Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

소사업체 사이버 보안 지침

내용 난이도
하 ●○○

cyber.gov.au

서론

소사업체의 경우, 작은 사이버 보안 사고도 치명적인 영향을 미칠 수 있습니다. 본 지침은 흔한 사이버 보안 위협으로부터 여러분의 사업체를 보호하는 데 도움이 되는 간단한 보안 조치를 포함합니다. 시작 단계로 다음 세 가지 조치를 권장합니다:

- 다중인증(multi-factor authentication) 활성화하기
- 소프트웨어 업데이트하기
- 정보 백업하기

본 지침은 여러분의 사업체에 해당하지 않는 조치들을 포함할 수 있고, 또는 여러분의 사업체가 더욱 복잡한 요건을 갖추고 있을 수 있습니다. 본 안내문을 정독한 후, 소사업체의 경우 8 가지 필수 항목(Essential Eight) 중 Maturity Level One을 실행하시길 권장합니다. 본 지침의 조언 또는 사이버 보안 관련 더 구체적인 질문이 있는 경우, IT 전문가 또는 신뢰하는 자문인에게 문의하시길 권장합니다.

각 조치의 실천 방법을 포함한 전체 안내문을 열람하려면 cyber.gov.au를 방문하세요.

목차

소사업체에 대한 위협

사기(스캠) 메시지

스캠은 사이버 범죄자들이 소사업체를 공격하는 흔한 방법입니다. 그들의 목적은 여러분이나 여러분의 직원이 다음 행동을 하도록 속이는 것입니다:

- 자금 또는 기프트 카드를 보내는 것
- 악성 링크 또는 첨부파일을 클릭하는 것
- 비밀번호와 같은 민감한 정보를 제공하는 것

사이버 범죄자들은 이메일, 문자 메시지, 전화, 그리고 소셜미디어를 통해 여러분의 사업체를 대상으로 사기를 치려고 할 수 있습니다. 그들은 종종 여러분이 신뢰하는 사람 또는 기관인 척 연기할 것입니다.

피싱(phishing) 공격

소사업체의 경우 특히 염려되는 사기 유형은 **피싱(phishing) 공격** 입니다. 이러한 스캠은 계정에 로그인하거나 기밀 정보를 입력하도록 유도하는 가짜 웹사이트 링크가 포함된 경우가 많습니다. 피싱(phishing) 공격은 일반적으로 여러분의 계정 비밀번호를 위험에 노출시킵니다. 사이버 범죄자들은 흔히 이 방법으로 소사업체의 소셜 미디어 계정을 "탈취"해 그 빌미로 사업체를 협박합니다.

위험 완화 방법

어떠한 메시지의 출처를 알고 있더라도 내용이 의심스럽다면 주의를 기울이세요. 관련 담당자 또는 사업체에 별도로 연락해 메시지의 진위성을 확인하세요. 의심스러운 메시지 속 연락처가 아닌 사업체의 공식 웹사이트와 같은 신뢰 가능한 출처에서 연락처를 찾아 사용하세요.

다음 자료를 이용해 스캠 및 피싱(phishing) 공격 식별에 관해 더 자세히 알아보세요:

- 스캠을 인식하고 신고하기(Recognise and report scams)
- 피싱 공격 식별 방법 배우기(Learn how to spot phishing scams)
- 소셜 엔지니어링된 메시지 식별하기(Detecting Socially Engineered Messages).

사례 연구:

한 택배 회사 직원은 간부로부터 $500 상당의 사전 결제 MasterCard 신용카드 6개를 구입하라는 이메일을 받았습니다. 간부는 해당 카드가 다른 직원들에게 상품권으로 증정될 것이라고 하면서 직원에게 이를 비밀로 하라고 했습니다. 구매 후, 직원은 간부로부터 구매 인증을 위해 각 카드의 양면을 사진으로 찍어 자신에게 보내라는 요청을 받았습니다.

지시 받은대로 직원은 우체국으로 가 자신의 개인 신용카드로 기프트 카드를 구매했습니다. 직원은 간부의 이메일로 답장해 기프트 카드 사진을 증빙자료로 보냈습니다.

