسی کو بھی بغیر تصدیق کے آپ کے وائرلیس نیٹ ورک سے مُنسلک ہونے کی اجازت دیتے ہیں-
- کئی وائرلیس نیٹ ورکس میں ایک سپورٹ موجود ہوتی ہے جو کہ گیسٹ نیٹ ورک کہلاتی ہے- اِس کے ذریعے لوگ انٹرنیٹ سے مُنسلک ہو جاتے ہیں لیکن آپ کے گھر کا نیٹ ورک محفوظ رہتا ہے کیوں کہ یہ لوگ آپ کے گھر کے نیٹ ورک پر موجود کسی بھی دوسرے آ لہ سے مُنسلک نہیں ہو سکتے ہیں- اگر آپ گیسٹ نیٹ ورک کا اضافہ کرتے ہیں تو اِس بات کو یقینی بنائیں کہ آپ نے WPA2 فعّال کر دیا ہے اور آپ اِس نیٹ ورک کے لیئے ایک منفرد پاس ورڈ استعمال کر رہے ہیں-
- آپ وائی-فائی پروٹیکٹڈ سیٹ-اپ یا کسی بھی ایسے دوسرے طریقہ کار کو غیر فعّال کر دیں جس کے ذریعے ایک نیا آلہ بغیر پاس ورڈ یا کنفیگریشن اختیارات کے، نیٹ ورک سے مُنسلک ہو جائے-
- اگر آپ کو ان مُختلف پاس ورڈز کو یاد رکھنے میں دِقّت ہوتی ہے تو ہمارا پُرزور مشورہ ہے کہ آپ پاس ورڈ مینیجر کا استعمال کریں تاکہ آپ کے پاس ورڈز محفوظ طریقے سے ذخیرہ ہو جائیں-

کیا آپ ان اقدامات پر عمل درآمد کرنے کے بارے میں تذبذب کا شکار ہیں؟ اِس سے متعلّق اپنے انٹرنیٹ سروس پروائڈر سے پوچھیں، اپنے انٹرنیٹ راؤٹر یا وائرلیس ایکسس پوائنٹ کے ساتھ آئی دستاویزات کا مطالعہ کریں یا اُن کی متعلقہ ویب سائٹ کا دورہ کریں-

آپ کے آلات

اگلا قدم یہ ہے کہ آپ یہ معلوم کریں کہ آپ کے گھر کے نیٹ ورک سے کون سے آلات مُنسلک ہیں اور اِس بات کو یقینی بنائیں کہ وہ تمام محفوظ ہیں- یہ اُس وقت آسان ہُوا کرتا تھا جب صرف چند آلات نیٹ ورک سے مُنسلک ہُوا کرتے تھے- تاہم آج کل کی «ہر وقت مُنسلک رہنے»

اپنے گھر کے نیٹ ورک کو محفوظ بنانا

کی دنیا میں تقریباً کوئی بھی چیز آپ کے نیٹ ورک سے مُنسلک ہو سکتی ہے جس میں ٹی وی، گیمنگ کنسولز، بےبی مانیٹرز، اسپیکرز، آپ کا تھرمواسٹیٹ یا شاید آپ کی گاڑی بھی شامل ہے- ایک آسان طریقہ اپنے گھر کے نیٹ ورک سے مُنسلک آلات دریافت کرنے کا یہ ہے کہ آپ ایک عام سے نیٹ ورک اسکینر کا استعمال کریں جیسے کہ «فِنگ»- یہ ایپلیکیشنز، جنہیں آپ اپنے کمپیوٹر یا موبائل آلہ پر انسٹال کر سکتے ہیں، آپ کے وائرلیس نیٹ ورک کو اسکین کرتی ہیں اور اِس سے مُنسلک تمام آلات کے بارے میں معلومات فراہم کرتی ہیں- ایک بار جب آپ اپنے گھر کے نیٹ ورک میں موجود تمام آلات کی شناخت کر لیں تو آپ اِس بات کو یقینی بنائیں کہ اِن میں سے ہر ایک آلہ محفوظ ہے- اِس پر عمل درآمد کرنے کا بہترین طریقہ یہ ہے کہ آپ اِس بات کو یقینی بنائیں کہ ہر آلہ، آپریٹنگ سسٹم/فرم ویئر کا جدید ترین ورژن چلا رہا ہو- جب بھی مُمکن ہو آپ اُن پر خود کار اپ ڈیٹنگ کو فعّال کر دیں- اگر آپ کے کسی بھی آلہ میں پاس ورڈ کی ضرورت ہو تو آپ ہمیشہ منفرد اور مضبوط پاس ورڈ کا استعمال کریں- آخری بات یہ کہ آپ اپنے انٹرنیٹ سروس پروائیڈر کی ویب سائٹ کا ضرور دورہ کریں کیونکہ ہو سکتا ہے کہ وہ آپ کو اپنے گھر کے نیٹ ورک کو محفوظ بنانے کے لیۓ مفت ٹُولز فراہم کر رہے ہوں-

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:

پاس فریزز: https://www.securingthehuman.org/ouch/2015#april2015

پاس ورڈ مینیجر: https://securingthehuman.sans.org/ouch/2015#october2015

اپنے ٹیبلیٹ کو محفوظ بنانا: https://securingthehuman.sans.org/ouch/2016#january2016

اپنے گھر کے نیٹ ورک کو میپ کرنا: http://l.rud.is/home-network-mapping

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

ترجمہ: شعیب ہاشمی