عوامی Wi-Fi کو محفوظ طریقے سے استعمال کرنے کے لئے تجاویز

خراب اداکار آپ کا آنلائن فائدہ اٹھا سکتے ہیں۔ اگر آپ کو عوامی Wi-Fi استعمال کرنے کی ضرورت ہے تو اس پر غور کرنے کے لئے کچھ تجاویز کے لئے ذیل میں پڑھیں۔

کورونا وائرس کے پھیلنے اور کاروبار اور لائبریریوں کی بندش کے جواب میں، ہم میں سے بہت سے لوگ آنلائن زیادہ وقت گزار رہے ہیں۔ اس کے نتیجے میں،ہمیں انٹرنیٹ سے رابطہ قائم کرنے کے لئے عوامی Wi-Fi کے استعمال کی ضرورت پڑسکتی ہے۔ اگر آپ خود کو عوامی Wi-Fi کو استعمال کرنے کی ضرورت محسوس کرتے ہیں تو، برائے مہربانی اپنے اعداد و شمار کی حفاظت میں مدد کے لئے ریاست کے چیف پرائیویسی آفیسر کی درج ذیل سفارشات پر غور کریں:

1. تصدیق کریں کہ آپ کے پاس درست نیٹ ورک ہے۔

یقینی بنائیں کہ آپ صحیح نیٹ ورک سے مربوط ہو رہے ہیں۔ برے اداکار ایسے نیٹ ورک تیار کرسکتے ہیں جو ان کے نام کی بنیاد پر بے ضرر دکھتے ہیں لیکن در حقیقت آپ کی انٹرنیٹ سرفنگ دیکھنے کے لیے نیٹ ورک کے سیٹ اپ سے مربوط کرنے کے لئے آپ کو ہدایت دے رہے ہیں۔ اس کا مطلب ہے کہ اگر آپ ویب سائٹس میں لاگ ان کی اسناد یا پاسورڈز درج کرتے ہیں تو، ہیکر آپ کی معلومات چوری کرنے کے قابل ہو جائے گا۔ اس کے خلاف حفاظت کے لئے،بہت احتیاط سے نیٹ ورک کا نام پڑھیں اور اگر ممکن ہو تو،کسی ملازم سے پوچھیں یا نیٹ ورک کی قانونیت کو یقینی بنانے کے لئے کاروباری اشارے چیک کریں۔

مشہور نیٹ ورکس،جیسے واقف کافی چینوں کی طرح،ممکنہ طور پر کم مشکوک ہے کیونکہ کمپنی اپنے کاروبار کے ساتھ اس نیٹ ورک کو بطور سروس چلارہی ہے۔ جانے پہچانے نیٹ ورکس عام طور پر بے تکے مفتWi-Fiنیٹ ورکس سے زیادہ محفوظ ہوتے ہیں جو آپ کے فون پر عوامی جگہ پر نظر آتے ہیں۔

2. خودکار رابطے کو بند کریں۔

بہت سارے آلات(اسمارٹ فونز،لیپ ٹاپس اور ٹیبلٹس)میں خودکار مربوط ہونے کی ترتیبات ہوتی ہیں۔ یہ ترتیبات آپ کے آلات کو قریب کے نیٹ ورکس کے ساتھ آسانی سے مربوط ہونے کی اجازت دیتی ہیں۔ قابل بھروسہ نیٹ ورکس کے ساتھ تو یہ ٹھیک ہے،لیکن یہ آپ کے آلات کو ایسے نیٹ ورکس سے بھی مربوط کر سکتا ہے جو نا محفوظ ہوسکتے ہیں۔ آپ اپنے آلے کی ترتیبات کے ذریعے سے اس خصوصیت کو غیر فعال کرسکتے ہیں۔ ان ترتیبات کو بند رکھیں،خاص طور پر جب آپ اجنبی جگہوں پر سفر کررہے ہوں۔ اضافی پیش بندی کے طور پر،آپ عوامی Wi-Fi کے استعمال کے بعدنیٹ ورک بھولکو چیک کرسکتے ہیں۔

