OUCH! اگست ۲۰۱۸

SANS SECURITY AWARENESS

OUCH!

تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

گھر کے اسمارٹ آلات

اسمارٹ ہوم آلات کیا ہیں؟

روایتی طور پر گھر میں چند ہی آلات ہوتے تھے جو انٹرنیٹ سے مُنسلک ہوا کرتے تھے جیسے کہ لیپ ٹاپ، اسمارٹ فون یا گیمنگ کنسول- البتہ آج کافی زیادہ آلات انٹرنیٹ سے مُنسلک ہو رہے ہیں، آپ کے لائٹ بلب اور ٹی وی کے اسپیکرز سے لے کر آپ کے گھر کے دروازے کے تالے، یہاں تک کہ آپ کی گاڑی تک اس میں شامل ہے- عنقریب آپ کے گھر کے تقریباً تمام آلات انٹرنیٹ سے مُنسلک ہو سکیں گے- ان آلات کو اکثر انٹرنیٹ آف تِھنگز (IoT) یا اسمارٹ ہوم ڈیوائسز کے نام سے جانا جاتا ہے- یہ آلات جہاں آپ کو سہولت فراہم کرتے ہیں، وہیں ان کے ساتھ کچھ خطرات بھی لاحق ہیں-

مسئلہ کیا ہے؟

آپ کے گھر کے نیٹ ورک سے جتنے زیادہ آلات مُنسلک ہوں گے اُتنی ہی زیادہ پریشانیاں ہو سکتی ہیں- ہیکرز آپ کے آلات کو اس طرح پروگرام کر سکتے ہیں کہ اُس کے ذریعے وہ دوسروں پر حملہ کر سکیں- وینڈرز آپ کی سرگرمیوں سے متعلق معلومات اکٹھی کر سکتے ہیں یا آپ کے آلات کسی میلویئر کے ذریعے متاثر ہو سکتے ہیں اور آپ کو اس سے لاک آوٹ کر سکتے ہیں- ان آلات کو بنانے والی تنظیموں کے پاس سائبر سکیورٹی کا کوئی تجربہ نہیں ہوتا ہے اور وہ سکیورٹی کو اضافی خرچے کے طور پر دیکھتے ہیں- اس کا نتیجہ یہ ہوتا ہے کہ کافی سارے آلات جو آپ خریدتے ہیں اُن میں سکیورٹی سے متعلق بہت کم خُصوصیات شامل ہوتی ہیں یا سرے سے کوئی بھی خصوصیت شامل نہیں ہوتی ہے- مثال کے طور پر کچھ آلات میں ایسے ڈیفالٹ پاس ورڈز موجود ہوتے ہیں جو کہ بہت زیادہ معروف ہوتے ہیں یا پھر آپ اُنہیں اپڈیٹ یا کنفیگر نہیں کر سکتے ہیں-

میں اپنی حفاظت کیسے کر سکتا ہوں؟

تو آپ کر کیا سکتے ہیں؟ ہم بالکل چاہتے ہیں کہ آپ انٹرنیٹ سے مُنسلک آلات کا فائدہ اٹھائیں لیکن محفوظ طریقے سے- یہ آلات آپ کو ایسی زبردست خصوصیات فراہم کرتے ہیں جن سے آپ کی زندگی آسان ہو جاتی ہے- مزید یہ کہ ٹیکنالوجی جس طرح آگے بڑھتی جا رہی ہے، عنقریب آپ کے پاس اسمارٹ آلات استعمال کرنے کے علاوہ کوئی اور چارہ رہ نہیں جائے گا- اپنی حفاظت کے لیئے مندرجہ ذیل اقدامات اپنائیں:

صرف وہ آلہ انٹرنیٹ سے مُنسلک کریں جس کی آپ کو ضرورت ہے: اپنے آلہ کو محفوظ بنانے کا سب سے آسان طریقہ یہ ہے کہ آپ اسے انٹرنیٹ سے مُنسلک نہ کریں- اگر آپ چاہتے ہیں کہ آپ کا آلہ آن لائن نہ ہو تو آپ اُسے وائی- فائی سے مُنسلک نہ کریں- کیا آپ کے ٹوسٹر کو آپ کے فون پر نوٹیفکیشن بھیجنے کی ضرورت ہے؟

آپ کو معلوم ہونا چاہیئے کہ آپ کا کون سا آلہ انٹرنیٹ سے مُنسلک ہے: آپ کے کون سے آلات گھر کے نیٹ ورک سے مُنسلک ہیں؟ کیا آپ کو پتہ نہیں ہے یا یاد نہیں ہے؟ آپ اپنا وائرلیس نیٹ ورک بند کر دیں اور پھر دیکھیں کہ کون سے آلات کام نہیں کر رہے ہیں- اس سے شاید آپ کو سارے آلات کا پتہ نہیں چل سکے لیکن آپ حیران ہوں گے کہ آپ کتنے آلات کو بُھول گئے ہیں-

آپ اپڈیٹ رہیں: آپ کمپیوٹر اور موبائل آلات کی طرح باقی تمام آلات کو اپڈیٹ اور تازہ ترین ورژن پر رکھیں- اگر آپ کے آلہ میں خودکار اپڈیٹ کا اختیار موجود ہے تو آپ اُسے فعّال کر دیں-

پاس ورڈز: آپ اپنے آلات کے پاس ورڈز کو ایک ایسے منفرد اور مضبوط پاس فریز (جملے) کے ذریعے بنائیں جو کہ صرف آپ کو معلوم ہو- آپ کو شاید یہ پاس ورڈ ایک بار ہی اِن آلات میں ڈالنا ہوگا- کیا آپ تمام پاس فریزز یاد نہیں رکھ سکتے ہیں؟ پریشان نہ ہوں کیونکہ ہم بھی سب کو یاد نہیں رکھ سکتے ہیں- آپ اِن تمام پاس ورڈز کو محفوظ طریقے سے پاس ورڈ مینیجر کے ذریعے ذخیرہ کر سکتے ہیں-

پرائیویسی اختیارات: اگر آپ کا آلہ آپ کو پرائیویسی اختیارات کنفیگر کرنے کی اجازت دیتا ہے تو آپ اُس کے ذریعے معلومات اکٹھی کرنے اور اس کے اشتراک کرنے کی مقدار کو کم کر دیں- یہاں ایک اختیار آپ کے پاس یہ ہے کہ آپ معلومات اشتراک کرنے کی صلاحیت کو صرف غیر فعّال کر دیں-

وینڈر: آپ اپنے آلات کو اس کمپنی کے ذریعے خریدیں جسے آپ جانتے ہیں اور بھروسہ کرتے ہیں- آپ ان مصنوعات کو ڈھونڈیں جو سکیورٹی کی حمایت کرتی ہیں جیسے کہ خودکار اپڈیٹ کو فعّال کرنا، ڈیفالٹ پاس ورڈ کو تبدیل کرنا اور پرائیویسی سیٹنگز میں ترمیم کرنا-

آلات میں ہمیشہ سننے کی صلاحیت: اگر کوئی آلہ آواز کے ذریعے ہدایات لیتا ہے تو اس کا مطلب ہے کہ اس میں ہر وقت سننے کی صلاحیت موجود ہے- مثال کے طور پر الیکسزا اور گُوگل ہوم جیسے آلات آپ کی حسّاس گفتگو سُن سکتے ہیں- آپ اس بات کا خیال اُس وقت رکھیں جب آپ ان آلات کو گھر میں کسی مقام پر رکھنے کا تعیّن کر رہے ہوں اور اُن کی پرائیویسی اختیارات کا بھی جائزہ لیں-

گیسٹ نیٹ ورک: آپ اپنے گھر کے اسمارٹ آلات کو گھر کے بنیادی وائی فائی نیٹ ورک، جسے آپ کمپیوٹرز اور موبائل آلات کے لیئے استعمال کرتے ہیں، کے بجائے ایک علیحدہ «گیسٹ» وائی فائی نیٹ ورک پر رکھنے کے لیئے غور کریں- اس طرح اگر کوئی اسمارٹ آلہ متاثر ہو بھی جاتا ہے تو پھر بھی آپ کے مرکزی نیٹ ورک سے مُنسلک کمپیوٹرز اور موبائل آلات محفوظ رہیں گے-

جدید ٹیکنالوجی سے ڈرنے کی بالکل بھی ضرورت نہیں ہے لیکن اس سے لاحق خطرات کے بارے میں آپ کو پتہ ہونا چاہیئے- اوپر بیان کیئے گئے اقدامات کو اپنا کر آپ ایک بہت محفوظ اسمارٹ ہوم بنا 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-

مہمان مُدیر

رابرٹ ایم لی(@RobertMLee) SANS کے سرٹیفائیڈ انسٹرکٹر اور FOR578 - سائبر تھریٹ انٹیلیجنس اور آئی سی ایس ایکٹو ڈیفینس اینڈ انسیڈینٹ رسپانس کے مصنف بھی ہیں- رابرٹ انڈسٹریل سائبر سکیورٹی کی فرم ڈراگوس کے سی ای او بھی ہیں-

وسائل:

پاس فریزیز: https://www.sans.org/u/GEB

پاس ورڈمینیجرز: https://www.sans.org/u/GEG

اپنے گھر کے نیٹ ورک کو محفوظ بنانا: https://www.sans.org/u/GEL