

# 사무실 안과 밖에서 조직을 안전하게 지키는 방법

재택 근무를 하든 사무실에서 근무하든, 보안은 조직에서 가장 중요한 문제입니다. 집과 사무실은 아주 다르게 느껴질 수 있지만 어디서 일하든 상관없이 동일한 예방 조치를 사용할 수 있습니다. 아래에서는 몇 가지 중요한 사이버 보안 규칙에 대해 알아보고 해당 규칙이 사무실에서 그리고 재택 근무 시 어떻게 사용될 수 있는지 살펴보겠습니다.

## 안전한 기기만 사용

- 기기의 보안은 기기에서 실행되는 앱의 보안 수준에 달려 있습니다. 애플리케이션이나 플러그인은 먼저 IT 부서에 확인한 후 설치하십시오.
- 업무용 기기는 업무용으로만 사용하십시오. 개인 컴퓨터를 업무용으로 사용하는 경우, 고유한 사용자 이름 및 암호가 지정된 별도의 사용자 계정을 생성하는 것이 좋습니다.
- 사무실의 경우 네트워크 보안은 IT 부서에서 관리할 것입니다. 집에서 인터넷 연결을 안전하게 유지하려면 라우터에 복잡한 암호를 사용하십시오. 조직에서 가상 사설망(VPN)에 대한 액세스를 제공하는 경우에는 VPN에도 연결하십시오.

## 물리적 작업 공간 보호

- 사무실에서는 피기배킹 및 테일게이팅을 조심하십시오. 피기배킹은 누군가 조직의 일원인 척하며 배지나 출입 코드를 사용하지 않고 보안 구역에 따라 들어오는 행위입니다. 테일게이팅은 누군가 보안 구역에 들어가거나 보안 구역에서 나오기를 기다렸다가 문이 닫히기 전에 몰래 들어가는 행위입니다. 모르는 사람이라면 일단 의심하고 주저 없이 신원 확인을 요청하십시오.
- 집에서는 업무 중 아무도 화면을 볼 수 없는 공개되지 않는 편안한 작업 공간을 찾습니다. 모든 민감한 정보는 배우자, 자녀 및 친구를 포함하여 권한 없는 사람의 눈에 띄지 않게 해야 합니다.
- 자리를 비울 때는 항상 컴퓨터를 잠그십시오. 컴퓨터를 잠그지 않은 채로 두면 누구나 컴퓨터를 사용하여 민감한 데이터에 액세스하거나, 로그인 자격 증명을 훔치거나, 맬웨어를 설치할 수도 있습니다.

## 클릭하기 전에 먼저 생각하기

- 예상하지 못한 이메일을 받은 경우 포함된 링크를 클릭하거나 첨부 파일을 절대로 다운로드하지 마십시오. 보낸 사람이 합법적인 조직의 구성원인 것처럼 보여도 해당 이메일 주소가 도용되었을 수 있습니다.
- 이메일에 계정이나 온라인 서비스에 로그인하도록 요청하는 내용이 포함된 경우 브라우저를 통해 해당 서비스로 이동하십시오. 이메일에서 링크를 바로 클릭하면 절대 안 됩니다. 브라우저에서 사이트로 직접 이동해야 비슷하게 생긴 가짜 사이트가 아니라 실제 웹사이트에 로그인할 수 있습니다.
- 확실하지 않은 경우 이메일을 보낸 사람에게 전화하여 요청, 링크 또는 첨부 파일이 합법적인지 확인합니다. 이메일에 제공된 전화번호는 가짜일 수 있으므로 해당 번호로는 전화하지 마십시오.

