# 법인 내부 데이터 유출 테스트

진행일자: 2023.02.06.~16.  
보고자: 강민송 .

목차

[법인 내부 데이터 유출 테스트 1](#_Toc127447676)

[**1.** **구글 드라이브** 2](#_Toc127447677)

[**2.** **휴대폰** 3](#_Toc127447678)

[**3.** **외부 메일(구글, 네이버)** 4](#_Toc127447679)

[**4.** **카카오톡** 6](#_Toc127447680)

[**5.** **깃 bash** 7](#_Toc127447681)

[**6.** **Git server (issues 탭)** 10](#_Toc127447682)

[**7.** **시그니처 변조** 11](#_Toc127447683)

[**8.** **Notion** 15](#_Toc127447684)

[**9.** **모바일 메일** 17](#_Toc127447685)

[**10.** **OUTLOOK 취약성** 18](#_Toc127447686)

## **구글 드라이브**

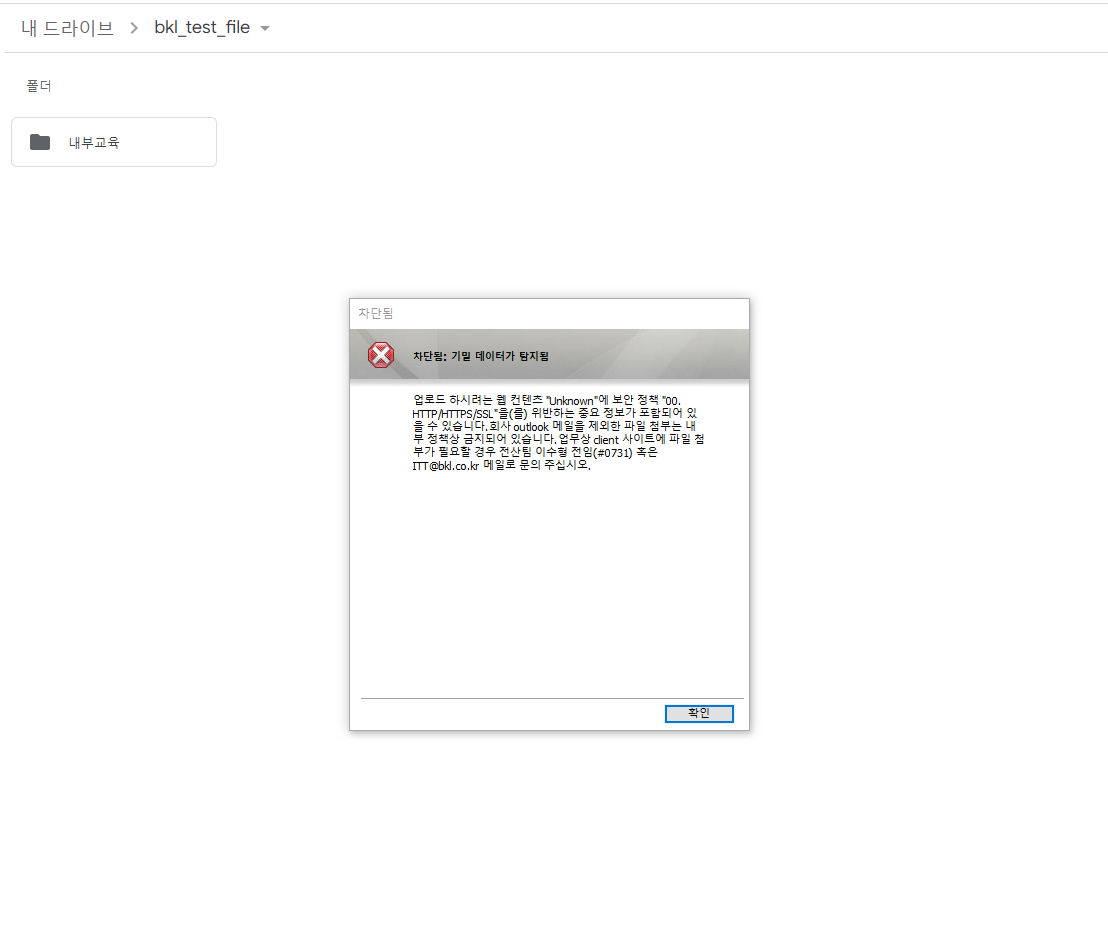


그림 1) 클라우드 업로드 기밀탐지O

폴더 전체를 업로드 한 경우 ) 기밀탐지 확인

