

عوامی Fi-Wi

شرکاء عوامی Fi-Wi نیٹ ورکس اور ان کے فوائد اور خطرات کے بارے میں جانیں گے۔ خاص طور پر، وہ اپنے لیے غیر محفوظ Fi-Wi دستیاب ہونے پر ان کی پہچان کرنے کا طریقہ جانیں گے، غیر محفوظ Wi کہ گے کریں فیصلہ باخبر میں بارے اس اور گے سمجھیں کو انہیرینٹ آفس ٹریڈ میں استعمال کے Fi غیر محفوظ Fi-Wi سے کب منسلک ہوتا ہے اور اس کب استعمال کرنا ہے۔

وسائل

وائریس موڈیم تصویر
کنکشن کے تحفظ کا دستاویز

یہ؟ کیا Wi-Fi

حصہ اول

اپنے طلباء سے پوچھیں

انٹرنیٹ تک رسائی حاصل کرنے کے لیے آپ کن آلات کو استعمال کرتے ہیں؟

وہ آلات انٹرنیٹ سے کیسے مربوط ہوتے ہیں؟

Image Class Interaction

آلات کے کر استعمال کا سگنلز ریڈیو Wi-Fi ہے۔ طریقہ عام کا کرنے مربوط سے انٹرنیٹ کو آلات Wi-Fi کو فزیکل یا تار والے کنکشن کے بغیر مربوط کرتا ہے۔

تصور کریں کہ آپ کے گھر میں تین لیپ ٹاپ ہیں جنہیں آپ انٹرنیٹ سے مربوط کرنا چاہتے ہیں۔ ایسا کرنے کے لیے، آپ کو مندرجہ ذیل کی ضرورت ہوگی:

1- رسائی کا پوائنٹ: رسائی پوائنٹ کوئی بھی ایسی چیز ہے جو Fi-Wi سگنل کی ترسیل (براڈکاسٹ؟) کرتی ہے اور انٹرنیٹ تک رسائی فراہم کرتی ہے۔ انٹرنیٹ سے مربوط ہونے کے لیے آپ کے آلات کو ان سگنلز کو منتخب کرنا ہوتا ہے۔ کبھی کبھی سائن ان کرنے اور AP کے براڈکاسٹ کردہ وائریس سگنل کو استعمال کرنے کے لیے آپ کو خاص اجازت (جیسے، صارف نام یا پاس ورڈ) کی ضرورت پڑ سکتی ہے۔

2- راؤٹر: راؤٹر ایسا آلہ ہے جو کسی فراہم کردہ مقام (جیسے اسکول، لائبریری یا آپ کے گھر) میں سبھی آلات (جیسے کمپیوٹرز، ٹیلیفون، موبائل فون) کے درمیان نیٹ ورک تخلیق کرتا ہے۔ عام طور پر، راؤٹرز میں ایک رسائی پوائنٹ بنا ہوتا ہے (درج بالا ڈایا گرام دیکھیں)۔

راؤٹرز میں محدود (عام طور پر مختصر) رینج ہے۔ اسی وجہ سے اگر آپ کا آلہ راؤٹر سے کافی دور ہے تو آپ کو کمزور Fi-Wi سگنل یا کوئی بھی نہیں ملے گا۔ نیز، اگر آپ اور راؤٹر کے درمیان کوئی چیز ہے (جیسے عمارت یا اینٹ کی دیوار) تو اس سے سگنل کم ہو جائے گا۔

اگرچہ راؤٹر سے مربوط ہونے سے نیٹ ورک تک رسائی مل جاتی ہے، لیکن اس سے انٹرنیٹ تک رسائی نہیں ملتی ہے۔ کسی نیٹ ورک پر متعدد آلات کو انٹرنیٹ سے مربوط ہونے کا اہل بنانے کے لیے، راؤٹر کو موڈم سے مربوط ہونا ضروری ہے۔

