

Microsoft 365 Exchange Online 보안

발표자 : 안 태윤

<http://bit.do/taeyoun>



Contents

Ep1.Office 365 그룹 개요

Ep2. 랜섬웨어 대응과 정보 추출 방지 기능

- A. 랜섬웨어에 대한 전자 메일 규칙 만들기
- B. 전자 메일 자동 전달 중지
- C. 피싱 방지 보호 기능 설정

Ep3. ATP 안전 첨부 파일 및 링크 관리

- A. ATP 안전 첨부 파일 관리
- B. ATP 안전 링크 관리



Microsoft 365 그룹 개요

발표자 : 안 태윤

<http://bit.do/taeyoun>



Office 365 Groups

Microsoft 365에서
협업 강화



이메일, 일정 관리, 문서 등을 사용하여
지식 및 정보 공유



안전하고 통제 된 방식으로
커뮤니케이션 가능



협업 기능 생성 및 사용 간소화



셀프 서비스 기능을 활용하여
비용 절감 및 시간 절약

Microsoft 365에서 협업 강화

Membership service for Microsoft 365 teamwork apps

22+ Apps



Advanced sharing



Office 365 Groups

Partner ecosystem



atwork

AvePoint

LawToolBox.com

ShareGate

Centrally managed, secured, and governed






Azure Active Directory

그룹 비교 테이블

	설명
보안 그룹	파일서버 또는 Sharepoint 리소스에 대한 액세스 권한을 부여 하는 데 사용 됩니다.
메일 그룹	Exchange 또는 Exchange Online 에서 사용자가 구성원 들에게 대표 메일을 구성 하는 경우에 사용 됩니다.
메일 사용이 가능한 보안 그룹	파일서버 또는 Sharepoint 리소스에 대한 액세스 권한을 부여 하고 대표 메일을 구성 하는 경우에 사용 됩니다.
공유 사서함	대표 회사 메일 주소를 동일한 사서함에 액세스 해야 하는 사용자가 여러 명 인 경우에 사용 됩니다.
Office 365 그룹	Office 365 그룹은 회사 내부 및 외부의 사용자 간 공동 작업에 사용 됩니다. 각 Office 365 그룹에서 구성원은 대화, 파일, 일정에 대한 그룹 전자 메일 및 공유 작업 영역을 가져옵니다.

Office Apps의 Office 365 그룹 가시성

<p>Create</p> 	 <h2>Outlook</h2> <p>아웃룩에서 만든 Office 365 그룹은 Teams에서 보이질 않습니다.</p>	 <h2>Teams</h2> <p>Teams에서 만든 Office 365 그룹은 아웃룩에서 보이질 않습니다.</p>
---	---	---

Office 365 Groups 은 Microsoft 365 Groups 변경 예정 입니다.
2020년 9월말



감사합니다.