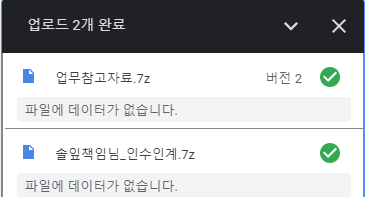


그림 2) 클라우드 업로드 기밀탐지X

PDF, DOCX 파일 혹은 7Z으로 압축하여 업로드 한 경우 ) 기밀탐지X + 파일 데이터 없앰  
→ 다운로드 가능하나 빈 파일이 열림

## **휴대폰**

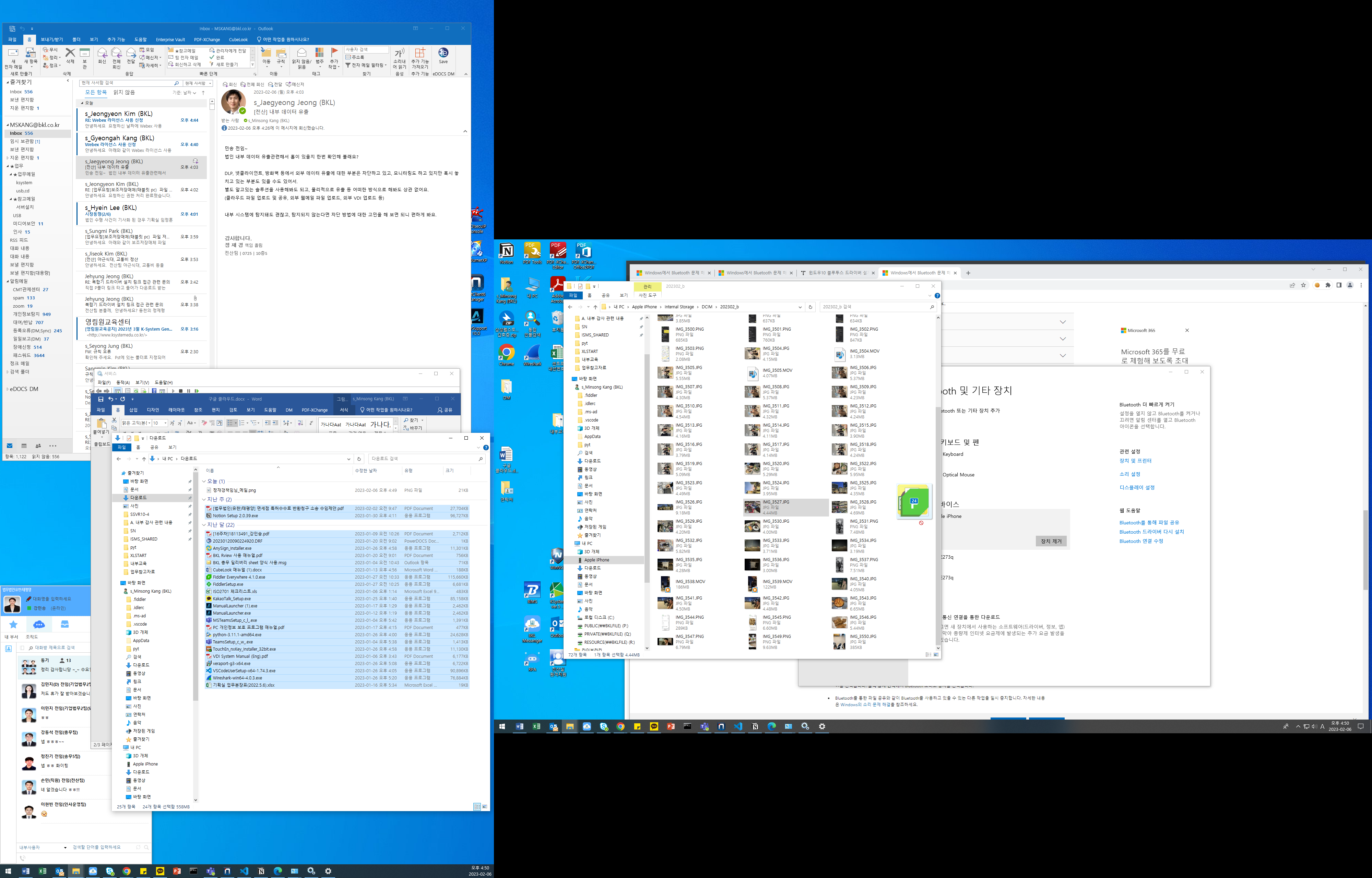


그림 3) 휴대폰 연결 후 드래그 앤 드롭

막혀 있음을 확인(그룹 권한 부여 시 가능)

## **외부 메일(구글, 네이버)**

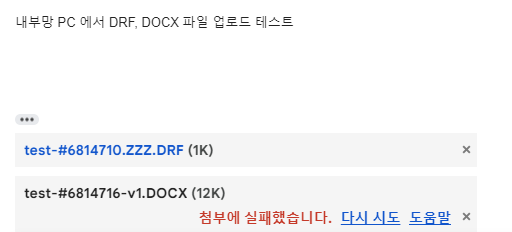


그림 4) 구글 메일

첨부 실패 혹은 기밀탐지에 걸림

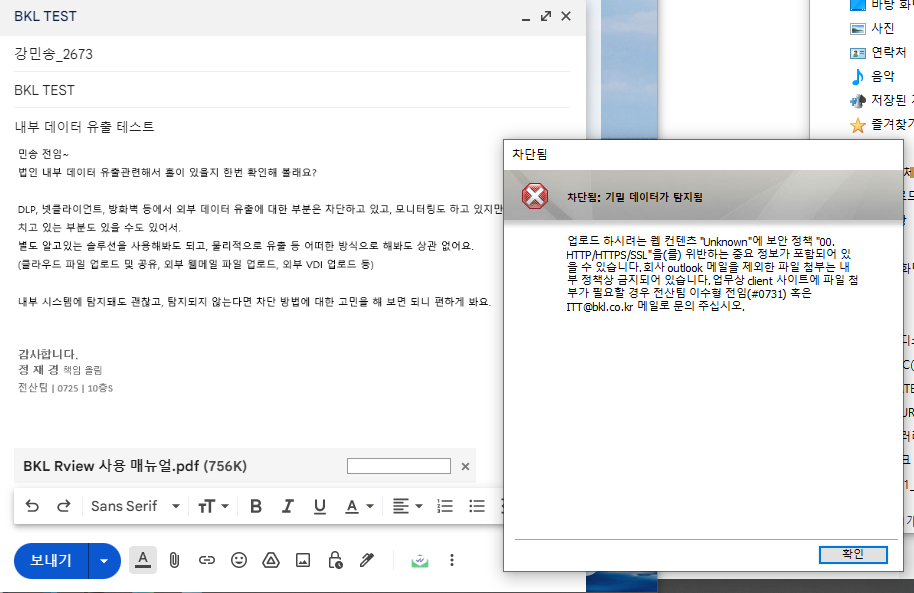


그림 5) 차단 확장자

기밀탐지 O: PDF , EXE, XLS(X), DOCX, 확장자 없음, MSG   
→ txt, drf, png 로 변경해 올려도 기밀탐지됨

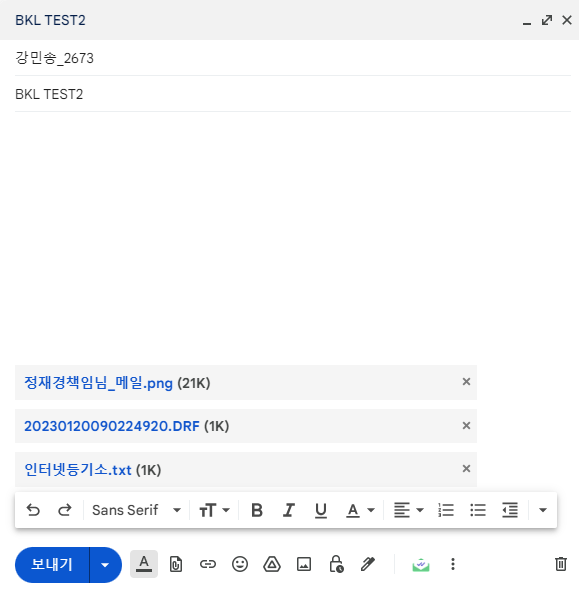


그림 6) 허용 확장자

기밀탐지 X: Txt, drf, png   
→ pdf 등으로 변경해 올려도 기밀탐지 안됨 (시그니처가 원인 같음, 차후 시그니처 변경 시도)  
이외) PDF 파일을 캡처(png)하여 업로드 시 기밀탐지 X