3- موڈم: موڈم ایسا آلہ ہے جو انٹرنیٹ تک آپ کو رسائی فراہم کرنے کے لیے آپ کے انٹرنیٹ سروس فراہم کنندہ (ISP) تک کنکشن تخلیق کرتا اور اسے برقرار رکھتا ہے۔ یہ آپ کے فراہم کردہ محل وقوع کے باہر سے سگنلز کو ان سگنلز میں منتقل کرتا ہے جنہیں آپ کا کمپیوٹر اور دیگر ڈیجیٹل آلات پڑھ سکتے ہیں۔

کسی مثالی سیٹ اپ میں، AP اور راؤٹر واحد آلہ ہوتا ہے جو انٹرنیٹ کیبل سے معروف خاص کیبل کا استعمال کر کے، موڈم سے فزیکل طور پر مربوط ہوتا ہے۔ جب لوگ "تار والے" انٹرنیٹ کنکشن کے بارے میں بات کرتے ہیں تو اسے یہی مطلب ہوتا ہے۔

انٹرنیٹ سے مربوط ہونے کے لیے موبائل آلات سیلولر کنکشن بھی استعمال کر سکتے ہیں، خاص طور پر اگر وہ اسکول، لائبریری یا گھریلو نیٹ ورک نہیں ہیں۔ سیلولر کنکشن وائرلیس ریڈیو سگنل کی قسم ہیں جن میں راؤٹر سے کافی زیادہ کوریج ایریا ہوتا ہے۔ سیلولر کنکشنز آپ کے موبائل آلہ کو انٹرنیٹ سے مربوط کرنے کے لیے، مخصوص آلہ ترسیل و وصول استعمال کرتے ہیں، جنہیں سیل ٹاورز کہا جاتا ہے۔

حصہ دوم

اپنے طلباء سے پوچھیں

ہیں؟ فوائد کیا کے Wi-Fi

ہیں؟ کیا خامیاں کچھ کی Wi-Fi

تار والے انٹرنیٹ کنکشن کے مقابلے Fi-Wi استعمال کرتے وقت سیکیورٹی کے کچھ خدشات کیا ہو سکتے ہیں؟

جب آپ کسی عمارت سے روانہ ہوتے ہیں تو آپ کے فون پر آپ کی Fi-Wi رسائی کیوں ختم ہو جاتی ہے؟

کرنا انتخاب کا ورک نیٹ Wi-Fi

حصہ اول

اپنے طلباء سے پوچھیں

کیا تمام Fi-Wi نیٹ ورک محفوظ ہوتے ہیں؟ کیوں/کیوں نہیں؟

اپنے طلباء کو بتائیں

کبھی کبھی آپ کو یہ انتخاب کرنے کا موقع دیا جاتا ہے کہ آپ کس Fi-Wi نیٹ ورک کا استعمال کرنا چاہتے ہیں۔ یہ یاد رکھنا بہت ضروری ہے کہ اگر آپ غلط نیٹ ورک سے مربوط ہوتے ہیں تو اس میں سنگین خطرات ہوتے ہیں۔ مثال کے طور پر، غیر محفوظ Fi-Wi نیٹ ورک وہ ہوتے ہیں جن میں لاگ ان کرنے کے لیے پاس ورڈ کی ضرورت نہیں ہوتی۔ اگر آپ کسی غیر محفوظ نیٹ پر ہوتے ہیں، تو یہ ممکن ہے کہ اسی نیٹ ورک پر موجود دیگر افراد آپ کی معلومات کو دیکھ لیں۔ وہ نیٹ ورک پر آپ کے ذریعے بھیجی گئی معلومات کی چوری کر سکتے ہیں یا آپ کیا کر رہے ہیں اس کی نگرانی کر سکتے ہیں۔

دوسری جانب، محفوظ اور معتبر Fi-Wi نیٹ ورک وہ نیٹ ورک ہوتے ہیں جنہیں پاس ورڈ درکار ہوتا ہے، جن کی خفیہ کاری فعال ہوتی ہے، اور جس پر آپ کو یقین ہے کہ آپ جس نیٹ ورک میں سائن ان کر رہے ہیں وہ اس نیٹ ورک کے نام کی نمائندگی کرتا ہے مثال کے طور پر، آپ کے اسکول کے نیٹ ورک کے نام کی نقالی کرنے والے نیٹ ورک میں سائن ان کرنے سے اکاؤنٹ کی معلومات کے انکشاف کا خطرہ ہو سکتا ہے۔ لہذا، محفوظ اور معتبر نیٹ ورک وہ ہیں جو سب سے زیادہ تحفظ فراہم کرتے ہیں۔

