کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سیکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:
- آپ کا وائرلیس نیٹ ورک
- اوپن ڈی این ایس
- آپکے آلات

اپنے گھرکے نیٹ ورک کو محفوظ کرنا

جائزہ

کئی سالوں پہلے گھرکے نیٹ ورک نسبتاً آسان ہوتے تھے، یعنی کہ ایک وائرلیس ایکسس پوائنٹ اور ایک دو کمپیوٹر جنکے ذریعے انٹرنیٹ استعمال کیا جاتا تھا یا آن لائن گیمز کھیلی جاتی تھیں۔ تاہم اب گھر کے نیٹ ورک کافی پیچیدہ ہو رہے ہیں۔ نہ صرف یہ کہ ہم اپنے گھر کے نیٹ ورک سے زیادہ ڈیوائیسز منسلک کر رہے ہیں بلکہ ہم اس سے کہیں زیادہ چیزیں کر رہے ہیں۔ اس شمارے میں ہم چند ایسے بنیادی اقدامات کا جائزہ لیں گے جنکے ذریعے گھر کا نیٹ ورک محفوظ بنایا جا سکے۔

مہمان ایڈیٹر

کیون جانسن سیکیور آئیڈیاز کے CEOہیں ، وہ MySecurityScanner.comچلاتے ہیں اور SANS انسٹیٹیوٹ میں سینئر انسٹکٹرہیں ۔آپ انکے بارے میں مزید معلومات www.secureideas.comپر حاصل کر سکتے ہیں۔

آپ کا وائرلیس نیٹ ورک

تقریباً ہر گھر کا نیٹ ورک وائرلیس نیٹ ورک(جسے ہ وائی فائی نیٹ ورک بھی کہا جاتا ہے)سے شروع ہوتا ہے۔ اسکے ذریعے ہی آپ اپنی ڈیوائیسز کو بغیر کسی تارکے انٹرنیٹ سے منسلک کرتے ہیں۔ یہ ڈیوائیسز لیپ ٹاپ اور ٹیبلیٹ سے لے کر گیمنگ کنسول اور ٹیلی وژن ہو سکتی ہیں۔ ایسا کرنے کیلئے آپکے وائرلیس نیٹ ورک کو ایک چیز کی ضرورت ہوتی ہے جسے وائرلیس ایکسس پوائنٹ کہتے ہیں۔ یہ ایک فزیکل ڈیوائس ہوتی ہے جو آپ کے انٹر نیٹ راؤٹرکے ساتھ منسلک ہوتی ہے (یا شاید پہلے سے آپکے انٹر نیٹ راؤٹر میں موجود ہوں) اور وائرلیس سگنل بھیجتی ہے جسکے ذریعے آپ کی ڈیوائس منسلک ہوتی ہے۔ ایک بار آپ کی ڈیوائیسز ایکسس پوائنٹ سے منسلک ہوجائیں تو پھر وہ آپکے گھرکے نیٹ ورک کی دوسری ڈیوائیسزسے بھی منسلک ہو سکتی ہیں اور انٹر نیٹ سے بھی – وائر لیس ایکسز پوائنٹ آپکے گھرکے نیٹ ورک کا اہم ترین جز ہے ۔ ہم مندرجہ ذیل تجاویز پیش کرتے ہیں اسے محفوظ کرنے کیلئے۔

- زیادہ تر وائرلیس ایکسس پوائنٹس کا ڈیفالٹ ایڈمنسٹریٹر لاگ ان اور پاس ورڈ معروف ہوتا ہے اور اکثر انٹر نیٹ پر موجود ہوتا ہے۔ آپ اس بات کی تاکید کرلیں کہ آپ ڈیفالٹ ایڈمنسٹریڑ لاگ ان اور پاس ورڈکو ایسے پاسورڈسے تبدیل کریں جو صرف آپ کو معلوم ہو۔ اس بات کا یقین کرلیں کہ یہ پاسورڈ منفرد ہے اور دوسرے اکاؤنٹس کیلئے استعمال نہیں ہو رہا ہے۔
- ایک اور آپشن جسے آپ کو کنفیگر کرنا ہوگا وہ آپکے وائرلیس نیٹ ورک کا پاسورڈ ہے (بعض دفعہ ایس ایس آئی ڈی بھی کہلاتا ہے)۔ یہ وہ نام ہے جو آپ کی ڈیوائیسز دیکھیں گی جب وہ لوکل وائرلیس نیٹ ورک کو ڈھونڈیں گی۔ آپ اپنے نیٹ ورک کو منفرد نام دیں تاکہ آپ باآسانی اس کی شناخت کرسکیں لیکن اس بات کی یقین دہانی کرلیں کہ اس میں کوئی ذاتی معلومات شامل نہ ہوں۔ اسکے علاوہ اپنے نیٹ ورک کو کنفیگر کرتے وقت چھپانے (یا براڈ کاسٹ نہ کرنا) کی بہت کم اہمیت ہے۔ زیادہ تر وائرلیس اسکیننگ ٹولز یا کوئی بھی ہنر مند حملہ آور با آسانی چھپے ہوئے نیٹ ورک کی تفصیلات دریافت کر سکتا ہے۔

