Herkese Açık Wi-Fi

Öğrenciler herkese açık Wi-Fi ağları hakkında bilgi edinecek, ilgili avantajları ve risklerini öğrenecekler. Daha detaylı ifade edersek; güvenli olmayan Wi-Fi ağlarını nasıl tanıyacaklarını öğrenecek, güvenli olmayan Wi-Fi bağlantısı kullandıklarında hangi riskleri aldıklarını anlayacak ve güvenli olmayan Wi-Fi ağlarını kullanma konusunda bilgiye dayalı kararlar verebilecekler.

Kaynaklar

Kablosuz Modem Görseli
Bağlantı Güvenliği Alıştırma Kağıdı

Wi-Fi nedir?

Birinci Bölüm

Öğrencilerinize Sorun

İnternete erişmek için hangi cihazları kullanıyorsunuz?

Bu cihazlar internete nasıl bağlanıyor?

Görsel Sınıf Etkileşimi

Wi-Fi, cihazların internete bağlanması için yaygın olarak kullanılan bir yöntemdir. Wi-Fi, fiziksel veya kablolu bir bağlantı olmadan sadece radyo sinyallerini kullanarak cihazları internete bağlar.

Evinizde internete bağlamak istediğiniz üç tane dizüstü bilgisayarınızın olduğunu düşünün. Bunu yapabilmek için aşağıdakilere ihtiyacınız olacaktır:

1. Bir erişim noktası: Erişim noktası, bir Wi-Fi sinyali ileten (yayınlayan) ve internete erişim sağlayan bir noktadır. Cihazınızın internete bağlanabilmesi için bu sinyalleri alması gerekir. Bazen bir giriş yapmak ve erişim noktasının yayınladığı kablosuz sinyali kullanmak için özel bir izninizin olması gerekebilir (ör. kullanıcı adı ve şifre).

2. Bir yönlendirici: Yönlendirici, belirli bir yerde (okul, kütüphane veya eviniz gibi) bulunan tüm cihazlar (ör. bilgisayarlar, tabletler, cep telefonları) arasında bir ağ oluşturan bir cihazdır. Yönlendiriciler genellikle entegre birer erişim noktasına sahiptir (yukarıdaki şemayı inceleyin).

> Yönlendiricilerin kapsama alanı sınırlıdır. Bu nedenle cihazınız yönlendiriciden çok uzaksa zayıf bir Wi-Fi sinyali alırsınız veya hiç sinyal alamazsınız. Ayrıca yönlendirici ile sizin aranızda bir engel (bir bina veya duvar gibi) olması da sinyal kuvvetini düşürecektir.
>
> Yönlendirici ile kurulan bağlantı bir ağa erişime olanak verir ancak bu internet erişimi anlamına gelmez. Bir ağda bulunan cihazların internete bağlanabilmesi için yönlendiricinin bir modeme bağlanmış olması gerekir.

3. Bir modem: Modem, size internet erişimi sağlamak amacıyla İnternet Hizmet Sağlayıcınız ile bir bağlantı kuran ve bunu sürdüren bir cihazdır. Bulunduğunuz konumun dışından aldığı sinyalleri, bilgisayarınız veya diğer dijital cihazlar tarafından okunabilecek sinyallere dönüştürür.

> Tipik bir kurulumda erişim noktası ve yönlendirici tek bir cihazdır ve Ethernet kablosu adı verilen özel bir kabloyla modeme fiziksel olarak bağlanır. "Kablolu"

internet bağlantısı dendiğinde anlatılmak istenen yapı budur.

Mobil cihazlarda, özellikle de okul, kütüphane veya ev ağı dışındayken internete bağlanmak için hücresel bağlantı da kullanılabilir. Hücresel bağlantılar, yönlendiricilere kıyasla kapsama alanı çok daha geniş olan bir çeşit kablosuz radyo sinyalidir. Hücresel bağlantılar, baz istasyonları adı verilen özel alıcılar kullanarak mobil cihazınızı internete bağlar.

İkinci Bölüm

Öğrencilerinize Sorun

Wi-Fi hangi avantajları sunar?

Wi-Fi kullanmanın bazı dezavantajları nelerdir?

Kablosuz internet bağlantısıyla karşılaştırıldığında, Wi-Fi kullanmakla ilişkili bazı güvenlik endişeleri neler olabilir?

Bir binadan çıktığınızda telefonunuzdaki Wi-Fi erişimini kaybetmenizin nedeni nedir?

Wi-Fi Ağı Seçme

Birinci Bölüm

Öğrencilerinize Sorun

Tüm Wi-Fi ağları güvenli midir? Neden?