غور کرنے والی ایک بات Fi-Wi نیٹ ورک کا سیاق یا محل وقوع ہوتا ہے۔ مثال کے طور پر، اگر آپ کسی تھیٹر میں ہیں اور Fi-Wi کنکشن کی تلاش کرتے ہوئے آپ کو اپنے فون پر اپنے اسکول کے نام والا نیٹ ورک دکھائی دیتا ہے، تو آپ اس بات پر غور کر سکتے ہیں کہ یہ نیٹ ورک غیر متوقع طلباء سے پاس ورڈ جمع کرنے کے لیے آپ کے اسکول کا نیٹ ورک کی نقل یا "اسپوف" کر رہا ہے۔

پاس ورڈ سے تحفظ یافتہ Fi-Wi نیٹ ورک سیٹ اپ کرتے وقت، مالک کو روٹر کی خفیہ کاری کا پروٹوکول آن کرنے کا انتخاب کرنا ہوگا۔ عام خفیہ کاری پروٹوکول، وائرڈ مساوی رازداری (WEP)، Fi-Wi کی تحفظ یافتہ رسائی (WPA)، یا WPA2۔ یہ پروٹوکول اسے بناتے ہیں تاکہ نیٹ ورک پر وائر لیس کے ذریعے بھیجی گئی معلومات خفیہ کردہ ("خلط ملط کردہ") ہو۔

خفیہ کاری کی تخلیق کی گئی تھی تاکہ آپ جو مواد بھیج رہے ہیں وہ ہیکرز کو نظر آنا زیادہ مشکل ہو جائے۔ تاہم، ان پروٹوکول (WPA، WPA2، WEP) کو ہیکنگ کے لیے زد پذیر ظاہر کیا گیا ہے۔ لہذا، آن لائن معلومات کی اشاعت کے دوران محفوظ ویب کنکشن پر بھی اعتبار کرنا ضروری ہے۔

ہے۔ جانا کیا استعمال پر سائٹ ویب لیے کے کاری خفیہ کی ڈیٹا پر انٹرنیٹ جسے بے معیار ایک HTTPS خفیہ کاری کسی بھی فریق ثالث کو آپ کے کنکشن سے ڈیٹا کو آسانی سے دیکھنے سے روک سکتا ہے۔ یہ سلامتی کی ایک اضافی سطح فراہم کرتی ہے اور آپ کے استعمال کردہ URL کے سامنے "https://" شامل کر کے کسی بھی براؤزر میں استعمال کیا جا سکتا ہے (مثلاً <https://www.mysite.com>)۔ تاہم، تمام ویب سائٹس HTTPS کی معاونت نہیں کرتیں۔

1. آپ کو صرف HTTPS:// سابقہ والے ویب صفحات پر حساس معلومات (مثلاً، پاس ورڈ، کریڈٹ کارڈ کی معلومات) درج کرنی چاہیے۔

2. کئی براؤزر میں HTTPS کنکشن کی نشاندہی کرنے کے لیے ایڈریس بار کے نزدیک قفل کی طرح نظر آنے والے سلامتی انڈیکٹر ہوتے ہیں۔

3. بدقسمتی سے، HTTPS اس بات کی ضمانت نہیں دیتا ہے کہ آپ محفوظ ہیں کیونکہ کچھ مضر ویب سائٹس HTTPS کی بھی معاونت کر سکتی ہیں۔ HTTPS کنکشن کو تحفظ دیتی ہے لیکن یہ یقینی نہیں بناتی کہ ویب سائٹ ایک اچھی عامل ہے۔

