

# 마이크로소프트 팀즈:

- 안전한 협업을 제공하는 보안 알아보기

## 팀즈의 보안 개요

이 준 형



Windows and Device for IT MVP

✉ [randy\\_ljh@hotmail.com](mailto:randy_ljh@hotmail.com)





# |준비한 내용



- Teams에 탑재된 보안 기능



1. Teams의 인증 및 접근 보안:

- ✓ Conditional Access, MFA
- ✓ Information Barriers



2. Teams의 정보 보안:

- ✓ Data Loss Prevention
- ✓ Mobile Application Management



3. Teams의 위협 대응:

- ✓ ATP(Safe-link, Safe-attachment)

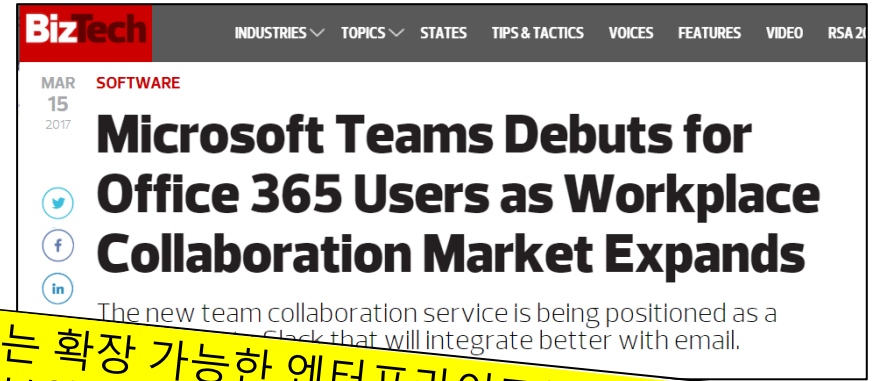
# |마이크로소프트 팀즈의 보안

## 이미 단단한 기반 위에서 서비스

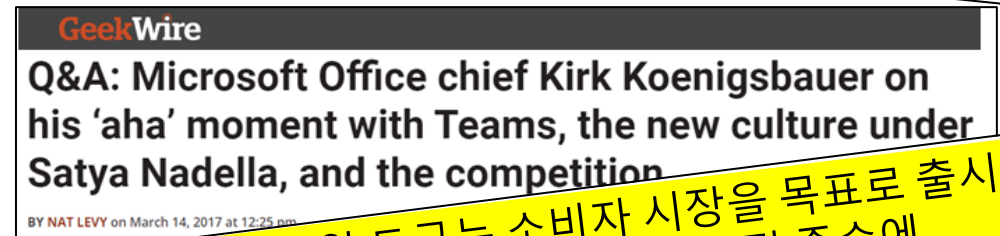
- Office 365, Microsoft 365, 그리고 Azure를 기반으로 구축
- 머신러닝과 AI를 기반으로 한 지능형 보안 그래프 플랫폼

## 마이크로소프트 팀즈의 주요 보안 원칙

- 물리적: 비 인가 접근의 방지, 전체 활동의 감사
- 데이터: 생성, 전달, 공유, 저장에 이르는 보호
- 계정(ID): 인증 및 액세스를 위한 여러 계층의 제어 기능
- 거버넌스: 쉬운 설정과 확장 연계가 가능한 정책
- 에코시스템: 조건부 액세스, 엔드포인트 관리자, 애저 정보 보호, 애저 액티브 디렉토리와 같은 보안 요소를 완벽하게 통합 지원



O365는 확장 가능한 엔터프라이즈급의 클라우드 서비스와 고급 보안 기술과 컴플라이언스를 제공  
search, eDiscovery and legal hold for channels, chats and files as well as mobile application management with Microsoft Intune. And starting today, Microsoft Teams is automatically provisioned within Office 365."



대다수의 많은 협업 도구는 소비자 시장을 목표로 출시를 했기 때문에 기업이 기대하는 보안 및 규정 준수에 투자를 하지 않았다  
Teams is part of that and inherits all those standards. We've got all these things that we know our customers care about. When I go to groups and companies they want to deliver these great end user tools but they want to make sure they are also secure because they have seen enough horror stories.

# 팀즈의 접근 보안

---

## Episode 1



### MFA, Conditional Access(다단계 인증, 조건부 액세스)

강력하지만 간편한 인증 방식의 적용과, 무단 접근의 위험으로 부터 보호

## Episode 2



### Information Barriers (정보 장벽)

특정 조직이나 게스트와의 검색과 커뮤니케이션을 차단하기 위한 서로 다른 세그먼트로 분리

# 팀즈의 정보 보안

---

## Episode 3



### Data Loss Prevention(데이터 손실 방지)

중요한 콘텐츠의 공유나 위반을 감지하여 민감한 정보나 개인 정보의 유출을 방지

## Episode 4



### Mobile Application Management (모바일 앱 관리)

모바일 앱을 통한 대한 데이터의 공유를 제어 및 관리하여 중요한 데이터 보호

# 팀즈의 위협 대응

---

## Episode 5



### Safe-Link, Safe-Attachment(안전한 링크, 안전한 첨부파일)

첨부된 링크와 파일도 안전하게 검사를 통해서 실행이 되도록 하여 위협으로부터 보호

# 팀즈의 인증 및 접근 보안

---

## Episode 1



### MFA, Conditional Access(다단계 인증, 조건부 액세스)

강력하지만 간편한 인증 방식의 적용과, 무단 접근의 위험으로 부터 보호

## Episode 2



### Information Barriers (정보 장벽)

특정 조직이나 게스트와의 검색과 커뮤니케이션을 차단하기 위한 서로 다른 세그먼트로 분리

# Multi-factor authentication(다단계 인증)

81%

의 사이버 침해가  
도난 당했거나  
취약한 암호를 활용

MFA를 사용하면

99.9%

의 계정 기반  
공격을 차단



자격 증명을 강화하기 위해서는...