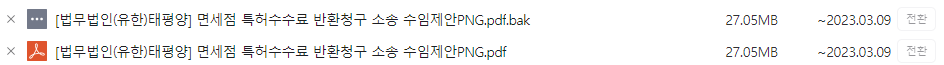
 

그림 7) 네이버 메일 확인

기밀탐지 O: PDF , EXE, XLS(X), DOCX, MSG  
기밀탐지 X: Txt, drf, png, 시그니처 변경한 PDF, bak(백업파일) 등

## **카카오톡**

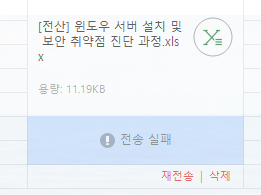
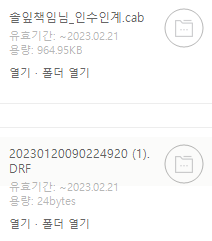


그림 8) 카카오톡 파일전송

기밀 탐지 되는 확장자와 아닌 확장자가 구분됨 (구글 메일과 동일)  
기밀탐지 O: PDF , EXE, XLS(X), DOCX, MSG, PPTX,   
기밀탐지 X: 7z, DRF, cab, iso, txt, png



그림 9) 대용량 전송 테스트

1GB 압축파일 전송 시 300MB 초과로 막힘(기밀탐지X)  
→ 300MB 이하의 대용량 파일 유출 가능성

## **깃 bash**

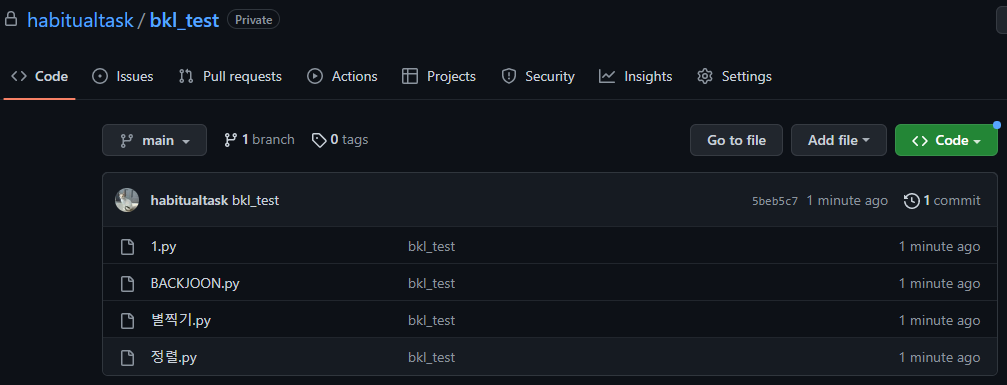


그림 10) 깃 허브 업로드

.py 소스코드 파일 업로드 가능

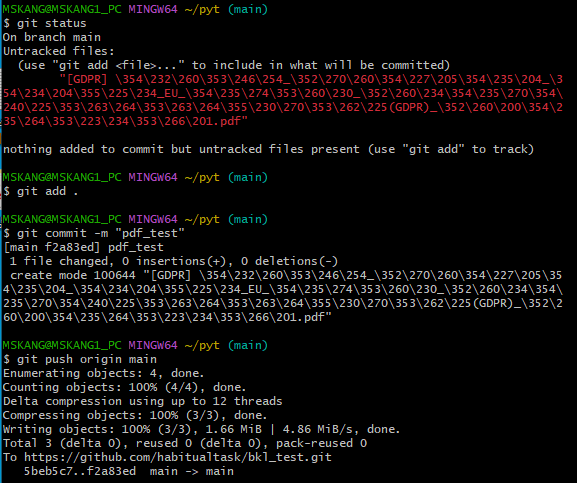
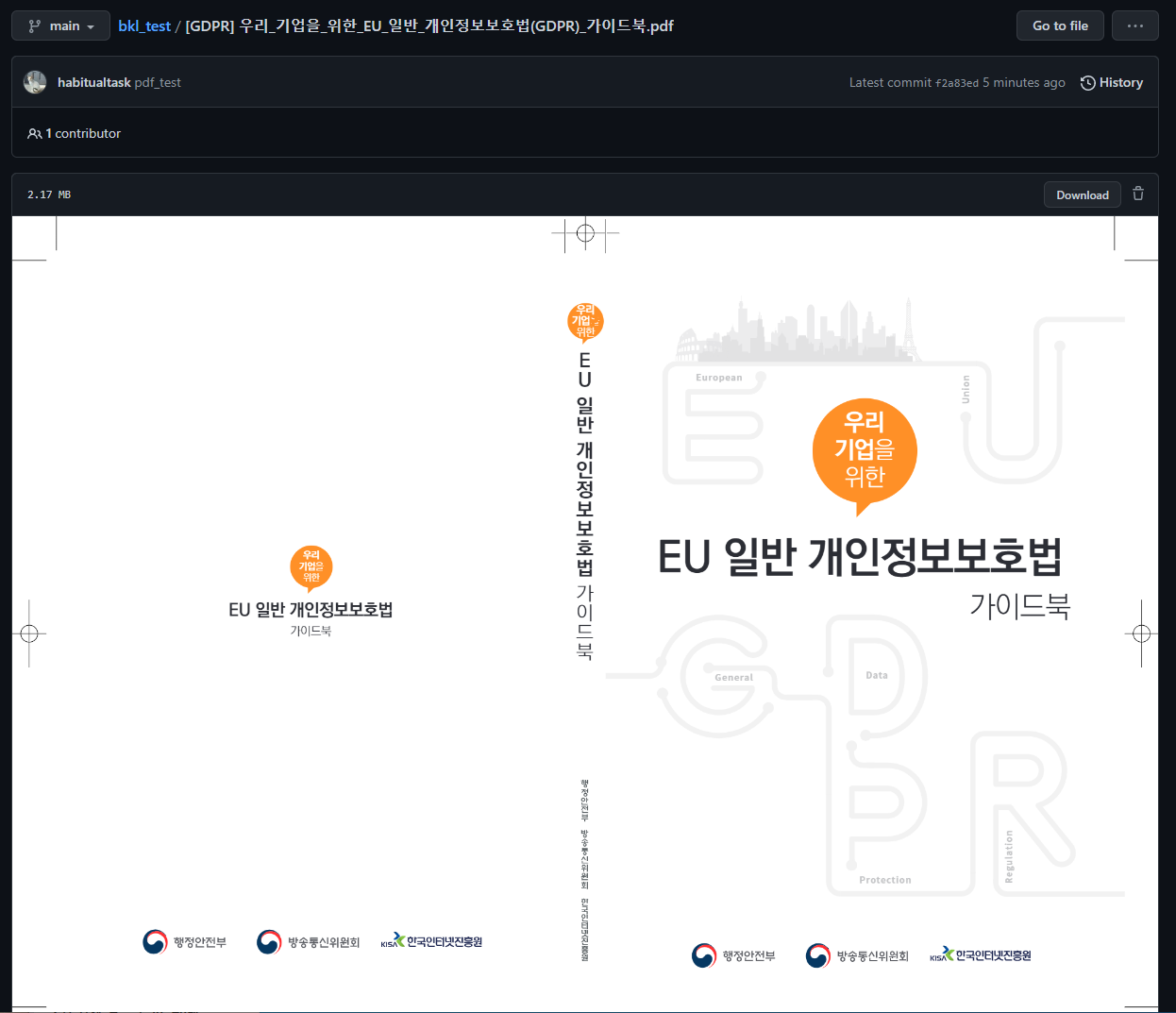