우체국에서 돌아온 후 직원은 물리적인 카드를 간부에게 건넸지만 간부는 이 카드에 대해 전혀 아는 바가 없었습니다. 상황 검토에 따르면 **기프트 카드와 관련된 모든 이메일은 출처 모를 이메일 주소로부터 온 것으로 간부의 실제 이메일 계정으로부터 온 것이 아니었습니다. 스캠(사기)이었던 것이었습니다.**

이메일 공격

피싱(phishing)과 같은 사기에 더불어 소사업체를 대상으로 하는 흔한 이메일 공격 방법에는 **기업 이메일 침해**(Business Email Compromise, BEC)가 있습니다. 범죄자들은 임의의 이메일 계정 또는 실제 기업과 비슷해 보이는 도메인 이름을 이용하는 등의 기타 방법으로 특정 사업체의 담당자인 척 연기할 수 있습니다. 정보를 훔치는 것 외에도 이러한 공격의 목표는 일반적으로 사기꾼이 운영하는 은행 계좌로 자금을 보내도록 피해자를 속이는 것입니다.

위험 완화 방법

이메일 공격에 대한 가장 좋은 방어는 직원들을 훈련시키고 이에 대한 이해도를 높이는 것입니다. 직원들이 다음을 포함하는 이메일에는 항상 주의를 기울이도록 하세요:

- 자금 지급 요청(특히 급하거나 연체된 경우)
- 은행계좌 정보 변경
- 어딘가 이상해 보이는 이메일 주소(예: 이메일 도메인 이름이 공급업체 이름과 딱히 일치하지 않는 경우)

이러한 공격은 치명적일 수 있지만 위험 완화 조치는 쉽고 비용이 거의 들지 않습니다. **직원들이 이러한 이메일을 받게 되면 가장 효과적인 위험 완화 방법은 보낸 사람에게 직접 전화해 진위성을 확인하는 것입니다.** 이메일에 적힌 연락처는 속이기 위한 수단일 수도 있으므로 사용해서는 안 됩니다. 지불 요청을 받거나 은행 계좌정보가 변경될 때 직원들이 따를 수 있는 정식 절차를 수립하세요.

다음 자료를 통해 여러분의 사업체를 기업 이메일 침해(BEC) 사기 및 이메일 침해로부터 보호하는 방법을 배우세요:

- 기업 이메일 침해(Business email compromise)
- 이메일 사기 및 침해로부터 사업체 보호하기(Protect your business from email fraud and compromise)
- 여러분의 사업체가 이메일 사기 및 침해의 표적이 된 경우 해야 할 일(What to do if your business has been targeted by email fraud or compromise).

사례 연구:

한 소규모 건축업체는 공급업체로부터 은행이 변경됐다는 내용의 이메일을 받았습니다. 이 공급업체는 인보이스 대금이 지급될 새로운 계좌의 정보를 제공했습니다. 이메일이 진짜처럼 보였기에 **건설업체는 공급업체에게 연락해 은행 계좌 정보 변경에 대해 별도로 확인하지 않았습니다.**

건설업체는 공급업체에 해당 인보이스에 대해 $70,000 이상의 대금을 지급했습니다. 다음 날, 또 다른 직원은 실수로 같은 인보이스에 대해 $70,000 이상의 대금을 추가 지급했습니다. 새로운 은행계좌로 도합 $150,000이 넘는 금액이 지급됐습니다.

건설업체는 공급업체에 연락해 이중 지급된 대금에 대한 회수를 요청했으나 공급업체는 해당 은행계좌 정보가 잘못됐다고 전달했습니다. 그 즉시 조사가 진행됐고 공급업체는 당사의 이메일 계정 중 하나가 해킹되어 사기 목적의 은행 계좌정보를 제공하고 있다는 것을 알게 됐습니다. **그 어떠한 대금도 회수되지 못했습니다.**

악성 소프트웨어 (Malicious software)

악성 소프트웨어는 랜섬웨어, 바이러스, 스파이웨어 및 트로이 목마와 같이 피해를 입히도록 설계된 악성 소프트웨어를 일컫는 포괄적인 용어입니다. 악성 소프트웨어는 다음을 초래할 수 있습니다:

- 여러분의 기기 속 파일의 도난 및 잠금
- 은행 또는 신용카드 번호 도난
- 유저네임 및 비밀번호 도난
- 여러분의 컴퓨터에 대한 통제 또는 감시

악성 소프트웨어는 여러분의 기기가 정상 작동하지 않도록 방해할 수 있고, 여러분의 파일을 삭제 또는 손상시킬 수 있으며, 또는 타인이 여러분의 개인 정보 또는 사업 정보에 접근할 수 있도록 합니다. 여러분의 기기가 악성 소프트웨어에 감염되면 다른 공격에도 노출될 수 있습니다. 악성 소프트웨어는 여러분 네트워크에 접속되어 있는 다른 기기에도 이전될 수 있습니다.

여러분의 기기는 다음을 포함한 다양한 방법으로 악성 소프트웨어(malware)에 감염될 수 있습니다:

- 악성 소프트웨어(malware)에 감염된 웹사이트 방문
- 인터넷에서 감염된 파일 또는 소프트웨어 다운로드
- 감염된 이메일 첨부파일 열람

랜섬웨어(Ransomware)

랜섬웨어(Ransomware)는 흔하고 위험한 유형의 악성 소프트웨어(malware)입니다. 더 이상 열람할 수 없도록 파일을 잠그거나 암호화하는 방식으로 작동합니다. 파일에 대한 접근권을 복원하기 위해 일반적으로 암호화폐 형태의 대가가 요구됩니다. 또한 사이버 범죄자들은 대가가 지불되지 않으면 데이터를 온라인 상에서 공개하거나 판매할 거라고 협박할 수 있습니다.

위험 완화 방법

바이러스 방어 또는 보안 소프트웨어가 여러분을 악성 소프트웨어로부터 보호할 수는 있지만, 그 어떤 소프트웨어도 100% 효과적이지는 않습니다. 직원들은 계속해서 안전하기 위해 반드시 이메일, 웹사이트 및 파일 다운로드와 관련해 주의를 기울이고 기기를 주기적으로 업데이트해야 합니다.

여러분의 사업체를 랜섬웨어(ransomware)로부터 보호하는 방법에 관한 더 자세한 정보는 다음 자료를 참조하세요:

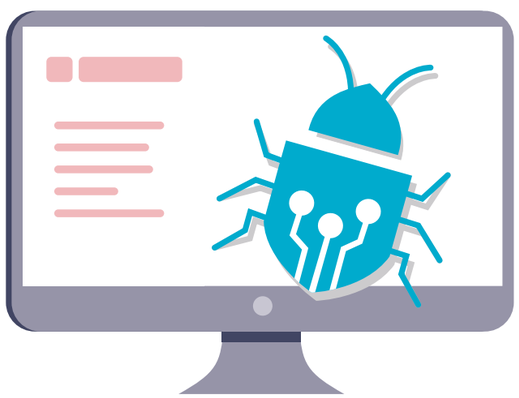
- 랜섬웨어(Ransomware)
- 랜섬웨어 공격으로부터 스스로를 보호하세요 (Protect yourself against ransomware attacks)
- 협박의 대상이 된 경우 해야 할 일(What to do if you're held to ransom)

사례 연구:

한 자동차 부품 매장의 직원들이 어느 날 출근했는데 서버 컴퓨터를 부팅할 수 없었습니다. 매장의 IT 서비스 제공업체가 서버에 접근했을 때 하나의 창이 열려 있었고, 해당 창에는 컴퓨터 데이터가 암호화됐다는 노트가 있었습니다. 또한 노트에는 파일을 풀려면 비트코인으로 대가를 지불하라는 요구가 있었습니다.

컴퓨터에는 백업 드라이브도 연결되어 있었지만, 이 또한 암호화됐었습니다. 직원들은 더 많은 백업 드라이브를 연결하려고 시도했지만 파일들은 몇 초 안에 자동으로 암호화되었습니다. **직원들은 데이터 복구를 시도하기 전에 랜섬웨어를 제거하지 못했고 가지고 있던 모든 백업 파일을 잃었습니다.**

유일하게 남은 선택지는 서버를 공장 초기화하고 새 시스템으로 새로 시작하는 것이었습니다. 그들의 사업은 수 년간 축적된 데이트를 잃었고 다시 처음부터 시작해야 했습니다.