- 암호를 사용하지 않는 체계로의 전환
- 빠르고 안전한 다단계 인증 체계의 적용

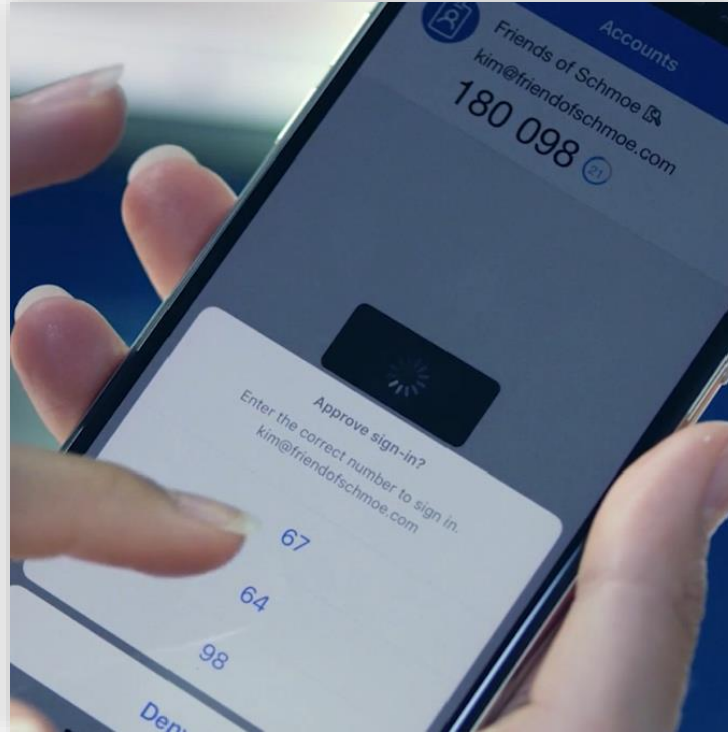


# 암호를 사용하지 않는 보안 변화

윈도우 헬로



마이크로소프트 인증 앱

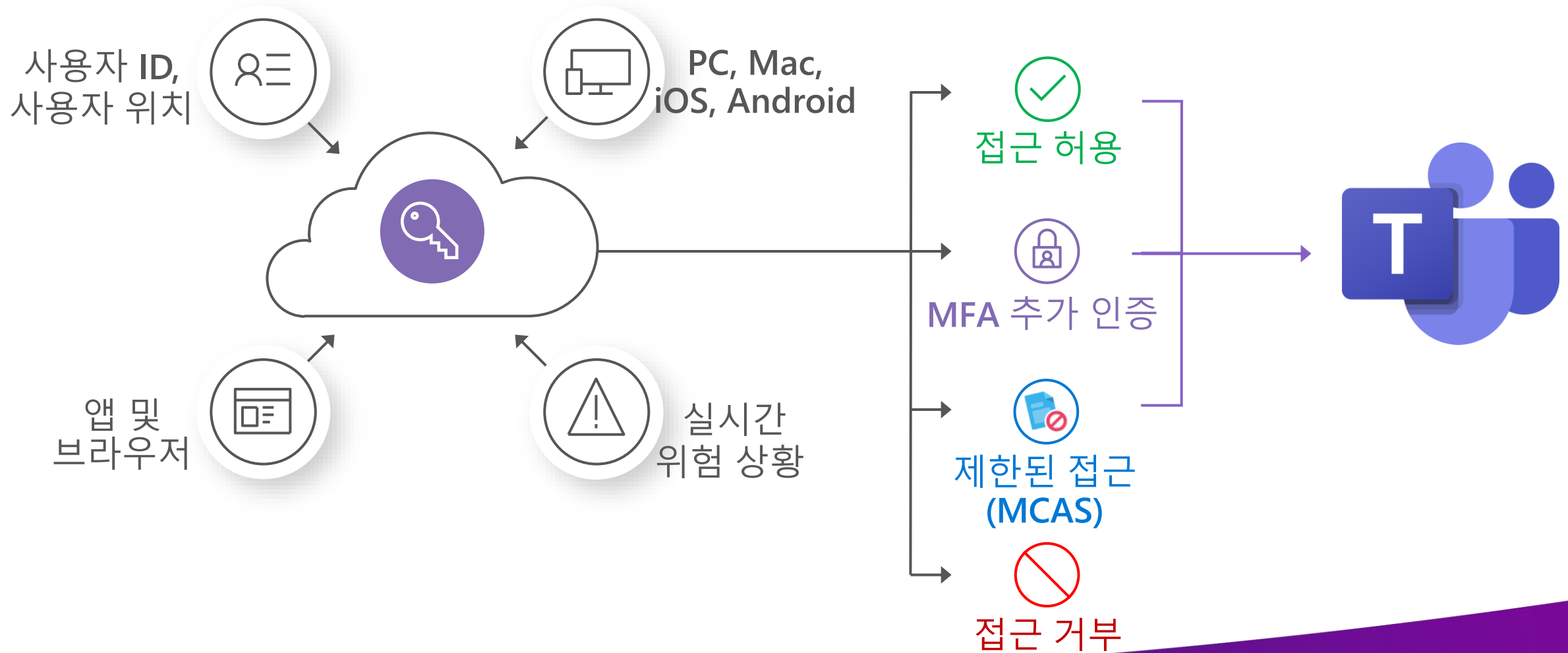


FIDO2 보안 키



**100M+** 암호를 사용하지 않는  
MSA & Azure AD 사용자

# Conditional Access(조건부 액세스)



# 조건부 액세스 정책으로 접근 차단

Microsoft Azure

리소스

홈 > 조건부 액세스 | 정책 > Conditional Access for Device Enrollment

Conditional Access for Device Enrollment

조건부 액세스 정책

삭제

이전 구성 환경으로 다시 전환하시겠습니까? 미리 보기를 종료하려면 클릭하세요. →

조건부 액세스 정책에 따라 사용자 액세스를 제어하여 신호를 하나로 통합하고 의사 결정을 내리고 조직 정책을 적용하세요. [자세한 정보](#)

모든 또는 특정 클라우드 앱 또는 작업을 기반으로 사용자 액세스를 제어합니다. [자세한 정보](#)

이 정책을 적용할 항목을 선택합니다.

클라우드 앱

사용자 작업

포함

제외

☐ 없음

☐ 모든 클라우드 앱

☒ 앱 선택

선택

Microsoft Teams

Microsoft Teams

cc15fd57-2c6c-4117-a88c-83b1d56b...

...

이름 \*

Conditional Access for Device Enrollment

할당

사용자 및 그룹 ①

특정 사용자가 포함됨

클라우드 앱 또는 작업 ①

앱 1개 포함됨

조건 ①

조건 2개 선택됨

액세스 제어

허용 ①

컨트를 2개 선택됨

세션 ①

앱 적용 제한 사용

Microsoft

지금은 액세스할 수 없습니다.

정상적으로 로그인되었지만 이 리소스에 액세스할 수 있는 기준을 충족하지 않습니다. 예를 들어 관리자가 제한하는 브라우저, 앱 또는 위치에서 로그인하는 것일 수도 있습니다.

[다른 계정으로 로그인 및 로그인](#)

[추가 정보](#)

Microsoft

여기서는 거기에 접근할 수 없습니다.

이 애플리케이션에는 중요한 정보가 포함되어 있으며 다음에서만 액세스할 수 있습니다.

- MWA: 관리 준수 정책을 충족하는 디바이스 또는 클라이언트 애플리케이션입니다.

Chrome을 사용 중이므로 이 [확장](#)을 설치해야 합니다. Windows 10 1703 버전 이상을 사용하거나 Microsoft Edge나 Internet Explorer를 사용하여 이 애플리케이션에 액세스할 수 있습니다.

이 작업을 지금 수행할 계획이 없다면 다른 MWLab 사이트로 이동할 수 있습니다. 그렇지 않으면 [계정 보호를 위해 로그인](#)하세요.

[다른 계정으로 로그인 및 로그인](#)

[추가 정보](#)

IP 기준으로 지정된 위치가 아닌 곳에서 접근했을 경우

인증된 사용자가 허용되지 않는 장치에서 접근했을 경우

# 데모: 팀즈의 인증 및 접근 보안

MFA(다단계 인증),  
Conditional Access (조건부 액세스)