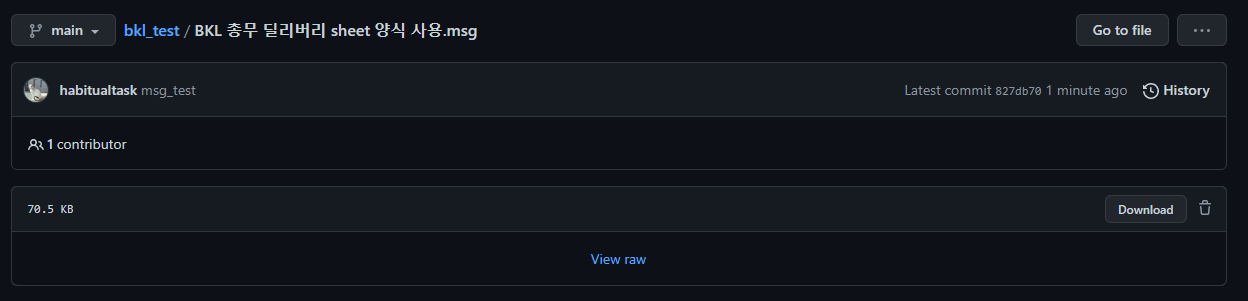
그림 11) 깃 push 과정

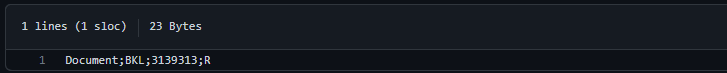


그림 12) 깃 허브 허용 확장자

Pdf, msg(메일), drf(사건), xlsx(엑셀), 7z(압축) 전부 업로드 가능했음 (**데이터 유출 가능성多**)

<Pdf의 경우> 다운 및 뷰어 가능  


<msg, 7z, xlsx의 경우> 다운 가능 (\*외부 어디서든 유출 가능)  
  

<drf의 경우> 유출 가능성은 있으나 git 자체에서 확장자 지원 안하는 것 같음(다운 불가능)  


## **Git server (issues 탭)**

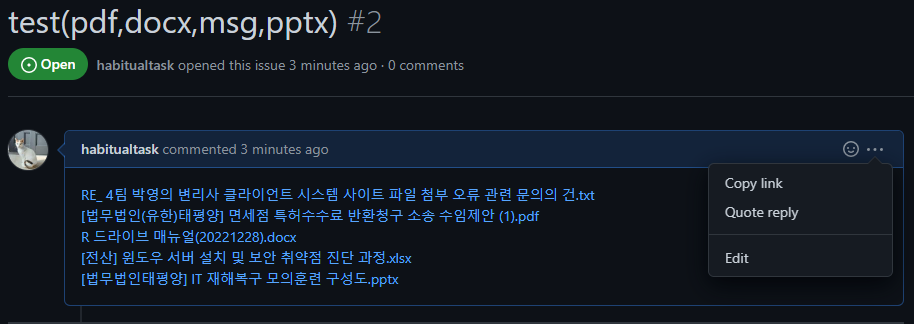


그림 13) git 서버 issue 탭 업로드

다양한 확장자가 자료명 그대로 올라감을 확인 (iso, 7z 제외)  
→ 다운까지 가능했으나, 다운된 파일은 빈 파일임 (txt, png제외)  
→ 이슈 탭 자체가 사진 넣기가 가능하기 때문에 txt와 png만 가능한 것으로 추측

→ Ppt, xlsx 등 pdf 변환 후 png 시그니처로 변경하여 업로드 및 유출 가능  
Copy link 기능으로 외부 어디든 공유 가능할 것으로 예상

## **시그니처 변조**



그림 14) 시그니처 변경 시 pdf 첨부 가능

업로드 및 다운 가능

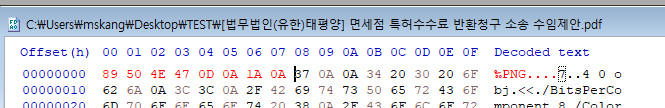
<변조과정#1> pdf 파일을 png 시그니처로 변조하여 구글에 업로드  


그림 15) Header Signature 변경

기밀 탐지되었던 pdf 확장자에서 기밀 탐지 되지 않았던 png 확장자로 헤더 시그니처 변경

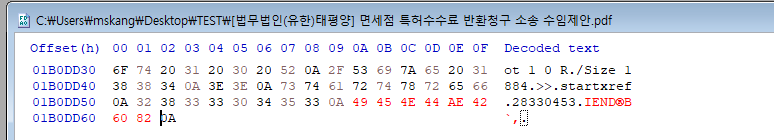


그림 16) Footer Signature 변경

기밀 탐지되었던 pdf 확장자에서 기밀 탐지되지 않았던 png 확장자로 푸터 시그니처 변경

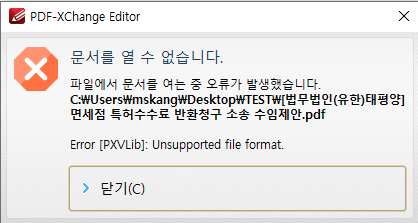


그림 17) 변경 후 파일 확인

Png 확장자 시그니처이지만 이름 상 .pdf 확장자 이므로 파일이 열리지 않음을 확인 후 업로드

* 추가사항

<변조과정#2> png 파일의 hxd 사이에 유출하고자 하는 파일(pdf 등)의 hxd를 끼워 넣는 방법

<변조과정#3> pdf의 header/footer 시그니처를 따로 삭제할 필요 없이 앞 뒤로png 시그니처만 입력하는 방법

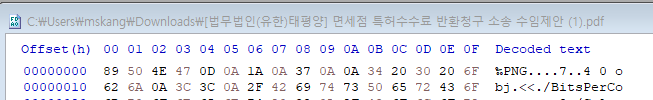
<복구과정#1> 구글에 업로드 된 (시그니처 변경된)pdf 다운 후 복구 과정  


