개방형 Wi-Fi

개방형 Wi-Fi 네트워크와 그 장단점을 알아봅니다. 좀 더 구체적으로는 보안되지 않은 Wi-Fi를 인식하고, 보안되지 않은 Wi-Fi 사용의 장단점을 이해하며, 언제 보안되지 않은 Wi-Fi에 연결하여 사용할 것인가에 대해 합리적으로 판단할 수 있게 됩니다.

참고 자료

무선 모뎀 이미지
보안 연결 레슨 자료

Wi-Fi란?

파트 1

질문

어떤 기기를 사용하여 인터넷을 이용하나요?

그 기기는 어떻게 인터넷에 연결되나요?

이미지 준비 및 참고 사항:

Wi-Fi는 기기를 인터넷에 연결하는 일반적인 방법입니다. Wi-Fi는 무선 신호를 사용하여 물리적 연결이나 유선 연결 없이 기기를 연결합니다.

집에 인터넷에 연결하려는 노트북이 3대 있다고 가정해봅시다. 인터넷에 연결하려면 필요한 것이 몇 가지 있습니다.

1. 액세스 포인트: 액세스 포인트는 Wi-Fi 신호를 전송(브로드캐스트)하여 인터넷에 액세스하게 해주는 것을 말합니다. 인터넷에 연결하려면 기기에서 이 신호를 수신해야 합니다. 액세스 포인트를 브로드캐스트하는 무선 신호에 로그인하여 사용하려면 특별한 권한(예: 사용자 이름 및 비밀번호)이 필요할 수도 있습니다.

2. 라우터: 라우터는 주어진 위치(예: 학교, 도서관, 집)에 있는 모든 기기(예: 컴퓨터, 태블릿, 휴대폰) 간에 네트워크를 만드는 기기입니다. 일반적으로 라우터에는 액세스 포인트가 내장되어 있습니다(위 다이어그램 참조).

    라우터의 범위는 제한되어 있으며 대개 범위가 좁기 때문에 기기가 라우터에서 너무 멀리 떨어져 있는 경우 Wi-Fi 신호가 약하거나 전혀 수신되지 않기도 합니다. 또한 건물이나 벽돌 벽처럼 라우터와 사용자 사이에 가로막은 것이 있으면 신호의 강도가 줄어듭니다.

    라우터에 연결하면 네트워크에 액세스할 수 있지만 이것이 인터넷 액세스를 의미하지는 않습니다. 네트워크에 있는 여러 기기에서 인터넷에 연결하려면 라우터를 모뎀에 연결해야 합니다.

3. 모뎀: 모뎀은 인터넷 서비스 공급자(ISP)에 연결하여 인터넷에 액세스할 수 있도록 해주는 기기입니다. 주어진 위치의 외부에서 신호를 컴퓨터 및 기타 디지털 기기에서 읽을 수 있는 신호로 변환합니다.

    일반적인 설정에서 액세스 포인트와 라우터는 이더넷 케이블이라는 특수한 케이블을 사용하여 모뎀에 물리적으로 연결된 하나의 기기입니다. 이 기기가 바로 '유선' 인터넷 연결을 이야기할 때 언급되는 기기입니다.

    학교, 도서관 또는 집의 네트워크를 벗어났을 때 모바일 기기에서는 무선 연결을

사용하여 인터넷에 연결할 수 있습니다. 무선 연결은 라우터보다 도달하는 영역이 넓은 일종의 무선 라디오 신호입니다. 무선 연결은 모바일 기기를 인터넷에 연결하기 위해 '셀 타워'라고 하는 특정 송수신기를 사용합니다.

파트 2

질문

Wi-Fi의 장점은 무엇일까요?

Wi-Fi의 단점으로는 어떤 것들이 있을까요?

유선 인터넷 연결과 비교했을 때 Wi-Fi를 사용하는 경우 어떤 보안 문제가 발생할 수 있나요?

건물을 벗어나면 휴대폰에 연결되어 있던 Wi-Fi 액세스가 해제되는 이유가 무엇일까요?

Wi-Fi 네트워크 선택하기

파트 1

질문

모든 Wi-Fi 네트워크가 안전한가요? 그 이유는 무엇인가요?

