SANS SECURITY AWARENESS

OUCH! جنوری ۲۰۱۸

تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

- آپ کا وائرلیس نیٹ ورک
- آپ کے آلات
- پاس ورڈز
- بیک اپس

اپنے گھر کے انٹرنیٹ کو محفوظ بنانا

جائزہ

کئی سالوں پہلے اپنے گھر کے انٹرنیٹ کو محفوظ بنانا بہت آسان ہوتا تھا؛ کئی گھروں میں صرف ایک وائرلیس نیٹ ورک اور کئی کمپیوٹرز ہوتے تھے- آج ٹیکنالوجی کہیں زیادہ پیچیدہ ہو گئی ہے اور یہ ہماری زندگیوں کا حصّہ بن چکی ہے، موبائل آلات اور گیمنگ کنسولز سے لے کر گھر کے تھرمو اسٹیٹ اور آپ کے ریفریجریٹر تک ہر چیز اس میں شامل ہے- آپ مندرجہ ذیل چار آسان اقدامات اپنا کر اپنے گھر کے انٹرنیٹ کو محفوظ بنا سکتے ہیں-

مہمان ایڈیٹر

میٹ برومائیلی، انسیڈنٹ ریسپانڈر کے طور پر کام کرتے ہیں اور وہ چھوٹے بڑے ہر طرح کے کسٹمرز کو معلومات کی حفاظت سے متعلق مدد فراہم کرتے ہیں- میٹ SANS میں انسٹرکٹر کی حیثیت سے بھی کام کرتے ہیں جہاں وہ FOR508 ، ایڈوانسڈ ڈیجیٹل فارینزک اینڈ انسیڈنٹ رسپانس کورس پڑھاتے ہیں- آپ میٹ سے @mbromileyDFIR کے ذریعے ٹوئیٹر پر رابطہ کر سکتے ہیں-

آپ کا وائرلیس نیٹ ورک

تقریباً ہر گھر کا نیٹ ورک وائرلیس نیٹ ورک یا وائی-فائی سے شروع ہوتا ہے جس کی بدولت آپ اپنے تمام آلات انٹرنیٹ سے منسلک کر سکتے ہیں- زیادہ تر گھر کے وائرلیس نیٹ ورک کا انتظام انٹرنیٹ راؤٹر یا ایک علیحدہ، مخصوص وائرلیس ایکسیس پوائنٹ کے ذریعے ہوتا ہے- یہ دونوں ایک ہی طرح سے کام کرتے ہیں یعنی وائرلیس سگنلز کو براڈکاسٹ کر کے- آپ کے گھر میں موجود آلات پھر ان سگنلز کے ذریعے انٹرنیٹ سے منسلک ہوتے ہیں- جس کا مطلب ہے کہ اپنے گھر کے نیٹ ورک کی حفاظت کے لیئے اپنے وائرلیس نیٹ ورک کو محفوظ بنانا بہت اہم ہے- ہم حفاظت کے لیئے مندرجہ ذیل اقدامات تجویز کرتے ہیں:

- اپنے انٹرنیٹ راؤٹر یا وائرلیس ایکسیس پوائنٹ، جو بھی آپ کے نیٹ ورک کا منتظم ہے، کے ڈیفالٹ ایڈمنسٹریٹر پاس ورڈ کو تبدیل کر دیں- ایڈمن اکاؤنٹ کے ذریعے آپ اپنے وائرلیس نیٹ ورک میں سیٹنگز کنفیگر کر سکتے ہیں-
- آپ اس بات کو یقینی بنائیں کہ آپ کے وائرلیس نیٹ ورک سے صرف قابل بھروسہ لوگ ہی منسلک ہو سکتے ہیں- آپ مضبوط سکیورٹی کو فعّال کر کے یہ ممکن بنا سکتے ہیں- فالحال سب سے بہترین طریقہ WPA2 کے سکیورٹی کے طریقہ کار کو فعّال کرنا ہے- اس طریقے کو فعّال کرنے سے جب بھی آپ کے گھر کے نیٹ ورک سے کوئی شخص منسلک ہونے کی کوشش کرتا ہے تو اسے پاس ورڈ درکار ہوتا ہے- ایک بار جب وہ منسلک ہو جاتا ہے تو پھر اس کی آن لائن سرگرمیاں انکرپٹڈ ہو جاتی ہیں-
- آپ اس بات کو یقینی بنائیں کہ آپ کے وائرلیس نیٹ ورک کا پاس ورڈ مضبوط ہے اور وہ ایڈمن کے پاس ورڈ سے مختلف ہے- یاد رہے کہ آپ کو ہر آلہ کے لیئے صرف ایک دفعہ پاس ورڈ لکھنا پڑتا ہے کیونکہ یہ پاس ورڈ اس آلہ میں محفوظ ہو جاتا ہے اور اسے یاد رکھتا ہے-
- کئی وائرلیس نیٹ ورکس میں گیسٹ نیٹ ورک کا اختیار موجود ہوتا ہے- اس کے ذریعے مہمان انٹرنیٹ سے منسلک ہو سکتے ہیں لیکن آپ کے گھر کا نیٹ ورک محفوظ رہتا ہے کیونکہ وہ آپ کے گھر کے نیٹ ورک میں موجود آلات سے منسلک نہیں ہو سکتے ہیں- اگر آپ گیسٹ