그림 18) Header Signature 확인

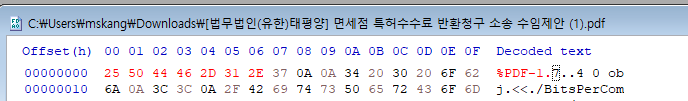


그림 19) Header Signature 복구

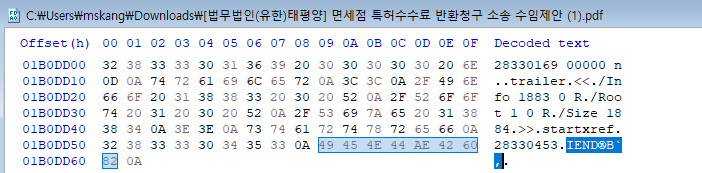


그림 20) Footer Signature 확인

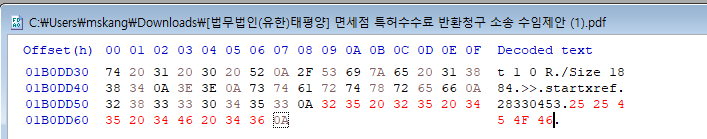


그림 21) Footer Signature 복구



그림 22) 파일 확인

정상적으로 파일이 열림을 확인 **(데이터 유출)**

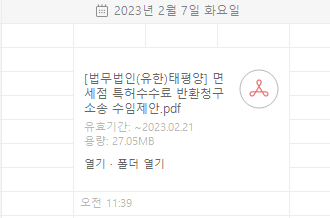


그림 23) 카카오톡 파일 전송 가능

시그니처가 png로 변경된 pdf 파일은 카카오톡에서도 업로드 가능 (+외부메일)

## **Notion**

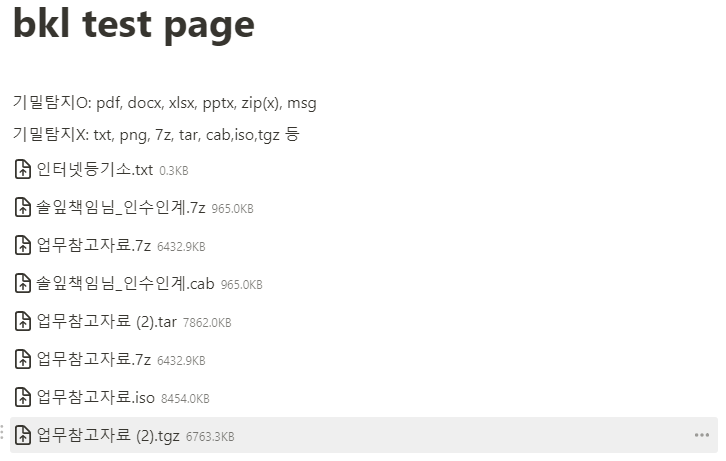


그림 24) 업로드 확장자 확인

Exe, zip, zipx 등 알려진 압축 외 다양한 압축 확장자는 막혀있지 않은 상태  
→ 7z, iso, tgz, tar, cab 등 …

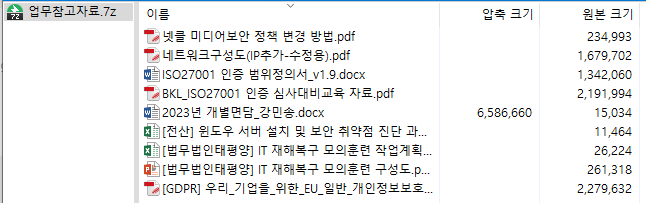


그림 25) 업로드 된 7z 폴더 내부 확인

기본적인 Pdf, xlsx 확장자 파일은 기밀탐지 되어 막힘  
7z으로 압축 시 pdf, xlsx, pptx 등 용량 상관없이 모두 업로드 가능



