شبكة Fi-Wi العامة

سيتعرف المشاركون على شبكات Fi-Wi العامة وفوائدها ومخاطرها. وبشكل أكثر تحديداً، سيتعلمون كيفية التعرف على شبكة الـ Fi-Wi غير المؤمنة عند توفرها لهم، وفهم التنازلات التي ينطوي عليها استخدام شبكة الـ Fi-Wi غير المؤمنة، واتخاذ قرارات مدروسة بشأن وقت الاتصال بشبكة الـ Fi-Wi غير المؤمنة واستخدامها.

الموارد

صورة لمودم لاسلكي
مذكرة سلامة الاتصال

ما المقصود بـ Fi-Wi؟

الجزء الأول

اطرح أسئلة على طلابك

ما الأجهزة التي تستخدمها للوصول إلى الإنترنت؟

كيف تتصل تلك الأجهزة بالإنترنت؟

صورة تفاعل في الفصل

تعتبر تقنية Fi-Wi طريقة شائعة لتوصيل الأجهزة بالإنترنت. تستخدم Fi-Wi إشارات لاسلكية لتوصيل الأجهزة دون اتصال مادي أو سلكي.

تخيل أن لديك ثلاثة أجهزة كمبيوتر محمولة في منزلك ترغب في توصيلها بالإنترنت. للقيام بذلك، يجب توفر ما يلي:

1. نقطة وصول: نقطة الوصول هي أي شيء يعمل على نقل (بث؟) إشارة Fi-Wi ويوفر الوصول إلى الإنترنت. لا بد أن تلتقط أجهزتك هذه الإشارات للاتصال بالإنترنت. قد تحتاج في بعض الأحيان إلى أذونات خاصة (على سبيل المثال، اسم مستخدم وكلمة سر) من أجل تسجيل الدخول واستخدام الإشارة اللاسلكية التي ترسلها نقطة الوصول.

2. جهاز توجيه: جهاز التوجيه هو جهاز يقوم بإنشاء شبكة بين جميع الأجهزة (مثل أجهزة الكمبيوتر والأجهزة اللوحية والهواتف المحمولة) في موقع محدد (مثل مدرسة أو مكتبة أو منزل). عادة ما يكون لدى أجهزة التوجيه نقطة وصول مدمجة بها (انظر الشكل أعلاه).

تمتلك أجهزة التوجيه نطاقًا محدودًا (عادةً ما يكون قصيرًا). لذلك، إذا كان جهازك بعيدًا جدًا عن جهاز التوجيه، فستحصل على إشارة Fi-Wi ضعيفة أو لا شيء على الإطلاق. أيضًا، إذا كان هناك حاجز بينك وبين جهاز التوجيه (مثل مبنى أو جدار من الطوب)، فإن ذلك سيؤدي إلى ضعف الإشارة.

على الرغم من أن الاتصال بجهاز توجيه يوفر الوصول إلى شبكة، فإن هذا لا يعني الوصول إلى الإنترنت. حتى تتمكن العديد من الأجهزة الموجودة على إحدى الشبكات من الاتصال بالإنترنت، يجب توصيل جهاز التوجيه بمودم.

3. مودم: المودم هو جهاز يقوم بإنشاء اتصال بمزود خدمة الإنترنت (ISP) مع الحفاظ على هذا الاتصال لمنحك الوصول إلى الإنترنت. ويقوم بتحويل الإشارات الواردة من خارج موقعك المحدد إلى إشارات يمكن قراءتها بواسطة الكمبيوتر والأجهزة الرقمية الأخرى.

في الإعداد النموذجي، تكون نقطة الوصول وجهاز التوجيه عبارة عن جهاز واحد متصل فعليًا بالمودم، باستخدام كبل خاص يسمى كبل إيثرنت. هذا هو ما يشار إليه عند التحدث عن اتصال إنترنت "سلكي".