عوامی جگہوں پر رہتے ہوئے آپ کو اپنے Bluetooth کی بھی نگرانی کرنی چاہئے۔ Bluetooth رابطہ مختلف آلات کو ایک دوسرے کے ساتھ برابطہ کرنے کی اجازت دیتا ہے اور ایک ہیکر آپ کے آلات تک پہنچ حاصل کرنے کے لئے کھلے Bluetooth سگنل تلاش کرسکتا ہے۔ جب آپ کسی احنبی جگہ ہوں تو اپنے فون اور دیگر آلات پر اس ضابطے کو بند رکھیں۔

3. فائل کی تقسیم بند کردیں۔

عوامیWi-Fiپر ہوتے وقت فائل کی تقسیم کے اختیار کو بند کرنا یقینی بنائیں۔ آپ اپنے آپریٹنگ سسٹم کے حساب سےسسٹم کی ترجیحات یاکنٹرول پینلسے فائل کی تقسیم کو بند کرسکتے ہیں۔ AirDropفائل کی تقسیم کی خصوصیت کی ایک مثال ہے جسے آپ بند کرنا چاہیں گے۔ کچھ آپریٹنگ سسٹم جیسے Windows/PCپہلی بار کسی نئے عوامی نیٹ ورک سے مربوط ہونے پر "عوامی" اختیار کا انتخاب کرکے آپ کے لئے فائل کی تقسیم کو بند کردیں گے۔

فائل کی تقسیم بند کرنے کے اقدامات

ایک PC پر:

1. نیٹ ورک اور شیئرنگ سینٹر پر جائیں۔
2. پھر اعلی درجے کی شیئرنگ کی ترتیبات کو تبدیل کریں کریں۔
3. فائل اور پرنٹر کی تقسیم کو بند کریں۔

Macs کے لئے:

1. سسٹم کی ترجیحات۔ پر جائیں۔
2. شیئرنگ کا انتخاب کریں۔
3. ہر چیز کونا چنیدہ کریں۔
4. فائنڈر میں اگلا،AirDrop پر کلک کریں اور مجھے ڈھونڈنے کی اجازت دیں: کوئی بھی نہیں کو منتخب کریں۔

iOS کے لئے،صرف کنٹرول سنٹر میںAirDrop تلاش کریں اور اسے بند کریں۔

4. VPN کا استعمال کریں۔

اپنے آلےپر VPN (Virtual Private Network) انسٹال کرنے پر غور کریں۔ VPN عوامی Wi-Fi ڈیجیٹل رازداری کے لئے سب سے زیادہ محفوظ اختیار ہے۔ یہ آپ کے ڈیٹا سے گزر کے اس کوانکرپٹ کرتا ہے اورایک حفاظتیسرنگ کے طور پر کام کرتا ہے تاکہ آپ کا ڈیٹا جب کسی نیٹ ورک سے گزرے تو نظر نہ آئے۔

5. FBI کی خفیہ ویب سائٹوں کے بارے میں انتباہ - HTTPS۔

FBI نے"https" ایڈریس سے شروع والی ویب سائٹوں کے بارے میں متنبہ کیا ہے۔ "https" کی موجودگی اور لاک آئیکن کو اس بات کی نشاندہی سمجھا جاتا ہے کہ ویب ٹریفک کی خفیہ کاری کی گئی ہے اور یہ کہ مہمان محفوظ طریقے سے ڈیٹا کی تقسیم کرسکتے ہیں۔ تاہم،سائبر مجرم اب لوگوں کے بھروسے کے زریعے لالچ دیکر ان کا رجہان ایسی بد خوانی والی ویب سائٹوں کی طرف راغب کررہے ہیں جوhttps کو شامل کرتی ہیں اور بظاہر محفوظ نظر آتی ہیں جب کہ وہ نہیں ہوتیں۔

