공공 Wi-Fi 를 안전하게 사용하기 위한 팁

불순한 의도가 있는 사람이 온라인상에서 사용자 정보를 악용할 수 있습니다. 공공 Wi-Fi 를 사용해야 하는 경우, 고려해야 할 팁을 아래에서 읽어보십시오.

코로나바이러스 발생으로 인한 사업체와 도서관이 폐쇄 이후 많은 사람들이 온라인에서 시간을 보내고 있습니다. 그 결과로 인터넷 연결을 위해 공공 Wi-Fi 를 사용해야 할 수 있습니다. 공공 Wi-Fi 를 사용해야 하는 경우, 주 최고 개인정보 보호 담당자(Chief Privacy Officer) 의 다음 권장 사항을 참고하여 데이터를 보호하시기 바랍니다:

1. 네트워크가 올바른지 확인하십시오.

올바른 네트워크에 연결되어 있는지 확인하십시오. 불순한 의도가 있는 사람이 이름만 보면 무해해 보이지만 실제로는 사용자의 인터넷 이용 내역을 훔쳐볼 수 있는 네트워크 설정에 연결하도록 유도하는 네트워크를 만들 수 있습니다. 즉, 사용자가 웹사이트의 로그인 자격 증명이나 비밀번호를 입력하면, 해커가 사용자 정보를 도용할 수 있습니다. 이 문제를 방지하려면 네트워크 이름을 주의 깊게 읽고, 가능하면 직원에게 문의하거나 사업체의 사이니지를 확인하여 네트워크가 합법적인지 확인하십시오.

친숙한 커피 체인 같은 잘 알려진 네트워크는 해당 기업이 사업체와 함께 네트워크를 서비스 형태로 운영하기 때문에 의심을 덜 받을 가능성이 높습니다. 알려진 네트워크는 일반적으로 공공 장소에서 전화기에 표시되는 임의의 무료 Wi-Fi 네트워크보다 안전합니다.

2. 자동 연결 기능을 끄십시오.

많은 장치(스마트폰, 노트북, 태블릿)에는 자동 연결 설정 기능이 있습니다. 이러한 설정 기능을 사용하면 장치를 주변 네트워크에 편리하게 연결할 수 있습니다. 신뢰할 수 있는 네트워크에 연결되는 경우에는 문제가 없지만, 장치가 안전하지 않은 네트워크에 연결될 수도 있습니다. 장치의 설정에서 이러한 기능을 비활성화할 수 있습니다. 특히 낯선 장소를 여행하는 경우 이러한 설정을 해제한 상태로 유지하십시오. 추가적인 예방 조치로 공공 Wi-Fi 를 사용한 후 “네트워크 삭제”를 체크할 수 있습니다.

또한 공공 장소에 있는 동안에는 Bluetooth 를 모니터링해야 합니다. Bluetooth 연결을 사용하면 다양한 장치가 서로 통신할 수 있으며, 해커가 열려 있는 Bluetooth 신호를 검색하여 장치에 액세스할 수 있습니다. 익숙하지 않은 지역에 있을 때는 전화기와 다른 장치에서 이러한 기능을 꺼놓으십시오.

3. 파일 공유를 해제하십시오.

공공 Wi-Fi 를 사용하는 동안에는 파일 공유 옵션을 해제해야 합니다. 운영 체제에 따라 시스템 기본 설정 또는 제어판에서 파일 공유를 해제할 수 있습니다. AirDrop 은 해제해야 하는 파일 공유 기능의 예입니다. Windows/PC 등의 일부 운영 체제에서는 새 공공 네트워크에 처음 연결할 때 "공개" 옵션을 선택하여 파일 공유를 해제합니다.

파일 공유 해제 단계

PC 에서:

1. 네트워크 및 공유 센터로 이동합니다.
2. 그런 다음 고급 공유 설정을 변경합니다.
3. 파일 및 프린터 공유를 끕니다.

Macs 에서:

1. 시스템 기본 설정으로 이동합니다.
2. 공유를 선택합니다.
3. 모든 것을 선택 해제합니다.
4. 파인더 에서 AirDrop 을 클릭하고 상대가 나를 발견하도록 허용(Allow me to be discovered by): 수신 끔(No One)을 선택합니다.

iOS 의 경우 통제실 에서 AirDrop 을 찾아서 끕니다.

4. VPN 을 사용하십시오.

장치에 VPN(가상사설망)을 설치하십시오. VPN 은 공공 Wi-Fi 의 디지털 개인정보 보호를 위한 가장 안전한 옵션입니다. VPN 은 장치를 통해 데이터를 주고받을 때 데이터를 암호화하고 네트워크를 통과할 때 데이터가 보이지 않도록 보호하는 "터널"의 역할을 합니다.

5. 암호화 된 웹사이트에 대한 FBI 경고 – HTTPS.

FBI 는 주소가 "https"로 시작하는 웹 사이트에 대해 경고했습니다. "https"와 자물쇠 아이콘이 있는 것은 웹 트래픽이 암호화되어 있으며 방문자가 안전하게 데이터를 공유할 수 있음을 나타냅니다. 하지만 이제 사이버 범죄자는 사람들의 신뢰를 이용해 https 가 포함되어 있고, 안전하지 않지만 안전해 보이는 악의적인 웹사이트로 사람들을 유인하는 방식을 사용합니다.