اپنے طلباء کو بتائیں

سیکور سائٹس لیئر (SSL) / ٹرانسپورٹ لیئر سیکورٹی (TLS) ان تکنیکوں کے نام ہیں جو HTTPS کو محفوظ رکھتی ہیں۔ TLS/SSL ڈیجیٹل خفیہ کاری کی کلیدی استعمال کرتی ہیں، جو حقیقی کلیدوں کی طرح کام کرتی ہیں۔ اگر آپ کاغذ کے ایک ٹکڑے پر اپنے دوست کے لیے کوئی راز لکھتے ہیں، تو جس شخص کو وہ کاغذ مل جائے وہ آپ کا راز جان سکتا ہے۔ اس کے بجائے، تصور کریں کہ آپ نے انہیں ذاتی طور پر کلید کی ایک نقل دی تھی، اور پھر ملتے جلتے مقفل باکس میں اپنے راز بھیج دیے۔ اگر کسی شخص نے باکس کو روک دیا ہے، تو انہیں چابی کے بغیر آپ کا راز دیکھنے میں مشکل ہو گی۔ اگر کسی نے مشابہ باکس کو تبدیل کرنے کی کوشش کی ہے، تو آپ دیکھیں گے کہ آپ کی چابی کام نہیں کرے گی۔ TLS/SSL اسی طریقے سے کام کرتی ہے لیکن ویب سائٹ کے ساتھ۔

براؤزر سلامتی انڈیکٹرز بھی توسیعی تحقیق (EV) سرٹیفکیٹ کی معلومات کی بھی مواصلت کرتے ہیں۔ EV سرٹیفکیٹ ان ویب سائٹس کو دیئے جاتے ہیں جو سرٹیفکیٹ اتھارٹی کو ان کی شناخت کی توثیق کراتے ہیں۔ براؤزر میں، کبھی کبھی EV انڈیکٹر ایڈریس بار کے سامنے سائٹ کے نام یا رجسٹر کرنے والے ہستی کی شکل اختیار کر لیتا ہے۔ اگر آپ کسی خاص ویب سائٹ پر مواد سے مشکوک ہیں تو آپ "سرٹیفکیٹ دیکھیں" پر کلک کر کے یہ دیکھنے کے لیے جانچ کر سکتے ہیں کہ سرٹیفکیٹ میں موجود URL براؤزر میں موجود URL کے مماثل ہے یا نہیں۔ [یہ پروجیکشن اسکرین پر شرکاء کو "سرٹیفکیٹ دیکھیں" کو تلاش کرنے کے طریقے کی وضاحت کے لیے مددگار ثابت ہو سکتا ہے۔ مختلف براؤزر کے ذریعے آپ کس طرح نیویگیٹ کرتے ہیں مثال کے طور پر، Chrome پر "دیکھیں" میں "ٹولپر" پر اور پھر "ٹولپر ٹولز" پر کلک کریں۔ "ٹولپر ٹولز" سے "سلامتی" ٹیب پر، پھر "سرٹیفکیٹ دیکھیں" پر کلک کریں۔

اپنے طلباء سے پوچھیں

سی بھی نئے نیٹ ورک سے مربوط ہونے کے بارے میں آپ کو کیا سوچنا چاہیے؟

1. ممکنہ جوابات میں شامل ہے: محل وقوع (یا نیٹ ورک کا مالک)، رسائی (کوئی اور جو نیٹ ورک سے مربوط ہے)، اور سرگرمی (یا آپ نیٹ ورک پر کیا کام کر رہے ہیں)۔

گھر پر آپ کے Fi-Wi نیٹ ورک کا مالک کون ہے؟ اسکول میں؟ کافی شاپ میں؟

1. آپ کے والدین/دیکھ بھال کرنے والے آپ کے گھر کے وائی فائی نیٹ ورک، منتظمین اور/یا ضلع کے اسکول میں نیٹ ورک کے مالک ہیں، اور مالک، کافی شاپ نیٹ ورک کا مالک ہے۔

کیا آپ ان لوگوں کو ذاتی طور پر جانتے ہیں؟ کیا آپ ان لوگوں پر بھروسہ کرتے ہیں؟

1. شرکاء کو اس گفتگو میں شامل کریں کہ وہ ان لوگوں پر بھروسہ کیسے کر سکتے ہیں۔

اپنے طلباء کو بتائیں

آپ کو Fi-Wi نیٹ ورک کی میزبانی کرنے والے شخص کو جاننا اور اس پر بھروسہ ہونا چاہیے۔ کبھی کبھی آپ اس بات کا تعین کر سکتے ہیں کہ مالک نیٹ ورک کے SSID کا استعمال کر رہا ہے۔

