

온라인 상의 조직 안전

사이버 보안이 지역사회 단체와 조직에 중요한 이유는?

이 페이지에서는 사이버 보안 위협으로부터 지역사회 단체나 조직을 보호하기 위한 조언과 우리가 취할 수 있는 몇 가지 조치에 대해 설명합니다. 개개인이 온라인에서 자신을 안전하게 지키기 위한 안내 자료도 별도로 마련되어 있습니다.

이 조언은 가장 일반적이고 심각한 위협에 대비한 것입니다.

업데이트

기기 소프트웨어를 최신 상태로 유지하여 보안상의 허점을 막으세요.

- 지역사회 단체나 조직의 기기를 최신 상태로 업데이트하세요. 휴대폰, 컴퓨터, WiFi 라우터뿐 아니라 인터넷에 연결하는 것이면 무엇이든(스마트 기기 포함) 여기에 해당됩니다.
- 가능하다면 자동 업데이트 기능을 사용하세요.

2단계 인증(2FA)

비밀번호에다 별도의 절차를 하나 더(휴대폰의 앱에서 생성되는 코드 등) 요구하면 계정 보안이 강화됩니다.

- 참고: 이것은 다단계 인증(MFA), 2단계 확인(2SV) 등 여러 가지 이름으로 불립니다.
- 모든 지역사회 단체나 조직의 계정에서 2FA 기능을 사용하세요.

- 가능하다면 피싱을 막아내는 2FA 방식을 사용해 보세요. 그러면 피싱 공격에 속아 계정이 탈취되는 일이 없습니다. 이것은 물리적 보안 키일 수도 있고, 지문 또는 얼굴 ID와 같은 것일 수도 있습니다.

온라인 계정 관리

구성원이 지역사회 단체나 조직을 떠난 후에도 계정 접속 권한을 계속 보유하지 않도록 조치하세요.

- 동일한 계정에 여러 사람이 접속하는 경우, 각자 로그인 정보를 달리하고 모두 2FA를 사용하도록 하세요.
- 모든 사용자 계정의 목록을 작성해 두었다가 직원이 그만둘 때와 같은 경우 등 더 이상 필요하지 않게 된 계정은 비활성화하세요.
- 구성원에게 제공한 모든 기기의 등록부를 비치하고, 그 사람이 조직을 떠날 경우 이것을 회수해 완전히 초기화하는 것을 잊지 마세요. 건물 출입에 필요한 물리적 코드를 변경해야 할 수도 있습니다.

누가 온라인 계정 접속 권한이 있는지 확인

지역사회 단체나 조직의 구성원은 필요한 것에만 접근권이 있어야 합니다.

- 이렇게 하면 어떤 한 사람의 계정이 해킹당하더라도 공격자가 입힐 수 있는 피해가 제한됩니다.
- 정기적으로 확인해서 불필요한 접근 권한을 제거하세요.
- 여러 사람이 단일 '관리자' 계정을 사용하는 경우, 비정상적인 활동이 있는지 모니터링하세요. 특히 일상적인 업무에 대해 이러한 종류의 계정을 두는 것을 제한하세요.
- 이러한 규칙은 라우터와 같은 기기에 대한 관리자 접근권에도 적용됩니다.

서비스 제공업체와의 계약 재검토

IT 업체에 서비스 운영을 위탁한 경우

- 해당 업체가 지역사회 단체나 조직이 필요로 하는 바를 충족해 줄 사이버 보안 장치를 갖추도록 조치하세요.

모든 계정과 시스템이 서로 어떻게 연결되어 작동하는지 파악

그 연결성을 이해하면 공격자가 어디로 침입할 수 있는지 알아내는 데 도움이 됩니다.

- 시스템(예: 이메일, 클라우드 스토리지, 회계 플랫폼) 간 연결성을 재검토해 보세요.
- 온라인 보안을 강화하기 위해 가상 사설망(VPN)의 사용을 고려해 보세요. VPN을 사용하면 사용자를 추적하려는 사람으로부터 자신의 온라인 활동을 숨길 수 있습니다. 이것은 지역사회 단체나 조직의 구성원이 원격으로 접속하는 경우에 특히 유용합니다.

구성원들이 항상 '사이버 스마트'하도록 교육

시스템 자체보다는 지역사회 단체나 조직의 구성원이 표적이 될 가능성이 더 큽니다.

- 모든 직원을 대상으로 기본적인 사이버 보안 교육을 실시하세요. Own Your Online 웹사이트 [Own Your Online | NCSC](#)에는 온라인에서 자신의 안전을 지키고 스캠을 식별하는 데 도움이 되는 다양한 조언과 팁이 나옵니다.
- 이것은 조직에서 사용하는 직원 계정뿐만 아니라 자신의 개인 계정에도 중요하다는 점을 상기시켜 주세요.
- [개개인이 온라인에서 자신을 안전하게 지키기 위한 안내 자료도 따로 마련되어 있습니다.](#)

사고 대비

대응 계획을 세워놓는 것은 사고 발생 시 사람들이 당황하지 않도록 하는 데 중요합니다.

- 사고 대응 계획에는 사고 발생 시 누가 무엇을 하는지가 간략하게 명시됩니다. 계획서 표준 서식은 여기에 있습니다. [사고 관리 | NCSC](#)
- 전화, 컴퓨터 또는 기타 시스템에 장애가 발생할 경우, 어떻게 해야 하는지에 대한 계획을 포함하세요. 지속적으로 이 계획을 업데이트하세요.
- 필요한 모든 사람의 연락처 정보를 보관하고, 1차적 연락 수단(예: 이메일)이 불통일 경우에 쓸 대체 연락 방법을 정해 두세요.
- 액세스할 수 없는 경우를 대비하여 시스템 밖의 어딘가에 계획서를 보관해 두세요.