# 팀즈의 인증 및 접근 보안

---

## Episode 1



### MFA, Conditional Access(다단계 인증, 조건부 액세스)

강력하지만 간편한 인증 방식의 적용과, 무단 접근의 위험으로 부터 보호

## Episode 2



### Information Barriers (정보 장벽)

특정 조직이나 게스트와의 검색과 커뮤니케이션을 차단하기 위한 서로 다른 세그먼트로 분리

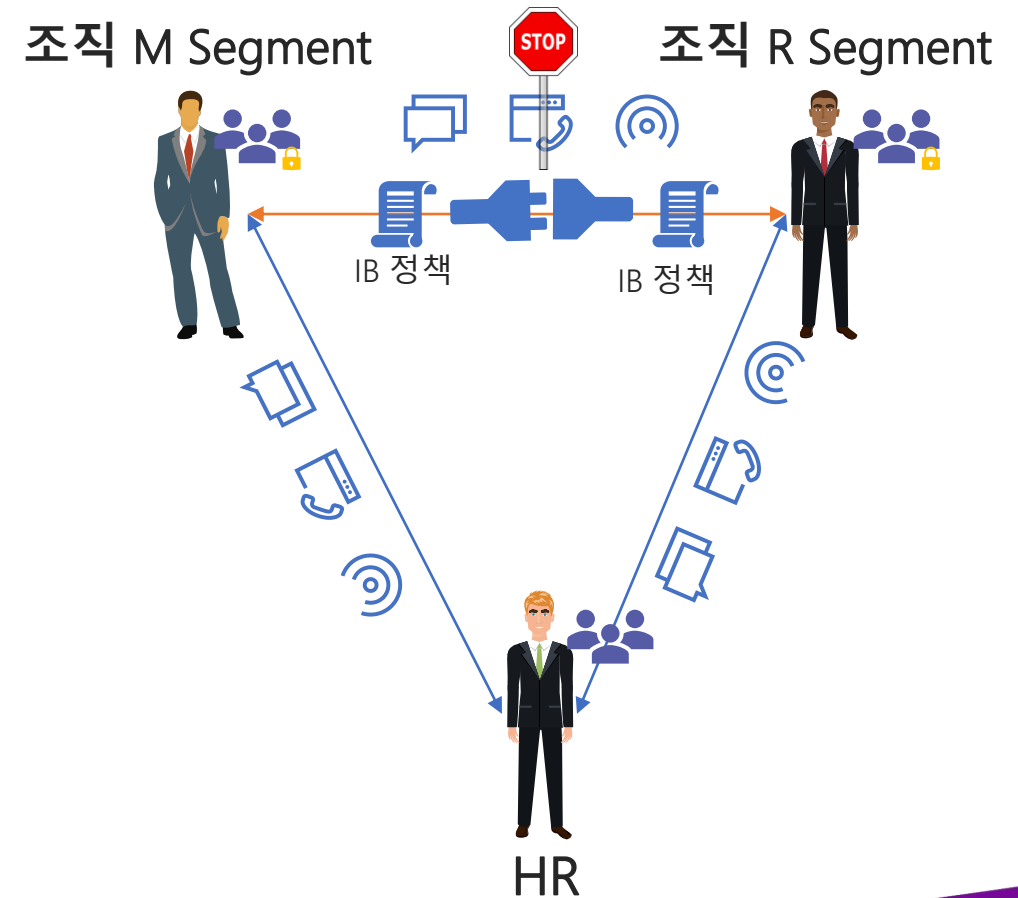