계정을 보호하세요

다중인증(multi-factor authentication)을 활성화하세요

다중인증(multi-factor authentication, MFA)은 사이버 범죄자들이 여러분의 계정에 접근하기 더욱 어렵도록 만듭니다.

다중인증(MFA)은 계정에 하나의 보안 단계를 추가합니다. 타인이 여러분의 계정에 접근하지 못하도록 계정을 보호하는 가장 효과적인 방법 중 하나이므로 가능한 한 사용하는 것이 좋습니다. 여러분의 계정에 로그인하는 모든 사람은 여러분의 유저네임과 비밀번호에 추가로 또 다른 정보를 제공해야 할 것입니다. 이는 문자 메시지로 받는 일회성 코드 또는 인증 앱이 될 수 있습니다. 더 자세한 정보를 원하시면 **cyber.gov.au/mfa**에서 저희가 제공하는 MFA 조언(advice on MFA)을 열람하세요.

✓ **여러분의 가장 중요한 계정부터 가능한 한 다중인증(MFA)을 활성화 시키세요.**

접근 통제 기능을 실행하세요

사용자 접근 권한을 제한함으로써 사이버 보안 사고로 인한 피해 규모를 최소화할 수 있습니다.

접근 통제 기능은 특정 파일 및 시스템에 대한 접근성을 제한하는 방법입니다. 일반적으로 직원들은 사업 내 모든 데이터, 계정 및 시스템에 대한 전체 접근 권한을 필요로하지 않습니다. 각자의 업무를 수행하는 데 필요한 정보에 대한 접근 권한만 있어야 합니다.

접근권을 제한함으로써 사이버 보안 사고로 인한 피해 규모를 최소화할 수 있습니다. 예를 들어, 특정 직원의 컴퓨터가 랜섬웨어(ransomware)에 감염된 경우에도 적절한 접근 통제 기능이 설정되어만 있다면 전체 비즈니스가 아닌 소수의 파일에만 영향을 미칠 수 있습니다.

✓ **각 사용자가 각자의 직책에 필요한 것만 접근할 수 있도록 확인하세요.**

강력한 비밀번호 또는 암호문구 (passphrase)를 사용하세요

안전한 비밀번호 또는 암호문구(passphrase)를 사용함으로써 여러분의 계정을 사이버 범죄자로부터 보호하세요.

많은 소사업체의 경우 안전하지 않은 비밀번호 유형을 사용하면서 사이버 공격의 대상이 됩니다. 예시로는 여러 계정에 같은 비밀번호를 사용하는 경우입니다. 강력한 비밀번호를 만들기 위해 비밀번호 매니저 및 암호문구(passphrase)를 모두 사용할 수 있습니다.

비밀번호 매니저는 여러분의 비밀번호를 위한 가상 금고 역할을 합니다. 이를 통해 여러분의 각 계정을 위한 강력하고 **독특한** 비밀번호를 생성 및 보관할 수 있습니다. 이는 여러 계정이 있는 경우 독특한 비밀번호를 모두 외워야 하는 부담을 덜어줍니다. 모든 정보가 비밀번호 매니저에 기록되기 때문에 비밀번호 또는 그 비밀번호가 어느 계정의 것인지를 외울 필요가 없습니다.

자주 접속하는 계정이나 어떤 이유에서든 비밀번호 매니저를 사용하고 싶지 않은 경우, 비밀번호로 암호문구(passphrase)를 사용하는 것을 고려해 보세요. 암호문구(passphrase)는 여러 단어를 무작위로 조합한 것입니다. 예: 'crystal onion clay pretzel'. 기억하기 쉬운 안전한 비밀번호를 원하는 경우 유용합니다. 연관성이 없는 4개 이상 단어를 조합해 비밀번호의 독특함을 유지하세요 - 여러 계정에 걸쳐 **같은 암호문구(passphrase)를 재사용하지 마세요.** 더 자세한 정보를 원하시면 **cyber.gov.au/passphrases**에서 암호문구 및 비밀번호 매니저에 관한 조언(advice on passphrases and password managers)을 열람하세요.