سروس سیٹ آئیڈنٹیفایر (SSID) ایک Fi-Wi کو نام دیا گیا جسے آپ مربوط کرنے کی کوشش کرتے وقت دیکھ سکتے ہیں۔ SSID اکثر بات چیت کرنے کے لیے استعمال کیا جاتا ہے جو نیٹ ورک کے مالک اور نیٹ ورک کے بارے میں مزید تفصیلات ہیں۔ محتاط رہیں اگرچہ تقریباً کوئی شخص (جو جانتا ہے کہ کس طرح) ایک SSID تخلیق کیا جا سکتا ہے۔ مثال کے طور پر، کوئی شخص ایک ویسی ہی SSID تخلیق کر سکتا ہے جو آپ کے ذریعے اسکول میں استعمال کی جاتی ہے۔ یہ صارف نام اور پاس ورڈ کو ممکنہ طور پر حاصل کرنے کے لیے ایک معروف اور معتبر نیٹ ورک کو متاثر کرنے کی ایک مثال ہے۔

نیٹ ورک کی میزبانی کرنے والے کو جان کر آپ کو یہ تعین کرنے میں مدد کر سکتے ہیں کہ نیٹ ورک محفوظ ہے یا نہیں۔ اگر یہ آپ کے کسی معتبر شخص یا تنظیم سے تعلق رکھتا ہے، تو شاید اس سے مربوط ہونے میں اطمینان محسوس کریں گے۔ تاہم، اگر یہ ایک نامعلوم نیٹ ورک ہے، تو جب تک آپ اس بات کو نہ جانیں کہ روٹر کا مالک کون ہے جس سے آپ مربوط ہو رہے ہیں تب تک آپ کو اس سے مربوط نہیں ہونا چاہیے۔ کیوں کہ نیٹ ورک کا سارا ٹریفک راؤٹر کے ذریعے جاتا ہے، اس لیے مالک آپ کے ویب ٹریفک کی نگرانی یا ریکارڈنگ کر سکتا ہے۔

جب آپ کسی Fi-Wi سے مربوط ہوتے ہیں، تو آپ کا آلہ، آلات کے مقامی نیٹ سے مربوط ہو جاتا ہے، اور وہ نیٹ ورک وسیع اٹرنیٹ سے مربوط ہوتا ہے۔ چونکہ آپ کا آلہ اس نیٹ ورک کے ساتھ معلومات کا تبادلہ کر رہا ہے، اس لیے آپ سے مربوط کردہ دیگر آلات پر بھروسہ ہونا ضروری ہے — اور اس کا مطلب ہے کہ نیٹ ورک پر موجود کوئی بھی آلہ۔ یہ آپ کے ذریعے اسکول میں کیے گئے اجتماعی کام جیسا ہی ہے — آپ ان دیگر افراد پر بھروسہ کرنے کے قابل ہونا چاہتے ہیں جن کے ساتھ آپ کام کر رہے ہیں!

نیٹ ورک پر پاس ورڈ کا استعمال کرنے سے اس بات کی حد بندی ہو سکتی ہے کہ کون اس سے مربوط ہو سکتا ہے۔ اس کا مطلب ہے کہ آپ کو اس کا بہتر طریقے سے خیال ہوگا کہ آپ کے نیٹ ورک پر کون ہے — کیا یہ آپ کا خاندان، آپ کے دوست، یا کافی شاپ کے دیگر گاہک ہیں — جب کہ نیٹ ورک پوری طرح سے عوامی تھا۔

چاہے آپ کسی نیٹ ورک میں شامل ہونے کا فیصلہ کریں یا نہیں، جو تجارتی مجرموں کی آن لائن سلامتی کے لحاظ سے مشکوک لگتا ہے۔ آپ غور کر سکتے ہیں کہ دستیاب نیٹ ورک میں شامل ہونے کی اجازت کے مقابلے میں اکاؤنٹ کی خلاف ورزی کرنے کے امکان کا وزن کس طرح اٹھایا جانا چاہیے؟