# Information barrier(정보 장벽): “윤리적인 벽”

조직에서 공유를 제한하고, 정보의 흐름을 제어하며, 전체 사용자를 세그먼트로 분리하여 서로 격리해야 하는 경우

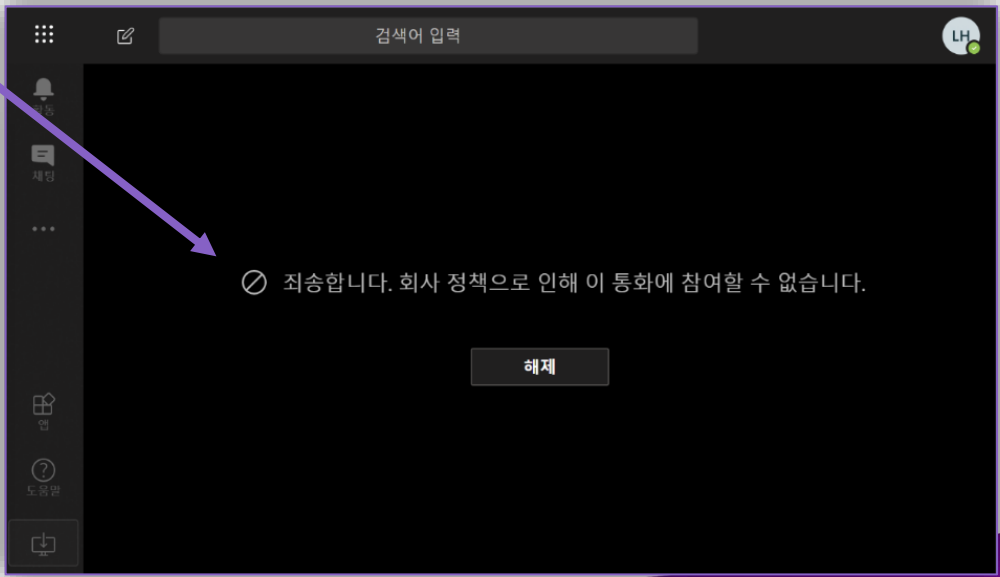
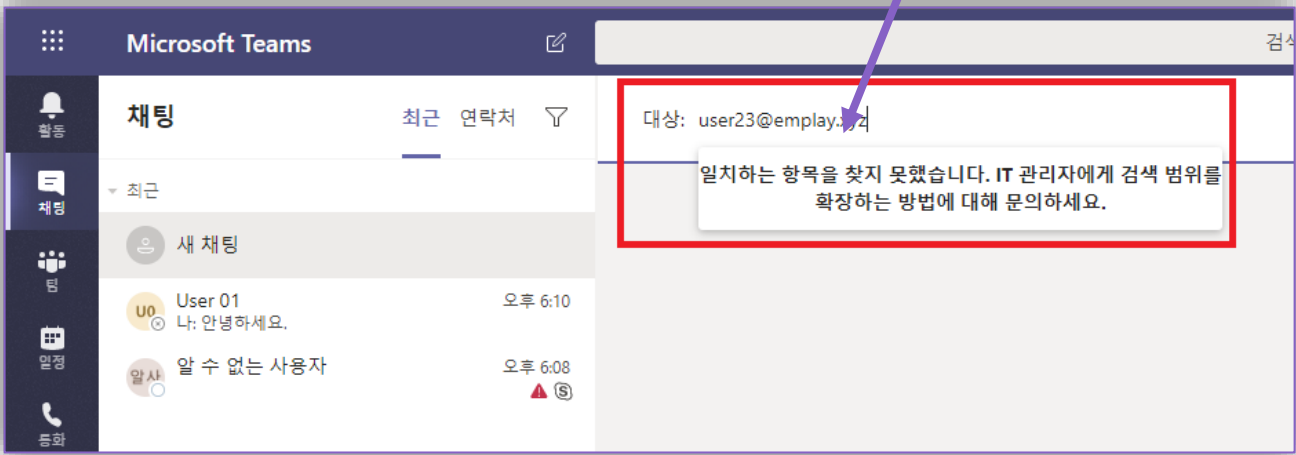
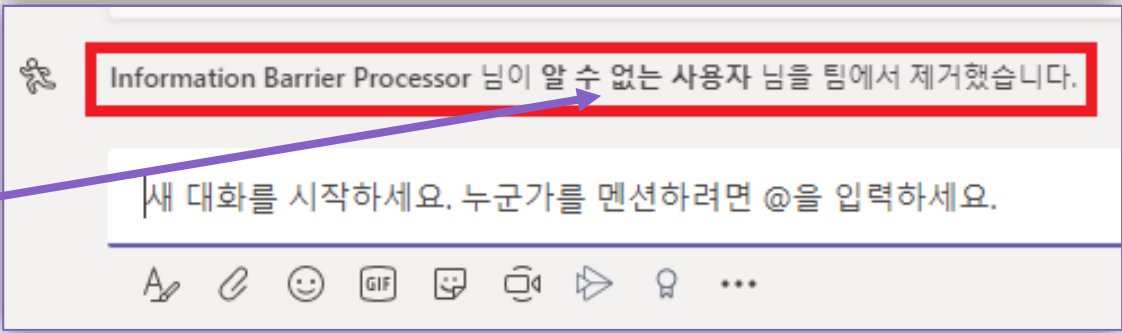
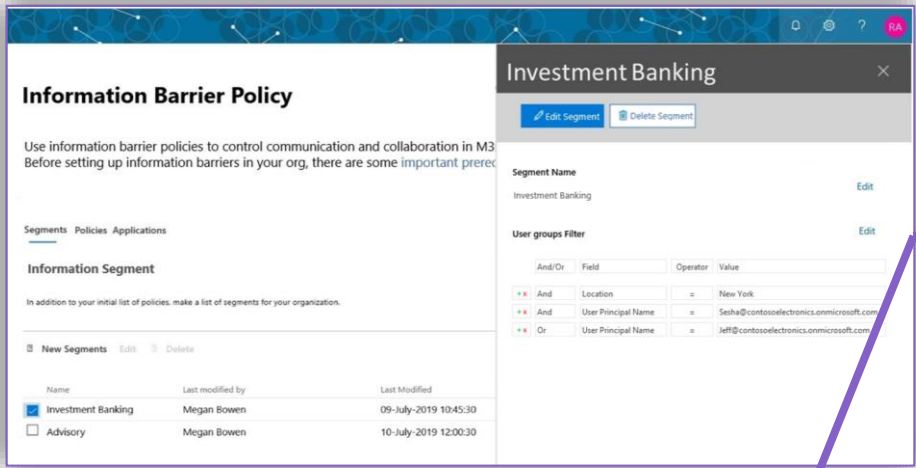
Information Barriers의 차단 역할:

- 팀이나 회의에 사용자를 초대하기 위한 사용자 검색
- 채널 대화와 채팅 메시지, 화면 공유, 통화 및 회의
- SharePoint의 파일 접근에도 적용



# 정보 장벽 정책

채널 대화



모임

사용자 검색

# 데모: 팀즈의 인증 및 접근 보안

Information Barriers(정보 장벽)



Type here to search



# 팀즈의 정보 보안

---

## Episode 3



### Data Loss Prevention(데이터 손실 방지)

중요한 콘텐츠의 공유나 위반을 감지하여 민감한 정보나 개인 정보의 유출을 방지

## Episode 4



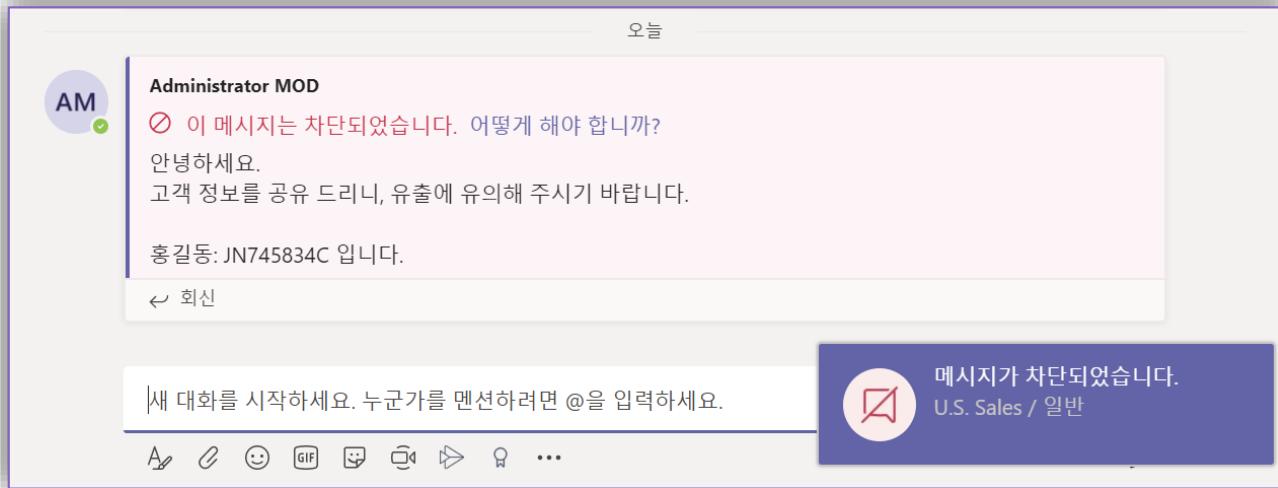
### Mobile Application Management (모바일 앱 관리)