다음 에피소드
랜섬웨어 대응과 정보 추출 방지 기능

함께 빛나는 우리



@TaeYoun.Community

랜섬웨어 대응과 정보 추출 방지 기능

발표자 : 안 태윤

<http://bit.do/taeyoun>

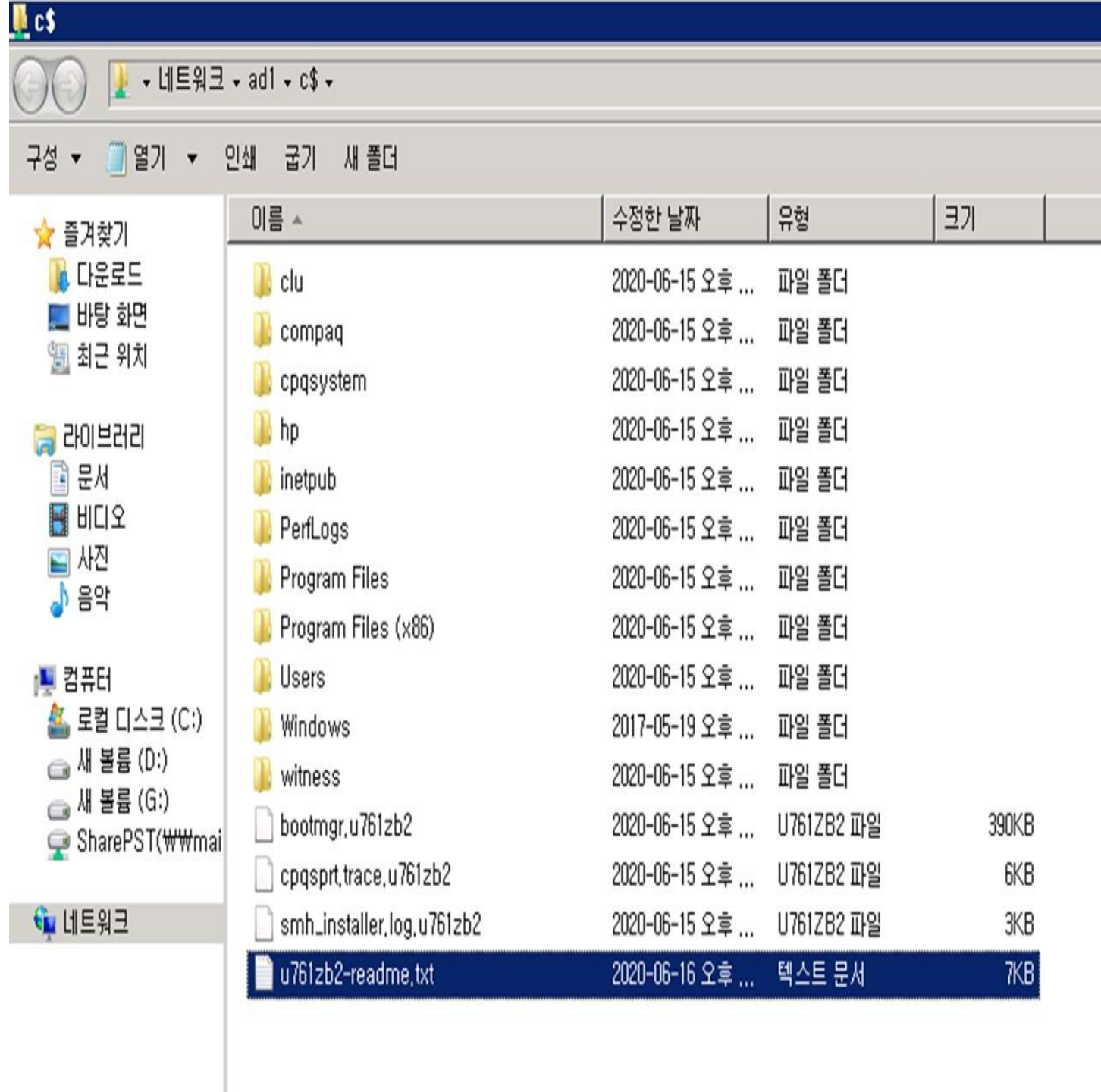


Contents

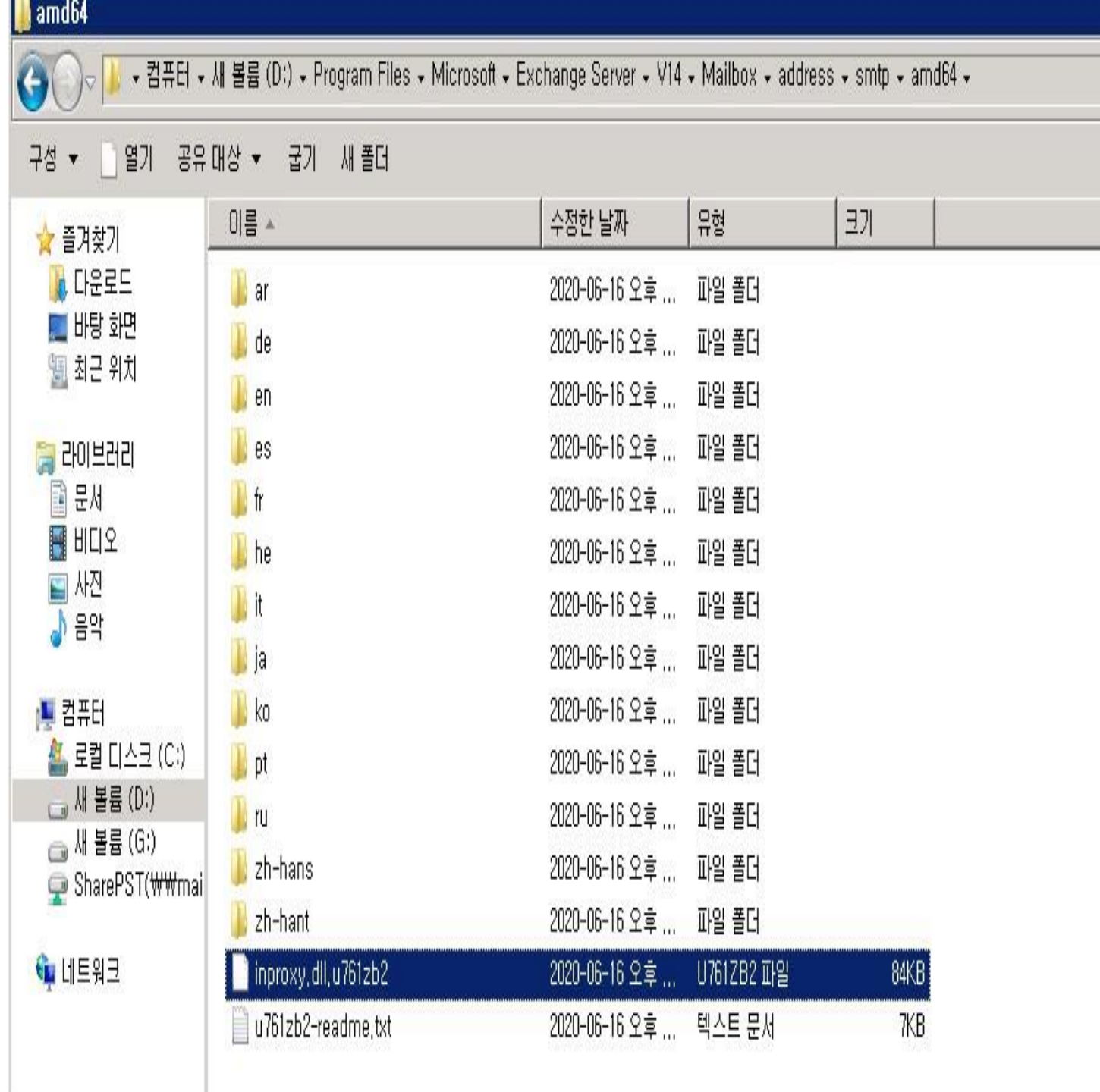
1. 랜섬웨어에 대한 전자 메일 규칙 만들기
2. 전자 메일 자동 전달 중지
3. 피싱 방지 보호 기능 설정



랜섬웨어 감염된 화면



랜섬웨어 감염된 화면



1. 랜섬웨어에 대한 전자 메일 규칙 만들기

- 마이크로소프트 365는 JavaScript, 배치, 실행 파일 등 잠재적으로 위험한 파일이 Outlook에서 열리지 않도록 하여 랜섬웨어로부터 비즈니스를 보호하도록 도움을 줍니다.
- 추가로 파일 형식을 차단하거나 경고하는 규칙을 추가하여 보호 수준을 높이려면 다음 단계를 수행합니다.

조건 추가

* 다음 작업을 수행...

✕ 설명이 포함된 메시지 거부...

및

✕ 문제 보고서 생성 및 다음으로 보내기

및

✕ 받는 사람에게 메시지로 알립니다...

'Wrap'

문제 보고서를 보낼 대상: 안 우재 콘텐츠 포함: 사용자 지정 콘텐츠

'악의적인 코드가 시스템에서 실행될 수 있는 매크로가 포함될 수 있기 때문에 모르는 사람으로부터 이러한 유형의 문서를 열지 마십시오.'

차단된 파일 확장자를 검토해 보세요!

Python 스크립트

".py", ".pyc", ".pyo", ".pyw", ".pyz", ".pyzw"

PowerShell 스크립트

".ps1", ".ps1xml", ".ps2", ".ps2xml", ".psc1", ".psc2",
".psd1", ".psdm1", ".cdxml", ".pssc"

MDAC (Microsoft Data Access Components)

".udl"

Windows ClickOnce

".appref-ms"

차단된 파일 확장자를 검토해 보세요!

Windows 샌드 박스

".wsb"

디지털 인증서

".cer", ".crt", ".der"

Java 프로그래밍

".jar", ".jnlp"

다음 확장은 다양한 응용 프로그램에서 사용됩니다.

관련 취약점이 수년 동안 패치되었지만 (대부분의 경우) 구 버전의 응용 프로그램 소프트웨어가 여전히 사용 중인 확장자명이 차단되었습니다.