اپنے طلباء سے پوچھیں

کیا آپ کو اپنے گھر پر Fi-Wi نیٹ ورک کا استعمال کر کے خبریں/بلاگ پڑھنا چاہیے؟ اسکول میں؟ کافی شاپ میں؟

1. وضاحت کریں کہ ویب صفحہ کا مواد عام طور پر حساس معلومات نہیں ہوتی ہے۔ آپ اسے شاید کسی بھی نیٹ ورک پر کر سکتے ہیں۔

کیا آپ کو اپنے گھر پر Fi-Wi نیٹ ورک کا استعمال کر کے کریڈٹ کارڈ کا نمبر بھیجنا چاہیے؟ اسکول میں؟ کافی شاپ میں؟ کیوں؟

1. اپنے گھر کے Fi-Wi کے ساتھ ایسا کرنا محفوظ کیوں ہے اور کافی شاپ Fi-Wi کے ساتھ کیوں

نہیں، اس بارے میں ایک بحث میں مشغول رہیں۔ اس بات پر بحث کریں کہ کس طرح، جبکہ اسکول کا نیٹ ورک ممکنہ طور پر قابل اعتماد ہے، یہ اس خطرے کے قابل نہیں ہوسکتا ہے جب کہ یہ مخصوص معلومات انتہائی حساس ہے۔

کیا آپ کو اپنے گھر پر Fi-Wi نیٹ ورک کا استعمال کرتے ہوئے اپنے ذاتی ای میل کی جانچ کرنی چاہیے؟ اسکول میں؟ کافی شاپ میں؟

1. ای میل اکاؤنٹ کے مواد کی بنیاد پر تبادلہ خیال کریں کہ آپ کے گھر کے نیٹ ورک ایسا کرنے کے لیے شاید سب سے محفوظ کس طرح ہے۔ مثال کے طور پر، بعض افراد کے متعدد ای میل اکاؤنٹس ہوتے ہیں جنہیں وہ مختلف مقاصد کے لیے استعمال کرتے ہیں (مثلاً، مارکیٹنگ / ایک اکاؤنٹ کے لیے ترویجی ای میل؛ دوسرے اکاؤنٹ پر دوست اور اہل خانہ کے ای میلز)۔

اپنے طلباء کو بتائیں

حساس معلومات بشمول پاس ورڈ اور بینک کی معلومات مشترکہ عوامی نیٹ ورک کی بجائے بھیجی سے طریقے بہتر پر ورک نیٹ محفوظ اور ذاتی، پر سائٹس ویب والی کرنے استعمال SSL/TLS اور دیکھی جا سکتی ہے۔ یہ نجی معلومات خطرے میں پڑ سکتی ہے اگر آپ اسے ارسال یا اس تک رسائی کرتے ہیں جب کہ اس مشترکہ نیٹ ورک کو ناواقف یا غیر معتبر افراد کے ذریعے استعمال کیا جا رہا ہے۔

یہ واضح نہیں ہو سکتا ہے کہ حساس معلومات کتنی حساس یا حساس نہیں ہے کیونکہ رازداری ایک ذاتی فیصلہ ہے جسے آپ خود کے لیے لیتے ہیں۔ یہ تعین کرنے کے لیے ہر صورتحال پر غور کرنا چاہیے کہ آیا آپ کو نیٹ ورک سے مربوط ہونا چاہیے یا نہیں۔ خود سے پوچھیں کہ کیا آپ اس نیٹ ورک کے مالک پر اعتماد کرتے ہیں، جس سے دیگر مربوط ہیں، آپ کس سرگرمی کو آن لائن کر رہے ہیں، اور مربوط ہونے یا نہ ہونے کا فیصلہ لینے سے پہلے آپ کون سی معلومات کا اشتراک کر رہے ہیں۔

