사물인터넷(IoT) 기기를 안전하게 보호하는 방법

호주 사이버 보안 센터(Australian Cyber Security Centre)는 지역사회가 사물인터넷(Internet of Things, IoT) 기기를 안전하게 구매하고 사용할 수 있도록 돕기 위해 본 정보를 제작했습니다. IoT 기기란 인터넷 연결 기능이 탑재된 일상적인 물품입니다. 예시로는 베이비 모니터, 드론, 보안 카메라, 스마트 TV, 그리고 태양광 인버터 등이 있습니다. 가정집 및 사업장 내에서 사용되는 IoT 기기는 인터넷에 연결되기 위해 보통 와이파이 또는 셀룰러 네트워크(예: 4G 또는 5G)를 이용합니다.

호주 가정집 및 사업장 내에서 흔히 볼 수 있는 많은 IoT 기기는 보안을 염두에 두고 설계되지 않았습니다. 이로 인해 이들 기기는 인터넷을 통해 쉽게 침해될 수 있는 취약한 상태가 되었습니다. 이러한 상태는 사이버 범죄자들이 악의적인 목적으로 여러분의 기기와 개인 정보를 무단으로 접근할 수 있도록 합니다.

IoT 기기를 구매하기 전

제조사마다 제공하는 보안 수준이 다르기 때문에 기기를 구입하기 전에 이에 대해 조사하는 것이 중요합니다. 기기를 구입하기 전, 다양한 제조사에서 판매하고 있는 유사한 기기들을 비교해 보세요. 고려할 점은 다음과 같습니다:

1. **기기가 잘 알려져있고 평판이 좋은 회사에서 만들어졌으며, 잘 알려져있고 평판이 좋은 매장에서 판매되고 있나요?** 잘 알려져있고 평판이 좋은 회사들은 기기를 제조할 때 보안을 고려했을 가능성이 더 높습니다. 잘 알려져 있고 평판이 좋은 매장은 잘 알려져 있고 평판이 좋은 회사의 기기만 판매할 가능성이 더 높고, 제조사가 의도한 대로 기기가 소비자에게 전달되도록 시스템이 더 엄격한 공급망을 갖추고 있습니다.

2. **비밀번호를 바꿀 수 있나요?** 비밀번호를 바꾸는 것이 항상 좋습니다. 기기의 기본 설정 비밀번호가 취약한 경우 이는 더욱 중요해집니다. 보안이 잘 갖춰진 기기는 고유하고 예측 불가능하며, 복잡하고 추측하기 어려운 비밀번호를 갖추고 있어야 합니다. 이는 추측하기 쉬운 기본 설정 비밀번호가 기기를 침해할 수 있는 가장 쉬운 방법이기 때문입니다.

3. **제조사가 업데이트를 제공하나요?** 제조사가 기기의 취약점이 발견되는 대로 이를 고치기 위한 업데이트를 제공하는 것이 중요합니다. 예를 들어, 기기의 소프트웨어에 알려진 취약점이 있거나 해커가 기기를 손상시키는 새로운 방법을 개발하는 경우 이를 고칠 수 있는 업데이트가 필요합니다.

4. **기기는 어떤 데이터를 수집하고 이 데이터는 누구와 공유되나요?** 제조사들은 어떤 데이터가 수집될 것이며 이 데이터가 어떻게 사용될 것인지에 대한 정보를 누구나 볼 수 있도록 자사의 웹사이트 또는 보안 정책에 설명하고 있어야 합니다. 온라인 또는 모바일 앱이 어떤 정보를 수집하고 있는지 항상 알아보는 것이 중요합니다.

5. **기기는 여러분이 원하는 대로만 작동하나요?** 여러분이 필요로하는 것보다 더 많은 기능(인터넷 연결 포함)이 갖춰진 기기는 여러분의 보안을 낮출 수도 있습니다. 사용하지 않는 기기 기능은 여러분에게 어떠한 이점도 제공하지도 않으면서 기기의 공격 취약성을 증가시킬 수 있습니다.

사물인터넷(IoT) 기기

기기를 처음 셋업할 때, 네트워크 및 데이터를 더욱 안전하게 보호하는 데 도움이 되는 몇 가지 간단한 질문을 스스로에게 물어보세요.

1. **기기가 인터넷에 연결되어야 하는가?** 연결할 수 있다고 해서 꼭 연결해야만 하는 것은 아닙니다. 인터넷에 연결하지 않은 기기가 침해당할 가능성이 훨씬 낮습니다. 인터넷 연결이 요구되는 기능을 사용하지 않을 거라면, 인터넷에 굳이 연결될 필요가 있는지를 고려해 보세요.

