تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

- سفر سے پہلے کی فہرست
- گمُ/چوری شُدہ آلات
- وائی فائی تک رسائی
- عوامی کمپیوٹرز

سفر کے دوران محفوظ رہنا

جائزہ

ہم چاہتے ہیں کہ آپ ٹیکنالوجی کا استعمال زیادہ سے زیادہ کریں بشمول سفر کے دوران- اس نیوزلیٹر میں ہم اس بات پر نظر ڈالیں گے کہ سفر کے دوران آپ کس طرح انٹرنیٹ سے مُنسلک ہو کر اپنے ٹیکنالوجی آلات استعمال کر سکتے ہیں-

مہمان ایڈیٹر

مارک ولیمز ٹینیسسی کی بُلوکراس بُلوشیلڈ میں انٹرپرائز سکیورٹی آرکیٹیکٹ ہیں- اس کے علاوہ وہ SANS کے انسٹرکٹر اور ISSA چٹّانُوگا چیپٹر کے صدر ہیں- وہ سفر کا کافی وسیع تجربہ رکھتے ہیں اور سفر کے دوران ٹیکنالوجی آلات کو درپیش مسائل سے بخوُبی واقف ہیں-

سفر سے پہلے کی فہرست

گھر یا دفتر میں آپ کا نیٹ ورک محفوظ ہو سکتا ہے لیکن سفر کے دوران آپ کو یہ بات ذہن میں رکھنی چاہیئے کہ آپ جس کسی نیٹ ورک سے بھی مُنسلک ہو رہے ہیں، وہ قابل بھروسہ نہیں ہے- آپ کو نہیں معلوم کہ اس نیٹ ورک میں مزید کون موجود ہے اور کیا کر رہا ہے- آپ مُندرجہ ذیل اقدامات اپنا کر اپنی معلومات کو سفر کے دوران دیرپا تحفّظ فراہم کر سکتے ہیں:

- محفوظ ترین معلومات وہ ہوتی ہیں جو آپ کے پاس نہیں ہوتی- آپ اُن معلومات کی نشاندہی کریں جن کی آپ کو اُن آلات میں ضرورت نہیں ہے جنہیں آپ سفر میں اپنے ساتھ لے جا رہے ہیں اور پھر اُن معلومات کو حذف کر دیں- اس طرح ان آلات کے گُم ہونے، چوری ہونے یا کسٹم حُکّام یا بارڈر سکیورٹی کے اُسے ضبط کرنے کی صورت میں زیادہ گہرے اثرات مُرتّب نہیں ہوتے ہیں- اگر آپ کا سفر کام سے متعلق ہے تو آپ اپنے سُپروائزر سے پوچھیں کہ آیا آپ کی تنظیم سفر کے لیئے مخصُوص آلات فراہم کرتی ہے-
- آپ اپنے موبائل آلات اور/یا لیپ ٹاپ کو مضبوط پاس ورڈ کے ذریعے محفوُظ کریں- اس طرح اگر وہ چوری یا گم بھی ہو جاتے ہیں تو لوگ آپ کی معلومات تک رسائی حاصل نہیں کر سکتے ہیں- اس کے علاوہ آپ اپنے موبائل آلات اور لیپ ٹاپس میں فُل ڈسک انکرپشن انسٹال یا فعّال کر دیں- زیادہ تر موبائل آلات میں یہ اسکرین لاک کرنے کے ساتھ ہی خودکار طور پر فعّال ہو جاتا ہے-
- آپ اپنے آلہ میں ایسے سافٹ ویئر انسٹال یا فعّال کر دیں جن کو دور بیٹھ کر ٹریک کیا جا سکے اور چوری یا گُم ہونے کی صورت میں آپ دور سے بیٹھ کر وائپ کر سکیں-
- آپ سفر پر نکلنے سے پہلے اپنے آلات، ایپلیکیشنز اور اینٹی-وائرس سافٹ ویئر کو جدید ترین ورژن سے اپڈیٹ کر لیں- کئی حملے اپنی توجّہ سسٹمز کے سافٹ ویئر کے فرسودہ ہونے پر مرکوز کرتے ہیں-
- آپ اپنے آلات کا مُکمّل بیک اپ کریں- اس طرح اگر سفر کے دوران ان آلات میں کچھ ہو بھی جاتا ہے تو آپ کے پاس اصل معلومات محفوظ جگہ پر موجود ہوتی ہیں-
- بیرونِ ملک سفر کرتے وقت آپ اپنے موبائل سروس پرووائیڈر سے اپنے سروس پلان کی تفصیلات طلب کریں- اکثر سروس پرووائیڈرز بیرون ملک