محفوظ اور غیر محفوظ نیٹ ورکس

حصہ اول

جماعت میں تعامل

براہ کرم نوٹ کریں: اس سرگرمی کے مواد کا کچھ حصہ "سرگرمی # 2 میں شامل کیا گیا ہے: Fi-Wi نیٹ ورک کا انتخاب کرنا"۔ آپ اس مواد کو دوبارہ دیکھنا چاہیں گے یا نہیں یا اسے نظر انداز کرنا چاہیں گے، اس بارے میں ہم آپ پر فیصلہ چھوڑتے ہیں۔

اپنے طلباء کو بتائیں

جیسا کہ پہلے ذکر کیا گیا ہے کہ غیر محفوظ Fi-Wi نیٹ ورک وہ ہوتے ہیں جن میں لاگ ان کرنے کے لیے پاس ورڈ کی ضرورت نہیں ہوتی۔ غیر محفوظ نیٹ ورک کے استعمال سے اس ڈیٹا کے لیے خطرہ پیدا ہوتا ہے، جسے آپ ایک نیٹ ورک پر ارسال اور موصول کرتے ہیں۔

محفوظ Fi-Wi نیٹ ورک وہ ہوتے ہیں جن میں لاگ ان کرنے کے لیے پاس ورڈ کی ضرورت ہوتی ہے اور جن میں خفیہ کاری فعال ہوتی ہے۔ جو شخص نیٹ ورک کو ترتیب دیتا ہے، وہی خفیہ کاری کو فعال کرنے یا نہ کرنے کے اختیار کا انتخاب کرتا ہے۔ خفیہ کاری وہ معلومات کو چھپا دیتا ہے، جسے آپ نیٹ ورک پر ارسال و موصول کرتے ہیں، تاکہ اسی Fi-Wi نیٹ ورک پر موجود کسی ہیکر کے لیے یہ دیکھنا زیادہ مشکل ہو جاتا ہے کہ آپ کیا ارسال و موصول کر رہے ہیں۔

صرف اس لیے کہ کوئی نیٹ ورک محفوظ ہے، اس کا یہ مطلب نہیں ہے کہ آپ کا ڈیٹا محفوظ ہے۔ یہ کسی غیر محفوظ نیٹ ورک استعمال کرنے سے یقینی طور پر محفوظ ہے، تاہم اگر کوئی ضدی ہیکر چاہے تو آپ کی معلومات تک پھر بھی رسائی حاصل کر سکتا ہے۔

رازداری مساوی وائرڈ یہ: ہیں ہوتے پروٹوکول کاری خفیہ عام مختلف تین لیے کے ورک نیٹ Wi-Fi اور ہیں گئے ہو پرانے WPA اور WEP ہیں۔ WPA2 یا (WPA) رسائی یافتہ تحفظ کی Wi-Fi، (WEP) ان پر منحصر نیٹ ورک کو غیر محفوظ سمجھا جانا چاہیے۔ اس کے علاوہ، WPA2 کو ہیکنگ کے لیے زد پذیر بھی بتایا گیا ہے۔

اس بات کو یقینی بنانے کے لیے کہ آپ کی معلومات مکمل طور پر محفوظ ہے، یہ جانچ کریں کہ آپ جن ویب سائٹس کا استعمال کر رہے ہیں وہ TLS/SSL سے خفیہ کی گئی ہیں۔

اپنے طلباء سے پوچھیں

کیا کوئی پاس ورڈ کے ذریعے محفوظ شدہ نیٹ ورک کی ایسی مثال سوچ سکتا ہے جس کا اس نے استعمال کیا ہو؟

1. اس کی کچھ مثالوں میں ان کے گھر کا Fi-Wi، اسکول کا Fi-Wi، اور کیفے جیسے عوامی مقامات پر موجود Fi-Wi نیٹ ورک شامل ہیں۔

کیا کوئی ایک غیر محفوظ نیٹ ورک کی ایسی مثال سوچ سکتا ہے جس کا اس نے استعمال کیا ہو؟

محفوظ نیٹ ورک کی مثالیں کون سی ہیں؟

اپنے طلباء کو بتائیں

آپ اپنے آلہ کے نیٹ ورک یا وائرلیس ترتیب کی جانچ کر کے یہ دیکھ سکتے ہیں کہ Fi-Wi نیٹ ورک خفیہ کردہ ہے یا نہیں۔