2. **기기가 안전한 곳에 있는가?** 만약 기기가 안전하지 않은 곳에 설치될 이유가 없다면, 안전한 곳에 설치하는 것이 기기의 물리적 손상의 위험을 줄일 수 있습니다.

3. **기본 설정 사용자 이름과 비밀번호를 바꿔야 하는가?** 강력한 비밀번호나 암호문구(passphrase)를 사용하는 것이 중요합니다. 기기의 기본 설정 비밀번호가 고유하고 예측 불가능하며, 복잡하고 추측하기 어렵지 않다면, 비밀번호를 바꿔야 합니다. 기본 설정 사용자 이름과 비밀번호는 수집되어 온라인에 게시되므로, 여러분의 기기의 보안이 취약해집니다.

4. **와이파이 네트워크가 안전하게 설정되어 있고 안전한 비밀번호가 있는가?** 공격자가 여러분의 기기와 네트워크에 접근하기 어렵게 하기 위해 와이파이 네트워크와 라우터를 보호하세요.

추가 조치

IoT 기기만을 위한 추가 와이파이 네트워크를 라우터에 설정하세요. 이는 여러분의 와이파이 라우터에 '손님용' 네트워크로 설정될 수 있습니다. IoT 기기 간에 통신이 필요하지 않은 경우 '클라이언트 격리(client isolation)' 기능을 활성화하세요. IoT 기기를 민감한 데이터로부터 격리하면 IoT 기기가 침해되어도 다른 기기나 데이터에 접근할 수 없게 됩니다.

5. **불필요한 기기의 기능은 비활성화되어 있는가?** 기기에 원하지 않거나 필요하지 않은 기능(예: 카메라, 마이크)이 있다면, 가능한 이러한 기능을 비활성화해야 합니다.

추가 조치

로컬 LAN 또는 WAN/인터넷에서 기기의 웹 관리 인터페이스에 대한 원격 접근권을 활성화하는 기능을 언급하는 구성 설정을 찾으세요. 원격으로 직접 접속해야 하는 경우가 아니라면 로컬 LAN으로 설정하세요.

IoT 기기의 유지관리

IoT 기기를 셋업한 후 사용할 때 기억해야 할 몇 가지 중요한 사항이 있습니다.
중요 사항에는 다음이 포함됩니다:

1. **기기를 정기적으로 재부팅하세요.** IoT 기기가 느려지거나 사용이 불가능해지면 이는 바이러스가 있음을 의미할 수도 있습니다. 대부분의 악성코드(malware)는 메모리에 저장되기 때문에 기기 재부팅으로 쉽게 제거될 수 있습니다. 재부팅이란, 기기의 전원을 껐다 다시 키는 것을 의미합니다. 재부팅을 했는데도 기기가 느리거나 사용이 불가능하다면 공장 초기화(factory reset)를 시도해 보세요. 단, 이 방법은 여러분의 사용 데이터와 맞춤 설정을 모두 삭제할 수도 있습니다.

2. **업데이트를 정기적으로 실행하세요.** 일부 기기는 업데이트를 자동으로 실행합니다. 그렇지 않은 기기의 경우, 제조사의 정보를 주기적으로 확인하고 제공되는 대로 업데이트를 실행하세요. 업데이트가 더 이상 제공되지 않는 기기의 경우, 업데이트가 제공되는 더 최신 기기로 업그레이드하는 것을 고려해 보세요. 보안 업데이트가 제공되지 않는 기기는 새로운 취약점이 발견되더라도 보호되지 않으며, 이러한 기기는 여러분의 네트워크, 개인 정보 및 데이터에 위협이 될 수 있습니다.

3. **사용하지 않을 때는 기기의 전원을 끄세요.** 사용 및 감시하지 않는 기기의 전원을 켠 채로 와이파이 네트워크에 장시간 연결해 놓는 것은 여러분의 기기가 공격 대상이 될 가능성을 증가시킵니다. 이 문제점을 해결할 수 있는 한 가지 방법은 전원 콘센트 타이머를 사용하여 지정된 시간 동안만 장치에 전원을 공급하는 것입니다.

