SANS SECURITY AWARENESS

# 보안 인식 배포 가이드 - 안전하게 자택에서 근무하기

# 개요

코로나 바이러스로 인해 많은 조직에서 직원들의 자택 근무를 장려하고 있습니다. 하지만 정책, 기술, 안전한 원격 근무를 위한 교육의 부족으로 쉽지 않은 일입니다. 또한, 많은 직원들이 집에서 일한다는 것에 익숙하지 않거나 불편함을 느낍니다. 이 가이드의 목적은 안전하게 업무를 볼 수 있도록 최대한 빠르게 교육하는 것입니다. 이 가이드 사용법에 대한 문의는 support@sans.org 로 보내세요.

현재 직원들은 큰 스트레스와 변화를 겪고 있을 것이며, 당신의 조직 역시 시간과 자원이 제한되어 있을 것입니다. 그래서 이 전략 가이드는 최대한 간단한 교육을 제공하는 데 집중하고 있습니다. 우선 아래 설명한 가장 큰 충격이 될 수 있는 주요 위협에 집중하는 것을 권합니다. 이것을 시작점으로 생각하시면 됩니다. 그 외에 다른 위협이나 추가하고 싶은 주제가 있다면 얼마든지 추가할 수 있습니다. 다만 직원에게 너무 많은 행동, 절차, 기술을 요구할 경우 직원들이 이를 모두 수행하기가 어려워진다는 것은 유념해야 합니다.

# 본 가이드의 사용법

먼저 이 가이드에 있는 내용을 읽은 뒤, 다른 자료의 링크를 다시 열람해보면 어떤 것들을 이용할 수 있는지 대략 파악될 것입니다. 저희는 각 위협마다 조직을 교육하거나 실전에 적용할 수 있는 다양한 자료를 제공하고 있습니다. 여기에서 조직의 필요나 조직 문화에 가장 효과적인 방법을 선택할 수 있습니다. 이 문서를 모두 읽은 후에 이 키트와 함께 제공되는 소통 양식과 팩트시트를 모두 읽고 달성하려는 목표를 더 잘 이해하세요. 이 문서를 검토하고 나면, 이제 협업을 해야 하는 두 개 그룹이 있습니다.

1. **보안팀**: 보안팀과 협업하여 이제부터 관리하려는 위협에 대한 보다 깊은 이해를 얻을 수 있습니다. 이 가이드에서는 직원들이 집에서 겪을 수 있는 가장 일반적인 위협을 최우선으로 꼽았지만, 위협 우선순위는 조직마다 다를 수 있습니다. 미리 안내하자면, 보안팀의 가장 일반적인 실수는 모든 위협을 관리하기 위해 지나치게 많은 정책과 요구를 요구한다는 것입니다. 관리하고자 하는 위협은 최소한으로 유지하세요. 여러 가지 위협을 인식하고 우선순위를 설정하고 나면, 이러한 위협을 관리하기 위한 행동을 확인할 차례입니다. 앞서 말했듯이 자신의 조직에 이를 위한 시간이나 자원이 없다면, 아래 기재한 내용을 활용하시면 됩니다.

2. **소통**: 사람으로 인한 최고 위협을 인식하고 이러한 위협을 관리하기 위한 주요 행동을 파악했다면, 의사소통 담당 팀과 협업하고 직원들에게 이러한 행동을 교육해야 합니다. 의사소통 담당 팀과 긴밀한 협업이 있어야 가장 효과적인 보안 인식 프로그램을 만들 수 있습니다. 가능하면 의사소통 담당 팀원을 보안팀에 포함시키세요. 직원들과 소통할 때 적극적으로 참여할 수 있게 해줄 좋은 동기는 회사에서의 보안 교육뿐 아니라 집에서도 사이버 보안을 구축함으로써 가족과 자신을 지킬 수 있다고 알려주는 것입니다.

최종적으로 이 두 그룹과 협업을 하면 직원들로 하여금 간단한 행동으로 보안을 지킬 수 있게 해주고, 또한 동기 의식을 유발할 수 있습니다. 이 둘은 행동 변화를 불러오는 가장 큰 주요 두 개 요소입니다. 프로그램 배포를 위해 피드백과 의견을 줄 주요 인력이 포함된 자문단을 구성하는 것도 권장합니다. 보안팀과 의사소통 담당 팀 외에도 협업이 필요한 팀으로는 인사팀과 법무팀이 있을 수 있습니다.