✓ **비밀번호 매니저를 사용해 여러분의 각 계정을 위한 독특한 비밀번호를 생성 및 보관하세요.**

공유 계정을 관리하세요

계정 공유는 보안을 위험에 노출시킬 수 있으며 악의적 활동을 추적하기 어렵도록 만듭니다.

소사업체의 경우, 직원들이 계정을 공유해야만 하는 충분한 사유가 있을 수는 있으나 이는 가능한 한 피해야 하는 행위입니다. 여러 직원이 동일한 계정을 사용하는 경우 특정 직원의 활동을 다시 추적하기 어려울 수 있으며 침입한 사이버 범죄자를 추적하기는 더욱 어렵습니다. 비밀번호를 변경하지 않는 이상, 직원들은 퇴사 이후에도 해당 계정에 접근할 수도 있습니다.

✓ **공유 계정의 사용을 최소화하고 사업체에서 공유 계정이 사용되는 경우 계정을 안전하게 보호하세요.**

여러분의 기기 및 정보를 보호하세요

소프트웨어를 업데이트하세요

소프트웨어를 가장 최신 버전으로 유지하는 것이 여러분의 사업을 사이버 공격으로부터 보호하는 가장 좋은 방법 중 하나입니다.

업데이트는 여러분이 사용하는 운영 시스템 및 기타 소프트웨어의 보안 취약점을 고쳐 사이버 범죄자들이 침입하기 더욱 어렵도록 합니다. 새로운 취약점은 늘 발견되기 때문에 업데이트를 하라는 안내를 간과하지 마세요. 주기적인 소프트웨어 업데이트는 사이버 범죄자들이 이미 알고 있는 취약점을 이용해 여러분의 기기에 악성 소프트웨어(malware)를 실행하거나 해킹할 가능성을 줄일 것입니다. 도움이 필요한 경우 ACSC에서 게시한 업데이트 지침을 참조하세요.

기기 또는 소프트웨어가 너무 오래된 경우, 실행할 수 있는 업데이트가 없을 수 있습니다. 제조사가 제품 업데이트를 더 이상 지원하지 않는 경우, 계속해서 안전하기 위해 신규 제품으로 업그레이드 하는 것을 고려해 보세요. 중대 업데이트를 더 이상 지원받지 않는 시스템의 예시로는 **아이폰 7** 및 **Microsoft 윈도우 7**이 있습니다.

더 자세한 정보를 원하시면 **cyber.gov.au/updates**에서 업데이트에 관한 지침(guidance on updates)을 열람하세요.

✓ **기기 및 소프트웨어에 자동 업데이트를 활성화하세요.**

보안 소프트웨어를 사용하세요

바이러스 방어 및 랜섬웨어 보호와 같은 보안 소프트웨어는 여러분의 기기를 보호할 수 있습니다.

보안 소프트웨어를 사용해 여러분의 기기에서 악성 소프트웨어(malware)를 인식 및 제거하세요. 의심스러운 파일과 프로그램을 주기적으로 검사하기 위해 바이러스 방어 소프트웨어를 실행할 수 있습니다. 위협이 발견되면 여러분에게 알림이 갈 것이며 해당 의심 파일은 격리되거나 제거됩니다.

많은 소사업체의 경우 자신들을 바이러스 및 악성 소프트웨어(malware)로부터 보호하기 위해 **Windows Security를 사용합니다.** Windows Security는 Windows 10과 Windows 11 기기에 탑재되어 있으며 무료 바이러스 및 위협 보호 기능을 포함하고 있습니다. 또한 기기에서 랜섬웨어 보호 기능을 활성화하는 데에도 사용할 수 있습니다.

대안 제품 및 옵션을 원하시면 cyber.gov.au에서 antivirus를 검색해 바이러스 방어 소프트웨어에 관한 조언(advice on antivirus)을 열람하세요.

✓ **기기에 대한 주기적인 검사를 진행할 수 있는 보안 소프트웨어를 설정하세요.**

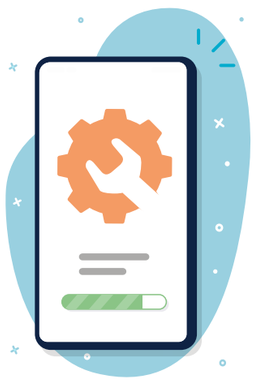
정보를 백업하세요

정기적인 백업은 정보가 손실되거나 손상된 경우 정보를 복구하는 데 도움이 될 수 있습니다.

