**방화벽을 선택하고 접근을 제한합니다**

**대부분 기업은 회사 방화벽을 갖추고 직원의 접근을 제한합니다. 즉, 개별 PC와 특정 웹 사이트가 방화벽을 통과할 수 있는지는 사무실 네트워크를 보호하는 중요한 단계입니다. 그뿐만 아니라 일부 방화벽에는 통합 VPN이 함께 제공됩니다. 이는 VPN이 제공하는 암호화로 인해 더 많은 보호 기능을 제공합니다. VPN이 없는 기업은 직원 PC와 서버 간 보안 장벽으로 사용할 수 있으므로 서버 접근 시 암호화된 통로에서 컴퓨터가 작동하도록 사무실 네트워크에 설치해야 합니다. 사용할 수 있는 무료 옵션이 있지만 최적의 보호 기능을 제공하려면 유료 VPN을 사용해서 항상 철통 보안 상태를 유지하는 것이 좋습니다.**[**VPN이 가진 강력한 암호화 및 보안 기능**](https://www.expressvpn.com/kr/what-is-vpn/vpn-encryption)**에 대해 더 자세히 알아보고 싶으시면 링크를 참조하시기 바랍니다.**

​

**매일 안티바이러스를 업데이트합니다**

**인생에서 대부분의 일과 마찬가지로 정기적인 유지 관리는 모든 것을 잘 운영되는 상태로 유지하는 데 중요합니다. 매일 바이러스 백신을 업데이트하는 일은 해커가 현재 보호 조치가 적용되지 않는 새로운 위협에 대한 자동 업데이트를 사용하지 않도록 설정해 예기치 않게 보호 기능이 저하되는 것을 방지해 줍니다. 기업은 최신 바이러스 백신 소프트웨어를 좇아가기보다는 출현하는 위협, 최신 바이러스, 일일 소프트웨어 업데이트에 지속해서 대처해야 이 문제를 해결하는 데 도움이 됩니다.**

​

**서버 접근을 제한합니다**

**서버를 여러 구획으로 나눠야 합니다. 현업 부서에서 부서별로 구분할 수 있으므로 각 컴퓨터 및 직원 로그인은 서버의 관련 부분에만 접근할 수 있도록 해야 합니다. 또한 기업은 퇴사 직원 계정을 비활성화하여 해커가 비활성 계정이나 사무실 네트워크에서 악의적인 활동을 수행했다고 인정된 퇴사자를 통해 침입할 가능성을 제한해야 합니다.**

​

**서버에 승인된 노트북만 접근을 허용합니다**

**기업에서는 서버의 특정 파일에 대한 접근을 제한할 수 있지만 승인되지 않은 외부 노트북, 태블릿, 스마트 기기를 제외하는 것도 고려해야 합니다. 이는 직원이 사무실 PC에서 서버 정보를 볼 수 있지만 외부 기기를 가져올 경우 방문자 와이파이에만 접근할 수 있으며 사무실 관리자나 IT관리자의 승인 없이는 서버 접근 권한이 전혀 없음을 의미합니다. 이는 사무실 서버에 저장된 데이터를 보호하기 위한 또 다른 단계입니다.**

​

**웹 사이트를 차단합니다**

**직원의 인터넷 사용을 제한하면 일부 웹 사이트에서 발견되는 바이러스와 악성 콘텐츠로부터 사무실 네트워크를 보호할 수 있습니다. 게다가 전반적인 연결 속도를 높이는 데도 도움이 됩니다.악의적인 웹 사이트를 차단할 방법은 여러 가지가 있지만, 가장 많이 사용되는 방법은 라우터를 사용하거나 개별 IP 주소와 방화벽 필터링을 사용하는 것입니다. 모든 방화벽은 다르지만 대부분 웹 사이트는 '필터링' 탭을 통해 차단할 수 있습니다.**

​

**와이파이에 암호를 겁니다.**

**사무실 보안을 강화하는 가장 마지막 방법은 와이파이에 암호를 거는 것입니다. 와이파이에 암호를 걸게되면 누군가 쉽게 연결해서 네트워크가 열리지 않도록 할 수 있습니다. 이렇게 하려면 사무실 네트워크에 WPA 또는 WPA2 보안의 엔터프라이즈 모드를 사용하는 것이 좋습니다. 이는 직원이 암호를 볼 수 없도록 하기 위한 것입니다. 또한 암호가 분실되거나 도난당한 경우 여러 컴퓨터 기기에 암호가 저장되지 않으므로 해킹당할 가능성이 줄어들게 됩니다.**

​

**일반적이지 않은 SSID 네트워크 이름을 사용합니다**

**공통 SSID를 사용하면 해커가 모든 네트워크에 쉽게 접근할 수 있습니다. 가장 기본적인 와이파이 네트워크 설정 중 하나로서, 회사명이나 공급 업체 이름처럼 쉽게 추축할 수 있는 이름은 사용하지 않는 것이 좋습니다. 특히 사무실이 공유 오피스 건물에 입주하여 있다면 해커는 이를 쉽게 눈에 띄고 공격을 가해올 수 있습니다. 이와 더불어 SSID 브로드 캐스트를 끄기만 하면 해커가 다른 네트워크 트래픽을 통해 올바른 도구에 접근할 수 있다는 것을 항상 염두해두는 것이 좋습니다.**