تستطيع الأجهزة المحمولة أيضًا استخدام اتصال خلوي للاتصال بالإنترنت، خاصةً إذا لم تكن في

مدرسة أو مكتبة أو شبكة منزلية. الاتصالات الخلوية هي نوع من إشارة الراديو اللاسلكية التي تمتلك مساحة تغطية أكبر بكثير من جهاز التوجيه. تستخدم الاتصالات الخلوية أجهزة إرسال واستقبال خاصة تسمى أبراج الهاتف المحمول لتوصيل جهازك المحمول بالإنترنت.

الجزء الثاني

اطرح أسئلة على طلابك

ما فوائد تقنية Fi-Wi؟

ما بعض عيوب تقنية Fi-Wi؟

ما بعض المخاوف الأمنية الناجمة عن استخدام Fi-Wi مقارنة باتصال الإنترنت السلكي؟

لماذا تفقد اتصال Fi-Wi على هاتفك أثناء مغادرة المبنى؟

Choosing a Wi-Fi Network

الجزء الأول

اطرح أسئلة على طلابك

هل جميع شبكات Fi-Wi آمنة؟ لماذا/لماذا لا؟

أخبر طلابك

في بعض الأحيان، يتم منحك فرصة اختيار شبكة Fi-Wi التي ترغب في استخدامها. من المهم أن تتذكر أن هناك مخاطر جسيمة مترتبة على الاتصال بالشبكة الخطأ. على سبيل المثال، شبكات Fi-Wi غير المؤمنة هي تلك الشبكات التي لا تتطلب كلمة سر لتسجيل الدخول. إذا كنت تستخدم شبكة غير مؤمنة، فمن الممكن أن يرى أشخاص آخرون على نفس الشبكة معلوماتك. قد يسرقون المعلومات التي ترسلها عبر الشبكة أو يراقبون ما تفعله.

على الجانب الآخر، شبكات Fi-Wi الآمنة والموثوق بها هي تلك التي تتطلب كلمة سر مع تمكين التشفير عليها، وتلك التي عند اتصالك بها تكون على يقين بأن الشبكة التي تسجل الدخول إليها هي التي يمثلها اسم الشبكة بالفعل. على سبيل المثال، قد يؤدي تسجيل الدخول إلى شبكة تنتحل اسم شبكة مدرستك إلى الكشف عن معلومات الحساب. لذلك، فإن الشبكات الآمنة والموثوق بها هي التي توفر أقصى قدر من الحماية.

لكن هناك شيء واحد يجب مراعاته، ألا وهو سياق أو موقع شبكة Fi-Wi. على سبيل المثال، إذا كنت في دار السينما وترى اسم شبكة مدرستك على هاتفك عند البحث عن اتصال Fi-Wi، يمكنك اعتبار أن الشبكة تحاول تقليد أو "انتحال" شبكة مدرستك لتجميع كلمات السر من طلاب غير منتبهين.

عند إعداد شبكة Fi-Wi محمية بكلمة سر، يجب على المالك اختيار تشغيل بروتوكول التشفير على جهاز التوجيه. بروتوكولات التشفير الشائعة هي الخصوصية المكافئة للشبكات السلكية (WEP) أو الوصول المحمي بالدقة اللاسلكية (WPA) أو الوصول المحمي بالدقة اللاسلكية 2 (WPA2). تعمل هذه البروتوكولات على تشفير (أو "تعمية") المعلومات التي يتم إرسالها لاسلكيًا عبر الشبكة.

تم إنشاء التشفير لجعل رؤية البيانات المرسلة عبر الشبكة أكثر صعوبة على المخترقين. ومع ذلك، فقد ثبت أن جميع هذه البروتوكولات (WEP وWPA وWPA2) عرضة للاختراق. لذلك، من المهم أيضًا الاعتماد على اتصالات الويب الآمنة عند نقل المعلومات على الإنترنت.