설명 및 활동 안내

사용할 Wi-Fi 네트워크를 선택해야 하는 경우도 있습니다. 잘못된 네트워크에 연결하면 심각한 위험이 따른다는 점을 기억하는 것이 중요합니다. 예를 들어, 보안되지 않은 Wi-Fi 네트워크는 비밀번호 없이 로그인할 수 있는 네트워크입니다. 이런 네트워크를 사용하는 경우 동일한 네트워크에 있는 다른 사람들이 여러분의 정보를 볼 수 있으며 네트워크를 통해 전송하는 정보를 훔치거나 여러분이 하는 활동을 감시할 수 있습니다.

반면에 안전하고 신뢰할 수 있는 Wi-Fi 네트워크는 비밀번호를 요구하고 암호화되며 로그인하는 네트워크가 네트워크 이름이 실제로 지칭하는 것과 동일하다고 확신할 수 있는 네트워크입니다. 예를 들어 학교 네트워크의 이름을 도용한 네트워크에 로그인하면 계정 정보가 공개될 수 있습니다. 따라서 안전하고 신뢰할 수 있는 네트워크는 가장 많은 보호 기능을 제공하는 네트워크입니다.

한 가지 고려해야 할 점은 Wi-Fi 네트워크의 상황 또는 위치입니다. 예를 들어, 영화관에서 Wi-Fi 연결을 찾고 있는데 휴대폰에 학교 네트워크 이름이 표시된다면 이를 의심하지 못하는 학생에게서 비밀번호를 수집하기 위해 학교 네트워크를 모방하거나 '스푸핑'하는 것은 아닌지 생각해볼 수 있습니다.

비밀번호로 보호된 Wi-Fi 네트워크를 설정하는 경우 소유자는 라우터의 암호화 프로토콜을 켜야 합니다. 일반적인 암호화 프로토콜에는 WEP(Wired Equivalent Privacy, 유선급 보호), WPA(Wi-Fi Protected Access, Wi-Fi 보호 접속) 또는 WPA2가 있습니다. 이러한 프로토콜은 네트워크를 통해 무선으로 전송되는 정보가 암호화('스크램블')되도록 합니다.

암호화는 해커들이 전송 내용을 쉽게 보지 못하도록 고안된 것이지만 위에 언급한 모든 프로토콜(WEP, WPA, WPA2)은 해킹에 취약한 것으로 드러났습니다. 따라서 온라인으로 정보를 보내는 경우 보안 웹 연결을 사용하는 것이 중요합니다.

HTTPS는 웹사이트에서 인터넷을 통해 전송되는 데이터를 암호화하는 데 사용하는 표준입니다. 암호화를 사용하면 연결 상태에서 전송되는 데이터를 제삼자가 쉽게 볼 수 없습니다. HTTPS는 보안 단계를 한층 더하며 사용하는 URL 앞에 'https://'만 추가하면 모든 브라우저에서 사용할 수 있습니다(예: https://www.mysite.com). 그러나 모든 웹사이트에서 HTTPS를 지원하는 것은 아닙니다.

1. 'HTTPS://'가 주소 앞에 있는 웹페이지에서만 중요한 정보(예: 비밀번호, 신용카드 정보)를 입력해야 합니다.

2. 대부분의 주요 브라우저에는 HTTPS 연결을 나타내기 위해 주소창 주변에 자물쇠처럼 보이는 보안 표시가 있습니다.

3. 안타깝게도 일부 악성 웹사이트에서도 HTTPS를 지원할 수 있으므로 HTTPS가 반드시 안전을 보장하는 것은 아닙니다. HTTPS는 인터넷 연결을 보호하지만 웹사이트가 악성이 아니라는 점을 보장할 수는 없습니다.

설명 및 활동 안내

SSL(Secure Sockets Layer, 보안 소켓 계층)/TLS(Transport Layer Security, 전송 계층 보안)는 HTTPS를 안전하게 유지하는 기술을 가리키는 이름입니다. SSL/TLS는 실제 열쇠와 거의 유사한 디지털 암호화 키를 사용합니다. 여러분이 친구에게만 알리고 싶은 비밀을 종이에 적었다면, 그 종이를 발견한 사람은 누구나 여러분의 비밀을 볼 수 있게 됩니다 하지만 친구에게 복제한 열쇠를 준 다음 열쇠가 맞는 상자에 비밀을 넣어 보냈다고 가정해보세요. 누군가가 상자를 훔쳐도 열쇠가 없으면 비밀을 보기가 어려울 것입니다. 누군가가 상자를 비슷한 것으로 바꾸려고 해도 여러분은 열쇠가 작동하지 않을 것임을 알고 있을 겁니다. SSL/TLS는 이러한 방식으로 웹사이트에서 작동합니다.