Öğrencilerinize Söyleyin

Bazen hangi Wi-Fi ağını kullanmak istediğinizi seçme şansınız olur. Yanlış ağa bağlandığınızda ciddi risklerin oluşabileceğini her zaman aklınızda bulundurmanız çok önemlidir. Güvenli olmayan Wi-Fi ağları giriş için şifre istemeyen ağlardır. Güvenli olmayan bir ağda bulunuyorsanız, aynı ağda olan diğer kişilerin bilgilerinizi görmesi mümkün olabilir. Bu kişiler ağ üzerinden gönderdiğiniz bilgileri çalabilir veya neler yaptığınızı izleyebilirler.

Güvenli ve güvenilir Wi-Fi ağları ise giriş için şifre gerektiren, şifreleme kullanan ve giriş yaptığınız ağın ağ adıyla temsil edilen ağ olduğundan emin olduğunuz ağlardır. Örneğin okulunuzun adını taklit eden bir ağa giriş yapmanız hesap bilgilerinizin açığa çıkmasına neden olabilir. Bu sebeplerle, güvenli ve güvenilir ağlar en yüksek korumayı sağlayan ağlardır.

Göz önüne alınması gereken bir nokta, Wi-Fi ağının çevresindeki koşullar ve konumudur. Örneğin sinemada Wi-Fi bağlantısı ararken telefonunuzda okulunuzun ağ adını görürseniz, bu ağın okulunuzun ağıymış gibi davranarak öğrencilerin şifrelerini toplamaya çalışan kötü amaçlı bir ağ olduğunu düşünmeniz gerekir.

Şifreyle korunan bir Wi-Fi ağı oluştururken, ağ sahibi yönlendiricinin şifreleme protokolünü devreye sokmayı seçmelidir. Yaygın kullanılan şifreleme protokolleri Wired Equivalent Privacy (WEP; Kabloluya Eşdeğer Gizlilik), Wi-Fi Protected Access (WPA; Wi-Fi Korumalı Erişim) veya WPA2'dir. Bu protokoller, ağ üzerinden kablosuz şekilde gönderilen bilgilerin şifrelenmesini (karıştırılmasını) sağlar.

Şifreleme, gönderdiğiniz bilgilerin bilgisayar korsanları tarafından görülmesini zorlaştırmak amacıyla oluşturulmuştur. Ancak tüm bu protokollerin (WEP, WPA ve WPA2) bilgisayar korsanlarına karşı zayıf olduğu görülmüştür. Bu nedenle internetten bilgi gönderirken, internet bağlantılarının da güvenli olduğundan emin olmak çok önemlidir.

HTTPS; internet üzerinden gönderilen verilerin şifrelenmesi için internet siteleri tarafından kullanılan bir standarttır. Şifreleme, üçüncü tarafların bağlantınızdan yararlanarak verilerinizi kolayca görmesini engelleyebilir. Ek bir güvenlik katmanı oluşturur ve kullandığınız URL'nin önüne "https://" eklenerek tüm tarayıcılarda kullanılabilir (ör. https://www.mysite.com). Ancak tüm internet siteleri HTTPS'yi desteklemez.

1. Hassas bilgilerinizi (ör. şifreler, kredi kartı bilgileri) sadece adının önünde HTTPS:// yazan internet sayfalarında girmelisiniz.

2. Yaygın kullanılan birçok tarayıcıda, HTTPS bağlantısını belirtmek için adres çubuğunun yanında kilit görünümlü bir güvenlik göstergesi bulunur.

3. Ancak bazı kötü amaçlı internet sitelerinde de HTTPS desteği bulunduğu için, maalesef HTTPS de güvenliğinizi garanti etmez. HTTPS, bağlantıyı güvenlik altına alır ancak internet sitesinin iyi niyetli olduğunu garanti etmez.

Öğrencilerinize Söyleyin

HTTPS'nin güvenli olmasını sağlayan teknolojiye Güvenli Yuva Katmanı (SSL)/Aktarım Katmanı Güvenliği (TLS) adı verilir. SSL/TLS, gerçek anahtarlara benzer şekilde çalışan dijital şifreleme anahtarları kullanır. Bir sırrınızı bir kağıda yazıp arkadaşınıza verirseniz, bu kağıdı bulan herkes sırrınızı öğrenir. Bunun yerine sırrınızı kilitli bir kutuya koyarak gönderdiğinizi ve arkadaşınıza da kilitli kutuyu açan anahtarın bir kopyasını verdiğinizi düşünün. Kutuyu birileri ele geçirse bile, anahtar olmadan bu kişilerin sırrınızı öğrenmeleri son derece zor olur. Birisi kutuyu benzer bir kutuyla değiştirmeye çalışırsa, anahtarınız işe yaramayacağı için bu durumu anlarsınız. SSL/TLS de bu şekilde çalışır, farkı ise bunu bir internet sitesinde yapmasıdır.