اپنے گھر کے نیٹ ورک کو محفوظ کرنا

اپنے گھر کے نیٹ ورک کو محفوظ رکھنے کیلئے آپ اس بات کی تاکید کرلیں کہ آپ کے پاس محفوظ وائرلیس نیٹ ورک ہے، آپ اوپن ڈی این ایس یا اس سے ملتی جلتی سروس استعمال کر رہے ہیں اور آپ کے گھر سے منسلک تمام ڈیوائسز جدید ترین اور موجودہ ہیں۔

- اگلا قدم اس بات کو یقینی بنانا ہے کہ صرف وہ لوگ آپ کے وائرلیس نیٹ ورک سے منسلک ہوں جن کو آپ جانتے ہوں اور بھروسہ کرتے ہوں۔ اس بات کو بھی یقینی بنائیں کہ وہ سارے کنیکشنز انکرپٹ ہوں۔ آپ کو اس بات کو یقینی بنانا ہے کہ آپ کے ہمسائے یاکوئی اجنبی آپ کے نیٹ ورک سے منسلک یا اس کا مشاہدہ نہ کر رہا ہو۔ آپ ان خطرات کو با آسانی سے حل کر سکتے ہیں اپنے وائرلیس ایکسس پوائنٹ پر مضبوط سیکیورٹی فعال کرکے۔ فالحال سیکیورٹی کا سب سے بہترین طریقہ کار WPA2کا استعمال ہے۔ اسے فعال کرنے کے بعد آپ کو ایک پاسورڈ درکار ہوتا ہے تاکہ لوگ آپ کے گھر کے نیٹ ورک سے منسلک پرانا سکیں۔ ایک بار اوتھنٹیکیٹ ہونے کے بعد کنیکشنز انکرپٹ ہو جاتے ہیں۔ آپ اس بات کی یقین دہانی کرلیں کہ آپ کوئی پرانہ فرسودہ سیکیورٹی طریقہ کار استعمال نہیں کررہے ہوں جیسے کہ WEPیا سرے سے کوئی سیکیورٹی استعمال نہیں کررہے ہوں جو کہ اوپن نیٹ ورک کہلاتا ہے۔ ایک اوپن نیٹ ورک کسی کو بھی وائرلیس نیٹ ورک سے منسلک ہونے کی اجازت دیتا ہے بغیر کسی اوتھنٹیکیشن کے۔
- اس بات کا یقین کرلیں کہ جو پاس ورڈ لوگ استعمال کریں گے وائرلیس نیٹ ورک سے منسلک ہونے کیلئے وہ مضبوط ہو، اس کا اندازہ لگانا مشکل ہو اور وہ ایڈمنسٹریٹر پاسورڈ سے مختلف ہو۔ یاد رہے کہ اس بات کا امکان زیادہ ہے کہ آپ کو ہر ڈیوائس کا پاسورڈ صرف ایک بار درج کرنا ہو کیونکہ وہ ڈیوائسز خود ہی پاسورڈ کو ذخیرہ کر لیتی ہیں اور انہیں یاد رکھتی ہیں۔
- کئی وائرلیس ایکسس پوائنٹس گیسٹ نیٹ ورک کو سپورٹ کرتے ہیں۔ ایک گیسٹ نیٹ ورک لوگوں کو آپ کے وائرلیس نیٹ ورک سے منسلک ہونے اور انٹر نیٹ استعمال کرنے کی اجازت دیتا ہے لیکن وہ لوگ آپ کے گھر کے نیٹ ورک سے منسلک ڈیوائسز سے منسلک نہیں ہو سکتے ہیں۔ اگر آپ گیسٹ نیٹ ورک شامل کرنے جا رہے ہیں تو اس بات کی تاکید کر لیں کہ آپ نے WPA2فعال کر دیا ہے اور اس نیٹ ورک کیلئے مختلف پاسورڈ استعمال کررہے ہیں۔
- اگر آپ مختلف پاسورڈ یاد نہیں رکھ سکتے ہیں تو آپ پاس ورڈ مینیجر کا استعمال کریں انہیں محفوظ طریقے سے ذخیرہ کرنے کیلئے۔

اوپن ڈی این ایس

ایک بار آپ کا وائرلیس نیٹ ورک کنفیگر ہو جائے تو ہمارا مشورہ یہ ہے کہ آپ اپنے گھر کے نیٹ ورک کو اس طرح کنفیگر کریں کہ وہ اوپن ڈی این ایس کو ڈی این ایس سرورز (یااس سے ملتی جلتی سروس جیسے کہ گھر کے استعمال کے لئے نورٹن کنیکٹ سیف)کے طور پر استعمال کریں۔ جب آپ اپنے براؤزرمیں کوئی نام لکھتے ہیں تو ڈی این ایس کی وجہ سے ہی آپ کے براؤزر کو پتہ چلتا ہے کہ انٹر نیٹ پر کس سرور سے رابطہ قائم کرنا ہے۔ اوپن ڈی این ایس جیسی سروسز ایسی ویب وسائٹس کی شناخت کرتی ہیں جو معروف اور متاثرہ ہوں اور آپ کے گھر کے وائرلیس نیٹ ورک سے منسلک کسی بھی ڈیوائس کو حادثاتی طور پر ان ویب سائٹس کا دورہ کرنے سے روکتی ہیں۔ اس کے علاوہ یہ سروس آپ کو قابل اعتراض ویب سائٹس کو فلٹر اور بلاک کرنے کی صلاحیت فراہم کرتی ہیں۔ اس طریقہ کار کو جو چیز مؤثر بناتی ہے وہ یہ ہے کہ آپ کو اپنی ڈیوائس پر کوئی سافٹ وئیر انسٹال نہیں کرنا پڑتا بلکہ آپ کو صرف اپنے وائرلیس ایکسس پوائنٹ میں تبدیلی کرنی پڑتی ہے۔

اپنے گھر کے نیٹ ورک کو محفوظ کرنا

آپ کی ڈیوائیسز

اگلا قدم یہ جاننا ہے کہ آپ کے نیٹ ورک سے کون سے ڈیوائیسز منسلک ہیں اور اس بات کی تاکید کرنا ہے کہ وہ ڈیوائیسز محفوظ ہیں۔ یہ پہلے آسان ہوا کرتا تھا کیونکہ عام طور پر آپ کی چند ڈیوائیسز ہی منسلک ہوا کرتی تھیں تاہم اب آپ کے گھر کے نیٹ ورک سے تقریباً ہر چیز منسلک ہو سکتی ہے جس میں ٹی ویز، گیمینگ کنسولز، بے بی مانیٹرز، اسپیکرز، آپ کے گھر کا تھرمامیٹر یا شاید آپ کی گاڑی بھی شامل ہے۔ ایک بار آپ اپنے گھر کے نیٹ ورک سے منسلک تمام ڈیوائیسز شناخت کرلیں تو آپ یہ دیکھ کہ حیران ہوں گے کہ آپ کے پاس کتنی ڈیوائیسز ہیں۔ اپنی ڈیوائیسز کو محفوظ رکھنے کا سب سے بہترین طریقہ یہ ہے کہ آپ اس بات کی تاکید کرلیں کہ وہ آپریٹنگ سسٹم کا جدید ترین ورژن چلا رہی ہوں۔ اس بات کی بھی تاکید کر لیں کہ جب بھی ممکن ہو خود کار اپڈیٹ کو فعال کردیں۔ اگر یہ ممکن نہ ہو تو آپ ماہانہ اس کا جائزہ لیں اور اپڈیٹ کریں۔ اس کے علاوہ آپ اس بات کو بھی یقینی بنائیں کہ آپ اپنے انٹرنیٹ سروس پروائیڈر کی ویب سائٹ کا دورہ کرتے رہیں کیونکہ وہ ایسے مفت ٹولز اور سروسز فراہم کرسکتے ہیں جو آپ کے گھر کے نیٹ ورک کو محفوظ رکھنے میں مدد گار ثابت ہوں۔

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:

اوپن ڈی این ایس:
http://www.opendns.org
نورٹن کنیکٹ سیف:
http://dns.norton.com/dnsweb/dnsForHome.do
نیٹ ورک سیکیورٹی اسکینر:
http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx
پاس ورڈ مینیجرز:
http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

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

ترجمہ: شعیب ہاشمی