그림 26) 대용량 유출 테스트



그림 27) 업로드 확인

1GB 이상의 압축파일 역시 별 다른 제제 없이 업로드 가능함을 확인

## **모바일 메일**

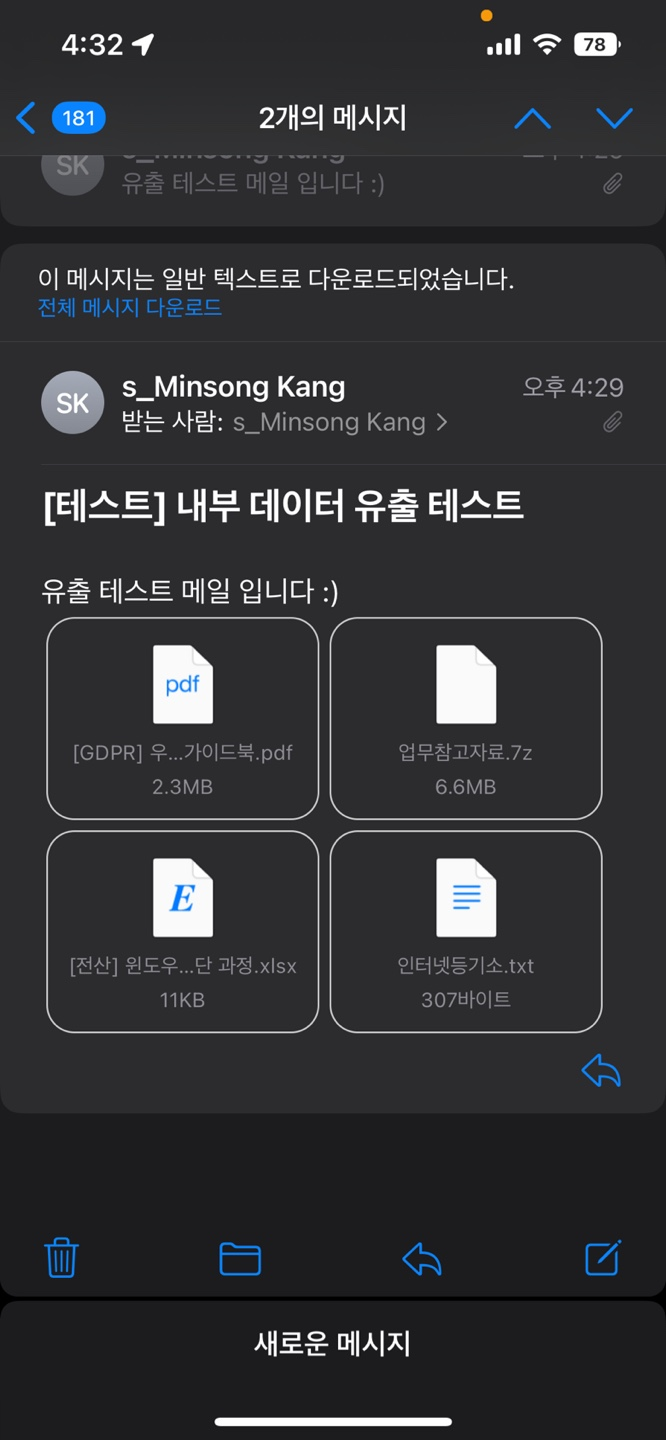
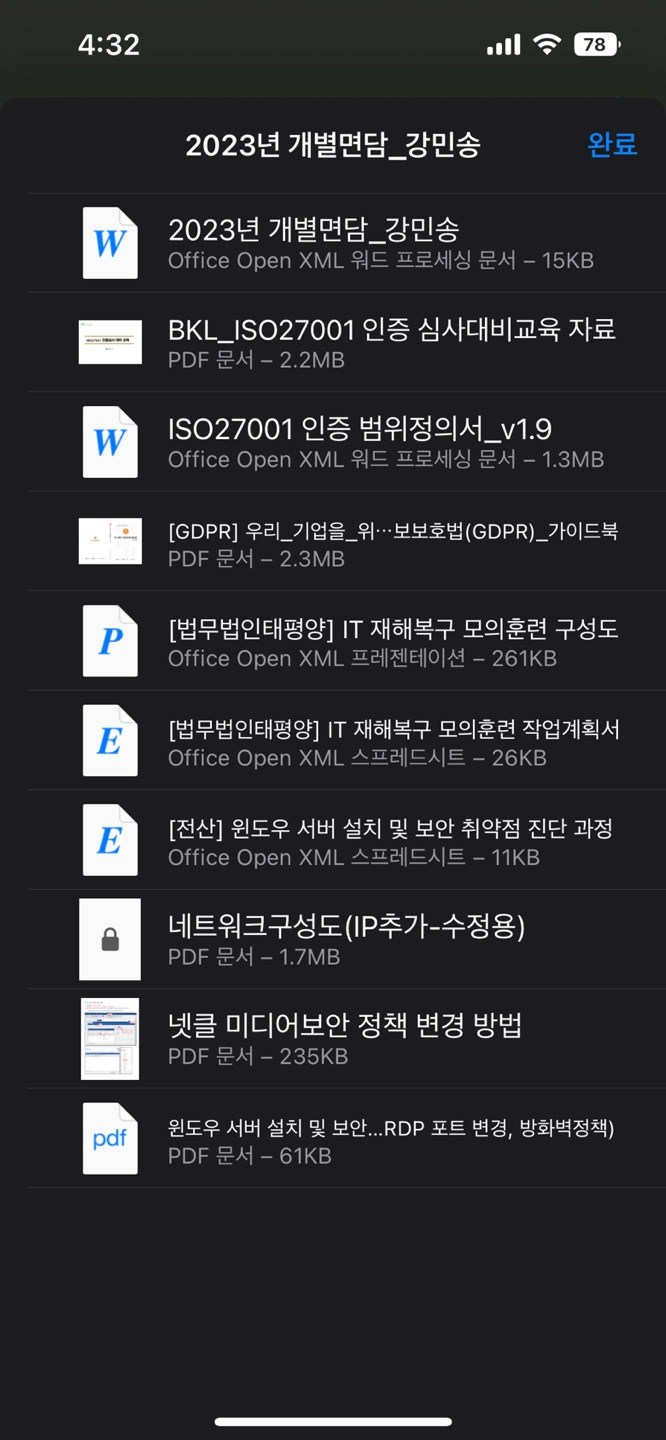


그림 28) 모바일 메일 유출

내부 PC에서 파일을 첨부하여 보낼 경우, 모바일에서 파일을 확인하고 카카오 등 유출이 가능

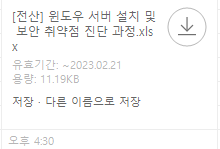
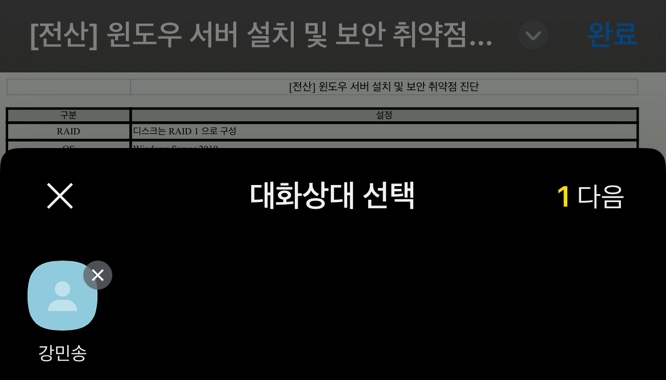


그림 29) 카카오톡 유출 확인

내부 PC → 카카오톡 전송 시 기밀탐지 되었던(전송X) 엑셀 파일이 모바일 메일을 통해 유출 가능함을 확인

## **OUTLOOK 취약성**

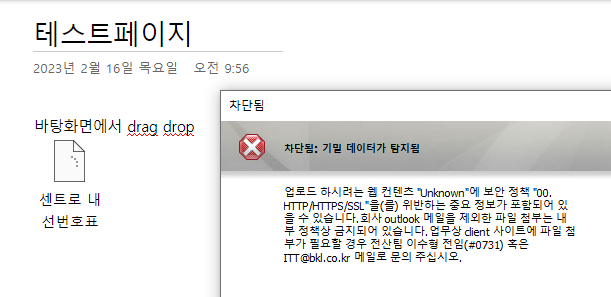


그림 30) 바탕화면→WEB ONENOTE,google

바탕화면에 있는 파일을 web버전의 onenote와 gmail에 드래그앤드롭 했을 경우 기밀탐지됨 (확장자전체)

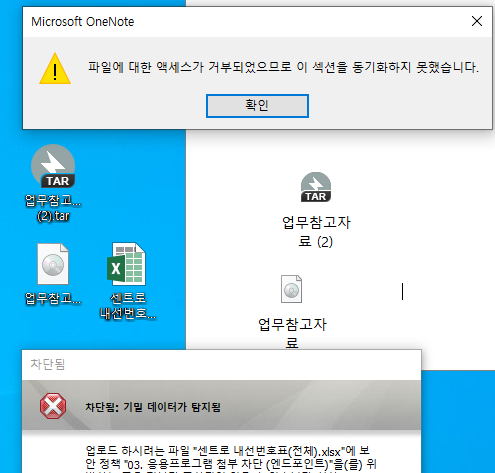


그림 31) 바탕화면→Program ONENOTE

바탕화면에 있는 파일을 program버전의 onenote에 드래그앤드롭 했을 경우 기밀탐지됨 (주요확장자만 탐지, ISO/TAR등 주요 제외 압축 확장자는 기밀탐지 되지 않았음)