سفر کے دوران محفوظ رہنا

ڈیٹا استعمال کرنے کے بہت زیادہ پیسے کاٹتے ہیں اس لیئے ہو سکتا ہے کہ سفر کے دوران آپ کو اپنے موبائل فون کی ڈیٹا کی صلاحیت کو غیر فعال کرنا پڑے یا بیرونِ ملک سفر کے لیئے آپ کو مقامی سِم خریدنی پڑے-

سفر کے دوران محفوظ رہنے کے لیئے آپ اپنے آلات کو گھر سے نکلنے سے پہلے محفوظ بنائیں، اُنہیں مادّی طور پر محفوظ بنائیں اور تمام آن لائن سرگرمیوں کو انکرپٹ کریں-

گُم/چوری شُدہ آلات

جب آپ ایک بار سفر شُروع کر دیں تو اپنے آلات کی مادّی حفاظت کو یقینی بنائیں- مثال کے طور پر آپ اپنے آلات کو ایسی جگہ پر گاڑی میں چھوڑ کر نہ جائیں جہاں لوگوں کی نظریں با آسانی پڑ جائیں کیونکہ مجرمان آپ کی گاڑی کا صرف شیشہ توڑ کر کوئی بھی قیمتی شے لے جا سکتے ہیں- جُرم بہرحال ایک خطرہ ہے لیکن ویریزون کی حالیہ تحقیق کےمطابق لوگوں کے آلات چوری ہونے سے سو گنا زیادہ خطرہ اُن کے کھونے کا ہے- اس کا مطلب ہے کہ آپ کو سفر کے دوران بار بار اس بات کی تصدیق کرنی پڑے گی کہ آپ کے آلات آپ کے پاس موجود ہیں جیسے کہ ائیرپورٹ پر سکیورٹی سے گُزرتے ہوئے، ٹیکسی یا ریسٹوُرینٹ سے نکلتے ہوئے، ہوٹل کے کمرے سے چیک آوٹ کرتے ہوئے یا ہوائی جہاز سے اُترنے سے پہلے نشست کی پچھلی جیب دیکھنا نہ بھُولیں-

وائی فائی تک رسائی

سفر کے دوران انٹرنیٹ استعمال کرنے کا مطلب ہے کہ عوامی وائی فائی ایکسیس پوائنٹس استعمال کرنا جیسے کہ ہوٹل، مقامی کافی کی دکان یا ہوائی اڈّے پر- عوامی وائی فائی کے دو مسائل: آپ کو یہ کبھی نہیں پتہ ہوتا ہے کہ یہ کس نے لگائے ہیں اور یہ بھی نہیں پتہ ہوتا ہے کہ ان سے کون مُنسلک ہے- اُنہیں ناقابلِ اعتبار سمجھنا چاہیئے- درحقیقت یہی وہ وجہ ہے جس کے لیئے آپ کو سفر شُروع کرنے سے پہلے اپنے آلات کی حفاظت کے لیئے تمام اقدامات اٹھانے پڑتے ہیں- مزید یہ کہ وائی فائی ریڈیو وےوز کا استعمال کرتا ہے جس کا مطلب یہ ہے کہ جسمانی طور پر آپ سے قریب کوئی بھی شخص آپ کی مواصلات کو مُمکنہ طور پر دیکھ سکتا ہے- اِن وجوہات کی بناء پر اگر آپ عوامی وائی فائی کا استعمال کرتے بھی ہیں تو آپ کو اس بات کو یقینی بنانا ہے کہ آپ کی تمام آن لائن سرگرمیاں اِنکرپٹڈ ہیں- مثال کے طور پر براؤزر کے ذریعے انٹرنیٹ سے منسلک ہوتے وقت آپ اِس بات کو یقینی بنائیں کہ جِن ویب سائٹس کا آپ دورہ کر رہے ہیں وہ انکرپٹڈ ہیں- آپ اس کی تصدیق اپنے ایڈریس بار یا یو-آر-ایل بار میں پیڈ لاک کی بند تصویر یا/اور ‹HTTPS://› کے ذریعے کر سکتے ہیں- مزید یہ کہ ہو سکتا ہے کہ آپ کے پاس وی-پی-این (ورچوئل پرائیویٹ نیٹ ورک) موجود ہو جو کہ اگر فعّال ہو تو آپ کی تمام آن لائن سرگرمیوں کو انکرپٹ کر سکتا ہے- ہو سکتا ہے کہ یہ آپ کو اپنے دفتر کی جانب سے ملا ہو یا آپ اِن وی-پی-این صلاحیات کو ذاتی استعمال کے لیئے خرید بھی سکتے ہیں- اگر آپ کو لگتا ہے کہ آپ کسی بھی وائی فائی پر بھروسہ نہیں کر سکتے ہیں تو آپ اپنے اِسمارٹ فون کے ذریعے ٹیتھرنگ کرنے پر غور کریں- انتباہ: جیسا کہ ہم نے پہلے بتایا تھا کہ بیرون ملک سفر کرتے وقت یہ کافی مہنگا پڑ سکتا ہے اس لیئے آپ اس کے بارے میں مزید تفصیلات پہلے اپنے سروس پرووائیڈر سے حاصل کریں-

سفر کے دوران محفوظ رہنا

عوامی وسائل

آپ عوامی کمپیوٹرز، جیسے کہ ہوٹل کی لابی یا سائبر کیفے، کا استعمال حسّاس معلومات تک رسائی یا اکاؤنٹس میں لاگ-اِن ہونے کے لیۓ نہیں کریں- آپ کو اس بات کا اندازہ نہیں ہے کہ آپ سے پہلے اِسے کون استعمال کر چکا ہے اور ہو سکتا ہے کہ اس نے وہ عوامی کمپیوٹر غلطی سے یا جان بوجھ کر متاثر کر دیا ہو- جب بھی مُمکن ہو، آپ صرف اُن آلات کا استعمال کریں جن پر آپ کو اختیار حاصل ہو اور آپ اُن پر بھروسہ کرتے ہوں- عوامی کمپیوٹرز کا سب سے بہترین استعمال عوامی معلومات تک رسائی حاصل کرنا ہے جیسے کہ موسم کا حال جاننا یا خبریں سُننا- اپنے کسی بھی اکاؤنٹ، جیسے کہ گوُگل اکاؤنٹ، میں سائن اِن کرنا ہیکرز کو دعوت دینے کے مُترادف ہے جو کہ ہو سکتا ہے کہ آپ کو پہلے سے ہی دیکھ 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 securingthehuman.sans.org/ouch/archives (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 فریز:	https://securingthehuman.sans.org/ouch/2015#april2015
بیک اپس:	https://securingthehuman.sans.org/ouch/2015#august2015
میلویئر:	https://securingthehuman.sans.org/ouch/2016#march2016
انکرپشن:	https://securingthehuman.sans.org/ouch/2016#june2016
OUCH نیوز لیٹر آرکائیوز/ ترجُمہ:	https://securingthehuman.sans.org/ouch/archives

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

ترجمہ: شعیب ہاشمی