Tarayıcı güvenlik göstergeleri Extended Validation (EV; Genişletilmiş Doğrulama) sertifika bilgilerini de gönderir. EV sertifikaları, kimliklerini bir onay kurumuna doğrulatmış internet sitelerine verilir. Tarayıcılarda EV göstergesi bazen sitenin adı şeklinde veya adres çubuğunun yanında tescil eden kurum bilgisi olarak yer alır. Belirli bir internet sitesindeki içerikten şüpheleniyorsanız, sertifikadaki URL'nin tarayıcıdaki URL ile aynı olup olmadığını "Sertifikayı Görüntüle" seçeneğine tıklayarak kontrol edebilirsiniz. ["Sertifikayı Görüntüle" seçeneğini nasıl bulacaklarını öğrencilere projeksiyon ekranında göstermek faydalı olabilir.] Bu seçeneğe nasıl gideceğiniz tarayıcıya göre farklılık gösterir. Örneğin Chrome'da "Görünüm" -> "Geliştirici" -> "Geliştirici Araçları" kısmındadır. "Geliştirici Araçları" kısmında "Güvenlik" sekmesine ve ardından "Sertifikayı Görüntüle" seçeneğine tıklayın.

Öğrencilerinize Sorun

Yeni bir ağa bağlanırken neleri düşünmeniz gerekir?

1. Olası cevaplara örnekler: Konum (ağ sahibi), erişim (ağa başka kimlerin eriştiği) ve hareket (ağda hangi işlemleri yaptığınız).

Evinizdeki Wi-Fi ağının sahibi kim? Okulunuzdaki? Kahve dükkanındaki?

1. Evinizdeki Wi-Fi ağının sahibi anne-babanız veya bakımınızı sağlayan kişi,

okuldaki ağın sahibi idareciler ve/veya ilçe müdürlüğü ve kahve dükkanındaki ağın sahibi dükkanın sahibidir.

Bu kişileri şahsen tanıyor musunuz? Bu kişilere güveniyor musunuz?

1. Öğrencilerin bu kişilerden hangilerine ne kadar güvendikleri hakkında konuşmasını sağlayın.

Öğrencilerinize Söyleyin

Wi-Fi ağını sisteminde barındıran kişiyi tanımanız ve ona güvenmeniz gerekir. Bazen ağın SSID bilgisini kullanarak ağ sahibinin kim olduğunu tespit edebilirsiniz.

Service Set Identifier (SSID; Servis Seti Tanımlayıcısı), Wi-Fi ağına verilen ve bağlanmaya çalıştığınızda gördüğünüz addır. SSID genellikle ağın sahibini ve ağ hakkındaki diğer detayları belirtmek amacıyla kullanılır. Ancak dikkatli olmalısınız, (nasıl yapıldığını bilen) neredeyse herkes bir SSID oluşturabilir. Örneğin birisi okulda kullandığınız ile aynı olan bir SSID oluşturabilir. Bu durum, kullanıcı adlarını ve şifreleri almak amacıyla bilinen ve güvenilen bir ağı taklit etmeye bir örnektir.

Ağın kimin sisteminde barındırıldığını bilmek, ağın güvenli olup olmadığı konusunda karar vermenize yardımcı olabilir. Ağ güvendiğiniz bir kişiye veya kuruluşa aitse, muhtemelen bağlanma konusunda kendinizi rahatsız hissetmezsiniz. Ancak bilinmeyen bir ağ söz konusuysa, bağlantı kurduğunuz yönlendiricinin kime ait olduğunu bilmediğiniz için bağlantı kurmamanız gerekir. Ağdaki tüm veri trafiği yönlendirici üzerinden gerçekleştiği için, ağ sahibi sizin internet trafiğinizi izleyebilir ve kaydedebilir.

Bir Wi-Fi ağına bağlandığınızda, cihazınız başka cihazların da bulunduğu yerel bir ağa bağlanır ve bu ağ da internete bağlanır. Cihazınız bu ağ ile bilgi alışverişinde bulunduğundan, bağlantıda olduğunuz diğer cihazlara yani ağda bulunan tüm cihazlara güvenmeniz önemlidir. Bu tıpkı okulda yaptığınız grup çalışmaları gibidir; birlikte çalıştığınız kişilere güvenebilmek istersiniz!