يمكن .الإنترنت عبر تمريرها يتم التي البيانات لتشفير الويب مواقع تستخدمه معيار هو HTTPS للتشفير أن يمنع أي جهة خارجية من عرض البيانات بسهولة أثناء اتصالك. إنه يوفر طبقة أمان إضافية ويمكن استخدامه في أي متصفح من خلال إضافة "https://:" في بداية عنوان URL الذي تستخدمه (مثل com.mysite.www//:https). لكن، ليست كل مواقع الويب تدعم HTTPS.

1. لا ينبغي إدخال المعلومات الحساسة (مثل كلمات السر ومعلومات بطاقة الائتمان) على صفحات الويب إلا باستخدام البادئة HTTPS://.

2. تحتوي معظم المتصفحات الرئيسية على مؤشرات أمان تشبه الأقفال بالقرب من شريط العنوان للإشارة إلى اتصالات HTTPS.

3. لسوء الحظ، لا يضمن HTTPS أنك في أمان حيث يمكن لبعض مواقع الويب الضارة دعم HTTPS أيضاً. يعمل HTTPS على الاتصال تأمين ولكنه أن يضمن لا موقع يكون أن يضمن لا الويب أصالة.

أخبر طلابك

يتم تأمين HTTPS عبر تقنية محكمة تحمل اسم طبقة مآخذ التوصيل الآمنة (SSL)/أمان طبقة النقل (TLS). تستخدم SSL/TLS مفاتيح التشفير الرقمي، والتي تعمل مثل المفاتيح الحقيقية إلى حد كبير. إذا كتبت سراً على ورقة لصديقك، فإن أي شخص يجد الورقة يستطيع رؤية سرّك. بدلاً من ذلك، تخيل أنك أعطيته في يده نسخة من مفتاح، ثم أرسلت أسرارك في صناديق مغلقة يمكن فتحها بذلك المفتاح. إذا عثر شخص ما على الصندوق، فسيجد صعوبة في رؤية سرك دون وجود المفتاح. إذا حاول أحدهم استبدال الصندوق بصندوق مشابه في الشكل، فسوف تلاحظ أن مفتاحك لن يعمل. تعمل TLS/SSL بنفس الطريقة، ولكن مع موقع الويب.

كما ستقوم مؤشرات أمان المتصفح بتوصيل معلومات شهادة التحقق من الصحة الموسّع (EV). يتم منح شهادات EV إلى مواقع الويب التي يتم التحقق من صحة هويتها إلى مرجع مصدق. في المتصفحات، أحيانًا ما يأخذ مؤشر EV شكل اسم الموقع أو الكيان المسجل بجوار شريط العنوان. إذا كنت تشك في المحتوى الموجود على موقع ويب معين، يمكنك التحقق لمعرفة ما إذا كان عنوان URL الموجود في الشهادة يتطابق مع عنوان URL في المتصفح عن طريق النقر على "عرض الشهادة". [قد يكون من المفيد أن تشرح للمشاركين على شاشة العرض كيفية العثور على "عرض الشهادة". تختلف كيفية انتقالك إلى هذا الخيار حسب المتصفح. على سبيل المثال، على Chrome، ضمن "عرض"، انقر على "المطور" ثم "أدوات المطور". من "أدوات المطور"، انقر على علامة التبويب "الأمان"، ثم "عرض الشهادة".

اطرح أسئلة على طلابك

ما الذي يجب وضعه في الاعتبار عند الاتصال بأي شبكة جديدة؟

1. تتضمن الإجابات المحتملة: الموقع (أو مالك الشبكة)، والوصول (أو المتصلون الآخرون بالشبكة)، والنشاط (أو ما تفعله على الشبكة).

من يمتلك شبكة Fi-Wi الخاصة بك في المنزل؟ في المدرسة؟ في المقهى؟

1. يمتلك الوالد/ولي الأمر شبكة Fi-Wi في المنزل، ويمتلك المسؤولون و/أو المنطقة التعليمية الشبكة في المدرسة، ويمتلك صاحب المقهى شبكة المقهى.

هل تعرف هؤلاء الأشخاص شخصيًا؟ هل تثق بهؤلاء الأشخاص؟

1. قم بإشراك المشاركين في مناقشة حول كيف قد يمكنهم الوثوق بهؤلاء الأشخاص بشكل مختلف.