브라우저 보안 표시도 EV(Extended Validation, 확장 검증) 인증서 정보를 알립니다. EV 인증서는 인증 기관이 신원을 확인한 웹사이트에 제공됩니다. EV 표시는 브라우저의 주소창 옆에 사이트 이름이나 등록 항목의 형태로 나타나는 경우가 있습니다. 특정 웹사이트의 콘텐츠가 의심스러운 경우 '인증서 보기'를 클릭하여 인증서의 URL이 브라우저의 URL과 일치하는지 확인할 수 있습니다. [프로젝션 화면으로 참가자에게 '인증서 보기'를 찾는 방법을 보여주면 도움이 될 수 있습니다.] '인증서 보기'를 찾는 방법은 브라우저에 따라 다릅니다. 예를 들어 Chrome의 경우 '보기'에서 '개발자'를 클릭한 다음 '개발자 도구'를 클릭합니다. 그런 후, '개발자 도구'에서 '보안' 탭을 클릭한 다음 '인증서 보기'를 클릭합니다.

질문

새로운 네트워크에 연결할 때 생각해봐야 할 것은 무엇일까요?

1. 예상 답변: 위치(네트워크 소유자), 액세스(네트워크에 연결된 다른 사람) 및 활동(네트워크에서 하고 있는 작업) 등.

가정 Wi-Fi 네트워크를 누가 소유하나요? 학교에서는 어떤가요? 카페에서는 어떤가요?

1. 가정에서는 부모님/보호자가, 학교에서는 관리자/관할 지역이, 카페에서는 카페 주인이 Wi-Fi 네트워크를 소유합니다.

이 사람들을 개인적으로 알고 있나요? 이 사람들을 신뢰하나요?

1. 참가자가 이 사람들을 각각 어느 정도 신뢰하는지에 대해 토론하도록 합니다.

설명 및 활동 안내

Wi-Fi 네트워크를 호스팅하는 사람이 누구인지 알고 신뢰할 수 있어야 합니다. 네트워크의 SSID를 사용하는 소유자가 누구인지 확인할 수 있는 경우도 있습니다.

SSID(Service Set Identifier, 서비스 세트 식별자)는 연결을 시도할 때 확인할 수 있는 Wi-Fi 네트워크에 주어진 이름입니다. SSID는 종종 네트워크를 소유한 사람과 네트워크에 대한 기타 상세 정보를 전송하는 데 사용됩니다. 방법을 아는 거의 모든 사람이 SSID를 만들 수 있으므로 주의해야 합니다. 예를 들어 누군가가 학교에서 사용하는 SSID와 동일한 SSID를 만들 수 있습니다. 이것은 사용자 이름과 비밀번호를 수집하기 위해 알려져 있고 신뢰할 수 있는 네트워크를 사칭하는 사례입니다.

어떤 사람이 네트워크를 호스팅하는지 알고 있다면 네트워크 안전성을 판단하는 데 도움이 됩니다. 네트워크를 호스팅하는 사람이 여러분이 믿을 수 있는 사람 또는 단체에 소속되어 있는 경우 편안하게 연결할 수 있을 것입니다. 그러나 알 수 없는 네트워크인 경우에는 연결하려는 라우터를 누가 소유하고 있는지 모르므로 연결해서는 안 됩니다. 네트워크의 모든 트래픽이 라우터를 통과하므로 소유자가 웹 트래픽을 모니터링하거나 기록할 수 있습니다.

Wi-Fi에 연결하면 기기가 로컬 기기 네트워크에 연결되며 해당 네트워크는 더 넓은 인터넷에 연결됩니다. 기기가 해당 네트워크와 정보를 교환하고 있으므로 연결된 다른 기기를 신뢰하는 것이 중요하며, 이것은 네트워크에 있는 모든 기기를 신뢰해야 한다는 것을 의미합니다. 이것은 학교에서 하는 그룹 프로젝트와 유사합니다. 여러분은 함께 프로젝트를 진행하는 사람을 신뢰할 수 있길 원할 것입니다.