## MGT433 디지털 다운로드 패키지

SANS Institute는 2일 교육 코스인 MGT433: 강력한 보안 인식 프로그램의 설계, 유지, 측정을 제공하고 있습니다. 이 밀도 높은 교육 프로그램에서는 강력한 인식 프로그램을 만들고, 인적 위협을 관리 및 측정할 수 있는 모든 이론, 스킬, 프레임워크, 자원을 제공합니다. 이 가이드의 일부로, 자원 계획 및 템플릿의 디지털 다운로드 패키지를 무료로 제공하고 있습니다. 이 자료는 본 프로젝트가 다루는 요구 사항을 훨씬 넘어서는 내용을 포함하고 있지만, 복잡한 원격 배치 또는 규모가 큰 조직에서는 매우 유용할 수 있습니다.

## 직원의 질문에 응답하기

직원들과의 의사소통과 교육 외에 추가로, 실시간으로 사람들의 문의를 받을 수 있는 기술 또는 포럼 사용을 권합니다. 여기에는 전용 이메일 주소, Skype, Slack 채팅 채널이나 Yammer 같은 기타 온라인 포럼이 포함될 수 있습니다. 또는 일주일 동안 여러 번 반복되는 보안 웹캐스트를 송출하면 사람들이 자신에게 가장 좋은 시간대에 실시간으로 참여하고 질문도 할 수 있습니다. 여기서 목표는 사람들이 보안을 쉽게 이해할 수 있게 돕고, 질문이 있는 사람들에게 대답해주는 것입니다. 이것은 직원들이 보안을 더욱 친근하게 여길 수 있는 기회이므로, 이번 기회를 유용하게 사용하시기 바랍니다. 잊지 마세요. 이것이 효과를 거두기 위해서는 보안 채널을 관리하거나 질문에 적극적으로 응답할 수 있는 전담 자원이 필요합니다.

# 위협 및 교육 자료

원격으로 일하는 직원들에게 발생할 수 있는 세 개의 주요 위협을 선정했습니다. 이것은 시작 지점이지만, 귀하의 조직에도 중요한 문제일 수 있습니다. 아래의 각 위협에는 해당 위협을 더 잘 이해하고 교육할 수 있는 다른 자원으로 이어지는 링크가 포함되어 있습니다. 여러 개의 소통 자료가 포함되어 있으니 조직 문화에 가장 잘 부합하는 자료를 선택하면 됩니다. 또한 거의 모든 자료는 다양한 언어로 제공되고 있습니다. 이 모든 것이 너무 힘들고 준비할 시간이 부족하다면, 아래에서 소개하는 두 개의 짧은 자료를 선정하여 배포하는 것을 추천합니다.

1. 안전하게 자택 근무하기 팩트시트 (배포 키트에 포함됨)
2. 사이버 보안 홈 비디오 만들기(영어)는 여기에서 다른 언어로도 이용할 수 있습니다.

## 사회 공학

큰 변화를 겪으며 위급한 환경에 노출된 지금 같은 때에, 원격으로 근무하는 직원들에게 일어날 수 있는 가장 큰 위협은 바로 사회 공학 공격입니다. 사회 공학은 심리를 이용한 공격으로 피해자가 실수하도록 유도하며 혼란스러운 변화의 시기에 특히 잘 통합니다. 사회 공학 공격이 무엇인지 교육할 때 가장 중요한 것은 사회 공학 공격의 가장 흔한 징후를 파악하고 이런 징후를 파악했을 때 어떻게 해야 하는지 알려주는 것입니다. 이메일 피싱 공격에만 집중하지 말고 전화 통화, 문자, 소셜 미디어, 가짜 뉴스 같은 다른 방법도 고려해야 합니다. 이 주제에 대한 교육을 실시하고 이해를 강화해줄 자료는 저희의 사회 공학 지원 자료(Social Engineering Support Materials) 폴더에 준비되어 있습니다. 또한, 여러 개의 언어를 지원하는 SANS 보안 인식 동영상 링크 2개도 제공해드립니다.

- 사회 공학(영어)은 여기에서 다른 언어로도 이용할 수 있습니다.
- 피싱(영어)은 여기에서 다른 언어로도 이용할 수 있습니다.

## 강력한 비밀번호

연례 Verizon DBIR에서 입증된 것처럼 약한 비밀번호는 전 세계적으로 가장 기본적인 침입 수단 중 하나로 활용되고 있습니다. 이 위협을 해소하기 위한 네 개의 주요 행동 지침을 아래에 소개합니다. 이 주제에 대한 교육을 실시하고 이해를 강화해줄 자료는 저희의 비밀번호(Passwords) 폴더에 준비되어 있습니다.