أخبر طلابك

يجب أن تعرف الشخص الذي يستضيف شبكة Fi-Wi وتثق به. يمكنك أحيانًا تحديد المالك الذي يستخدم معرف SSID الخاص بالشبكة.

معرف مجموعة الخدمات (SSID) هو الاسم المحدد لشبكة Fi-Wi والذي يمكنك رؤيته عند محاولة الاتصال. غالبًا ما يتم استخدام SSID لإفشاء المعلومات المتعلقة بمن يمتلك الشبكة وتفاصيل أخرى متعلقة بالشبكة كن حذرًا، فأي شخص الآن يمكنه إنشاء SSID (إن كان على دراية بذلك). على سبيل المثال، يستطيع شخص ما إنشاء SSID متطابق مع الذي تستخدمه في المدرسة. ويعد هذا مثالاً على انتحال هوية شبكة معروفة وموثوق بها، لتجميع أسماء المستخدمين وكلمات السر المحتملة.

يمكن أن تساعدك معرفة من يستضيف الشبكة في تحديد ما إذا كانت الشبكة آمنة أم لا. إذا كانت تنتمي إلى شخص أو مؤسسة تثق بهما، فمن المرجح أن تشعر بالراحة أثناء الاتصال. لكن، إذا كانت شبكة غير معروفة، ينبغي عدم الاتصال بها حيث إنك لا تعرف من يمتلك جهاز التوجيه الذي تتصل به. نظرًا لأن كل الزيارات على الشبكة تمر عبر جهاز التوجيه، يمكن للمالك مراقبة أو تسجيل زياراتك.

عند الاتصال بشبكة Fi-Wi، يكون جهازك متصلاً بشبكة محلية من الأجهزة، وبدورها تتصل تلك الشبكة بالإنترنت الأوسع. نظرًا لأن جهازك يتبادل المعلومات مع هذه الشبكة، فمن المهم الوثوق بالأجهزة الأخرى التي تتصل بها - وهذا يعني أي جهاز على الشبكة. الأمر يشبه العمل الجماعي الذي تقوم به في المدرسة - فأنت تريد أن يكون بإمكانك الثقة بالأشخاص الآخرين الذين تعمل معهم!

قد يؤدي استخدام كلمة سر على الشبكة إلى تقييد من يمكنه الاتصال بها. وهذا يعني أنه سيكون لديك فكرة أفضل عن الأشخاص الموجودين على الشبكة - سواء أكانوا أفراد عائلتك أم أصدقاءك أم عملاء آخرين في مقهى - أكثر مما لو كانت الشبكة مفتوحة تمامًا.

يتوقف قرارك بالانضمام أو عدم الانضمام إلى شبكة قد تبدو مشبوهة على التنازلات التي أنت على استعداد لتقديمها فيما يتعلق بالأمان على الإنترنت. يمكنك أن تضع في اعتبارك التساؤل التالي؛ كيف ينبغي لي أن أقيّم احتمال اختراق حسابي مقابل رفاهية الانضمام إلى شبكة متاحة؟

اطرح أسئلة على طلابك

هل ينبغي قراءة الأخبار/المدونات على الإنترنت باستخدام شبكة Fi-Wi في المنزل؟ في المدرسة؟ في المقهى؟

1. يمكنك توضيح أن محتوى صفحة الويب لا يتضمن معلومات حساسة بشكل عام. ربما يمكنك القيام بذلك على أي شبكة.

هل ينبغي إرسال رقم بطاقة الائتمان باستخدام شبكة Fi-Wi في المنزل؟ في المدرسة؟ في المقهى؟ ولماذا؟

1. شارك في مناقشة حول الأسباب التي تجعل إجراء ذلك عبر شبكة Fi-Wi المنزلية أكثر أمانًا من إجرائه عبر شبكة Fi-Wi في المقهى. ناقش أيضًا كيف، في حين أنه من المحتمل أن تكون شبكة المدرسة جديرة بالثقة، قد لا يستحق الأمر المخاطرة نظرًا لأن هذه المعلومات بالذات شديدة الحساسية.