FBI کی سفارشات:

- کسی بھی ای میل کے صرف نام پر بھروسہ نہ کریں:ای میل کے اجزا کے ارادے پر سوال کریں۔
- اگر آپ کو کوئی مشکوک ای میل کسی جان پہچان والے رابطے کے لنک سے موصول ہو تو،اسے کال یا ای میل کرکے پیغام کے جائز ہونے کی تصدیق کریں۔ کسی مشکوک ای میل کا فوراً جواب نہ دیں۔
- کسی لنک میں غلط ڈومینز یا غلط ہجے کی جانچ پڑتال کریں (مثال کے طور پر،اگر کوئی پتہ ".gov" میں ختم ہونا چاہئے تو اس کی بجائے ".com" میں ختم ہوتا ہو۔)
- کسی بھی ویب سائٹ پر بھروسہ نہ کریں کیونکہ اس میں براؤزر ایڈریس بار میں ایک لاک آئیکن یا "https" ہے۔

6. حساس معلومات تک رسائی کی تجویز نہیں دی جاتی۔

یہاں تک کہ اگر آپ کے پاس VPN ہے پھر بھی ذاتی بینک اکاؤنٹس یا اسی طرح کے حساس ذاتی ڈیٹا جیسے سوشل سیکیورٹی نمبر تک رسائی کسی غیر محفوظ پبلک نیٹ ورکس پر حاصل کرنے کی تجویز نہیں دی جاتی ہے۔ یہاں تک کہ عوامی محفوظ نیٹ ورک بھی خطرناک ہوسکتے ہیں۔ اگر آپ کو عوامیWi-Fiپر ان اکاؤنٹس تک رسائی حاصل کرنا ضروری ہے تو اپنے بہترین اندازےکا استعمال کریں۔ مالی معاملات کے لیے،اپنے اسمارٹ فون کے ہاٹ اسپاٹ فنکشن کا استعمال بہتر ہوسکتا ہے۔

7. محفوظ بمقابلہ غیر محفوظ

بنیادی طور پر عوامیWi-Fi نیٹ ورک کی دو اقسام ہیں:محفوظ اور غیر محفوظ۔

جب بھی ممکن ہو محفوظ عوامی نیٹ ورکس سے مربوط ہوں۔ ایک غیر محفوظ نیٹ ورک سے بنا کسی قسم کی سیکیورٹی کی خاصیت جیسے کے پاس ورڈ یا لاگ ان کے مربوط ہوا جاسکتا ہے۔ ایک محفوظ نیٹ ورک عام طور پر استعمال کرنے والے کو شرائط و ضوابط سے متّفق ہونے،اکاؤنٹ رجسٹر کرنےیا نیٹ ورک سے مربوط ہونے سے پہلے پاس ورڈ ٹائپ کرنے کی ضرورت ہوتی ہے۔

8. اپنی فائر وال کو فعال رکھیں۔

اگر آپ لیپ ٹاپ استعمال کررہے ہیں تو،عوامیWi-Fi پر اپنی فائر وال کو فعال رکھیں۔ فائر وال ایک رکاوٹ کا کام کرتا ہے جو آپ کے آلے کو میلویئر کے خطرات سے بچاتا ہے۔ پوپ اپس اور اطلاعات کی وجہ سے استعمال کرنے والے ونڈوز فائر وال کو غیر فعال کرتے ہیں اور پھر اس کے بارے میں بھول جاتے ہیں۔ اگر آپ اسے کسیPCپر دوبارہ شروع کرنا چاہتے ہیں تو پھرکنٹرول پینل، ، نظام اور حفاظت پر جائیں اور "Windows" فائر وال کا انتخاب کریں۔ اگر آپ Mac استعمال کرتے ہیں تو، سسٹم کی ترجیحات ،پھرسیکیورٹی اور رازداری پر جائیں،پھر اس خاصیت کو فعال کرنے کے لئے "فائر وال" ٹیب پر جائیں۔