네트워크에서 비밀번호를 사용하면 연결할 수 있는 사람을 제한할 수 있습니다. 즉, 네트워크를 완전히 공개할 때보다 비밀번호를 사용하는 경우에는 가족이든 친구든 카페의 다른 고객이든 네트워크에 있는 사람을 더 잘 알 수 있다는 것을 의미합니다.

의심스러워 보이는 네트워크를 사용할지, 사용하지 않을지 선택은 온라인 보안 측면에서 위험을 얼마나 감수할지에 달려 있습니다. 사용 가능한 네트워크를 사용하여 얻는 편리함과 계정이 침해될 가능성 사이에서 어떻게 결정을 내려야 할까요?

질문

가정 Wi-Fi 네트워크를 사용하여 온라인 뉴스/블로그를 읽어야 할까요? 학교에서는 어떤가요? 카페에서는 어떤가요?

1. 웹페이지의 내용은 일반적으로 민감한 정보가 아니라는 점을 설명합니다. 이런 활동은 어느 네트워크에서나 할 수 있습니다.

가정 Wi-Fi 네트워크를 사용하여 신용카드 번호를 전송해야 할까요? 학교에서는 어떤가요? 카페에서는 어떤가요? 그 이유는 무엇인가요?

1. 카페 Wi-Fi가 아닌 가정 Wi-Fi를 사용하는 것이 가장 안전한 이유에 대해 토론하세요. 또한 학교 네트워크는 신뢰할 수도 있지만 이러한 정보는 매우 민감하므로 위험을 감수하지 않는 것이 좋을 수 있습니다.

가정 Wi-Fi 네트워크를 사용하여 개인 이메일을 확인해야 할까요? 학교에서는 어떤가요? 카페에서는 어떤가요?

1. 이메일 계정의 내용에 따라 가정 네트워크에서 내용을 확인하는 것이 가장 안전한 이유에 대해 토론하세요. 예를 들어 용도가 다른 이메일 계정을 여러 개 가지고 있는 사람도 있을 수 있습니다(예: 마케팅/프로모션을 위한 이메일 계정과 친구 및 가족을 위한 다른 이메일 계정).

설명 및 활동 안내

비밀번호와 금융 정보를 비롯한 민감한 정보는 공유된 개방형 네트워크보다는 SSL/TLS를 사용하는 웹사이트에서 비공개 보안 네트워크를 통해 전송하고 확인하는 것이 좋습니다. 이러한 개인 정보는 사용자가 모르고 신뢰할 수 없는 사람들이 사용하는 개방형 네트워크를 사용하여 제출하거나 액세스하는 경우 위험할 수 있습니다.

개인 정보는 스스로 결정해야 하는 개인적인 판단이므로 정보가 민감하거나 민감하지 않은 정도는 명확하지 않을 수도 있습니다. 네트워크에 연결할지 판단하기 위해 각 상황을 자체적으로 고려하는 것이 중요합니다. 판단하기 전에 네트워크의 소유자와 네트워크에 연결된 다른 사람을 신뢰할 수 있는지와 온라인에서 하는 활동, 공유하는 정보가 무엇인지 자문해보세요.

보안 네트워크와 보안되지 않은 네트워크

파트 1

준비 및 참고 사항

참고: 이 활동의 일부 내용은 '활동 #2: Wi-Fi 네트워크 선택하기'에서 다뤘습니다. 이 자료를 다시 검토하거나 건너뛰는 것은 여러분의 판단에 달려 있습니다.

설명 및 활동 안내

이전에 언급했듯이 보안되지 않은 Wi-Fi 네트워크는 로그인할 때 비밀번호를 요구하지 않는 네트워크입니다. 보안되지 않은 네트워크를 사용하면 네트워크를 통해 전송하거나 수신하는 데이터가 위험해질 수 있습니다.

보안된 Wi-Fi 네트워크는 비밀번호를 요구하며 암호화가 활성화되어 있습니다. 네트워크를 구성한 사람이 암호화 사용 여부를 선택합니다. 암호화는 네트워크를 통해 주고받는 정보를 뒤섞으므로 동일한 Wi-Fi 네트워크를 사용하는 해커가 여러분이 주고받는 정보를 보는 것이 훨씬 어렵습니다.