Ağ üzerinde şifre kullanılması, ağa bağlanabilecek kişi sayısını sınırlandırabilir. Ağın herkese açık olduğu durumun aksine, burada ağda kimlerin olduğuyla ilgili daha iyi bir tahmin yürütebilirsiniz (aileniz, arkadaşlarınız veya kahve dükkanındaki diğer müşteriler).

Şüpheli görünen bir ağa katılıp katılmama kararınız, internetteki güvenliğinizle ilgili olarak alabileceğiniz risklere bağlıdır. Kendinize "Elimin altındaki bir ağa bağlanmanın verdiği keyifle, hesabımın ele geçirilmesi ihtimalini nasıl karşılaştırmalıyım?" diye sorabilirsiniz.

Öğrencilerinize Sorun

Evinizdeki Wi-Fi ağı üzerinden internetteki haberleri/blogları okumalı mısınız? Okulunuzdaki? Kahve dükkanındaki?

1. İnternet sayfalarındaki içeriklerin genel olarak hassas bilgiler olmadığını açıklayın. Bunu muhtemelen herhangi bir ağda yapabilirsiniz.

Evinizdeki Wi-Fi ağını kullanarak bir kredi kartı numarası göndermeli misiniz? Okulunuzdaki? Kahve dükkanındaki? Neden?

1. Bunu kahve dükkanındaki Wi-Fi yerine evdeki Wi-Fi üzerinden yapmanın neden en güvenli yöntem olduğuyla ilgili konuşulmasını sağlayın. Ayrıca okul ağının güvenilir olabileceği ancak söz konusu bilgi son derece hassas olduğu için bu riske girmeye değmeyebileceği üzerine konuşun.

Evinizdeki Wi-Fi ağını kullanarak kişisel e-postalarınızı kontrol etmeli misiniz? Okulunuzdaki? Kahve dükkanındaki?

1. E-posta hesabının içeriğine bağlı olarak, bunun için en güvenli ağın neden evdeki ağ olduğu üzerine konuşun. Örneğin bazı kişilerin farklı amaçlarla kullandıkları birden fazla e-posta hesabı olabilir (ör. pazarlama/tanıtım e-postaları için bir hesap; aile ve arkadaşlarla yazışmalar için başka bir hesap).

Öğrencilerinize Söyleyin

Şifreler ve banka bilgileri de dahil olmak üzere hassas bilgileri herkese açık ortak bir ağ yerine özel ve güvenli bir ağda ve SSL/TLS kullanan internet sitelerinde göndermek/görüntülemek daha iyidir. Tanımadığınız veya güvenmediğiniz kişiler tarafından da kullanılan ortak bir ağdayken bu özel bilgileri göndermeniz veya bu bilgilere erişmeniz, bu bilgileri riske atar.

Gizlilik kişinin kendi vermesi gereken bir karar olduğu için, hangi bilgilerin neden hassas olduğu veya olmadığı çok net olmayabilir. Bir ağa bağlanıp bağlanmama konusunda karar verirken her durumu kendi koşulları içerisinde değerlendirmek önemlidir. Bir ağa bağlanıp bağlanmama kararını vermeden önce ağın sahibine ve ağa bağlanan diğer kişilere güvenip güvenmediğinizi, internette neler yaptığınızı ve hangi bilgileri paylaştığınızı düşünün.

Güvenli Ağlar ve Güvenli Olmayan Ağlar

Birinci Bölüm

Sınıf Etkileşimi

Lütfen dikkat: Bu etkinliğin içerik kapsamı için bkz. "Etkinlik #2: Bir Wi-Fi ağı seçme." Bu materyaldeki bilgilerin üzerinden tekrar geçme veya bu bölümü atlamayla ilgili kararı tamamen size bırakıyoruz.

Öğrencilerinize Söyleyin

Daha önce de belirttiğimiz gibi, güvenli olmayan Wi-Fi ağları giriş için şifre istemeyen ağlardır. Güvenli olmayan ağları kullanmak, ağ üzerinden aldığınız ve gönderdiğiniz verilerin gizliliğini tehlikeye atar.

Güvenli Wi-Fi ağları ise giriş için şifre gerektiren ve şifreleme kullanan ağlardır. Şifrelemenin kullanılıp kullanılmayacağına da ağı yapılandıran kişi karar verir. Şifreleme, bir ağ üzerinden aldığınız ve gönderdiğiniz bilgileri karıştırır. Böylece aynı Wi-Fi ağındaki bir bilgisayar korsanı için hangi bilgileri gönderdiğinizi ve aldığınızı görmek çok daha zor hale gelir.