모바일 앱을 통한 대한 데이터의 공유를 제어 및 관리하여 중요한 데이터 보호

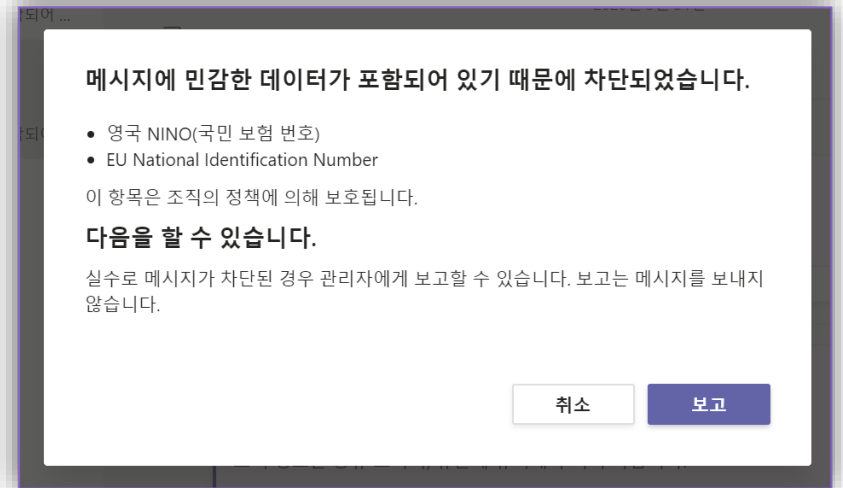
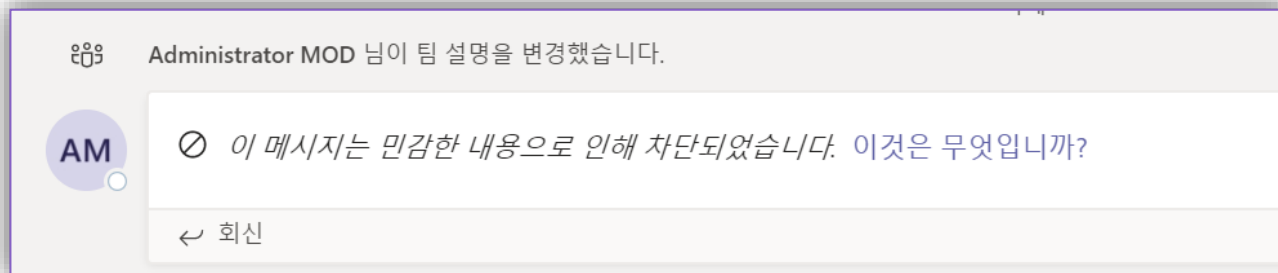
# Data Loss Prevention (데이터 손실 방지)

사용자가 의도하지 않은 실수로 고객이나 프로젝트의 기밀이 될 수 있는 중요한 정보를 대외적으로 공유하는 것을 방지

메시지  
발신자




메시지  
수신자







 Jordan Miller 7/3

$$+$$

...