FBI 의 권장 사항:

- 이메일상의 이름을 단순하게 신뢰하지 마십시오: 이메일 내용의 의도에 의문을 제기하십시오.
- 알려진 연락처로부터 링크가 포함된 의심스러운 이메일을 수신한 경우, 연락처에 전화하거나 이메일을 보내 해당 메시지가 올바른 것인지 확인하십시오. 의심스러운 이메일에 바로 회신하지 마십시오.
- 링크에 철자가 틀리거나 잘못된 도메인이 있는지 확인하십시오(예: ".gov"로 끝나야 하는 주소가 ".com"으로 끝나는 경우).
- 브라우저 주소 표시줄에 자물쇠 아이콘 또는 "https"가 있다고 해서 웹사이트를 신뢰하지 마십시오.

6. 민감한 정보에는 액세스하지 않는 것이 좋습니다.

VPN 이 있더라도 개인 은행 계좌 또는 보안되지 않은 공공 네트워크의 사회 보장 번호 같은 민감한 개인 데이터에는 액세스하지 않는 것이 좋습니다. 공공 보안 네트워크라 해도 위험할 수 있습니다. 공공 Wi-Fi 에서 이러한 계정에 액세스해야 하는 경우 최선의 판단을 하십시오. 금융 거래를 하는 경우 스마트폰의 핫스팟 기능을 대신 사용하는 것이 더 나을 수 있습니다.

7. 보안 Wi-Fi 대 무보안 Wi-Fi.

기본적으로 공공 Wi-Fi 네트워크의 종류는 두 가지입니다: 보안 Wi-Fi 와 무보안 Wi-Fi.

가능하면 보안 공공 네트워크에 연결하십시오. 무보안 네트워크는 비밀번호나 로그인 같은 보안 기능을 사용하지 않고 연결할 수 있습니다. 보안 네트워크에서는 일반적으로 사용자가 네트워크에 연결하기 전에 이용 약관에 동의하거나, 계정을 등록하거나, 비밀번호를 입력해야 합니다.

8. 방화벽을 활성화하십시오.

노트북을 사용하는 경우 공공 Wi-Fi 에서 방화벽을 사용하도록 설정하십시오. 방화벽은 장치를 악성 프로그램의 위협으로부터 보호하는 장벽 역할을 합니다. 사용자는 팝업 및 알림 때문에 Windows 방화벽을 사용하지 않도록 설정한 다음 잊어버릴 수 있습니다. PC 에서 해당 기능을 다시 시작하려면 제어판의 "시스템 및 보안"으로 이동하여 "Windows 방화벽"을 선택하십시오. Mac 사용자인 경우 "시스템 기본 설정" – "보안 및 개인 정보" – "방화벽" 탭으로 이동하여 기능을 활성화하십시오.

9. 바이러스 백신 소프트웨어를 사용하십시오.

또한 노트북에 최신 버전의 바이러스 백신 프로그램을 설치하십시오. 바이러스 백신 프로그램은 공유 네트워크를 사용하는 동안 시스템에 침투할 수 있는 악성 프로그램을 탐지하여 공공 Wi-Fi 를 사용하는 동안 사용자를 보호할 수 있습니다. 알려진 바이러스가 장치에 로드되어 있거나 의심스러운 활동, 공격 또는 악성 프로그램이 시스템에 침입하는 경우 경고가 표시됩니다.

10. 이중 인증 또는 다중 인증을 사용하십시오.

개인 정보로 웹사이트에 로그인할 때 다중 인증(MFA)을 사용하십시오. 이는 사용자를 더욱 잘 보호해주는 두 번째 인증 코드(전화기에 문자로 발송되거나 앱 또는 물리적 키로 제공됨)가 있다는 것을 의미합니다. 따라서 해커가 사용자 이름과 비밀번호를 획득하더라도 인증 코드가 없으면 사용자의 계정에 액세스할 수 없습니다.

11. 개인 장치를 추적하십시오.

공공 장소나 차량에 노트북, 태블릿 또는 스마트 폰을 방치하지 마십시오. Wi-Fi 네트워크에서 예방 조치를 취하더라도 다른 사람이 사용자의 소유물을 가져가거나 정보를 훔쳐보는 것을 막을 수는 없습니다. 주변 환경에 주의하고 주변에 있는 사람들을 신경 쓰십시오.

12. 다른 온라인 안전 팁.

특히 공공 Wi-Fi 연결을 사용하는 경우, 온라인 상태를 안전하게 유지하는 데 도움되는 몇 가지 팁을 소개합니다:

- 강력한 비밀번호를 사용하십시오.
- 장치를 암호화하십시오.
- 피싱 이메일에 주의하십시오.
- 소셜 미디어에 올리는 내용에 주의하십시오. 너무 많은 개인정보를 노출하면 해커가 비밀번호를 추측할 수도 있습니다.
- 더 이상 필요 없는 오래된 정보를 삭제하십시오.
- 네트워크에 추가 소프트웨어 또는 브라우저 확장 프로그램을 설치하라는 메시지가 표시되면 연결하지 마십시오.
- 알려진 문제로부터 보호하기 위해 장치에 최신 패치 및 소프트웨어 업데이트가 설치되어 있는지 확인하십시오.