هل ينبغي فحص بريدك الإلكتروني الشخصي باستخدام شبكة Fi-Wi في المنزل؟ في المدرسة؟ في المقهى؟

1. ناقش كيف قد يكون من الأسلم إجراء ذلك عبر الشبكة المنزلية الخاصة، حسب محتوى حساب البريد الإلكتروني. على سبيل المثال، لدى بعض الأفراد حسابات بريد إلكتروني متعددة

يستخدمونها لأغراض مختلفة (على سبيل المثال، رسائل البريد الإلكتروني المتعلقة بالتسوية/الترويج على أحد الحسابات؛ رسائل البريد الإلكتروني المتعلقة بالأصدقاء والعائلة على حساب آخر).

أخبر طلابك

من الأفضل أن يتم إرسال/عرض المعلومات الحساسة، بما في ذلك كلمات السر والمعلومات البنكية، على شبكة خاصة وآمنة، على مواقع الويب التي تستخدم TLS/SSL بدلاً من شبكة عامة مشتركة. تكون تلك المعلومات الخاصة عرضة للخطر إذا قمت بإرسالها أو الوصول إليها أثناء الاتصال بشبكة مشتركة يستخدمها أشخاص لا تعرفهم أو لا تثق بهم.

لا يمكن وضع مقاييس واضحة لتحديد مدى حساسية المعلومات لأن الخصوصية قرار شخصي يجب عليك اتخاذه بنفسك. من المهم مراعاة كل موقف على حدة لتحديد ما إذا كان ينبغي الاتصال بالشبكة أم لا. اسأل نفسك عما إذا كنت تثق في مالك الشبكة، وعن الآخرين المتصلين بها، وعن النشاط الذي تجريه على الإنترنت، وعن نوع المعلومات التي تشاركها قبل أن تتخذ قرارًا بالاتصال.

الشبكات المؤمنة وغير المؤمنة

الجزء الأول

تفاعل في الفصل

-يُرجى ملاحظة ما يلي: تمت تغطية جزء من محتوى هذا النشاط في "النشاط رقم 2: اختيار شبكة Wi Fi". يمكنك الاطلاع على هذه المادة مرة أخرى ،تخطيها أو حسب احتياجاتك.

أخبر طلابك

كما ذكرنا سابقًا، شبكات Fi-Wi غير المؤمنة هي تلك الشبكات التي لا تتطلب كلمة سر لتسجيل الدخول. يشكل استخدام الشبكات غير المؤمنة خطرًا على البيانات التي تقوم بإرسالها واستقبالها عبر الشبكة.

شبكات Fi-Wi المؤمنة هي تلك التي تتطلب كلمة سر مع تمكين التشفير عليها. الشخص الذي قام بتكوين الشبكة هو من يختار تمكين التشفير أم لا. يعمل التشفير على ترميز المعلومات التي ترسلها وتستقبلها عبر الشبكة، بحيث يصعب على أي مخترق موجود على نفس شبكة Fi-Wi رؤية ما ترسله أو تستقبله.

مجرد أن الشبكة مؤمنة لا يعني بالضرورة أن بياناتك آمنة. إنه بالتأكيد أكثر أمانًا من استخدام شبكة غير مؤمنة؛ ومع ذلك، يظل بإمكان أحد المخترقين المصممين العثور على طريقة للوصول إلى معلوماتك.

هناك ثلاثة بروتوكولات تشفير شائعة لشبكات الـ Fi-Wi: وهي الخصوصية المكافئة للشبكات السلكية (WEP) اللاسلكية بالدقة المحمي الوصول أو (WPA) اللاسلكية بالدقة المحمي الوصول أو 2 غير أنها عليهما تعتمد التي الشبكات اعتبار وينبغي WPAو WEP على التحديث يطرأ لم .(WPA2) مؤمنة. وعلاوة على ذلك، فقد تبين أيضًا تعرض الوصول المحمي بالدقة اللاسلكية 2 (WPA2) لخطر الاختراق.