중요한 정보를 백업하는 것은 사업을 운영하는 동안 정기적으로 또는 자동으로 수행되어야 합니다. 정기적인 백업 없이는 사이버 공격 후 정보를 복구하는 것이 불가능할 수 있습니다.

정보를 백업하는 데 사용할 수 있는 많은 방법과 제품이 있습니다. 사업체 정보 백업에 관한 자세한 조언을 원하시면 **cyber.gov.au/backups**에서 백업에 관한 조언(advice for backups)을 참조하세요. 최선의 선택은 사업체마다 다를 것이기 때문에 확실하지 않은 경우 IT 전문가에게 문의하세요.

✓ **정보를 정기적으로 백업할 계획을 수립하고 실행하세요.**



네트워크 및 외부 서비스를 보호하세요

네트워크의 잠재적인 취약점을 고려해 여러분의 사업체를 사이버 공격으로부터 보호하세요.

네트워크에 연결된 기기와 서비스는 사이버 범죄자의 주요 표적이 될 수 있습니다. 이러한 시스템의 대부분은 보안이 복잡할 수 있으므로 IT 전문가와 다음 권장사항을 논의하세요.

- **서버 보안 확보**: 가정이나 회사에서 NAS 또는 기타 서버를 사용하는 경우 보안에 각별히 주의하세요. 이러한 기기는 중요한 파일을 저장하거나 중요한 기능을 수행하는 경우가 많기 때문에 사이버 범죄자의 일반적인 표적입니다. 이러한 기기를 보호하는 데 필요한 위험 완화 전략이 많이 있습니다. 예를 들어, 모든 서버 또는 NAS 기기를 정기적으로 업데이트하는 것이 중요합니다. 관리자 계정은 강력한 암호문구(passphrase) 또는 다중인증(multi-factor authentication)으로 보호되어야 합니다.
- **외부 통신 범위 최소화**: 네트워크에서 인터넷에 노출된 모든 서비스를 감사하고 보호하세요. 이는 원격 데스크탑, 파일 공유 서비스, 웹메일 및 원격 관리 서비스 등을 포함할 수 있습니다.
- **클라우드 서비스로 이전:** 직접 관리하는 대신 기본 제공 보안을 제공하는 온라인 또는 클라우드 서비스 사용을 고려해 보세요. 예를 들어 이메일이나 웹사이트 호스팅과 같은 서비스를 직접 실행하고 보호하기보다는 온라인 서비스를 사용할 수 있습니다.
- **라우터 보안 개선:** 디폴트 비밀번호 업데이트, 고객 또는 방문자를 위한 "게스트" 와이파이 켜기, 가장 강력한 암호화 절차 사용 등에 관한 정보를 포함하는 라우터 보호 방법(ways to secure your router) 지침을 참조하세요. 더 자세한 정보를 원하시면 **cyber.gov.au**에서 router를 검색하세요.
- **사이버 공급망에 대한 이해:** 현대 기업들은 종종 여러 서비스를 외주합니다. 예를 들어, 회사의 IT를 관리하는 관리 서비스 제공업체(Managed Service Provider)를 고용합니다. 이러한 서비스나 제공업체와 관련된 보안 문제는 여러분의 사업체에 중대한 영향을 미칠 수 있습니다. 사이버 공급망 리스크 관리에 관한 자세한 조언을 원하시면 **cyber.gov.au**에서 사이버 공급망 지침(Cyber Supply Chain Guidance)을 참조하세요.

✓ **네트워크 보호 방법에 관해 IT 전문가와 상의하세요.**

웹사이트를 강화하세요

웹사이트는 사이버 공격의 주요 표적입니다.

간단한 보안 조치를 실행해 웹사이트가 하이재킹되지 않도록 보호하세요:

- 웹사이트 로그인을 다중인증(multi-factor authentication) 또는 강력한 비밀번호로 보호하세요
- 웹사이트의 컨텐츠 관리 시스템 및 플러그인을 주기적으로 업데이트하세요
- 사이버 공격 발생 시 다시 복구할 수 있도록 웹사이트를 주기적으로 백업하세요.