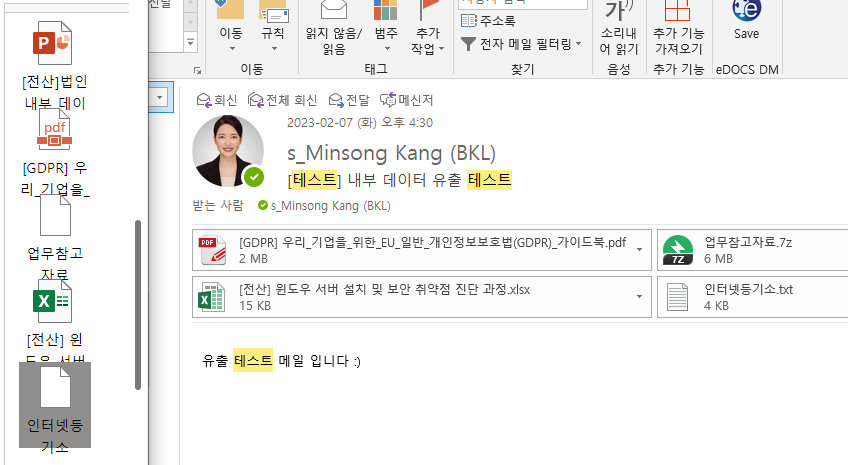


그림 32) Program outlook→WEB ONENOTE

One note의 경우 19mb 이하의 조건 하에 모든 확장자의 업로드가 가능했음(대용량x)

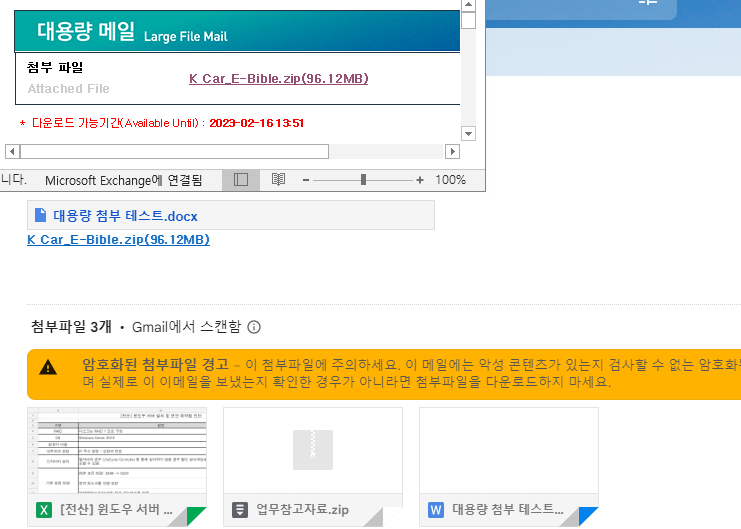
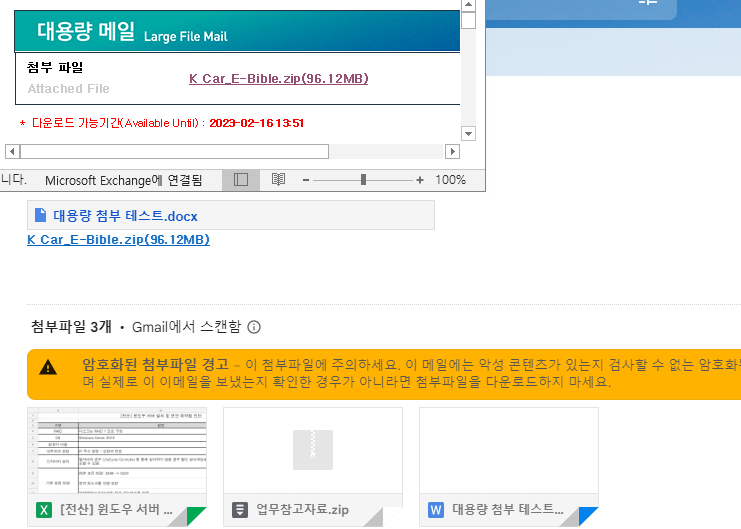
 

그림 33) Program outlook→WEB ONENOTE, google

외부(구글)메일에서도 동일한 홀 발견

Program outlook에서 주요확장자(xlsx, ppt, docx)가 모두 drag&drop 가능했음

대용량 링크 역시 복제하여 구글 메일에서 첨부가 가능했고, 정상적으로 다운됨을 확인

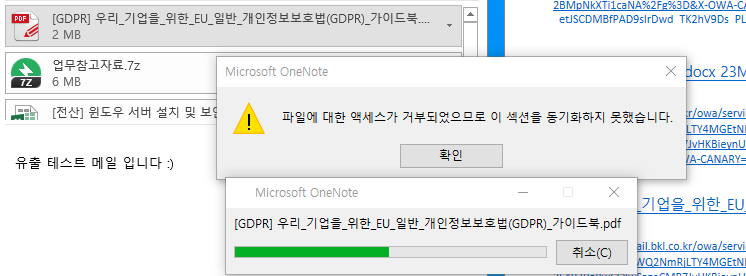


그림 34) Program outlook→Program ONENOTE

주요확장자들은 기밀차단 되어있는 반면, 압축확장자는 기밀차단 되어있지 않음

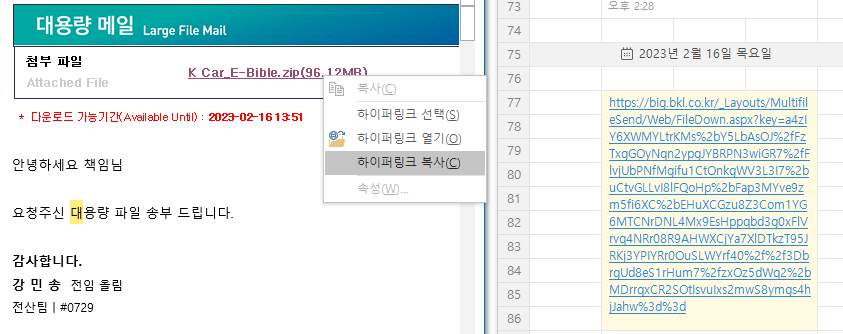


그림 35)\_Program outlook→Program kakao

outlook에서 첨부된 대용량 링크 복제 및 다운이 가능함을 확인

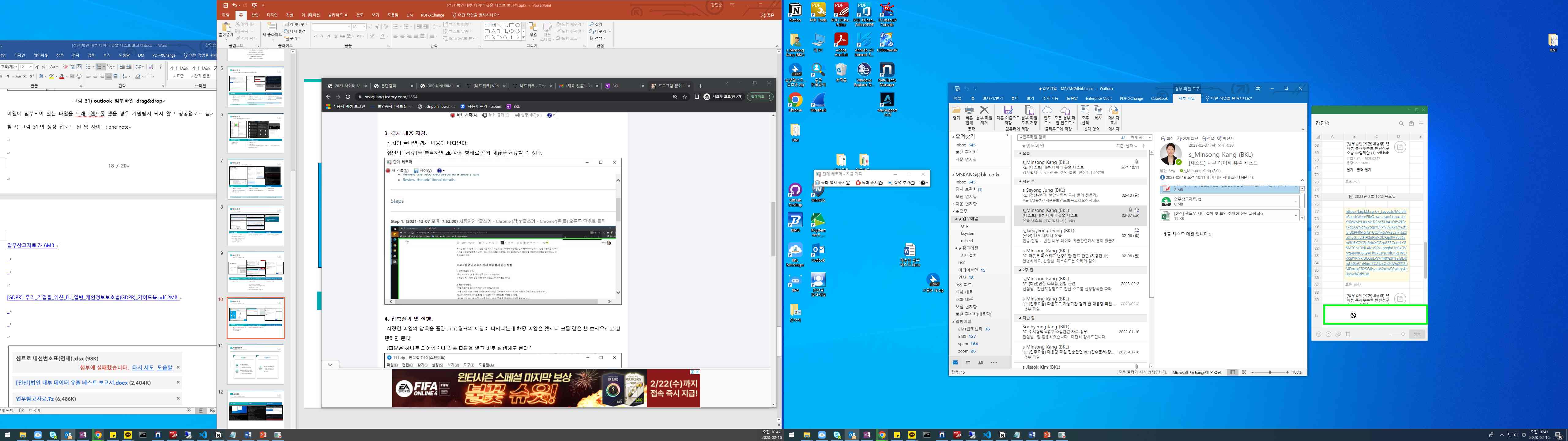


그림 36) Program outlook→Program kakao

이외의 확장자 파일은 drag 자체가 막혀 있음

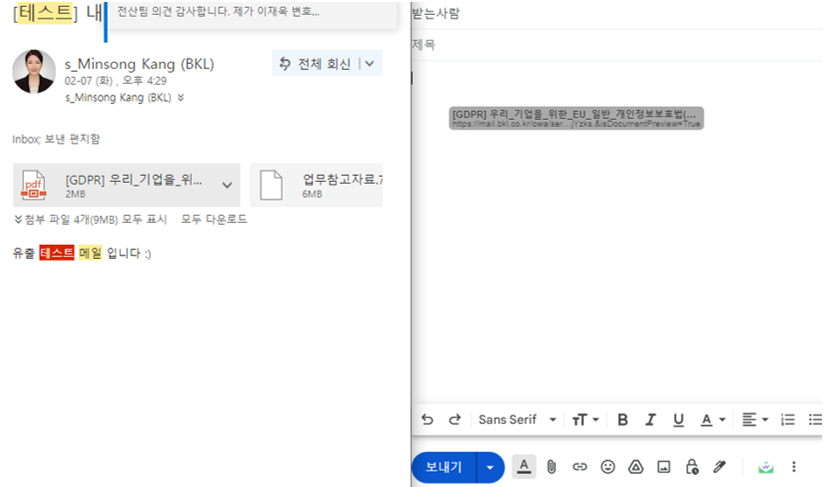


그림 37) Web outlook→WEB ONENOTE, gmail

Drag 자체가 막혀 있음

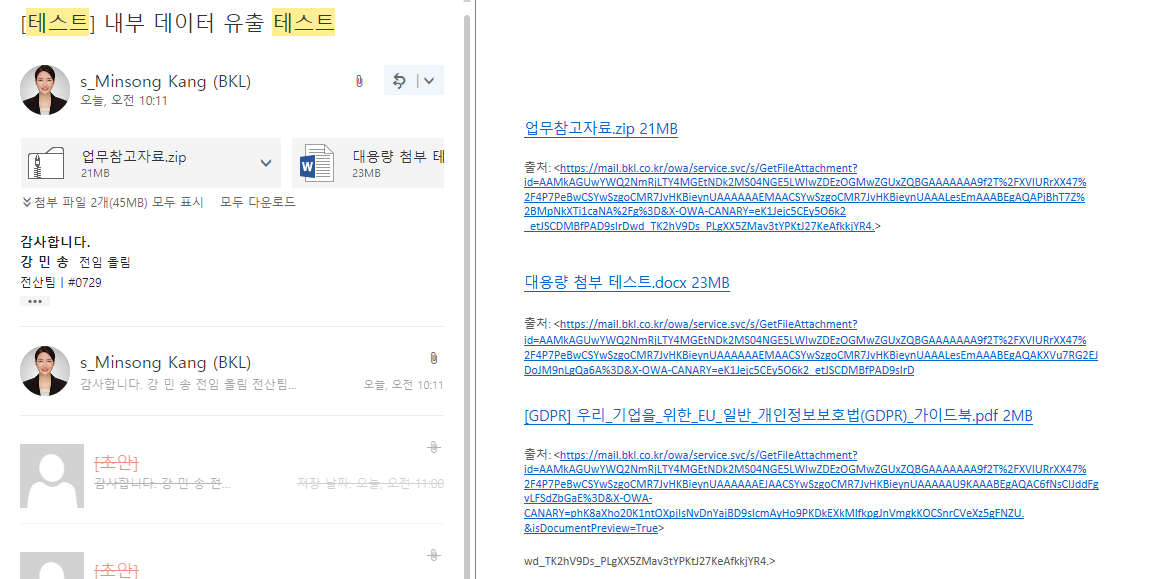


그림 38) Web outlook→Program ONENOTE

용량 상관 없이 모든 확장자의 파일이 업로드 가능함 (사진속의 ‘출처’ 링크를 누르면 자동다운)



그림 39) Web outlook→ Program KAKAO

Drag&drop은 가능하나 파일의 정보만 drop됨

실질적인 파일 유출보다는 파일 정보 및 경로의 유출이라고 봐야 함



그림 40) outlook 취약성 요약 표

참고