- 암호문(참고: 비밀번호 복잡성 및 비밀번호 만료는 작동 안 함).
- 계정마다 고유한 비밀번호 사용하기
- 비밀번호 관리자
- MFA (다중 인증). 다중 인증이나 이중 인증이라고 부르기도 합니다.

## 최신 시스템

세 번째 위협은 직원들이 사용하는 기술이 항상 최신 운영 시스템, 애플리케이션, 모바일 앱에서 실행되는지 여부입니다. 개인 장비를 사용하는 사람들의 경우에는 자동 업데이트를 활성화해야 할 수 있습니다. 이 주제에 대한 교육을 실시하고 이해를 강화해줄 자료는 저희의 악성코드(Malware) 또는 가정용 사이버 보안 구축하기(Creating a Cybersecure Home) 폴더에 준비되어 있습니다.

### 고려가 필요한 추가 주제

- **Wi-Fi**: Wi-Fi 액세스 포인트를 지키세요. 가정용 사이버 보안 구축하기(Creating a Cybersecure Home) 자료에서 이 주제를 다룹니다. 또한 가정용 사이버 보안 구축하기(영어)도 여기에서 다른 언어로도 이용할 수 있습니다.

- **VPN's**: VPN은 무엇이며 왜 사용해야 하는지 설명합니다. 저희는 VPN에 대한 OUCH 뉴스레터**를 추천합니다**.

- **원격 작업**: 이 내용은 원격으로 작업 중이지만, 집이 아닌 카페, 공항 터미널, 호텔 등에서 작업하는 직원을 위한 것입니다. 원격 작업 교육 영상(영어) 활용도 고려해보세요. 이 영상은 여기에서 다른 언어로도 이용할 수 있습니다.

- **자녀/손님**: 가족/손님이 작업용 기기를 사용하지 못하게 해야 한다는 생각을 강화하려면, 원격 작업 교육 영상(영어) 활용도 고려해보세요. 이 영상은 여기에서 다른 언어로도 이용할 수 있습니다.

- **탐지/대응**: 자택에서 근무하다 사고가 났다고 판단했을 때 사람들이 이를 보고하기를 원하시나요? 그렇다면 어떤 내용을, 언제 보고해야 할까요? 이 내용은 해킹(Hacked) 자료에서 다루고 있습니다.

# OUCH 뉴스레터

또한 20개 이상의 언어로 번역되었으며 공개되어 있는 OUCH 뉴스레터를 활용하여 교육 효과를 강화하세요. 아래는 안전하게 자택 근무하기 교육에 가장 적절한 OUCH 뉴스레터 목록입니다. 온라인 OUCH 보안 인식 뉴스레터 아카이브에서 모든 뉴스레터를 확인할 수 있습니다.

## 개요

Four Steps to Staying Secure ( 안전 유지를 위한 4단계)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home ( 홈 사이버 보안 구축)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

## 사회 공학

Social Engineering (사회 공학)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing ( 메시징/스미싱)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams ( 개인화된 사기)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud ( CEO 사기)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams ( 보이스피싱 전화 사기)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish ( 피싱 예방)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media ( 소셜 미디어를 통한 사기)

https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

### 비밀번호

Making Passwords Simple ( 간단하게 비밀번호 만들기)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) ( 온라인 계정 보안 강화)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

### 추가 자료

Yes, You Are a Target ( 우리가 바로 공격 대상입니다)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices ( 스마트 홈 기기)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

## 간단한 팁

양식에 맞춰 간단하고 쉽게 공유할 수 있는 팁입니다.

- 가정에서 무선 네트워크를 안전하게 지키는 가장 효과적인 방법은 기본 관리자 비밀번호를 변경하고, WPA2 암호화를 활성화하여 강력한 무선 네트워크용 비밀번호를 만드는 것입니다.
- 아기 모니터, 게임 콘솔, TV, 가전제품, 심지어 자동차까지, 가정 네트워크에 연결된 모든 기기를 인식하고 있어야 합니다. 모든 기기는 강력한 비밀번호로 보호해야 하며 최신 버전의 운영 체제를 사용해야 합니다.
- 집에서 컴퓨터를 안전하게 보호하는 가장 효과적인 방법은 바로 패치와 업데이트 설치로 운영 체제와 애플리케이션을 최신 상태로 유지하는 것입니다. 가능하다면 자동 업데이트를 설정해놓으세요.
- 마지막으로, 자신을 보호할 수 있는 가장 좋은 것은 바로 상식입니다. 이메일, 온라인 메시지, 전화

통화가 이상하거나 수상해 보이거나 사실이기에 너무 좋은 내용이면 공격일 수 있습니다.