حصہ دوم

جماعت میں تعامل

اس سیکھنے کے تجربے سے قبل یہ جائزہ لینے کے لیے ایک انٹرنیٹ کی تلاش کریں کہ مختلف آپریٹنگ سسٹم کے لیے Fi-Wi نیٹ ورک خفیہ کاری کی اقسام کی جانچ کس طرح کرتا ہے۔ پھر، کوئی نیٹ ورک کس قسم کی خفیہ کاری کا استعمال کر رہا ہے، اسے تلاش کرنے کے طریقے کی وضاحت کریں۔ مثال کے طور پر، MacOS پر، سسٹم کی ترجیحات -> نیٹ ورک -> Fi-Wi منتخب کریں -> مناسب نیٹ ورک کا نام منتخب کریں پر کلک کریں۔ Fi-Wi ٹیب کے تحت، معلوم نیٹ ورکس کی ایک فہرست اور استعمال کردہ خفیہ کاری کی اقسام کو دکھانے والا کالم ہوگا۔

اپنے طلباء کو بتائیں

تمام کنکشنز مساوی نہیں ہوتے۔ جب کوئی نیٹ ورک غیر محفوظ ہو، تو کوئی بھی شخص نیٹ ورک سے مربوط ہو سکتا ہے اور یہ غیر واضح ہوتا ہے کہ نیٹ ورک کو کون کنٹرول کر رہا ہے۔ کسی غیر محفوظ نیٹ ورک سے جڑنے پر آپ خطرے میں پڑ سکتے ہیں، کیونکہ اگر آپ TLS/SSL کنکشن استعمال نہیں کر رہے ہیں تو، آپ جو معلومات ارسال و موصول کرتے ہیں جیسے آپ کا ویب ٹریفک (صفحہ، پاس ورڈ، وغیرہ)، اسے ممکنہ طور پر نیٹ ورک پر کسی بھی شخص کے ذریعے دیکھا جا سکتا ہے۔

جماعت میں تعامل

آپ کے شرکاء کی تکنیکی معلومات پر منحصر ہو کر، ہو سکتا ہے کہ آپ Fi-Wi کا استعمال کرتے وقت سلامتی کی اضافی سطح کے طور پر مجازی نجی نیٹ ورک (VPN) استعمال کرنا چاہیں۔ براہ کرم اضافی معلومات کے لیے وسائل کے سیکشن میں VPN لنکس دیکھیں۔

کنکشن کے تحفظ شناخت کرنا

حصہ کا عنوان

جماعت میں تعامل

شرکاء کو 2-3 کے گروپس میں تقسیم کریں۔ کنکشن کا تحفظ پاس کریں: شرکاء کا دستاویزات اور ہر گروپ کو ایک منظر نامہ تفویض کریں۔ بحث کرنے کے لیے شرکاء کو 5 منٹ کا وقت دیں۔ اس کے بعد، گروپس سے ان کے جوابات کا اشتراک کرنے کو کہیں۔ جوابات دستاویز میں سبز رنگ میں ہوں گے۔

اسائمنٹ

حصہ اول

اسائمنٹ

شرکاء سے کہیں:

1. ایک عام دن کی ٹائم لائن بنائیں، ان Fi-Wi نیٹ ورک کو نشان زد کرتے ہوئے جن سے وہ مربوط ہیں۔

2. ٹائم لائن پر دکھائے گئے منتخب نیٹ ورک سے، شرکاء دو کا انتخاب کریں اور ہر ایک کے لیے ایک مختصر پیراگراف میں، نیٹ ورک کی وضاحت کرتے ہیں — اور کون اس سے مربوط ہے؟ یہ کتنا محفوظ ہے؟

3. اضافی طور پر — منتخب کردہ دو نیٹ ورک کے لیے — شرکاء کی وضاحت ہے کہ ان نیٹ ورک سے مربوط ہونے کے ساتھ کون سے مواقع حاصل ہوتے ہیں اور کون سے متعلقہ خطرات ہو سکتے ہیں۔