네트워크가 보호되었다고 해서 데이터가 안전하다는 것을 의미하지는 않습니다. 보안되지 않은 네트워크를 사용하는 것보다는 확실히 안전하지만 집요한 해커는 여전히 여러분의 정보에 액세스하는 방법을 찾아낼 수 있습니다.

일반적인 세 가지 암호화 프로토콜에는 WEP(Wired Equivalent Privacy, 유선급 보호), WPA(Wi-Fi Protected Access, Wi-Fi 보호 접속) 또는 WPA2가 있습니다. WEP와 WPA는 예전 방식으로, 여기에 의존하는 네트워크는 안전하지 않다고 간주해야 합니다. 또한 WPA2는 해킹에 취약한 것으로 나타났습니다.

정보를 최대한 보호하려면 사용하고 있는 웹사이트가 SSL/TLS를 사용하여 암호화되어 있는지 확인하세요.

질문

비밀번호로 보호된 네트워크를 사용해본 경험을 예로 들 수 있나요?

1. 가정 Wi-Fi, 학교 Wi-Fi, 카페와 같은 일부 공공장소의 Wi-Fi 네트워크 등이 그 예가 될 수 있습니다.

보안되지 않은 네트워크를 사용해본 경험을 예로 들 수 있나요?

보안된 네트워크의 예를 들 수 있나요?

설명 및 활동 안내

기기의 네트워크 또는 무선 설정을 검토하여 Wi-Fi 네트워크의 암호화 여부를 확인할 수 있습니다.

파트 2

준비 및 참고 사항

학습을 시작하기 전에 인터넷으로 검색하여 여러 운영 체제에서 Wi-Fi 네트워크 암호화 유형을 확인하는 방법을 검토합니다. 그런 다음 네트워크에서 어떤 종류의 암호화를 사용하는지 확인하는 방법을 보여줍니다. 예를 들어 MacOS의 경우 '시스템 환경설정' -> '네트워크' -> 'Wi-Fi 선택'에서 적절한 네트워크 이름을 클릭합니다. Wi-Fi 탭 아래 알려진 네트워크 리스트와 사용된 암호화 유형을 나타내는 열이 있습니다.

설명 및 활동 안내

연결마다 차이가 있을 수 있습니다. 네트워크 보안이 해제되면 누구나 네트워크에 연결할 수 있으므로 네트워크를 제어하는 사람이 명확하지 않습니다. 보안되지 않은 네트워크를 사용하는 경우 SSL/TLS 연결을 사용하지 않으면 웹 트래픽(페이지, 비밀번호 등)과 같이 주고받는 정보를 네트워크의 모든 사용자가 볼 수 있으므로 보안이 취약해질 수 있습니다.

준비 및 참고 사항

참가자의 기술 지식에 따라 Wi-Fi를 사용할 때 VPN(Virtual Private Networks, 가상 사설망) 사용과 관련된 추가 보안을 논의해보세요. 자세한 정보는 참고 자료 섹션의 VPN 링크를 참조하세요.

보안 연결 인식하기

파트 제목

준비 및 참고 사항

참가자를 2~3명씩 그룹으로 나눕니다. 보안 연결 레슨 자료를 나누어준 다음 각 그룹에 시나리오를 정해줍니다. 시나리오에 대한 토론을 5분 동안 완료하도록 합니다. 그런 다음, 의견을 그룹과 공유하도록 합니다. 답변은 레슨 자료에 초록색으로 표시되어 있습니다.

과제

파트 1

과제

참가자에게 다음과 같이 하도록 안내합니다.

1. 일반적인 하루의 타임라인을 그리고 연결하는 Wi-Fi 네트워크를 표시합니다.

2. 타임라인에 표시한 네트워크 중에서 두 가지를 선택하고 각각에 대해 짧은 단락을 작성하여 설명합니다. 누가 해당 네트워크에 연결되어 있나요? 보안 수준은 어떤가요?

3. 또한 선택한 두 네트워크에 대해 해당 네트워크에 연결했을 때 따르는 장점과 위험이 무엇인지 설명합니다.