SANS SECURITY AWARENESS

자택에서 안전하게 일하는 5단계 방법

집에서 일하는 것이 생소한 분들도 있을 것이고, 어쩌면 새로운 환경이 부담스러운 분도 있을지 모릅니다. 저희 목표 중 하나는 여러분이 집에서 최대한 안전하게 일하도록 도와드리는 것입니다. 다음은 안전하게 일할 수 있는 간단한 다섯 가지 단계입니다. 이 모든 단계의 가장 좋은 점은 집에서 안전하게 일할 수 있을 뿐 아니라, 당신과 당신의 가족을 위한 더욱 안전한 홈 사이버 보안을 구축할 수 있다는 것입니다.

나 자신: 우선, 기술은 자신을 완전히 보호할 수 없습니다. 오직 자기 자신이 최선의 방어책입니다. 공격자들은 당신의 기기나 컴퓨터보다는 당신 자체를 타겟으로 했을 때 더 쉽다는 것을 잘 알고 있습니다. 이들이 당신의 비밀번호, 작업 데이터, 컴퓨터에 대한 통제권을 원한다면, 긴급한 분위기의 메시지를 만들어 보내고 당신이 그러한 정보를 넘기도록 유도하려 할 것입니다. 예를 들어 Microsoft의 기술 지원팀인 척하면서 당신의 컴퓨터가 감염되었다고 말할 수 있습니다. 또는 당신에게 뭔가 보낼 게 있는데 보내지 못했다면서 악성 코드가 있는 링크를 클릭하게 할 수도 있습니다. 사회 공학 공격의 가장 일반적인 징후는 다음과 같습니다:

- 누군가가 두려움, 협박, 위기, 중요한 마감일 등을 이용해 긴급한 상황을 연출합니다. 사이버 공격자들은 은행이나 정부, 국제 조직과 같은 신뢰할 수 있는 조직으로 가장하여 설득력 있는 메시지를 만들어내는데 능합니다.
- 보안 정책 또는 절차를 무시하거나 우회하게 압박하거나, 복권 당첨처럼 사실이라고 보기 어려울 정도로 좋은 제안을 합니다.
- 아는 친구나 직장 동료에게 온 것처럼 보이는 메시지이지만, 메시지의 문장이나 서명, 어조가 그들처럼 보이지 않습니다.

마지막으로, 이러한 공격에 대한 최선의 방어는 바로 당신입니다.

홈 네트워크: 거의 모든 홈 네트워크에는 무선(Wi-Fi) 네트워크가 있습니다. 이를 통해 개인 장치가 무선으로 인터넷과 연결할 수 있습니다. 대부분의 홈 무선 네트워크는 인터넷 라우터 또는 분리된 전용 무선 액세스 포인트를 통해 통제되고 있습니다. 양쪽 모두 작동 원리는 같습니다. 집에 있는 기기를 연결할 수 있는 무선 신호를 전송하는 것이죠. 즉, 집을 지키기 위해서는 무선 네트워크를 안전하게 지켜야 합니다. 이를 위해서 다음 단계를 수행하는 것을 권장합니다:

- 사용하고 있는 무선 네트워크를 제어하는 기본 관리자 비밀번호를 변경하세요. 관리자 계정을 통해 사용하는 무선 네트워크 설정을 변경할 수 있습니다.
- 무선 네트워크에는 신뢰할 수 있는 사람만 연결하도록 하세요. 이것은 강력한 보안으로 가능합니다. 이를 활성화하면 무선 네트워크에 연결할 때 비밀번호를 입력해야 하며, 연결되고 나면 모든 온라인 활동이 암호화됩니다.
- 무선 네트워크에 접속할 때 사용하는 비밀번호는 복잡해야 하며, 관리자 비밀번호와 동일하면 안 됩니다. 각 기기는 일단 비밀번호를 입력하고 나면 그 비밀번호가 계속 저장되므로, 한 번만 비밀번호를 입력하면 됩니다.

이 단계를 어떻게 수행해야 하는지 모르시나요? 그렇다면 인터넷 서비스 제공자, 제공자의 웹사이트, 무선 액세스 포인트에 들어있던 매뉴얼, 판매자 웹사이트를 확인하거나 문의하세요.

비밀번호: 사이트에서 비밀번호를 생성하라고 할 경우, 강력한 비밀번호를 생성하세요. 길이가 길수록 더욱 강력해집니다. 강력한 비밀번호를 만드는 가장 간단한 방법 중 하나는 암호문을 사용하는 것입니다. 암호문은 단어로 만들어진 문장입니다. 예를 들어 "*꿀벌 벌집 맥주.*"가 될 수 있습니다. 각 기기 또는 온라인 계정마다 서로 다른 암호문을 사용하세요. 이렇게 함으로써 하나의 계정이 노출되더라도 다른 계정이나 기기를 안전하게 지킬 수 있습니다. 비밀번호를 모두 기억할 수 없나요?

비밀번호 관리자 같은 특화된 프로그램을 사용하면 모든 암호문을 암호화된 형태로 안전하게 보관할 수 있습니다. 그리고 이러한 프로그램에는 그 외 다양한 멋진 기능이 많이 준비되어 있습니다! 마지막으로, 지원하는 경우 2단계 인증, 또는 이중 인증을 활성화하세요. 비밀번호를 계속 사용하면서도 스마트폰으로 코드를 보내거나, 코드를 생성하는 앱을 이용하는 등 추가적인 두 번째 단계를 선택할 수 있습니다. 2단계 인증은 온라인 계정을 보호하는 가장 중요한 단계이며, 생각보다 훨씬 쉽습니다.

업데이트: 각 컴퓨터, 모바일 기기, 프로그램, 앱, 소프트웨어를 최신 버전으로 실행하세요. 사이버 공격자들은 당신이 사용하고 있는 기기와 소프트웨어에서 새로운 취약점을 계속 찾아내려 하고 있습니다. 이들이 그런 취약점을 발견하면, 특별한 프로그램으로 그 취약점을 이용하고 당신이 사용 중인 기기를 해킹할 수 있습니다. 그리고 소프트웨어나 기기를 제작한 회사에서는 계속 업데이트를 발표하며 이를 보완하기 위해 노력하고 있습니다. 컴퓨터와 모바일 기기에 이러한 업데이트를 즉시 설치하면 다른 사람이 해킹하기가 더 어려워집니다. 최신 상태를 유지하려면 언제든 자동 업데이트를 활성화하세요. 이 규칙은 업무용 기기뿐 아니라 인터넷에 연결된 TV, 아기 모니터, 보안 카메라, 홈 라우터, 게임 콘솔, 그리고 자동차 등 네트워크에 연결되는 거의 모든 기술에 적용됩니다.

어린이/손님: 사무실에 있을 때는 아이나 손님, 다른 가족이 업무용 노트북이나 다른 장비를 사용할까 봐 걱정할 필요가 없습니다. 가족과 친구들에게 업무용 기기를 사용하면 안 된다고 알려주세요. 실수로 정보를 삭제 또는 조작하거나, 더 나쁜 경우에는 기기를 감염시킬 수도 있습니다.