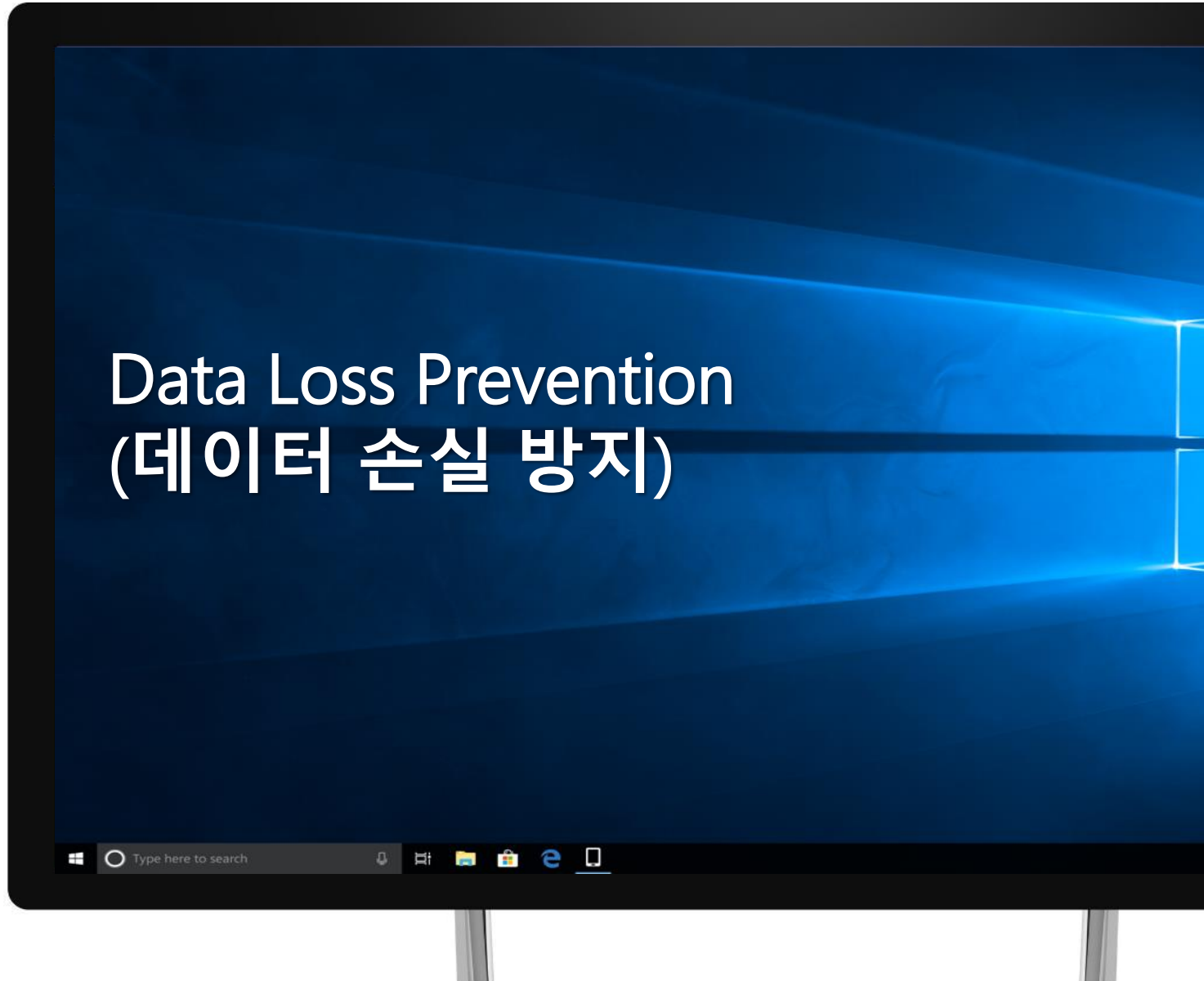


♥ 1

✎ ! 📎 😊 GIF 🗨️ 📅 🗂️ ⋮

# 데모: 팀즈의 정보 보안

Data Loss Prevention  
(데이터 손실 방지)



# 팀즈의 정보 보안

---

## Episode 3



### Data Loss Prevention(데이터 손실 방지)

중요한 콘텐츠의 공유나 위반을 감지하여 민감한 정보나 개인 정보의 유출을 방지

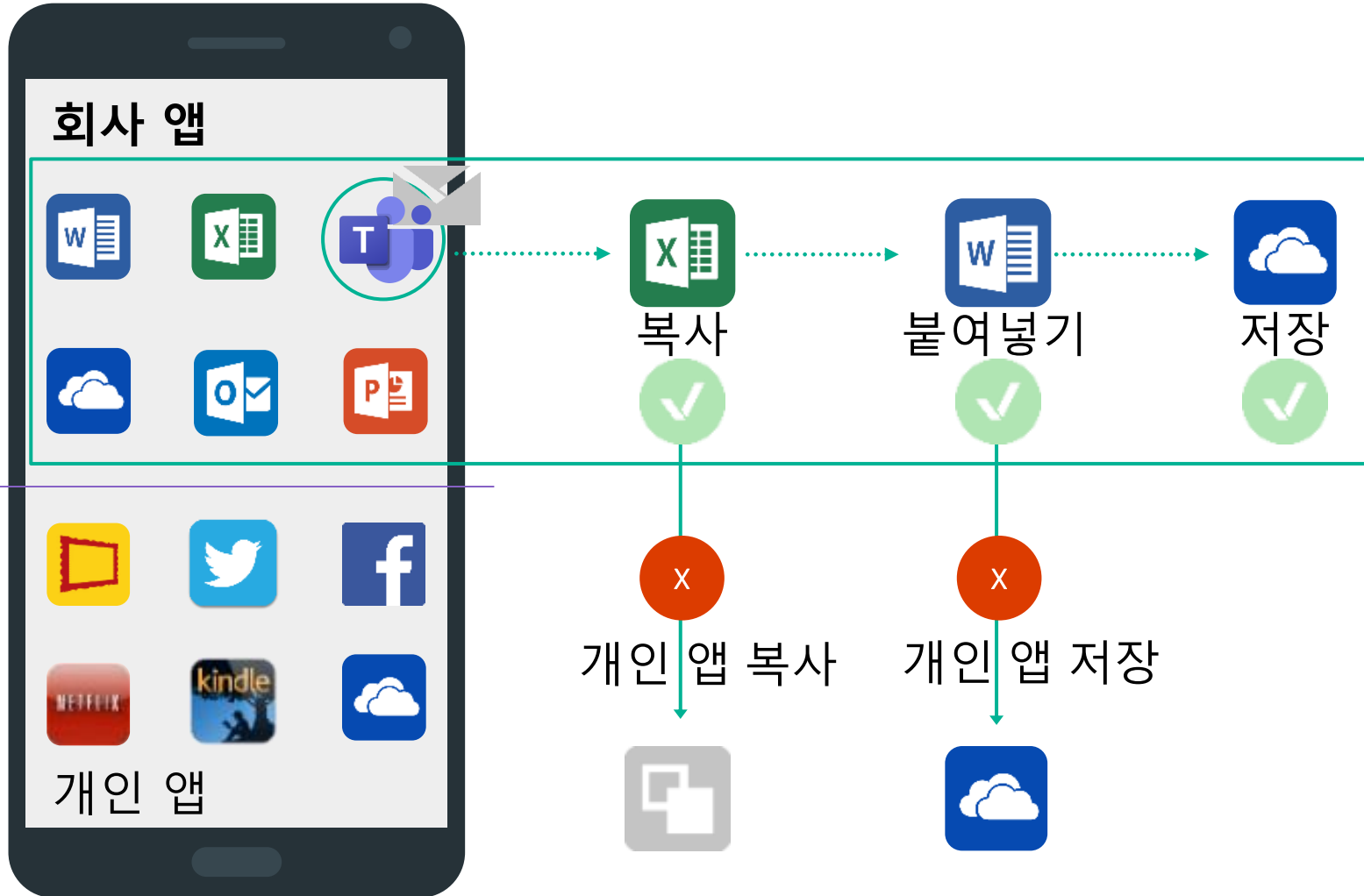
## Episode 4



### Mobile Application Management (모바일 앱 관리)

모바일 앱을 통한 대한 데이터의 공유를 제어 및 관리하여 중요한 데이터 보호

# Mobile Application Management (모바일 앱 관리)



모바일 앱 관리 정책:

- 회사 앱 실행 시 **PIN** 요구
- 회사 앱과 개인 앱 간의 데이터 이동 제어
- 내용의 복사/붙여넣기의 제어
- 조건부 액세스 정책을 기반으로 접근 제어

# 데모: 팀즈의 정보 보안

Mobile Application Management  
(모바일 앱 관리 a.k.a MAM)





# 팀즈의 위협 대응

---

## Episode 5



### Safe-Link, Safe-Attachment(안전한 링크, 안전한 첨부파일)

첨부된 링크와 파일도 안전하게 검사를 통해서 실행이 되도록 하여 위협으로부터 보호


# ATP (Safe-Links, Safe-Attachments)

## Safe-Links(안전한 링크)

Junhyoung Lee 오후 5:34  
다운로드가 안되시면 아래의 링크에서 받으세요.

[다운로드](#)

← 회신

 이 웹 사이트는 악성으로 분류되었습니다.

이 웹 사이트를 열면 위험할 수 있습니다.

<https://spamlink.contoso.com/>


이 웹 사이트를 열지 않는 것이 좋습니다. 웹 사이트를 열면 위험할 수 있으며, 컴퓨터가 손상되거나 개인 데이터가 악의적으로 사용될 수 있습니다.


제공: Office 365 Advanced Threat Protection

## Safe-Attachments(안전한 첨부 파일)


모두 축소

Junhyoung Lee 오후 5:40

 ReadMe.txt ...

 MarketingProposal.docx ...

← 회신



MarketingProposal.docx

To protect your PC and other files, we've removed Open, Share, and other commands. Contact your admin for options or [learn more.](#)

사용자가 위협을  
인지하지 못하더라도 ATP  
엔진이 확인 및 조치

사용자에게는 경고  
메시지 전송

ATP에서 위협을 판단하지  
못하면 Sandbox에서  
Detonation하여 위협의  
패턴을 감지

Teams를 포함하여  
SharePoint, Exchange  
지원

# 데모: 팀즈의 위험 대응

Safe-Links(안전한 링크),  
Safe-Attachments(안전한 첨부 파일)



# 더 많은 정보: 팀즈의 인증 및 접근 보안

---

Azure MFA 구성: <https://bit.ly/3iWHNkg>

MFA 상세: <https://bit.ly/2RNRTTrP>

Conditional Access(조건부 액세스) 배포: <https://bit.ly/33SYvdP>

SMS 로그인과 사용자 관리: <https://bit.ly/3cmMotm>

Information Barriers(정보 장벽): <https://bit.ly/3i0hGHD>

Guest 접근에 대한 개요: <https://bit.ly/33W8sqY>

Guest 접근 관리: <https://bit.ly/3606ngr>

Tenant Restrictions(테넌트 제한): <https://bit.ly/3kHx1yE>

# 더 많은 정보: 팀즈의 정보 보안

---

Teams compliance 개요: <https://bit.ly/3iXchCu>

Teams의 DLP: <https://bit.ly/303qXsr>

라이선스 요구사항: <https://bit.ly/3mT0ckv>

O365의 정보 보안과 거버넌스 및 데이터 보존: <https://bit.ly/32VCRGB>

Windows Information Protection: <https://bit.ly/301x8xn>

SharePoint의 위치 기반 접근 정책: <https://bit.ly/32UNw4D>



# 더 많은 정보: 팀즈의 위협 대응

---

Microsoft Endpoint Manager 개요: <https://bit.ly/33RfnSq>

Device 관리 (MDM) 개요: <https://bit.ly/3clqC9y>

App 관리 (MAM) 개요: <https://bit.ly/3cq7reU>

Microsoft Teams – Safe Links: <https://bit.ly/2RNwMWy>

Microsoft Teams – Safe Attachments: <https://bit.ly/3cq8n2U>

# 마이크로소프트 팀즈:

- 안전한 협업을 제공하는 보안 알아보기

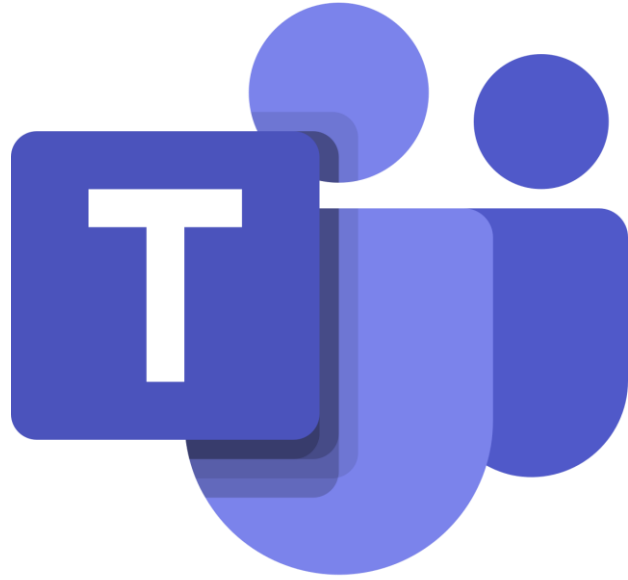
## 팀즈의 보안 개요

이 준 형



Windows and Device for IT MVP

✉ [randy\\_ljh@hotmail.com](mailto:randy_ljh@hotmail.com)



고맙습니다.

 [facebook.com/groups/M365forIT](https://facebook.com/groups/M365forIT)



3 Office MVPs and 2 Windows MVPs