".appcontent-ms", ".settingcontent-ms", ".cnt", ".hpj", ".website",

".webpnp", ".mcf", ".printerexport",

".pl", ".theme ", ".vbp ", ".xbap ", ".xll ", ".xnk ", ".msu ", ".diagcab ", ".grp "

**추가된 확장자를 제어 하기 위해서는
Exchange Online PowerShell 로 접근 하여 진행 합니다.**

BlockedFileTypes 리스트로 부터 확장자를 제거 하는 방법

```
Set-OwaMailboxPolicy -Identity "<Policy Name>" -BlockedFileTypes  
@{Remove=".pyw"}
```

AllowedFileTypes 리스트로 확장자를 추가 하는 방법

```
Set-OwaMailboxPolicy -Identity "<Policy Name>" -AllowedFileTypes  
@{Add=".pyw"}
```

BlockedFileTypes 또는 AllowedFileTypes 에 등재된 전체 확장자명
리스트를 보는 방법

```
Get-OwaMailboxPolicy | Select -ExpandProperty BlockedFileTypes
```

2.전자 메일 자동 전달 중지

- 해커가 사용자의 사서함 액세스 권한을 얻으면 사용자의 전자 메일을 외부 주소로 자동 전달하고 비공개 정보를 훔칠 수 있습니다.
- 메일 흐름 규칙을 만들어 중지할 수 있습니다.

이름:

전자 메일 자동 전달 중지

*다음의 경우 이 규칙 적용...

✕ 보낸 사람 위치...

조직 내부

및

✕ 메시지 유형...

자동 전달

조건 추가

* 다음 작업을 수행...

설명이 포함되 메시지 거부

'해커가 사용자의 사서함에 대 한 액세스 권한을 얻으면 사용자의

3. 피싱 방지 보호 기능 설정

- 피싱은 전자 메일이 익숙한 원본에서 전송된 것 처럼 보이지만 개인 정보를 수집 하려고 시도하는 악의적인 공격입니다.
- 기본적으로 마이크로소프트 365에는 일부 피싱 방지 보호가 포함되어 있지만 설정을 구체화 하여 해당 보호 기능을 높일 수 있습니다.

가장, 스푸핑, 및 기본 정책에 대한 고급 설정을 사용자 지정합니다. 사용자 지정 피싱 방지 정책으로 제어되는 추가적인 사용자, 그룹 또는 도메인 범위 정책과 함께 조직 내의 모든 사용자에게 기본 정책이 적용됩니다. [이 설정에 대한 자세한 정보](#)

상태
마지막으로 수정한 날짜

설정
2018년 11월 5일

정책 설정

정책 이름
설명

Office365 AntiPhish Default

가장

보호할 사용자
내가 소유한 모든 도메인 보호
특정 도메인 보호
작업 > 사용자 가장

해제
해제
해제
작업 적용 안 함



감사합니다.