9. اینٹی وائرس سافٹ ویئر کا استعمال کریں۔

اپنے لیپ ٹاپ پر اینٹی وائرس پروگرام کا نیاترجمہ انسٹال کرنا بھی یقینی بنائیں۔ اینٹی وائرس پروگرام سے عوامی Wi-Fi کا استعمال کرتے ہوئے آپ کی مالویئر سےحفاظت میں مدد مل سکتی ہے جو مشترکہ نیٹ ورک کا استعمال کرتے ہوئے آپ کے سسٹم میں داخل ہوسکتے ہیں۔ اگر آپ کے آلہ پر جانے پہچانے وائرس ڈالے گئے ہیں یا اگرکوئی مشکوک سرگرمی،حملہ یا مالویئر آپ کے سسٹم میں گھس گیا ہے تو ایک انتباہ آپ کو خبردارکرے گا۔

10. دو عنصر یا کثیر عنصر تصدیق کا استعمال کریں۔

اپنی ذاتی معلوماتی ویب سائٹوں میں لاگ ان کرتے وقت کثیر عنصر تصدیق (MFA) کا استعمال کریں۔ اس کا مطلب ہے کہ آپ کے پاس دوسرا تصدیقی کوڈ ہے (آپ کے فون پر ٹیکسٹ موجود ہے یا کسی ایپ نے دیا ہے یا مادی کلید کے ذریعے فراہم کردہ ہے)جو آپ کو مزید محفوظ رکھتا ہے۔ لہذا یہاں تک کہ اگر کسی ہیکر کو آپ کا استعمال ہونے والا نام اور پاس ورڈ مل بھی جاتا ہے،تو وہ تصدیقی کوڈ کے بنا آپ کے اکاونٹس تک نہیں پہنچ سکتا ہے۔

11. اپنے ذاتی آلات کی پیش رفت کرتے رہیں۔

اپنے لیپ ٹاپ،ٹیبلیٹ یا اسمارٹ فون کو کسی عوامی جگہ یا گاڑی میں نظر انداز مت چھوڑیں۔ حتّی کہ اگر آپ کسی Wi-Fi نیٹ ورک پر احتیاطی تدابیر اختیار کر رہے ہیں تو،وہ بھی کسی کو آپ کی ملکیت حاصل کرنے یا آپ کی معلومات میں تانک جھانک سے نہیں روکے گا۔ اپنے آس پاس کے بارے میں محطاط اور اپنے اردگرد کے لوگوں کے بارے میں حساس رہیں۔

12. دیگرحفاظتی آن لائن تجاویز۔

آن لائن محفوظ رہنےکی کچھ تجاویز یہ ہیں،خاص طور پر اگر آپ عوامی Wi-Fi کنیکشن استعمال کررہے ہیں:

- ٹھوس پاس ورڈ کا استعمال کریں۔
- اپنے آلات کو خفیہ کریں۔
- فشنگ ای میلوں سے ہوشیار رہیں۔

- محتاط رہیں کہ آپ سوشل میڈیا پر کیا پوسٹ کرتے ہیں۔ بہت زیادہ ذاتی تفصیلات سے ہیکرز کو پاس ورڈ کا اندازہ لگانے میں مدد مل سکتی ہے۔
- جن پرانی معلومات کی آپ کو ضرورت نہیں وہ مٹا دیں۔
- اگر کوئی نیٹ ورک آپ سے کوئی اضافی سافٹ ویئر یا براؤزر انسٹال کرنے کے لئے کہتا ہےتو مربوط نہ ہوں۔
- اس بات کو یقینی بنائیں کہ معلوم مسائل سے بچنے کے لئے آپ کے آلات پر نئے پیچزاور سوفٹویئراپڈیٹس انسٹالڈ ہیں۔