ACSC는 웹사이트 관리자들을 위한 추가 자료를 제공하고 있습니다. **cyber.gov.au**에서 다음 자료들을 찾아 보세요:

- 웹사이트를 위한 간단한 조치(Quick Wins for your Website)
- Certificates, TLS, HTTPS 및 Opportunistic TLS 실행하기(Implementing Certificates, TLS, HTTPS and Opportunistic TLS)
- 도메인 관리자들을 위한 DNS 보안(Domain Name System Security for Domain Owners)
- 서비스 거부 공격에 대한 대비 및 대응(Preparing for and Responding to Denial-of-Service Attacks)

✓ **웹사이트 보안에 관한 ACSC 자료들을 열람하세요.**

기기를 판매 또는 폐기하기 전 초기화하세요

이전 기기의 데이터에 낯선 사람이 접근할 수 있습니다.

기기를 안전하게 폐기하지 않으면 사이버 범죄자들이 해당 기기에 있는 정보를 이용할 수 있습니다. 이는 이메일, 파일 및 기타 사업 데이터를 포함할 수 있습니다. 사무 기기를 판매, 거래 및 폐기하기 전 기기에 담긴 모든 정보를 제거하세요. 예를 들어, 공장 초기화를 실행할 수 있습니다. 이는 기기에 남아있는 정보를 제거하고 기기를 최초 설정으로 초기화할 것입니다.

기기 초기화에 관한 조언을 원하시면 기기를 안전하게 폐기하는 방법(how to dispose of your device securely) 지침을 열람하세요. **cyber.gov.au**에서 dispose를 검색하세요.

✓ **사무 기기를 판매 또는 폐기하기 전 공장 초기화를 실행하세요.**

기기를 잠그고 물리적으로 보호하세요

사무 기기에 대한 접근을 제한함으로써 악의적인 활동의 가능성이 줄어듭니다.

사무 기기에 대한 물리적 접근 제한은 데이터 도난이나 기타 악의적인 활동을 방지하는 간단한 방법입니다. 승인되지 않은 직원이나 일반 대중이 접근할 수 있는 곳에 사무 기기를 보관해서는 안 됩니다.

보안 통제 기능을 사용해 사무 기기를 추가로 보호하세요. 기기들은 최소한으로 암호문구(passphrase), PIN 번호, 또는 바이오메트릭 인증으로 잠겨져 있어야 합니다. 기기가 짧은 시간 동안 사용되지 않으면 자동으로 잠기도록 설정되어 있는지 확인하세요.

✓ **기기가 짧은 시간 동안 사용되지 않으면 자동으로 잠기도록 설정하세요.**

사업 데이터를 보호하세요

사업체가 보유하고 있는 데이터는 사이버 범죄자에게 탐나는 표적입니다.

데이터 침해 사례는 계속해서 증가하고 있습니다. 여러분의 사업체가 희생양이 되지 않도록 주의하세요. 사업체에서 보유하고 있는 데이터와 보관 위치를 이해하는 것이 중요합니다. 이를 파악한 후, 본 지침의 권장사항을 따라 사이버 범죄자가 여러분의 데이터에 접근하지 못하도록 보호하세요. 일부 소사업체는 법률에 따라 추가 의무가 있을 수도 있습니다.

- **사업 데이터를 하나로 통합하세요.** 여러 기기 또는 서비스에 걸쳐 데이터가 저장되어 있을 수 있습니다. 데이터가 분산되면 보안을 유지하고 백업해야 하는 시스템의 수가 늘어납니다. 또한 다수의 시스템 보유는 사이버 범죄자가 공격할 더 많은 기회를 만들 수 있습니다. 가능한 한 사업 데이터를 안전하고 정기적으로 백업되는 하나의 중심 위치에 저장하세요. 데이터를 한 곳에 보관하게 되면 시스템 손상 시 더 큰 위반이 발생할 수 있으므로 이 중앙 위치가 안전한 설정과 제한된 접근으로 적절하게 보호되고 있는지 확인하세요. IT 또는 사이버 보안 전문가에게 조언을 구하세요.
- **정보 보호 관련 여러분의 의무를 숙지하세요.** 일부 소사업체의 경우 수집한 개인 정보 취급에 대한 법적 의무가 있을 수 있습니다. 더 자세한 정보를 원하시면 **oaic.gov.au**에서 호주정보위원회(OAIC)의 소기업을 위한 지침 (guide for small businesses)을 열람하세요. 확실하지 않은 경우 법률 전문가와 상담하세요.