اپنے گھر کے انٹرنیٹ کو محفوظ بنانا

نیٹ ورک شامل کرتے ہیں تو اس بات کی یقین دہانی کر لیں کہ آپ نے WPA2 فعّال کر دیا ہے اور اس نیٹ ورک کا ایک منفرد پاس ورڈ ہے-

کیا آپ کو لگتا ہے کہ آپ یہ اقدامات نہیں اٹھا سکتے ہیں؟ آپ اس کے بارے میں اپنے انٹرنیٹ سروس پرووائیڈر سے پوچھیں یا ان کی ویب سائٹ دیکھیں، اس دستاویز کو پڑھیں جو آپ کے انٹرنیٹ راؤٹر یا وائرلیس ایکسیس پوائنٹ کے ساتھ آئی ہے یا ان کی ویب سائٹ پر دیکھیں-

آپ ان چار آسان اقدامات کو اپنا کر اپنے گھر کے انٹرنیٹ کو محفوظ بنا سکتے ہیں؛ اپنے وائی فائی نیٹ ورک کو محفوظ بنا کر، خودکار اپڈیٹ کو فعّال کر کے، منفرد پاس فریزز استعمال کر کے اور بیک اپس کو فعّال کر کے-

آپ کے آلات

اگلا قدم یہ جاننا ہے کہ آپ کے گھر کے وائرلیس نیٹ ورک سے کون سے آلات منسلک ہیں اور اس بات کو یقینی بنانا کہ وہ تمام آلات محفوظ ہیں- یہ کرنا اس وقت آسان ہوتا تھا جب آپ کے پاس صرف ایک یا دو کمپیوٹرز ہوا کرتے تھے- تاہم آج تقریباً ہر چیز ہی گھر کے نیٹ ورک سے منسلک ہو سکتی ہے جس میں اسمارٹ فونز، ٹی ویز، گیمنگ کنسولز، بےبی مانیٹرز، اسپیکرز یا آپ کی گاڑی بھی شامل ہے- ایک بار آپ جب اپنے گھر کے نیٹ ورک سے منسلک آلات کی نشاندہی کر لیتے ہیں تو پھر اس بات کو یقینی بنائیں کہ ان میں سے ہر ایک آلہ محفوظ ہے- یہ کرنے کا سب سے بہترین طریقہ یہ ہے کہ آپ ان میں خودکار اپڈیٹس کو جب بھی ممکن ہو فعّال کر دیں- سائبر مجرمان ہمیشہ آلات اور آپریٹنگ سسٹمز میں کمزوریوں کی تلاش میں ہوتے ہیں- خودکار اپڈیٹس کو فعّال کر کے آپ اپنے کمپیوٹر اور آلات میں تازہ ترین سافٹ ویئر چلا سکتے ہیں جس کے بعد اسے ہیک کرنا کسی کے لیئے بھی بہت مشکل ہو جاتا ہے-

پاس ورڈز

اگلا قدم اپنے ہر آلہ اور ہر آن لائن اکاؤنٹ کے لیئے ایک مضبوط اور منفرد پاس ورڈ کا استعمال ہے- یہاں اہم الفاظ مضبوط اور منفرد ہیں- کیا آپ ان پیچیدہ پاس ورڈز سے تنگ آ گئے ہیں جنہیں یاد رکھنا اور لکھنا مشکل ہے؟ ہمارے ساتھ بھی ایسا ہی ہے- اس کا آسان حل پاس فریز یعنی جملے کا استعمال ہے- یہ پاس ورڈ کی ایسی قسم ہے جس میں کئی ایسے الفاظ کا استعمال ہوتا ہے جنہیں یاد رکھنا آسان ہوتا ہے، جیسے کہ «میری کافی کہاں ہے؟» یا «sunshine-doughnuts-happy-lost»- آپ کا پاس فریز جتنا لمبا ہوگا، اتنا ہی مضبوط ہوگا- ایک منفرد پاس ورڈ کا مطلب ہے کہ ہر آلہ اور ہر آن لائن اکاؤنٹ کے لیئے مختلف پاس ورڈ کا استعمال کرنا- اس طرح اگر آپ کا کوئی ایک پاس ورڈ چوری ہو بھی جاتا ہے تو باقی تمام آلات اور اکاؤنٹس محفوظ رہتے ہیں- کیا آپ تمام مضبوط اور منفرد پاس ورڈز یاد نہیں رکھ سکتے ہیں؟ پریشان نہیں ہوں کیونکہ ہم بھی سب یاد نہیں رکھ سکتے ہیں- اس لیئے ہم پاس ورڈ مینیجر کے استعمال کا مشورہ دیتے ہیں جو کہ ایک خاص سکیورٹی کا پروگرام ہے اور آپ کے تمام پاس ورڈز کو محفوظ طریقے سے ایک انکرپٹڈ ورچوئل سیف میں ذخیرہ کرتا ہے-

آخری بات یہ کہ ٹو اسٹیپ ویریفیکیشن جب بھی دستیاب ہو، آپ اسے ضرور فعّال کر دیں خصوصاً اپنے آن لائن اکاؤنٹس کے لیئے- ٹو اسٹیپ ویریفیکیشن کہیں زیادہ مضبوط ہوتی ہے- اس کے لیئے آپ کے پاس ورڈ کے علاوہ ایک دوسرے قدم کی بھی ضرورت ہوتی ہے، جیسے کہ آپ کے اسمارٹ فون پر بھیجا

اپنے گھر کے انٹرنیٹ کو محفوظ بنانا

گیا کوڈ یا آپ کے اسمارٹ فون پر موجود کسی ایپلیکیشن کے ذریعے نکلا ہوا کوڈ- ٹو اسٹیپ ویریفیکیشن اپنی آن لائن حفاظت کا واحد سب سے اہم ترین قدم ہے جسے آپ اٹھا سکتے ہیں اور یہ آپ کی سوچ سے کہیں زیادہ آسان ہے-

بیک اپس

کبھی کبھار ایسا بھی ہوتا ہے کہ آپ جتنا مرضی محتاط ہو جائیں، ہیک ہو سکتے ہیں- اگر ایسا ہے تو آپ کے لیئے اپنی ذاتی معلومات کو ریکوِر کرنے کا واحد طریقہ اسے بیک اپ کے ذریعے ری اسٹور کرنا رہ جاتا ہے- آپ اس بات کو یقینی بنائیں کہ آپ باقاعدگی سے اپنی اہم معلومات کا بیک اپ لے رہے ہیں اور اس بات کو بھی یقینی بنائیں کہ وہ بیک اپ صحیح طرح سے ری اسٹور ہو رہا ہے- زیادہ تر موبائل آلات کلاؤڈ پر خودکار بیک اپ کی سپورٹ فراہم کرتے ہیں- زیادہ تر کمپیوٹرز میں آپ کو بیک اپ سافٹ ویئر یا سروس الگ سے خریدنی پڑتی ہے جس کی قیمت کم ہوتی ہے اور اسے استعمال کرنا آسان ہوتا 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 پوسٹرز اور نیوز لیٹرز ۲۰ سے زائد زبانوں میں ہر ماہ دستیاب ہوتے ہیں 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 یا ہمارے فیس بک پیج https://www.facebook.com/Rewterz کو 'لائک' کریں یا ٹوئیٹر @Rewterz پر فالو کریں۔

وسائل:

پاس فریزز: https://securingthehuman.sans.org/ouch/2017#april2017

پاس ورڈ مینیجر: https://securingthehuman.sans.org/ouch/2017#september2017

ٹو فیکٹر آتھنٹیکیشن: https://securingthehuman.sans.org/ouch/2017#december2017

بیک اپس: https://securingthehuman.sans.org/ouch/2017#august2017

ایڈیٹوریل بورڈ: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley۔

ترجمہ: شعیب ہاشمی