4. **월간 인터넷 사용량 또는 요금이 크게 증가하는지 여부를 지켜보세요.** 인터넷 사용량 또는 요금이 크게 증가한다면, 이는 장치가 침해되었을 수도 있음을 의미합니다. 회사 IT 부서에서 해당 사안을 조사해야 하는 경우가 아니라면 공장 초기화(factory reset)를 실행한 후 비밀번호를 바꿔야 합니다.
(단, 이 방법으로 여러분의 사용 데이터와 맞춤 설정이 모두 삭제될 수도 있음을 유의하세요.)

IoT 기기의 처분

폐기 또는 판매를 통한 기기 처분은 타인이 여러분의 개인정보나 데이터에 쉽게 접근할 수도 있음을 의미합니다.
이를 방지할 수 있는 방법은 다음과 같습니다:

1. **모든 데이터와 개인정보를 지우세요.** 제조사는 기기와 관련 앱에서 데이터와 개인정보를 지우는 방법을 제시해야 합니다. 기기를 처분하더라도 개인정보를 지우면 아무도 이러한 정보에 접근할 수 없게 됩니다. IoT 기기를 없애면서 온라인 계정을 더 이상 사용할 필요가 없다면 계정을 삭제하세요.

2. **기기에 공장 초기화를 실행하세요.** 공장 초기화는 로컬 저장소에 저장된 데이터를 지우고 비밀번호, 사용자 이름 및 설정을 기본값으로 재설정하도록 설계되었습니다. 공장 초기화 방법은 기기의 사용자 매뉴얼 또는 제조사의 웹사이트에서 확인하세요.

3. **해당 기기와 휴대전화 또는 다른 기기 간 연동을 끊으세요.** 다른 기기, 네트워크 또는 온라인 계정과 연동되어 접근할 수 있는 기기를 폐기하면, 타인이 이에 접근할 수도 있게 됩니다. 다른 기기도 확인하고 폐기하려는 기기와의 연동을 모두 제거하세요. 더 이상 필요하지 않은 모바일 앱에 부여된 권한을 제거하세요.

4. **기기에 연결된 이동식 미디어(예: USB 플래시 드라이브, 메모리 카드 등)를 제거하세요.** 이동식 매체에는 공장 초기화로 삭제되지 않는 개인정보가 포함되어 있을 수 있으며, 이러한 데이터는 물리적으로 제거한 후 물리적으로 파기하고, 기기와 별도로 폐기해야 합니다.

지원

호주 신호국(Australian Signals Directorate) 산하 호주 사이버 보안 센터(Australian Cyber Security Centre)에 연락하려면 asd.assist@defence.gov.au에 이메일을 보내세요. 긴급 지원이 필요한 경우, 주7일 매일 24시간 운영되는 핫라인 **1300 CYBER1 (1300 292 371)**번으로 전화하세요.

www.cyber.gov.au/report로 ReportCyber에 사이버 범죄를 신고하세요.

신원 도용을 겪은 경우, 웹사이트 www.idcare.org를 통해 IDCARE에 연락하세요.

여러분과 여러분의 가족을 위한 조언이 필요한 경우, www.cyber.gov.au를 방문하세요. 최근 온라인 위협에 대한 ACSC의 무료 알림 서비스에 가입하세요.

함께 호주를 온라인에 접속할 수 있는 가장 안전한 나라로 만듭시다.

사이버 보안 조언이 필요한 경우, www.cyber.gov.au를 방문하세요.

면책 조항

본 지침의 자료는 일반적인 성격을 지니며 법률 자문으로 간주되어서는 안되며, 혹은 특정 상황이나 긴급 상황에서 도움을 받기 위해 의존되어서도 안 됩니다. 모든 중요한 문제에 대해서는 자신의 상황과 관련해 적절하고 독립적인 전문가의 조언을 구해야 합니다.

호주 연방정부는 본 지침에 포함된 정보에 의존한 결과로 발생한 어떠한 손해, 손실 또는 비용에 대해서도 책임을 지지 않습니다.

저작권

호주 연방정부 문장(Coat of Arms) 사용

호주 연방정부 문장의 사용 조건은 국무총리내각부(Department of the Prime Minister and Cabinet) 웹사이트에 자세히 기술되어 있습니다. Commonwealth Coat of Arms Information and Guidelines(호주 연방정부 문장 정보 및 지침) | pmc.gov.au.

더 자세한 정보를 원하시거나 사이버 보안 사고를 신고하시려면 다음으로 저희에게 연락주시기 바랍니다.

cyber.gov.au | 1300 CYBER1 (1300 292 371)
이 번호는 호주 내에서만 사용되는 번호입니다.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre