경찰청 보도자료 다시 대한민국! 새로운 국민의 나라

보도시점 2023. 11. 22.(수) 조간 누리망·방송 2023. 11. 21.(화) 12:00

북 해킹조직의 정부기관·언론사 등 사칭 전자우편 주의

- 랜섬웨어 유포에 이어 가상자산 절취·채굴까지 다각화된 공격
- 개인 전자우편 계정의 비밀번호 주기적 변경 등 보안 강화 당부

경찰청 국가수사본부(수사국)는 지난해 북한 해킹조직의 소행으로 규명한 「국회의원실·기자 등 사칭 전자우편 발송사건」을 계속 추적·수사한 결과, 올해에도 공격 대상을 확대하여 사칭 전자우편을 지속해서 발송하고 있고, 특히 다양한 방법으로 가상자산을 탈취하고 있는 사실을 확인하였다.

북한 해킹조직은 정부기관·기자·연구소 등을 사칭하여 '안내문'이나 '질의서' 등 수신자가 관심을 가질 수 있는 내용으로 위장한 전자우편을 발송하고 있으며, 전자우편에 첨부된 파일을 열람하면 개인용컴퓨터(PC) 내부의 정보를 유출할 수 있는 악성프로그램이 설치·실행되는 수법을 이용하고 있다.

발송일자	사칭대상	전자우편 내용	범행수법
'23. 3. 7.	○○○ 기자	인터뷰 질의문 송부	악성프로그램 유포
'23. 3. 13.	경찰청	사건 관련 안내	악성프로그램 유포
'23. 5. 19.	○○○○연구원	○○포럼 발표자료	피싱사이트 유도
'23. 7. 8.	국민건강보험	통지서 발송	피싱사이트 유도
'23. 9. 12.	국민연금공단	통지서 발송	피싱사이트 유도
'23. 10. 26.	국세청	국세납부 안내	피싱사이트 유도

[표 1] 북한발 사칭 전자우편 발송 사례

또한, 전자우편에 포함된 인터넷주소(URL)를 누르도록 유인하는 사례도 확인되는데, 이 경우 피해자가 신뢰할 수 있는 기관이나 정보 망라 누리집(포털사이트)을 모방한 가짜 누리집으로 접속을 유도(피싱, Phishing)하는 수법도 이용하여 계정정보를 탈취하고 있는 것으로 확인되었다.

특히, 북한 해킹조직은 사칭 전자우편 수신자의 소속기관 누리집을 제작하여 접속을 유도하며 피해자별로 특화된 공격을 전개하는 등 범행 수법은 더욱 교묘해지고 있다.

이번 추가 수사를 통해 확인된 전자우편 계정 탈취 피해자는 1,468명이며, 이중 외교·통일·국방·안보 분야의 전·현직 공무원 등 전문가는 57명이고, 이외에도 회사원·자영업자·무직자 등 다양한 직군의 일반인 1,411명도 피해를 입은 사실로 미루어, 공격 대상이 이제 특정 분야 종사자에 국한되지 않고 전방위적으로 확산되고 있는 것으로 판단된다.

합계	정보수집 대상(57)				전방위 공격피해	
	외교	통일	국방	안보	회사원	자영업자 등
1,468	15	16	14	12	587	824

[표 2] 피해자 직군별 분류 (단위: 명)

공격 대상이 확산되고 있는 이유는 가상자산을 노리고 있기 때문으로 분석된다.

작년 '금품 요구 악성프로그램(랜섬웨어)' 을 유포하여 가상자산을 갈취한 사실이 처음 확인된 데 이어, 올해에는 사칭 전자우편 피해자들의 가상자산거래소 계정에 부정 접속하여 절취를 시도한 사실과(금전적 피해 없음) 해킹으로 장악한 경유 서버 147대에서 '가상자산 채굴 프로그램'을 관리자 몰래 실행한 사실이 이를 뒷받침하고 있다.

근래 북한 해킹조직이 사칭 전자우편의 공격 대상을 확대하고, 가상자산 갈취·절취·채굴까지 다양화함에 따라, 경찰은 피해를 적극적으로 예방·저지하기 위해 외교부 등 관계기관, 미국 정부, 유엔 등과 정보를 공유하고 협력 대응하는 등 여러모로 노력을 기울이고 있다.

- (외교부) 북 소유 가상자산에 대해 「국내 최초 대북 독자 제재」('23. 6. 2.)
- (한·미 정부) 북 공격피해 예방을 위한 「한미 합동 사이버보안 권고문」 발표('23. 6. 2.)
- (유엔) 경찰 수사사례를 「유엔 대북제재위의 전문가패널 보고서」에 반영('23. 4. 5.)
- (한·미 정부) 북한 사이버위협 대응 실무그룹에서 '김수키' 관련 정보공유 ('23. 11. 6.)

또한, 경찰은 피해자들에게 전자우편에 대한 보안 조치를 권고하는 한편, 한국인터넷진흥원과 협력하여 북한 해킹조직이 운영하는 피싱 사이트를 차단하고, 국가사이버위기관리단 등 관계기관에 북한 해킹조직의 경유 서버 목록 등 관련 정보를 제공하여 정보보호 정책 수립에 활용하도록 하였다.

그러나 북한 해킹조직의 공격이 전방위적으로 확대되고 있는 만큼, 추가적인 피해가 발생하지 않도록 전자우편과 가상자산거래소 계정의 비밀번호를 주기적으로 변경하고, 2단계 인증* 및 일회용 패스워드(OTP) 설정, 해외 인터넷주소(IP) 접속 차단 등 보안 설정을 강화하도록 당부하였다.

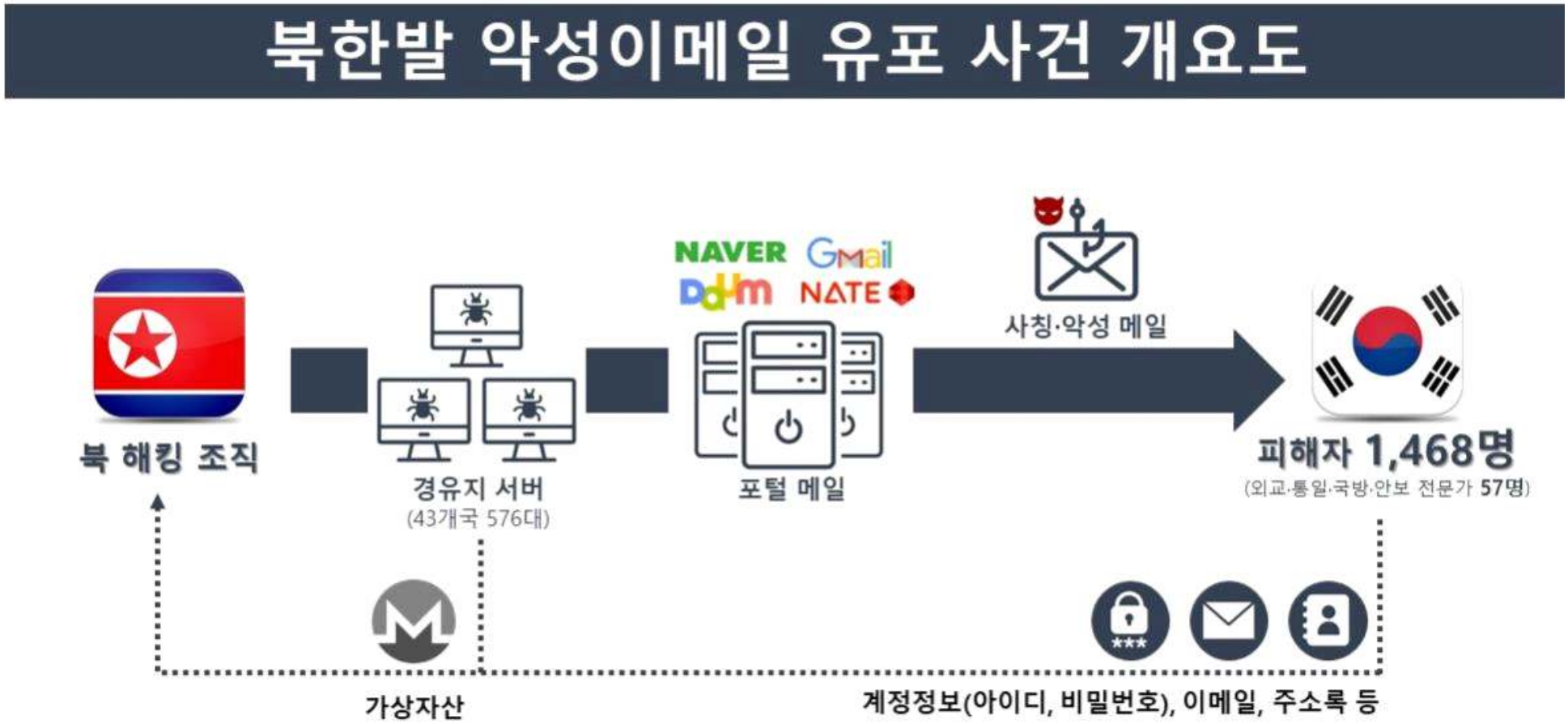
* 아이디·비밀번호 입력을 통한 1단계 인증 이후, 사용자가 미리 설정한 전화번호 또는 다른 전자우편을 통해 추가 인증을 거쳐 로그인하는 이중 보안 서비스

경찰청은 앞으로도 조직적 사이버 공격을 지속해서 탐지·추적함과 동시에, 관계기관과 긴밀히 협력하며 피해 방지를 위해 노력해 나갈 계획이다.

붙임 1. 사건 개요도
2. 사칭 전자우편 화면
3. 가짜 누리집 화면

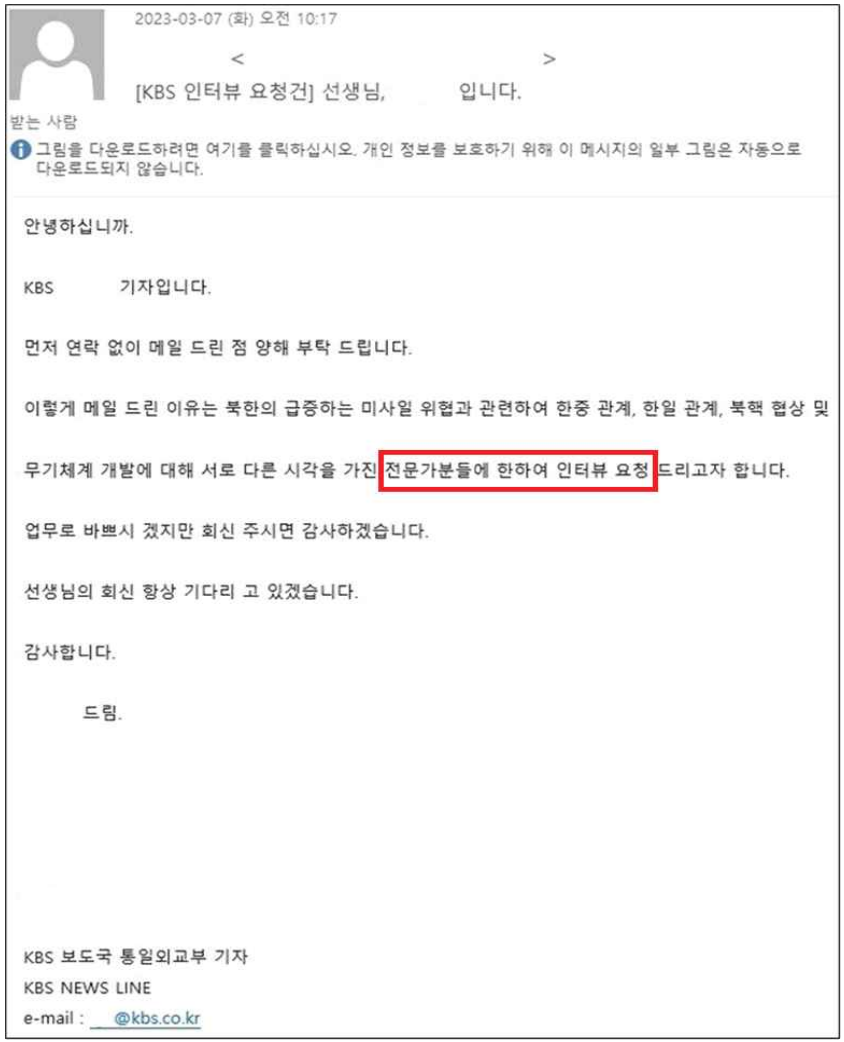
담당 부서	국가수사본부 수사국 사이버테러대응과	책임자	총경	정석화 (02-3150-0053)
		담당자	경정	이승운 (02-3150-1459)

붙임 1	사건 개요도


북한발 악성이메일 유포 사건 개요도
북 해킹 조직
경유지 서버
(43개국 576대)
NAVER
Gmail
DAUM
NATE
포털 메일
사칭·악성 메일
피해자 1,468명
(외교·통일·국방·안보 전문가 57명)
가상자산
계정정보(아이디, 비밀번호), 이메일, 주소록 등

붙임 2 사칭 전자우편

○ 기자 사칭 전자우편



2023-03-07 (화) 오전 10:17

< >

[KBS 인터뷰 요청건] 선생님, 입니다.

받는 사람

그림을 다운로드하려면 여기를 클릭하십시오. 개인 정보를 보호하기 위해 이 메시지의 일부 그림은 자동으로 다운로드되지 않습니다.

안녕하십니까.

KBS 기자입니다.

먼저 연락 없이 메일 드린 점 양해 부탁 드립니다.

이렇게 메일 드린 이유는 북한의 급증하는 미사일 위협과 관련하여 한중 관계, 한일 관계, 북핵 협상 및

무기체계 개발에 대해 서로 다른 시각을 가진 전문가분들에 한하여 인터뷰 요청 드리고자 합니다.

업무로 바쁘시 겠지만 회신 주시면 감사하겠습니다.

선생님의 회신 항상 기다리 고 있겠습니다.

감사합니다.

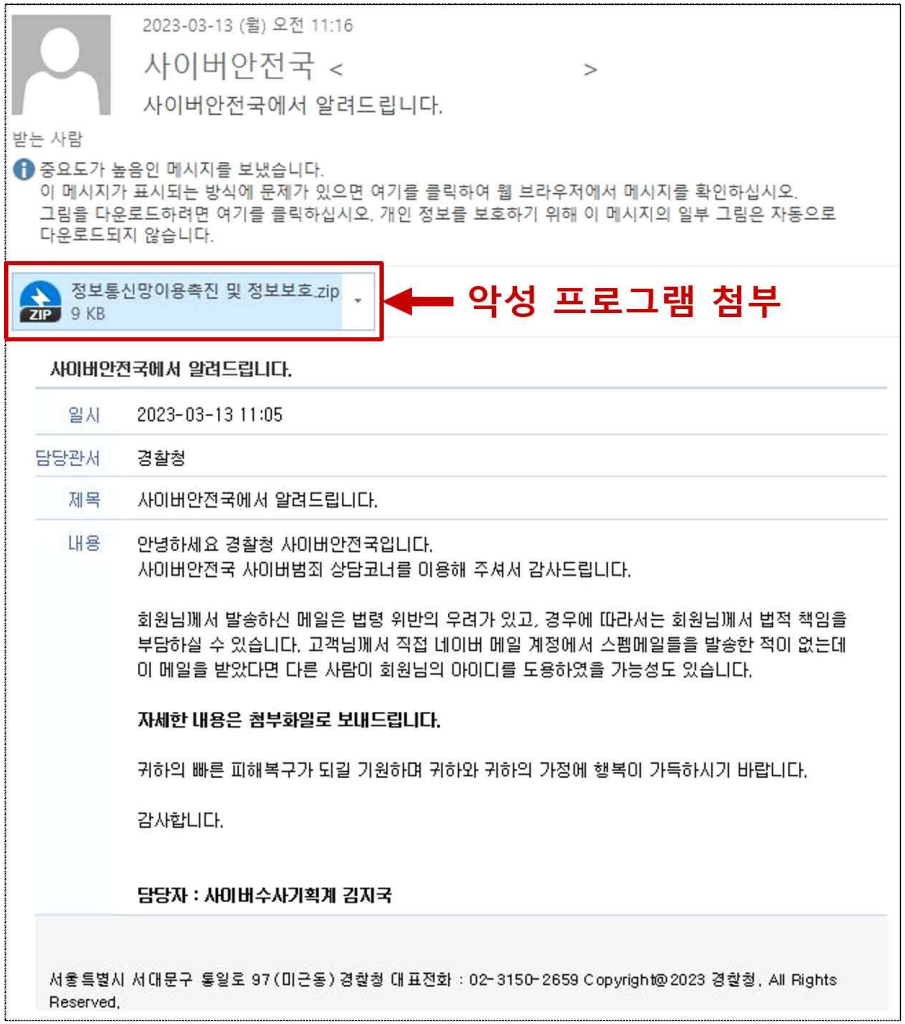
드림.

KBS 보도국 통일외교부 기자

KBS NEWS LINE

e-mail : @kbs.co.kr

○ 경찰청 사칭 전자우편



2023-03-13 (월) 오전 11:16

사이버안전국 < >

사이버안전국에서 알려드립니다.

받는 사람

중요도가 높음인 메시지를 보냈습니다.
이 메시지가 표시되는 방식에 문제가 있으면 여기를 클릭하여 웹 브라우저에서 메시지를 확인하십시오.
그림을 다운로드하려면 여기를 클릭하십시오. 개인 정보를 보호하기 위해 이 메시지의 일부 그림은 자동으로 다운로드되지 않습니다.

정보통신망이용촉진 및 정보보호.zip
9 KB

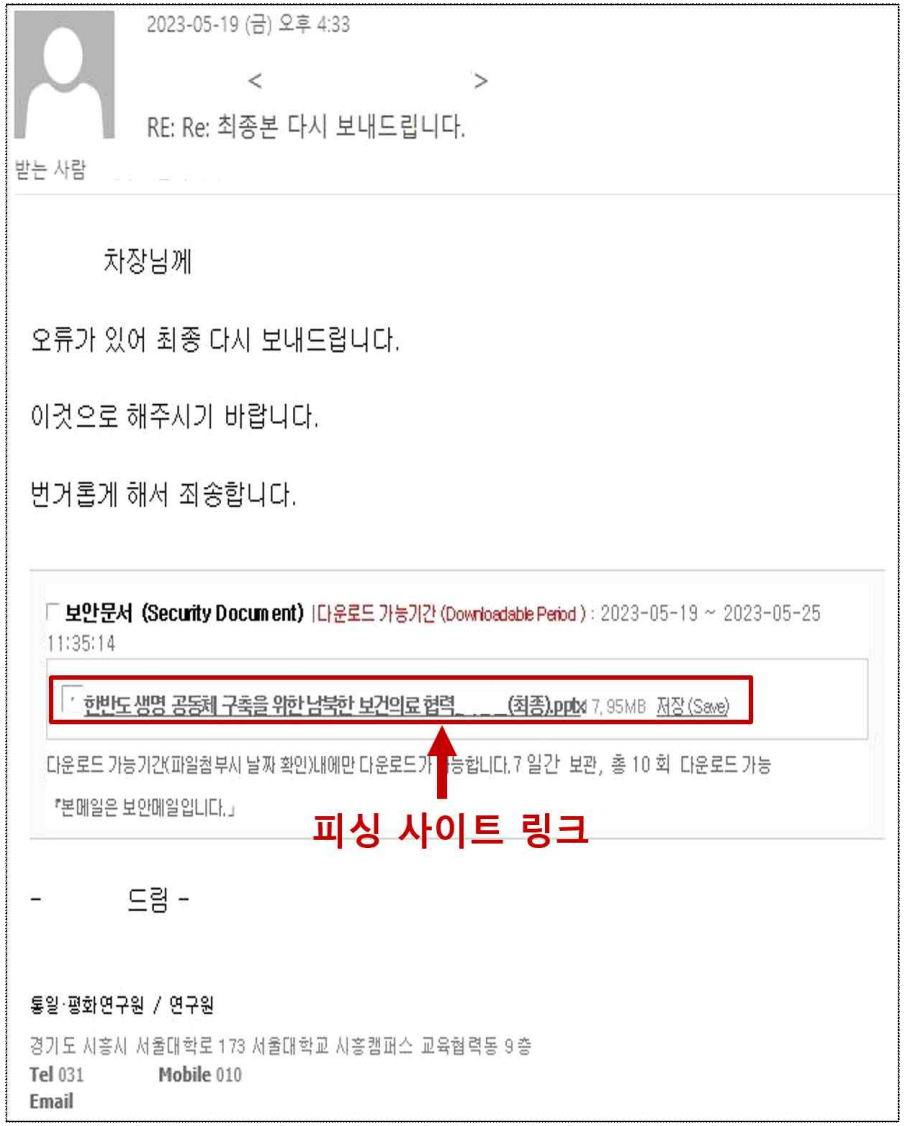
악성 프로그램 첨부

사이버안전국에서 알려드립니다.

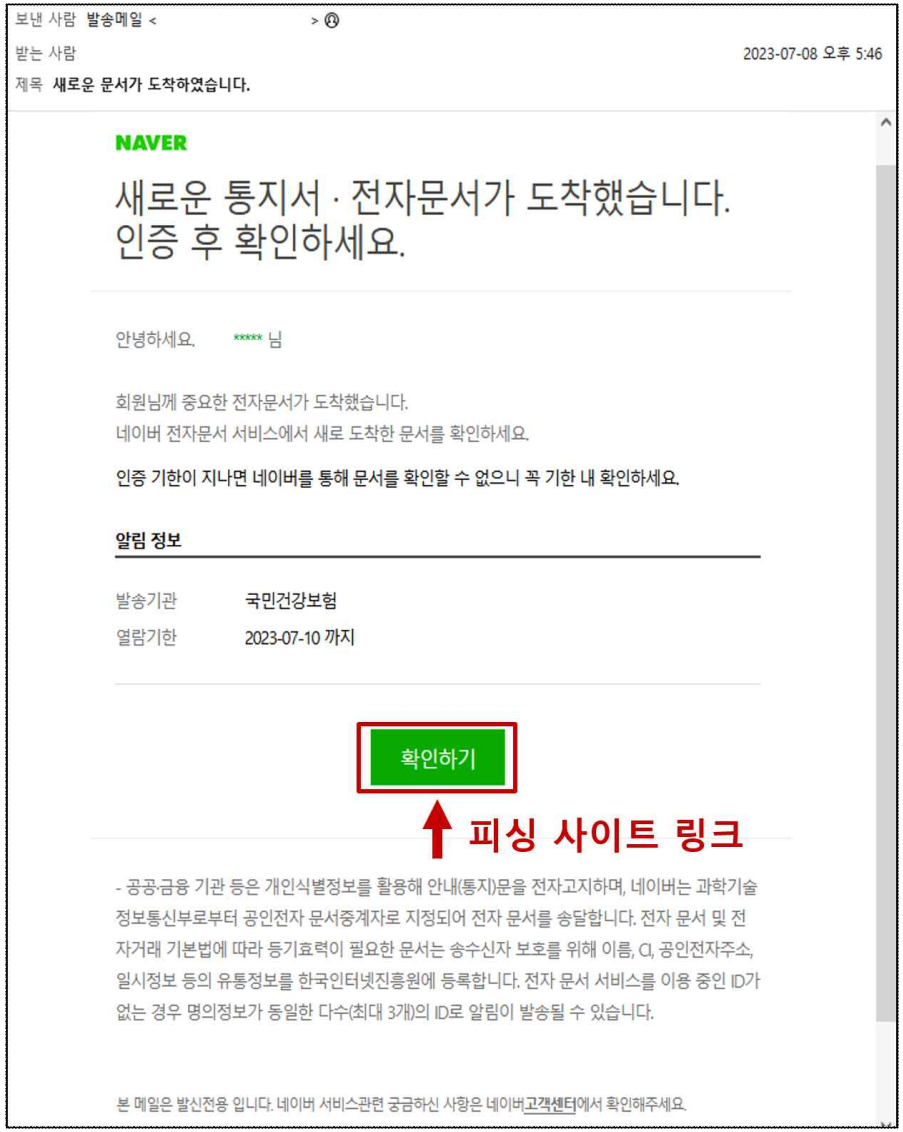
일시	2023-03-13 11:05
담당관서	경찰청
제목	사이버안전국에서 알려드립니다.
내용	안녕하세요 경찰청 사이버안전국입니다. 사이버안전국 사이버범죄 상담코너를 이용해 주셔서 감사드립니다. 회원님께서 발송하신 메일은 법령 위반의 우려가 있고, 경우에 따라서는 회원님께서 법적 책임을 부담하실 수 있습니다. 고객님께서 직접 네이버 메일 계정에서 스팸메일들을 발송한 적이 없는데 이 메일을 받았다면 다른 사람이 회원님의 아이디를 도용하였을 가능성도 있습니다. **자세한 내용은 첨부화일로 보내드립니다.** 귀하의 빠른 피해복구가 되길 기원하며 귀하와 귀하의 가정에 행복이 가득하시기 바랍니다. 감사합니다. **담당자 : 사이버수사기획계 김지국**

서울특별시 서대문구 통일로 97(미근동) 경찰청 대표전화 : 02-3150-2659 Copyright@2023 경찰청, All Rights Reserved.

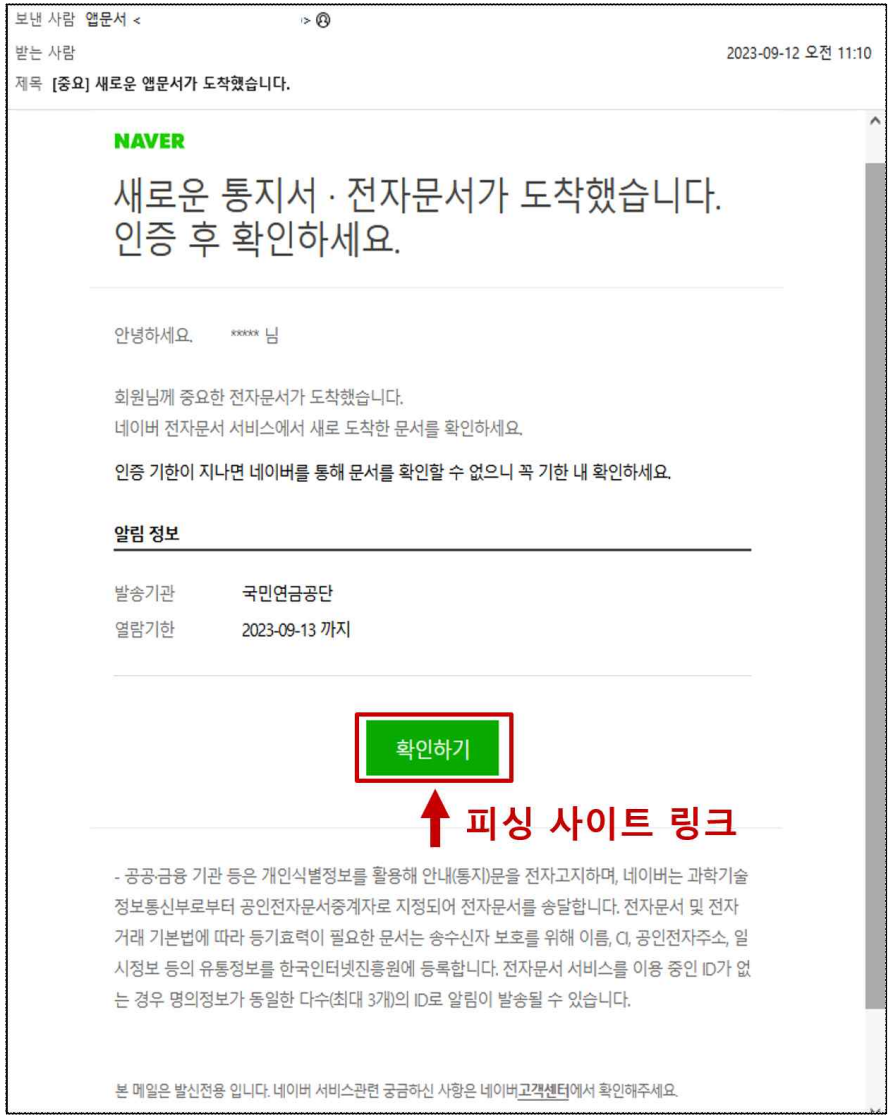
○ 연구원 사칭 전자우편



○ 국민건강보험 사칭 전자우편



○ 국민연금공단 사칭 전자우편



보낸 사람 앱문서 <

받는 사람 2023-09-12 오전 11:10

제목 [중요] 새로운 앱문서가 도착했습니다.

NAVER

새로운 통지서 · 전자문서가 도착했습니다.
인증 후 확인하세요.

안녕하세요. ***** 님

회원님께 중요한 전자문서가 도착했습니다.
네이버 전자문서 서비스에서 새로 도착한 문서를 확인하세요.

인증 기한이 지나면 네이버를 통해 문서를 확인할 수 없으니 꼭 기한 내 확인하세요.

알림 정보

발송기관	국민연금공단
열람기한	2023-09-13 까지

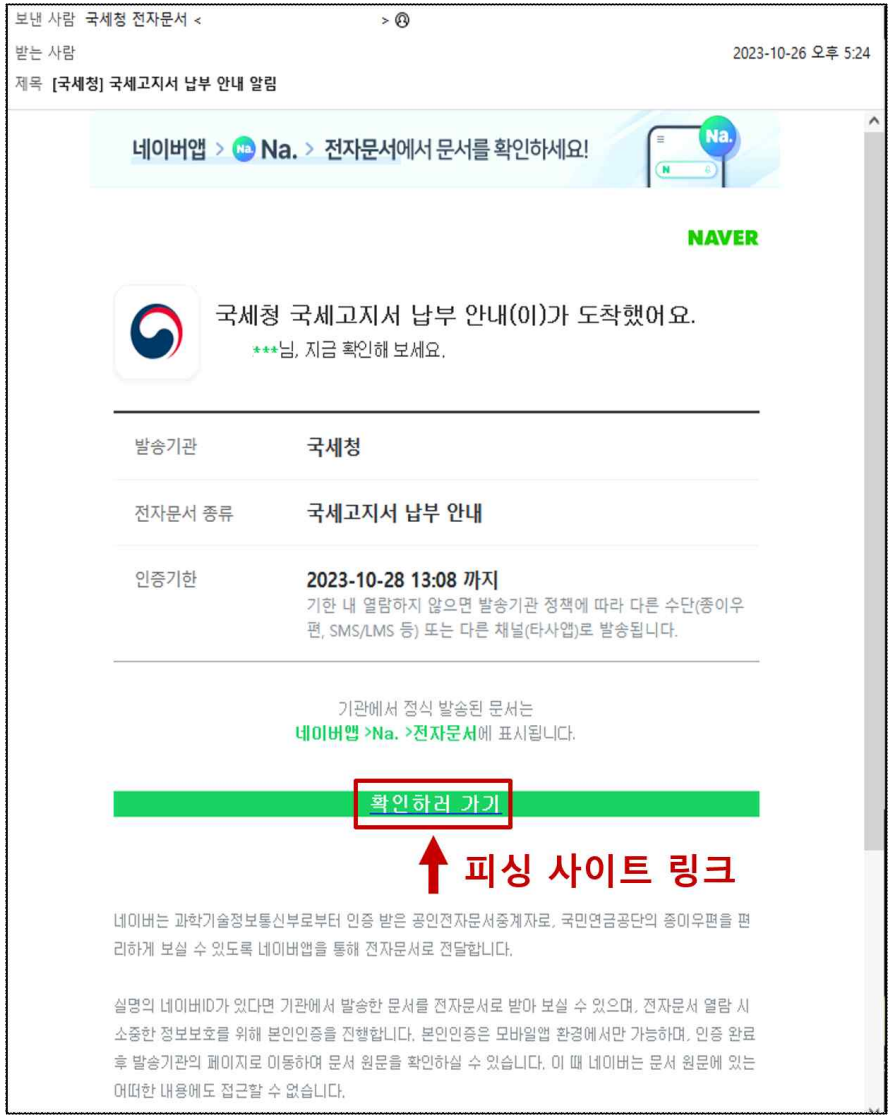
확인하기

피싱 사이트 링크

- 공공·금융 기관 등은 개인식별정보를 활용해 안내(통지)문을 전자고지하며, 네이버는 과학기술정보통신부로부터 공인전자문서중계자로 지정되어 전자문서를 송달합니다. 전자문서 및 전자거래 기본법에 따라 등기효력이 필요한 문서는 송수신자 보호를 위해 이름, CI, 공인전자주소, 일시정보 등의 유통정보를 한국인터넷진흥원에 등록합니다. 전자문서 서비스를 이용 중인 ID가 없는 경우 명의정보가 동일한 다수(최대 3개)의 ID로 알림이 발송될 수 있습니다.

본 메일은 발신전용 입니다. 네이버 서비스관련 궁금하신 사항은 네이버고객센터에서 확인해주세요.

○ 국세청 사칭 전자우편



보낸 사람 국세청 전자문서 <

받는 사람 2023-10-26 오후 5:24

제목 [국세청] 국세고지서 납부 안내 알림

네이버앱 > Na. > 전자문서에서 문서를 확인하세요!

NAVER

국세청 국세고지서 납부 안내(이)가 도착했어요.
***님, 지금 확인해 보세요.

발송기관	국세청
전자문서 종류	국세고지서 납부 안내
인증기한	2023-10-28 13:08 까지 기한 내 열람하지 않으면 발송기관 정책에 따라 다른 수단(종이우편, SMS/LMS 등) 또는 다른 채널(타사앱)로 발송됩니다.

기관에서 정식 발송된 문서는
네이버앱 >Na. >전자문서에 표시됩니다.

확인하러 가기

피싱 사이트 링크

네이버는 과학기술정보통신부로부터 인증 받은 공인전자문서중계자로, 국민연금공단의 종이우편을 편리하게 보실 수 있도록 네이버앱을 통해 전자문서로 전달합니다.

실명의 네이버ID가 있다면 기관에서 발송한 문서를 전자문서로 받아 보실 수 있으며, 전자문서 열람 시 소중한 정보보호를 위해 본인인증을 진행합니다. 본인인증은 모바일앱 환경에서만 가능하며, 인증 완료 후 발송기관의 페이지로 이동하여 문서 원문을 확인하실 수 있습니다. 이 때 네이버는 문서 원문에 있는 어떠한 내용에도 접근할 수 없습니다.

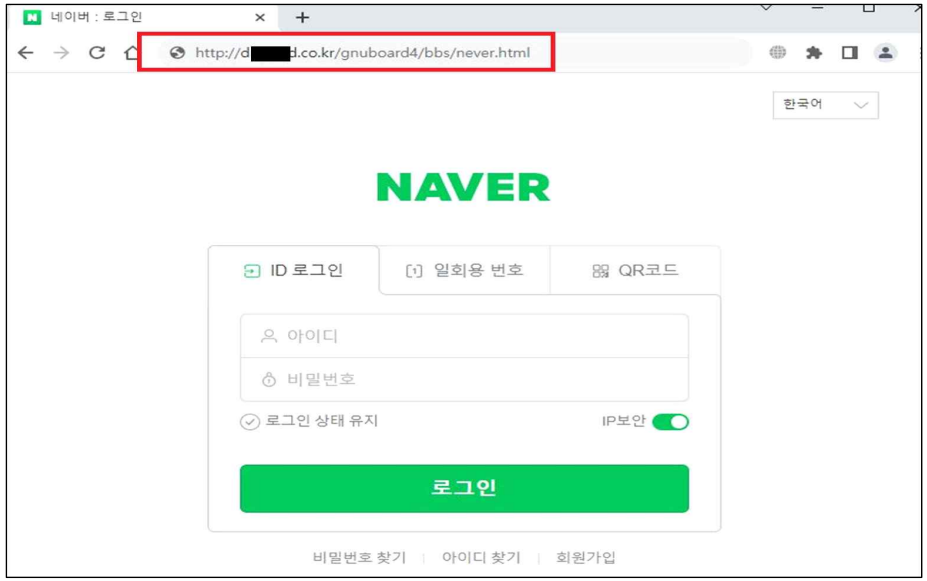
붙임 3 가짜 누리집 화면

○ 사칭이메일에 포함된 피싱사이트 링크는 **정상사이트와 외관이 동일**하여 **접속시 주의**가 필요

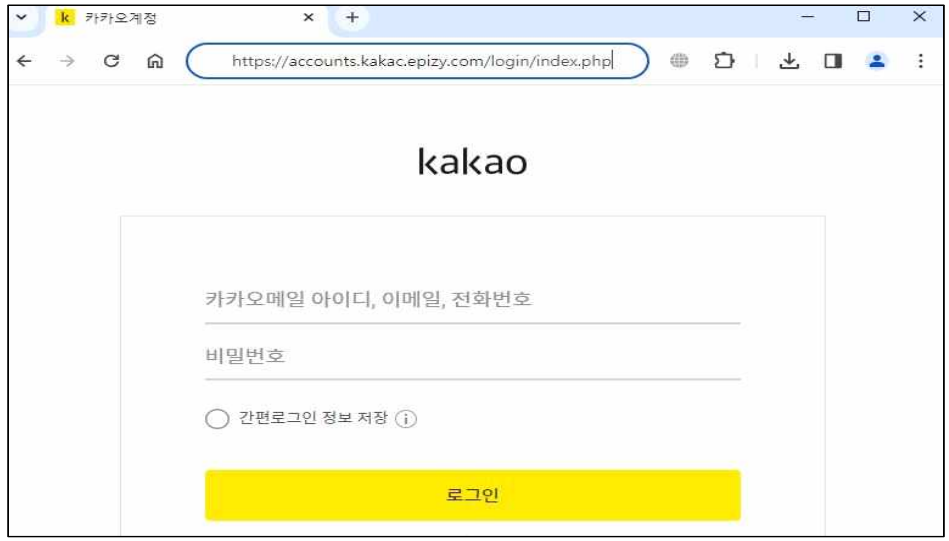
⇒ **(판별방법)** 인터넷주소가 포털사이트일 경우 naver.com, daum.net, nate.com등 주소가 정확한지 확인

(사례) navor, daurn, policynaver 등 유사 또는 아래와 같이 전혀 무관한 주소는 피싱사이트

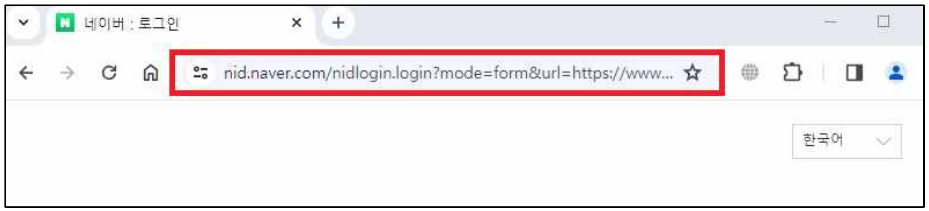
○ 가짜 누리집(Naver)



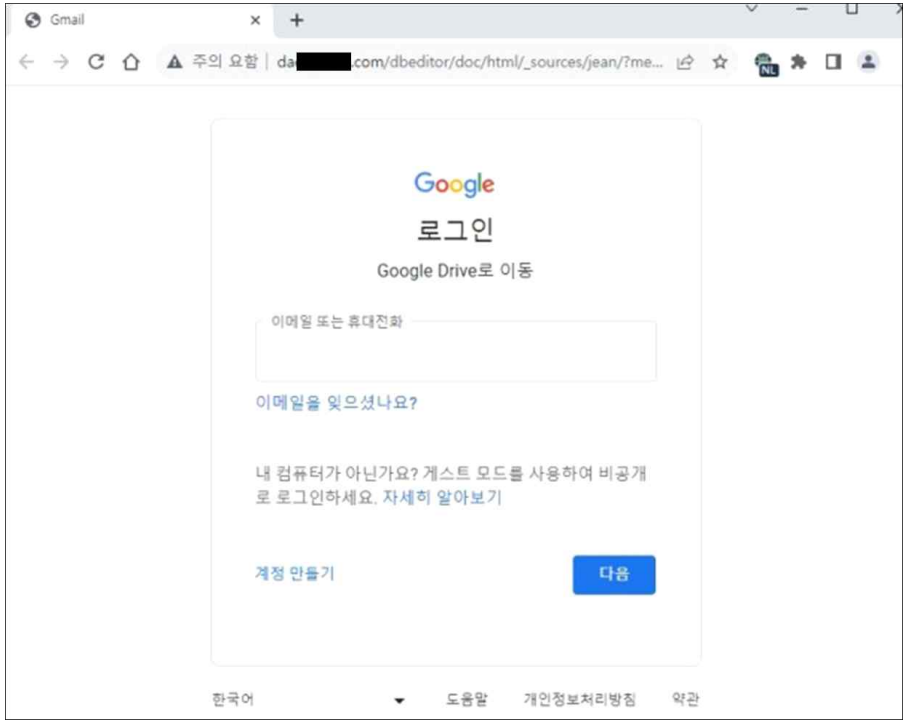
○ 가짜 누리집(Kakao)

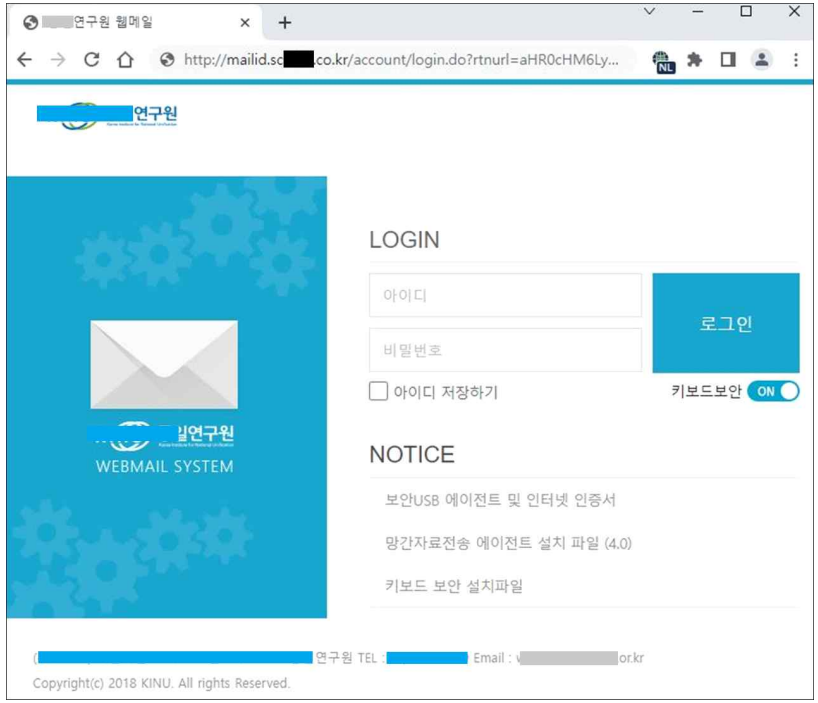


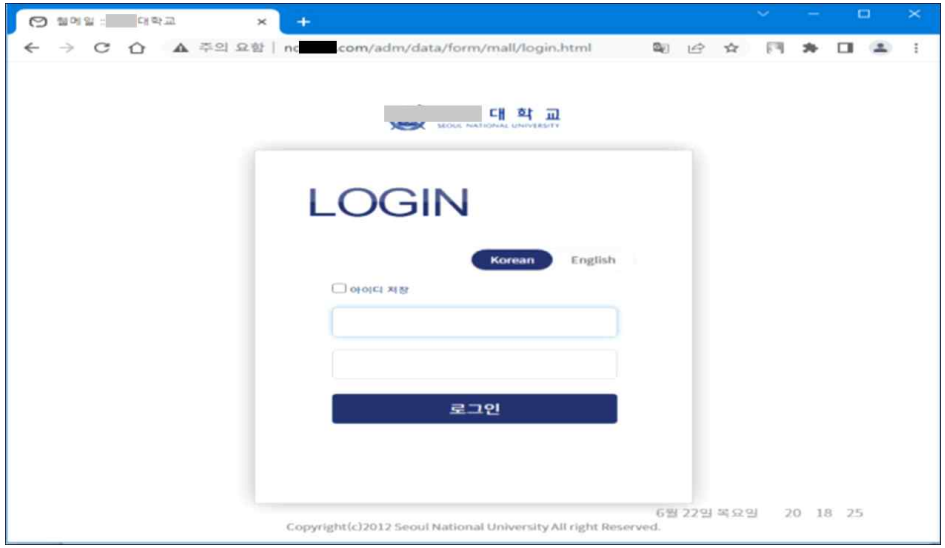
○ 진짜 누리집(nid.naver.com)

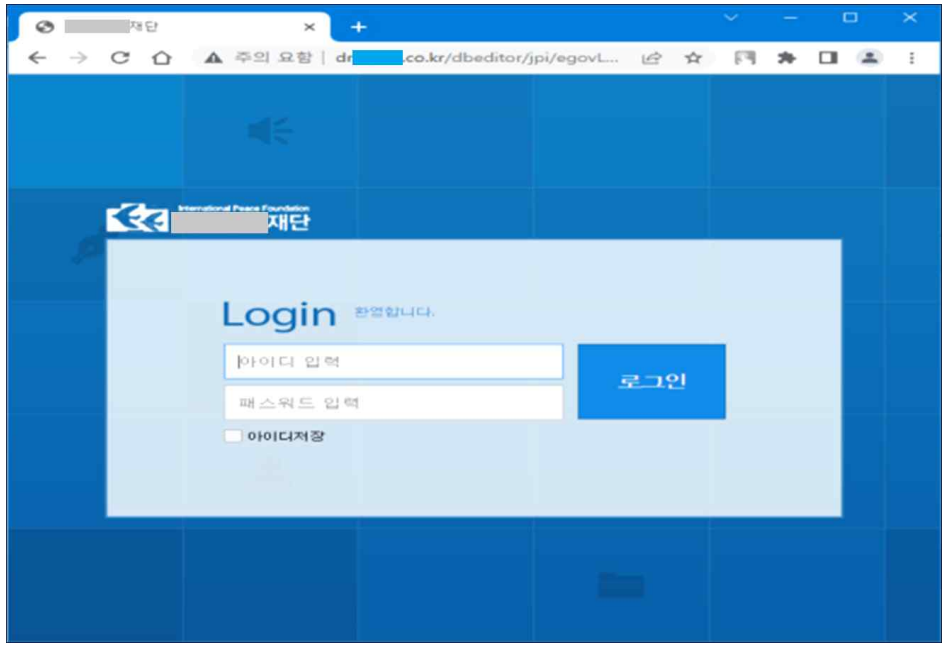


○ 진짜 누리집(accounts.kakao.com)


Gmail
주의 요함 | da[redacted].com/dbeditor/doc/html/_sources/jean/?me...
Google
로그인
Google Drive로 이동
이메일 또는 휴대전화
이메일을 잊으셨나요?
내 컴퓨터가 아닌가요? 게스트 모드를 사용하여 비공개로 로그인하세요. 자세히 알아보기
계정 만들기
다음
한국어
도움말
개인정보처리방침
약관


[redacted]연구원 웹메일
http://mailid.sc[redacted].co.kr/account/login.do?rtnurl=aHR0cHM6Ly...
[redacted]연구원
WEBMAIL SYSTEM
LOGIN
아이디
비밀번호
로그인
아이디 저장하기
키보드보안 ON
NOTICE
보안USB 에이전트 및 인터넷 인증서
망간자료전송 에이전트 설치 파일 (4.0)
키보드 보안 설치파일
[redacted] 연구원 TEL : [redacted] Email : [redacted].or.kr
Copyright(c) 2018 KINU. All rights Reserved.


웹메일 - [redacted]대학교
주의 요함 | nc[redacted].com/adm/data/form/mall/login.html
[redacted] 대 학 교
SEOUL NATIONAL UNIVERSITY
LOGIN
Korean
English
아이디 저장
로그인
6월 22일 목요일 20 18 25
Copyright(c)2012 Seoul National University All right Reserved.


[redacted]재단
주의 요함 | dr[redacted].co.kr/dbeditor/jpi/egovL...
[redacted]재단
Login 환영합니다.
아이디 입력
패스워드 입력
로그인
아이디저장