다음 에피소드

ATP 안전 첨부 파일 및 링크 관리

함께 빛나는 우리



@TaeYoun.Community

ATP 안전 첨부 파일 및 링크 관리

발표자 : 안 태운

<http://bit.do/taeyoun>



Contents

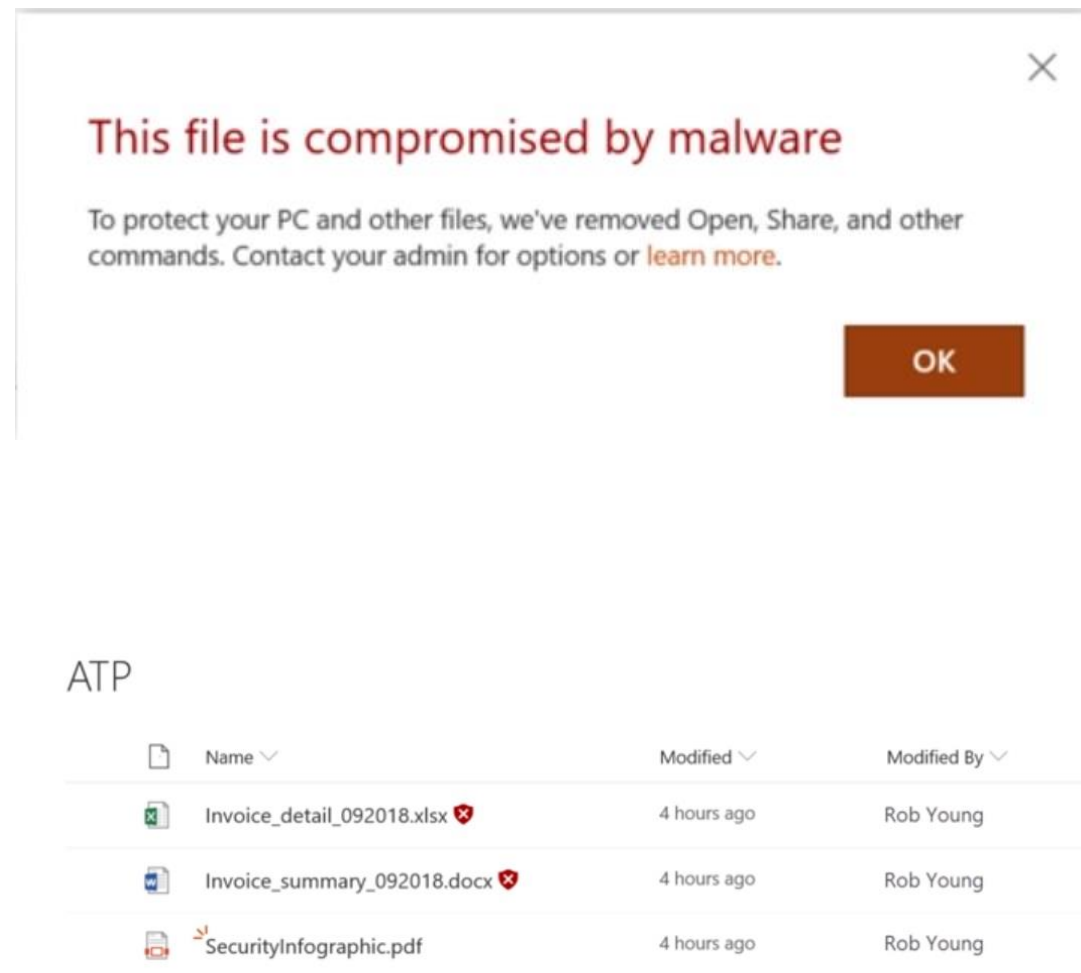
4.ATP 안전 첨부 파일 관리

5.ATP 안전 링크 관리



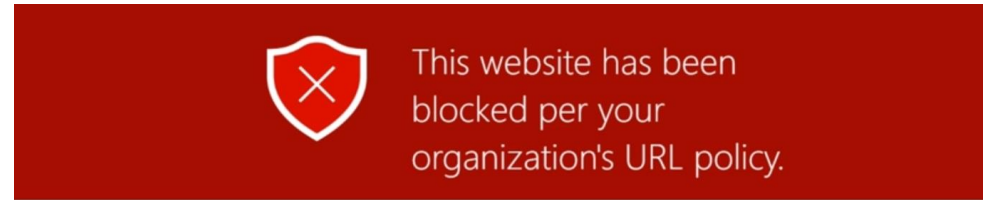
4. ATP 안전 첨부 파일 관리

- 마이크로소프트 365 ATP 또는 Advanced Threat Protection은 Outlook, OneDrive, SharePoint, 팀에서 악의적인 콘텐츠가 포함된 파일에 대해 비즈니스를 보호 하는 데 도움이 됩니다.
- 해당 파일 옆에는 빨간색 방패가 나타납니다.
- 차단된 파일을 열려고 하면 경고 메시지가 표시됩니다.



5. ATP 안전 링크 관리

- 마이크로소프트 365 ATP 또는 고급 위협 보호를 통해 사용자가 Office 앱에서 링크를 클릭할 때 악의적인 사이트로부터 비즈니스를 보호할 수 있습니다.
- 사용자가 링크가 포함된 전자 메일을 받으면 링크가 검색됩니다. 링크가 안전한 것으로 간주되면 클릭할 수 있습니다.
- 그러나 해당 링크가 차단된 목록에 있는 경우 사용자에게 링크가 차단되었다는 메시지가 표시됩니다.



Opening this website might not be safe.

<http://www.example.com/>

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

X Close this page

Powered by Office 365 Advanced Threat Protection

Also, have you seen these products before?

<http://example.com>

Example - up deals on popular products

<http://bit.do/taeyoun3>



감사합니다.

마무리 하며

Microsoft 365 그룹 개요

랜섬웨어 대응과 정보 추출 방지 기능

ATP 안전 첨부 파일 및 링크 관리

함께 빛나는 우리



@TaeYoun.Community