Bir ağın güvenli olması, verilerinizin güvende olduğu anlamına gelmez. Güvenli olmayan bir ağ kullanmaktan elbette daha güvenlidir; ancak azimli bir bilgisayar korsanı yine de bilgilerinize erişmenin bir yolunu bulabilir.

Wi-Fi ağları için yaygın olarak kullanılan üç şifreleme protokolü mevcuttur: Wired Equivalent Privacy (WEP; Kabloluya Eşdeğer Gizlilik), Wi-Fi Protected Access (WPA; Wi-Fi Korumalı Erişim) veya WPA2. WEP ve WPA eski protokollerdir ve güvenliği bunlarla sağlayamaya çalışan ağlar güvenli değildir. Ayrıca, WPA2'nin de bilgisayar korsanlığına karşı zayıf olduğu gözlemlenmiştir.

Bilgilerinizin en üst düzeyde korunduğundan emin olmak istiyorsanız, kullandığınız internet sitelerinde SSL/TLS şifreleme yönteminin uygulanıp uygulanmadığını kontrol edin.

Öğrencilerinize Sorun

Kullandığı şifre korumalı bir ağa örnek verebilecek kimse var mı?

1. Örneklerden bazıları evdeki Wi-Fi, okuldaki Wi-Fi ve kafeler gibi herkese açık alanlardaki Wi-Fi ağları olacaktır.

Kullandığı güvenli olmayan bir ağa örnek verebilecek kimse var mı?

Güvenli ağlara hangi örnekleri verebilirsiniz?

Öğrencilerinize Söyleyin

Wi-Fi ağının şifreleme kullanıp kullanmadığını, cihazınızdaki ağ ayarlarını veya kablosuz bağlantı ayarlarını inceleyerek kontrol edebilirsiniz.

İkinci Bölüm

Sınıf Etkileşimi

Bu öğrenme deneyiminden geçmeden önce, internette araştırma yaparak farklı işletim sistemleri için Wi-Fi ağ şifreleme türlerini inceleyin. Ardından bir ağın hangi tür şifreleme kullandığının nasıl bulunacağını gösterin. Örneğin MacOS'ta Sistem Tercihleri -> Ağ -> Wi-Fi Seç konumuna gittikten sonra ilgili ağ adını seçin. Wi-Fi sekmesinde, bilinen ağların listesi ve kullanılan şifreleme türünü belirtilen bir sütun göreceksiniz.

Öğrencilerinize Söyleyin

Tüm bağlantılar aynı değildir. Güvenli olmayan bir ağa herkes bağlanabilir ve ağı kimin kontrol ettiği net değildir. Güvenli olmayan bir ağa katılmak sizi saldırılara açık hale getirir çünkü SSL/TLS bağlantısı kullanmıyorsanız, gönderdiğiniz ve aldığınız bilgiler (sayfalar, şifreler vb.) ağdaki başka biri tarafından görülebilir.

Sınıf Etkileşimi

Öğrencilerinizin teknik bilgi seviyesine göre, Wi-Fi kullanırken ek bir güvenlik katmanı olarak Sanal Özel Ağ (VPN) kullanımı hakkında konuşabilirsiniz. Daha fazla bilgi için lütfen Kaynaklar bölümündeki VPN bağlantılarını inceleyin.

Bağlantı Güvenliğini Anlamak

Bölüm Başlığı

Sınıf Etkileşimi

Öğrencileri 2-3 kişilik gruplara ayırın. Bağlantı Güvenliği: Alıştırma Kağıdını dağıtın ve her gruba bir senaryo verin. Senaryoları üzerinde konuşmaları için öğrencilere 5 dakika verin. Daha sonra gruplardan yanıtlarını paylaşmalarını isteyin. Cevaplar alıştırma kağıdının üzerinde yeşil renkle belirtilir.

Ödev

Birinci Bölüm

Ödev

Öğrencilerden şunları isteyin:

1. Normal bir gün için bir zaman planı yapmalarını ve gün içinde bağlandıkları Wi-Fi ağlarını belirtmelerini isteyin.

2. Zaman planında belirttikleri ağlardan ikisini seçmelerini ve her biri için kısa bir paragrafla ağın özelliklerini ve ağa başka kimlerin bağlandığını açıklamalarını isteyin. Ağ ne kadar güvenli?

3. Seçilen iki ağ için ayrıca, bu ağlara bağlanmanın sunduğu fırsatları ve getirebileceği riskleri açıklamalarını isteyin.