لضمان حماية معلوماتك على أكمل وجه، تأكد من تشفير مواقع الويب التي تستخدمها بواسطة SSL/TLS.

اطرح أسئلة على طلابك

هل يمكن لأي شخص ذكر مثال على شبكة محمية بكلمة سر كان قد استخدمها من قبل؟

1. تشمل بعض الأمثلة شبكة Fi-Wi المنزلية وشبكة Fi-Wi للمدرسة وشبكات Fi-Wi في بعض الأماكن العامة مثل المقاهي.

هل يمكن لأي شخص ذكر مثال على شبكة غير مؤمنة كان قد استخدمها من قبل؟

ماذا عن تقديم أمثلة لشبكة مؤمنة؟

أخبر طلابك

يمكنك التحقق مما إذا كانت شبكة Fi-Wi مشفرة من خلال فحص الشبكة أو الإعدادات اللاسلكية على

جهازك.

الجزء الثاني

تفاعل في الفصل

قبل تجربة التعلم هذه، قم بإجراء بحث على الإنترنت لمراجعة كيفية التحقق من أنواع تشفير شبكات Wi-Fi على .الشبكة تستخدمه الذي التشفير نوع معرفة كيفية استعرض ثم .المختلفة التشغيل لأنظمة سبيل المثال، على MacOS، انقر على تفضيلات النظام -> الشبكة -> تحديد Fi-Wi -> تحديد اسم الشبكة المناسب. ضمن علامة تبويب Fi-Wi، ستكون هناك قائمة بالشبكات المعروفة وعمود يشير إلى نوع التشفير المستخدم.

أخبر طلابك

ليست كل الاتصالات متكافئة. عندما تكون الشبكة غير مؤمنة، يمكن لأي شخص الاتصال بالشبكة، ولا يتضح من يتحكم في الشبكة. إن الانضمام إلى شبكة غير مؤمنة يجعلك عرضة للاختراق، نظرًا لأن المعلومات التي ترسلها وتستقبلها، مثل زيارات الويب (الصفحات وكلمات السر وما إلى ذلك)، من المحتمل أن يشاهدها أي شخص على الشبكة إذا كنت لا تستخدم اتصال TLS/SSL.

تفاعل في الفصل

استنادًا إلى المعرفة الفنية لدى المشاركين، يمكنك مناقشة استخدام الشبكات الخاصة الافتراضية الموارد قسم في VPN روابط إلى الرجوع يرجى .Wi-Fi استخدام عند إضافية أمان كطبقة (VPN) للحصول على معلومات إضافية.

التعرف على سلامة الاتصال

عنوان الجزء

تفاعل في الفصل

قم بتقسيم المشاركين إلى مجموعات مكونة من اثنين أو ثلاثة. وزّع نسخة مذكرة سلامة الاتصال: الخاصة بالمشاركين وقم بتعيين سيناريو إلى كل مجموعة من المجموعات. امنح المشاركين 5 دقائق لمناقشة السيناريوهات المعينة إليهم. بعد ذلك، اطلب من المجموعات مشاركة إجاباتهم. تكون الإجابات باللون الأخضر في المذكرة.

المهمة

الجزء الأول

تكليف

اطلب من المشاركين:

1. رسم مخطط زمني ليوم عادي، مع وضع علامة على شبكات Fi-Wi التي يتصلون بها.

2. من الشبكات المحددة المبينة في المخطط الزمني، اطلب من المشاركين اختيار شبكتين وفي فقرة قصيرة لكل منهما، اطلب منهم كتابة وصف للشبكة - الأشخاص الآخرون المتصلون بها؟ ما مدى أمانها؟

3. بالإضافة إلى ذلك - بالنسبة للشبكتين المختارتين - اطلب من المشاركين وصف فرص الاتصال بهاتين الشبكتين وما المخاطر المرتبطة بذلك.