✓ **여러분의 사업체가 보유하는 정보와 이를 보호해야 하는 여러분의 의무를 이해하세요.**

직원을 훈련시키세요

직원들에게 교육을 제공하세요

올바른 사이버 보안을 실천하는 직원은 사이버 공격에 대한 제1방어선입니다.

직원들은 다음 주제를 포함한 사이버 보안에 대한 이해도가 있어야 합니다:

- 사무 이메일 손실 및 랜섬웨어(ransomware)와 같은 흔한 사이버 보안 위협
- 강력한 비밀번호 또는 암호문구 (passphrase), 다중인증(MFA) 및 소프트웨어 업데이트를 포함한 안전 조치
- 스캠(사기) 및 피싱(phishing) 공격 인식 방법
- 사업 고유 정책 (예: 의심 이메일 신고 절차 또는 대금 지급 전 인보이스 진위성 확인 절차 등)
- 비상상황 시 해야 할 일

ACSC 웹사이트 cyber.gov.au/learn에서 이러한 주제 대부분에 대한 자료를 제공하고 있습니다. 공식 과정 또는 내부 교육 제공 등 직원을 교육할 수 있는 다른 방법을 고려할 수 있습니다. 어느 방법을 선택하든, 사이버 보안 훈련은 일회성 요건이 아닌 주기적으로 실행되어야 하는 훈련임을 기억하세요.

✓ **여러분의 사업체에서 사이버 보안 인식을 어떻게 가르칠 것인지 결정하세요.**

비상계획을 수립하세요

비상계획은 사이버 공격이 여러분 사업체에 미치는 영향을 줄일 수 있습니다.

사이버 보안 사고 대응 시, 매 순간이 중요합니다. 비상계획을 수립함으로써 직원들은 무엇을 해야 할 지 생각하는 시간을 줄이고 사고에 실질적으로 대응하는 데 더 많은 시간을 투자할 수 있습니다.

비상계획을 구상할 때 다음 질문들을 고려해 보세요:

- 직원들이 잠재적 사이버 보안 사고를 신고하는 절차는 무엇인가?
- 지원을 받으려면 누구에게 연락해야 하는가? 예: IT 전문가 및 당사 은행.
- 직원, 이해관계자, 또는 고객에게 사고에 대한 정보를 어떻게 제공할 것인가?
- 주요 시스템이 오프라인으로 전환되면 사업을 어떻게 정상 운영할 것인가?

직원들이 각자 가질 수 있는 역할이나 책임을 포함해 비상계획을 잘 숙지하고 있도록 확인하세요. 시스템이 오프라인 상태일 경우를 대비해 필요시 사용할 수 있는 비상계획 하드카피를 보관하세요.

✓ **사이버 보안 사고를 위한 비상계획을 수립하세요.**

계속해서 정보를 열람하세요

ACSC로부터 최신 정보를 받기 위해 ACSC 파트너가 되세요.

ACSC 파트너가 되어 최신 사이버 보안 위협 및 취약점 관련 정보를 계속해서 열람하세요. 이 서비스는 월간 뉴스레터를 제공하고 새로운 사이버 위협이 식별되면 관련 알림을 보내줍니다.

사이버 보안은 빠르게 진화하고 있는 분야입니다. 사이버 범죄자들은 취약점을 발견한 후 몇 분 이내로 해당 취약점을 적극적으로 악용합니다. 사이버 보안 환경에 대한 정보를 유지하면 여러분의 사업체가 직면할 수 있는 위협과 위협으로부터 보호하는 방법을 이해하는 데 도움이 됩니다.

✓ **ACSC 파트너쉽 프로그램 (Partnership Program)에 여러분의 사업체를 등록하세요.**

면책 조항

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

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

더 자세한 정보를 원하거나, 사이버 보안 사고를 신고하려면 저희에게 연락하세요:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

이 번호는 호주 내에서만 사용되는 번호입니다.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre