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

OUCH!

اس شمارے میں شامل ہے:

- جائزہ
- سفر سے پیشگی فہرست
- گم / چوری شدہ آلات
- وائی فائی تک رسائی
- عوامی کمپیوٹرز

سفر کے دوران محفوظ رہنا

جائزہ

اس نیوز لیٹر کے شمارے میں ہم اس بات پر نظر ڈالیں گے کہ آپ سفر کے دوران کس طرح محفوظ طریقے سے انٹرنیٹ کا استعمال کرسکتے ہیں۔

سفر سے پیشگی فہرست

ہوسکتا ہے کہ آپ کے گھر اور دفتر کا نیٹ ورک محفوظ ہو لیکن سفر کرتے وقت آپ ہمیشہ یہ سمجھیں کہ آپ جس نیٹ ورک سے بھی منسلک ہورہے ہیں وہ ناقابلِ بھروسہ ہے- آپ کو یہ معلوم نہیں ہوتا ہے کہ اُس نیٹ ورک سے کون منسلک ہے اور اُس سے کس قسم کے خطرات لاحق ہیں۔ آپ سفر سے ایک یا دو ہفتے پہلے چند آسان اقدامات کو اپنا کر اپنی معلومات کو سفر کے دوران دیرپا تحفظ فراہم کرسکتے۔

- آپ سفر میں ساتھ لے جانے والے آلہ پر اُن معلومات کی نشاندہی کریں جن کی آپ کو ضرورت نہیں ہے اور پھر اُن غیر ضروری معلومات کو اُس میں سے نکال دیں- اگر آپ کے آلات گم، چوری یا کسٹمز یا سرحدی سلامتی کے عملے کے ذریعے ضبط ہوجاتے ہیں تو اس طریقے کو اپنانے سے نمایاں طور پر اس واقعہ کا اثر کم پڑتا ہے۔ اگر آپ کا سفر آپ کے دفتر کے کام سے متعلق ہے تو آپ اپنے سپروائزر سے پوچھیں کہ آیا آپ کی تنظیم سفر کے دوران صرف کام کے لیے مخصوص کوئی متبادل آلات فراہم کرتی ہے یا نہیں۔
- بین الاقوامی سفر کے لیے آپ اُس ملک میں استعمال ہونے والے پاورکنیکٹرز کی معلومات حاصل کرلیں کیونکہ آپ کو اپنے آلات کو چارج کرنے کے لیے اڈیپٹر کی ضرورت پڑسکتی ہے- اس کے علاوہ آپ اپنے موبائل سروس پرووائڈر سے اپنے فون کے سروس پلان کی جانچ کریں- بعض دفعہ سروس پرووائڈر بین الاقوامی ڈیٹا کے استعمال پر زیادہ پیسے کاٹتے ہیں- آپ کو چاہیئے کہ آپ اپنے موبائل فون کے ڈیٹا کی صلاحیت کو غیر فعال کردیں یا اپنے سروس پلان کو بین الاقوامی سفر کے مطابق تبدیل کردیں۔
- آپ اپنے آلات میں ایسا سافٹ ویئر انسٹال کریں جس کے ذریعے آپ دوُر رہ کر بھی اُس کی نگرانی کرسکیں اور اگر وہ گم یا چوری ہوجائیں تو اسے وائپ کرسکیں۔ کئی موبائل آلات میں یہ خصوصیات پہلے سے موجود ہوتی ہیں، آپ کو صرف اُن کو فعال کرنا ہوتا ہے (یاد رہے کہ اس کے لیئے انٹرنیٹ کی ضرورت ہوتی ہے)۔

سفر سے ایک یا دو دن قبل:

- اپنے آلات، ایپلیکیشنز اور اینٹی وائرس سافٹ ویئر کو اپڈیٹ کرلیں تاکہ آپ کے پاس جدید ترین ورژن آجائے۔
- اپنے آلہ میں موجود تمام سکیورٹی سیٹنگز کو فعال کردیں جیسے کہ فائروالز۔

مہمان ایڈیٹر

اسٹیوآرم آسٹرانگ "لاجیکلی سکیور" میں 'سائبرسی پی آر' کے ٹیکنیکل ڈائریکٹر، SANSکے سند یافتہ انسٹرکٹر اور کورس کے سابقہ مصنف رہ چکے ہیں- وہ ٹوئیٹر پر@Nebulator اور گوگل پلس پر +SteveArmstrongSecurity کے نام سے فعال ہیں۔

سفر کے دوران محفوظ رہنا

سفر کے دوران محفوظ رہنے کا سب سے اہم طریقہ یہ ہے کہ آپ گھر سے نکلنے سے پہلے اپنے آلات کو محفوظ بنادیں- آپ اُس آلہ کو بذات خود محفوظ کریں اور ہر وقت اُس پر نظر رکھیں اور تمام آن لائن سرگرمیوں کو انکرپٹ کریں۔

- اپنے تمام موبائل آلات کو مضبوط پاس ورڈ یا پاس کوڈ کے ذریعے بند کردیں- اس طرح اگر آپ کا آلہ گم یا چوری ہوجاتا ہے تو لوگ آپ کی معلومات تک رسائی حاصل نہیں کرسکیں گے۔
- اپنے تمام موبائل آلات کو انکرپٹ کردیں- اس طرح اگر کوئی آلہ گم یا چوری ہوجاتا ہے تو ان معلومات تک کوئی بھی رسائی حاصل نہیں کرسکتا ہے- کچھ آلات، جیسے کہ آئی فون میں، اگر آپ پاس ورڈ یا پاس کوڈ لگاتے ہیں تو انکرپشن خودکار طور پر فعال ہوجاتی ہے۔
- اپنے تمام آلات کا مکمل بیک اپ لے لیں- اس طرح اگر سفر کے دوران اُن آلات کو کچھ ہوبھی جاتا ہے تو آپ کے پاس تمام معلومات محفوظ مقام پر موجود ہوتی ہیں۔

گمشدہ یا چوری شدہ آلات

جب آپ سفر شروع کریں تو اپنے آلات کے تحفظ کو یقینی بنائیں- مثال کے طور پر اپنے آلات کو کبھی بھی گاڑی میں ایسی جگہ پر نہ چھوڑیں جہاں لوگ آسانی سے اُسے دیکھ سکیں کیونکہ مجرمان باآسانی آپ کی گاڑی کے شیشے توڑ کر کسی بھی قیمتی چیز کو چوُرا سکتے ہیں۔ ایک طریقہ کیبل لاک کا استعمال ہے تاکہ آپ اپنے آلات، جیسے کہ لیپ ٹاپ، کو لاک کرسکیں جب آپ اُنہیں چھوڑ کر جارہے ہوں- جرم، یقینی طور پر ایک خدشہ ہے لیکن ایک چیز جس کا شاید آپ کو ادراک نہ ہو وہ یہ ہے کہ آپ کے آلہ کا گُم ہونے سے زیادہ، چوری ہونے کا امکان کہیں زیادہ ہے۔ ویریزون کے دس سالہ مطالعے کے مطابق لوگوں کے آلہ کا چوری ہونے سے زیادہ گم ہونے کے امکانات 15%زیادہ ہیں- اس کا مطلب یہ ہے کہ سفر کے دوران آپ بار بار اپنے آلات کو دیکھتے رہیں کہ وہ آپ کے پاس ہی ہیں، جیسا کہ ایئرپورٹ پر سکیورٹی کلیئرنس کے بعد، ٹیکسی یا ریسٹورینٹ سے نکلتے وقت، ہوٹل کے کمرے سے چیک آؤٹ ہوتے وقت یا جہاز سے اُتر نے سے پہلے۔

وائی فائی تک رسائی

سفر کے دوران انٹرنیٹ استعمال کرنے کا مطلب ہے کہ اکثر عوامی وائی فائی ایکسس پوائنٹ کا استعمال کرنا، جیسے کہ ہوٹل میں، مقامی کافی کی دُوکان میں یا ایئرپورٹ میں- عوامی وائی فائی ایکسس پوائنٹس کے ساتھ مسئلہ یہ ہے کہ آپ کو نہ صرف یہ معلوم نہیں ہوتا ہے کہ اُسے کس نے لگایا ہے بلکہ آپ کو یہ بھی معلوم نہیں ہوتا ہے کہ اُس سے کون کون منسلک ہے- اس لیئے اُنہیں ناقابلِ بھروسہ سمجھنا چاہیئے، درحقیقت یہ وہی وجہ ہے جس کے لیئے آپ نے سفر پر نکلنے سے پہلے اپنے آلات کی حفاظت کے لیئے اقدامات اٹھائے تھے- اس کے علاوہ یہ کہ وائی فائی، آپ کے آلہ اور وائرلیس ایکسس پوائنٹ کے درمیان مواصلات کے لیئے ریڈیو ویوز کا استعمال کرتا ہے- اس کا مطلب ہے کہ جسمانی طور پر آپ کے نزدیک کوئی بھی شخص ممکنہ طور پر آپ کی مواصلات کو پڑھ سکتا ہے اور اُس پر نظر رکھ سکتا ہے۔

اس لیئے اگر آپ عوامی وائی فائی کا استعمال کرتے ہیں تو اس بات کی تاکید کرلیں کہ آپ کی تمام آن لائن سرگرمی انکرپٹڈ ہے- مثال کے طور پر اگر آپ براؤزر کے ذریعے انٹرنیٹ سے منسلک ہوتے ہیں تو آپ اس بات کی تاکید کرلیں کہ جس ویب سائٹ پر آپ جارہے ہیں وہ انکرپٹڈ ہے (اُس ویب سائٹ کے URLمیں ‹https://›ہوگا اور ایک بند تالے کی تصویر ہوگی) اس کے علاوہ یہ کہ آپ کے پاس VPN(Virtual Private Network)

سفر کے دوران محفوظ رہنا

اکاؤنٹ ہوسکتا ہے جو آپ کی تمام آن لائن سرگرمیوں کو انکرپٹ کردے گا- یہ اکاؤنٹ آپ کو اپنے دفتر کے ذریعے مل سکتا ہے یا آپ اسے ذاتی استعمال کے لیئے خرید سکتے ہیں- اگر آپ کو لگتا ہے کہ آپ کسی وائی فائی ایکسس پوائنٹ پر بھروسہ نہیں کرسکتے ہیں تو آپ اپنے اسمارٹ فون سے ٹیتھرنگ کرنے کے بارے میں غور کریں (انتباہ : جیسے کہ ہم نے پہلے بیان کیا ہے کہ یہ طریقہ بین الاقوامی سفر کے لیئے مہنگا ثابت ہوسکتا ہے اس لیئے آپ اپنے سروس پرووائڈر سے اس کے بارے میں جانچ پڑتال کرلیں)۔

عوامی وسائل

آپ عوامی کمپیوٹرز، جیسے کہ ہوٹل کی لابیز، لائبریریز یا سائبر کیفے میں موجود کمپیوٹرز کا استعمال نہیں کریں۔ آپ کو اندازہ نہیں ہے کہ یہ کمپیوٹر آپ سے پہلے کس نے استعمال کیا ہے، ہو سکتا ہے کہ اُنہوں نے غلطی سے یا جان بوجھ کر اُس عوامی کمپیوٹر کو متاثرکر دیا ہو۔ جب بھی ممکن ہو، صرف وہی آلات استعمال کریں جن کا اختیار آپ کے پاس ہو اور آپ اُس پر کسی بھی آن لائن سرگرمی کے لیئے بھروسہ کرتے ہوں۔ اگر آپ کو عوامی کمپیوٹر استعمال کرنے ضرورت پڑ جائے تو آپ کسی بھی ایسی سروس کا استعمال نہیں کریں جو آپ کو لاگ ان یا پاس ورڈ لکھنے کا کہے۔

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 ورڈز:	http://www.securingthehuman.org/ouch/2013#may2013
ٹُو اسٹیپ ویریفیکیشن:	http://www.securingthehuman.org/ouch/2013#august2013
انکرپشن:	http://www.securingthehuman.org/ouch/2014#august2014
اپنے نئے ٹیبلٹ کو محفوظ کرنا:	http://www.securingthehuman.org/ouch/2013#december2013
ویریزون ڈی بی آئی آر 2014:	http://www.verizonenterprise.com/DBIR/2014/

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

ترجمہ: شعیب ہاشمی