- 모든 계정에 강력하고 고유한 비밀번호를 사용하세요. 비밀번호를 모두 기억할 수 없나요? 비밀번호 관리자를 사용해 모든 비밀번호를 안전하게 보관하세요.
- 2단계 인증은 어떤 계정이든 안전하게 지킬 수 있는 가장 좋은 방법 중 하나입니다. 2단계 인증은 비밀번호와 모바일 기기에서 생성 또는 전송되는 코드 모두 있어야 합니다. 2단계 인증을 사용하는 주요 서비스로는 Gmail, Dropbox, Twitter가 있습니다.
- 피싱은 악성 링크를 클릭하거나 이메일의 첨부 파일을 열도록 속이는 공격입니다. 긴급한 분위기를 자아내거나, 맞춤법 또는 철자가 틀렸거나, 수신자를 '고객님'으로 부르는 등의 이메일 또는 온라인 메시지는 모두 의심하세요.

## 수치화

사람들이 집에서 하는 활동은 측정이 어렵기 때문에 행동을 수치화하기는 어렵습니다. 그리고 사람들의 어떤 행동은 업무와 관련이 없는 것일 수도 있습니다. (예: Wi-Fi 기기의 보안을 강화하는 행위) 하지만 사람들의 참여도는 측정이 가능합니다. 개인적이거나 감정적인 주제가 되면 사람들은 매우 적극적으로 변하고, 다른 주제보다 더 큰 흥미를 느낍니다. 따라서 다음 행동 수치는 나름의 가치를 가지고 있을 수 있습니다.

- **상호작용**: 호스팅 중인 보안 채널 또는 포럼에서 사람들이 얼마나 자주 질문을 하고, 아이디어를 게시하고, 도움을 요청합니까?
- **시뮬레이션**: 피싱, 문자 메시지, 전화 통화 공격 등 사회 공학 시뮬레이션을 실시해봅니다.

더 다양한 수치화 목록은 MGT433 디지털 다운로드 패키지의 상호작용 보안 인식 수치화 메트릭스에서 확인 가능합니다.

# 라이선스



# 배포 키트 저자

Lance Spitzner는 사이버 위협 연구, 보안 아키텍처, 보안 인식 및 교육 분야에서 20년 이상의 경험을 쌓아왔습니다. Honeynet Project의 창설자이며, 허니넷 제작을 통해 사이버 정보 및 첩보 분야를 개척했습니다. SANS 교육 강사로서 MGT433:보안 인식 및 MGT521: 보안 문화 코스를 개발했습니다. 또한 Lance는 세 권의 보안 서적을 출판했고, 25개국에서 보안 자문을 맡고 있으며 350개 이상 단체에서 보안 인식 및 문화 프로그램 설계를 도와 인적 위협을 최소화하는 데 공헌했습니다. Lance는 활발한 강연 활동 및 트위터 활동(@lspitzner)을 이어나가고 있으며, 다수의 커뮤니티 보안 프로젝트에도 참여 중입니다. 정보 보안을 하기 전 Spitzner는 군대의 긴급 배치군 기갑 장교로 복무했고, 일리노이 대학에서 MBA를 취득했습니다.

# SANS Institute 정보

SANS Institute는 1989년 협동 연구 및 교육 조직으로 설립되었습니다. SANS는 지금까지 가장 신뢰받고 있는 가장 규모가 큰 사이버 보안 교육 프로그램 제공자이자 세계 여러 국가의 정부 및 상업 기관의 전문가들을 육성해내는 인증 업체입니다. 명망 있는 SANS 교육 강사들이 200회 이상의 사이버 보안 교육 이벤트 및 온라인 교육으로 60개 이상의 코스를 교육 중입니다. SANS Institute의 협업체인 GIAC는 35개 이상의 실무 자격 및 사이버 보안 기술 증명서를 발급하는 인증 업체입니다. SANS Technology Institute는 지역 허가를 받은 독립 단체이며, 사이버 보안 석사 학위를 제공하고

있습니다. SANS는 InfoSec 커뮤니티에 합의 프로젝트, 연구 보고서, 뉴스레터 등 무수히 많은 무료 리소스를 제공합니다. 또한 인터넷 초기 경고 시스템인 Internet Storm Center를 운영하고 있기도 합니다. SANS의 중심에는 기업에서부터 대학에 이르기까지 세계적인 단체를 대표하는 많은 보안 실무 전문가들이 있으며, 이들은 공동으로 협업하여 정보 보안 커뮤니티의 발전을 돕고 있습니다. (https://www.sans.org)