



국정원, 국내 '포털사이트' 사칭한 北 해킹공격 주의 촉구

- 네이버·카카오(다음) 등을 사칭한 '해킹메일 전송'이 전체 北해킹수법의 74% 차지
- 국정원, 對국민 추가피해 방지 및 보안주의를 위해 北해킹공격 분석결과를 최초 공개

중학교 교사 이모씨는 '포털사이트 관리자' 명의로 발송된 메일을 무심코 열람했다가, 수년치 메일 송수신 내용은 물론, 클라우드에 저장된 이력서 및 개인 파일들이 통째로 유출되는 피해를 입었다. 이모씨가 수신한 메일은 북한 정찰총국이 보낸 해킹용 메일이었다.

회사원 김모씨는 '비밀번호가 유출되었습니다'라는 제목의 메일을 열람한 뒤 즉시 비밀번호를 변경했다. 하지만 김씨는 며칠 뒤 관계 기관으로부터 "메일에 저장돼 있던 업무자료 등이 모두 해커에게 절취됐다"는 통보를 받았다. 코로나19 상황 가운데 재택근무를 위해 개인메일 계정으로 전송했던 민감 업무자료가 모두 북한으로 빠져나간 것이었다.

북한 해킹조직들이 대한민국 국민들을 대상으로 무차별·지속적 해킹공격을 진행하고 있어, 국가정보원이 처음으로 北해킹공격 관련 통계를 공개하며 對국민 경각심 제고에 나섰다.

국정원은 국가·공공기관 및 국제·국가배후 해킹조직에 대응하는 과정에서 집계한 대한민국 대상 해킹공격 자료 중, 최근 3년(2020~2022년)간 발생한 북한 해킹조직으로부터의 사이버 공격 및 피해통계를 25일 공개했다.

이날 국정원이 공개한 내용에는 북한의 해킹공격 유형, 사칭기관, 해킹공격에 사용한 메일 제목 및 실제 사칭계정 등이 담겼다.

국정원 자료에 따르면, 북한은 보안프로그램의 약점을 뚫는 '취약점 악용'(20%)이나 특정사이트 접속시 악성코드가 설치되는 '워터링 홀'(3%) 수법 등도 활용했지만, 이메일을 악용한 해킹공격이 전체의 74%를 차지하며 압도적으로 많았다.

이에 대해 국정원 관계자는 "국민 대부분이 사용하는 상용 메일을 통한 해킹 공격을 한다는 것은, 결국 북한이 대한민국 국민 전체를 대상으로 해킹공격을 하고 있다는 뜻"이라며 "기존 북한의 주요 해킹타겟이었던 전·현직 외교안보 분야 관계자 이외에, 대학교수·교사·학생 및 회사원 등도 해킹피해를 보고 있다"고 했다.

북한은 메일 수신자가 해당 메일을 별다른 의심 없이 열람하도록 유도하기 위해 특히 '발신자명'과 '메일 제목'을 교묘하게 변형하고 있다는 것이 국정원의 설명이다.

먼저 북한은 메일 사용자들이 메일 발송자를 확인할 때 주로 '발신자명'을 보는 점에 착안하여, 해킹메일을 유포시 네이버·카카오(다음) 등 국내 포털사이트를 많이 사칭(약 68%)하고 있었다.



실제 북한은 메일 발송자명을 '네이버', 'NAVER고객센터', 'Daum게임담당자' 등 '포털사이트 관리자'인 것처럼 위장했다. 발신자 메일주소도 'naver'를 'navor'로, 'daum'을 'daurn'로 표기하는 등 오인(誤認)을 유도하고 있었다. 국정원은 "메일 수신자의 계정정보를 탈취하기 위해 열람을 유도하는, 사회 심리 공학적 피싱인 것"이라고 했다.

일례로 최근 국정원이 국내 해킹사고 조사과정에서 확보한 북한 해커의 해킹메일 공격 발송용 계정에는 1만여건의 해킹메일이 들어있었다. 또 다른 공격을 위한 것으로 생각되는데, 이 가운데 약 7,000개가 네이버·다음 등의 국내 포털사이트로 사칭한 메일이었다. 뿐만 아니라, 해킹 메일이 발송될 국내 가입자 이메일 주소 4,100여개도 발견됐다.

아울러 북한은 메일 사용자들을 속이기 위해 '새로운 환경에서 로그인되었습니다.', '[중요] 회원님의 계정이 이용제한되었습니다.', '해외 로그인 차단 기능이 실행되었습니다.' 등 계정 보안 문제가 생긴 것처럼 제목을 단 해킹메일을 발송하고 있었다.

국정원은 "북한은 해킹메일로 확보한 계정정보를 이용하여 메일계정 내 정보를 탈취하고, 메일함 수발신 관계를 분석해 2~3차 공격대상자를 선정해 악성코드 유포 등 공격을 수행하고 있다"고 밝혔다.

이날 국정원은 북한발 해킹피해를 예방하기 위해 실제 북한의 해킹메일 샘플과 이에 대한 대응요령도 안내했다.

국정원은 "메일 열람시 ①보낸사람 앞에 붙어있는 '관리자 아이콘'(네이버 : , 다음 : ) ② 보낸사람 메일주소 ③ 메일 본문의 링크주소 등 3가지를 반드시 확인해야 한다"며 메일 무단열람 방지를 위한 '2단계 인증 설정' 등 이메일 보안 강화를 당부했다.

보다 구체적인 국정원의 '해킹메일 대응요령'은 국가사이버안보센터 홈페이지 자료실에서 확인할 수 있다.

국정원 관계자는 "실효적인 해킹메일 차단 방안 마련을 위해서는 민간협력이 필수"라며 "네이버·다음 등 국내 주요 포털사이트 운영사와 관련 정보 공유를 강화해 나가겠다"고 밝혔다. 끝.

최근 3년간 북한발 해킹메일 공격 피해통계

1. 북한의 공격유형(2020~2022년)

공격유형	해킹메일	취약점악용	워터링홀	공급망	기타
비중	74%	20%	3%	2%	1%

2. 해킹메일 사칭기관

기관	네이버	카카오(다음)	금융·기업 · 방송언론	외교안보	기타
비중	45%	23%	12%	6%	14%

3 해킹메일 제목

순서	해킹메일 제목
1	새로운 환경에서 로그인 되었습니다.
2	[중요] 회원님의 계정이 이용제한되었습니다.
3	해외 로그인 차단 기능이 실행되었습니다.
4	회원님의 본인확인 이메일 주소가 변경되었습니다.
5	알림 없이 로그인하는 기기로 등록되었습니다.
6	회원님의 메일계정이 이용제한 되었습니다.
7	[Daum]계정아이디가 충돌하였습니다. 본인 확인이 필요합니다.
8	[Daum]고객님의 계정이 충돌되었습니다.
9	[경고]회원님의 아이디로 스팸이 대량 발송되었습니다.
10	[보안공지]비정상적인 로그인이 감지되었습니다.

4. 메일 발신자 사칭 방법

o 사칭 발신자명

사칭 대상	사칭 발신자명 예시			
네이버	네이버 (숫자 0)	네이버 (영어 O)	‘네이버 ’	네이버_
	네이버	(주)네이버	NAVER고객센터	‘네이버 MYBOX ’
카카오(다음)	?Daum 고객센터	Daum 보안센터	Daum 고객지원	[Daum] 고객센터
	다음메일 커뮤니케이션	Clean Daum	‘카카오팀’	Daum 캐쉬담당자


o 사칭 메일주소

구 분		공식 메일주소	사칭 메일주소
네 이 버	네이버	account_noreply@navercorp.com	account_noreply@naver corp .com accountst s _reply@navercorp.com account_help@`navercorp.com
	네이버 고객센터	help@help.naver.com	help@helpnaver.com help@help.naver admin .com help@help.nav or .com
	네이버 메일	navermail_noreply@navercorp.com	mail_notify@naver.com no_reply@navecorp.com navermail_noreply@ sian .com
카 카 오 · 다 음	카카오	noreply@kakaocorp.com	noreply@kakaoc orp .net norep ley @kakaocorps. co.kr no_re ply @kakaocorp.com
	다음 메일	notice-master@daum.net	noti se -master@dau rn .net notice-master@daum. nat notice-master@han mail .net
	카카오 메일	noreply_kakaomail@kakao.com	noreply- master @kakao.com nore ply @kakao.com noreply@kakao crp .com

북한이 사용한 해킹메일 샘플 및 대응요령

1. 해킹메일 샘플

가. 네이버 관리자 사칭

 **네이버** <help@help.navercorp.com>
회원님의 본인확인 이메일 주소가 삭제되었습니다.

회원님의 본인확인 이메일 주소가 삭제되었습니다.

안녕하세요 [redacted] 회원님.
회원님의 **본인확인 이메일 주소가 삭제되어** 해당 내역을 안내해 드립니다.

본인확인 이메일 주소 삭제에 따른 안내

변경 일시	2021-09-03(금) 11:55
변경 방법	내정보>회원정보>연락처 수정

회원님이 직접 본인확인 이메일 주소를 삭제한 적이 없는데 이 메일을 받았다면 다른 사람에 의해 본인확인 이메일 주소가 삭제되었을 수 있습니다.
다른 사람이 내 회원정보에 접근한 것은 아닌지 점검해 주세요.


더불어 본인확인 이메일 주소는 아이디, 비밀번호 찾기 등 본인확인이 필요한 경우 또는 비밀번호 변경 등 보안과 관련된 중요한 알림을 받을 때 사용되니 꼭 최신 정보로 업데이트 해주세요.

자세한 내용은 **도움말**을 참고해 주세요.

링크 [본인확인 이메일 주소 등록하러 가기](#)

링크 클릭시 계정입력 유도

나. 카카오(다음) 관리자 사칭

 **카카오팀** <master@kakaocorp.info>
[kakao] 카카오 계정 쿠키 정보가 도용되고 있습니다.

kakao 계정

타인에게 카카오 계정 쿠키 정보가 도용되고 있습니다.

안녕하세요. 카카오팀입니다.
귀 메일 계정에 1달 이상 로그인하지 않은 쿠키가 존재 합니다.
현재 이용중인 이 쿠키는 귀 메일계정에 보안 위협을 주고 있습니다.

이용 내역은 다음과 같습니다.
12/07/2022 10:27 AM (KST)에 창조된 이 쿠키의 마지막 이용시간은
01/11/2023 10:06 AM (KST)입니다.

귀 계정을 1달동안 한번이라도 로그인하거나 다른 기기를 이용하지 않았다면 이 쿠키는 외부에 유출되어 도용되고 있습니다.

링크 [현재 기기 제외한 모든 쿠키 삭제하기](#)


회원님의 소중한 자료를 위해 바쁘신 시간 내주셔서 감사합니다.

링크 클릭시 계정입력 유도

2. 대응요령

① 관리자 아이콘 확인

o 식별 방법



해킹메일 식별방법 ① 아이콘 확인

발신자 이름이 똑같이 '네이버' 및 'Daum게임담당자'지만 정상메일과 해킹메일 아이콘이 서로 다릅니다.

o 네이버



	받은메일함	프로모션	청구결제	SNS	카페
<input type="checkbox"/>	 네이버 사칭				
<input type="checkbox"/>	 Slack				
<input type="checkbox"/>	 네이버 정상				
<input type="checkbox"/>	 네이버메일				
<input type="checkbox"/>	 네이버메일				

 ← 정상적인 네이버 관리자 메일
 ← 관리자 사칭 해킹 메일

o 카카오(다음)



	Daum게임담당자 사칭	받은메일함	[다음게임] 계정 보호조치 안내
<input type="checkbox"/>	 Daum게임담당자 정상		
<input type="checkbox"/>	 Daum게임담당자		
<input type="checkbox"/>	 Daum게임담당자		
<input type="checkbox"/>	 다음메일		

 ← 정상적인 다음 관리자 메일
 ← 관리자 사칭 해킹 메일

② 보낸사람 메일주소 확인

○ 식별 방법



해킹메일 식별방법 ② 보낸사람 메일주소 확인

해킹메일 발신자의 메일주소를 확인해 보면,
포털 공식메일로 오인할 수 있는 주소를 사용하고 있습니다.

○ 네이버

회원님의 아이디가 로그인 제한중입니다. 2019-02-11 (월) 12:41

보낸 사람: 네이버 <notice@polycynaver.com>

받는 사람: <아이디가@naver.com>

☆ 네이버 <notice@polycynaver.com>

NAVER

회원님의 아이디가 로그인 제한중입니다

회원님의 아이디 : <아이디가> 비정상적인 방식으로 로그인 시도되었습니다.
해커가 계정에 액세스하려는 경우에 대비해 아이디 보호조치로 로그인을 제한했습니다.

아이디는 언제 보호되나요?

아이디/비밀번호가 판매사이트 등에서 정보노출이 확인된 경우
스팸메일 발송, 불법 게시물 작성 등의 행위가 신고 또는 발견된 경우
그 외, 타인에 의한 가입 또는 로그인이 의심되는 경우

! 관리자 사칭 계정 주의

○ 카카오(다음)

다음메일: notice-master@daum.net
[긴급] 지금 바로 비밀번호를 변경해 주세요.

다음메일 <notice-master@daum.net>

안녕하세요. Daum 입니다.

회원님의 비밀번호와 개인정보가 타인에게 도용되었을 수 있습니다.

회원님의 Daum 계정에서 로그인 불허로 등록된 아이디로 최근에 접근하였던 이력이 확인되었습니다.
회원님의 계정에 접근하였던 IP : 176.241.221.89 는(은) 로그인 불허로 등록된 IP 이며 Daum 에서 현재 로그인 시도를 차단하고 있으나 안전한 사용을 위하여 비밀번호를 변경할것을 권합니다.

회원님의 비밀번호가 외부에 유출 되었을 가능성이 매우 높고, 개인정보 보호 조치가 필요한 상황입니다.

개인정보 보호를 위한 첫 걸음


회원님의 소중한 정보를 안전하게 보호하기 위해 지금 바로 새로운 비밀번호로 변경해주세요.

[지금 비밀번호 변경하러 가기](#)

! 관리자 사칭 계정 주의

③ 메일 본문의 링크 주소 확인

○ 식별 방법



해킹메일 식별방법 ③ 링크 주소 확인

피싱메일 본문의 링크에 마우스를 올려보면
브라우저 왼쪽 아래에서 수상한 링크를 확인할 수 있습니다.

○ 네이버



회원님의 아이디가 로그인 제한중입니다

회원님의 아이디 : **car***sion**이(가) 비정상적인 방식으로 로그인 시도되었습니다.
해커가 계정에 액세스하려는 경우에 대비해 아이디 보호조치로 로그인을 제한했습니다.

아이디는 언제 보호되나요?

아이디/비밀번호가 판매사이트 등에서 정보노출이 확인된 경우
스팸메일 발송, 불법 게시물 작성 등의 행위가 신고 또는 발견된 경우
그 외, 타인에 의한 가입 또는 로그인이 의심되는 경우

정상적인 계정활동을 원하신다면, **비밀번호를 변경하고 로그인 제한을 해제**하세요.

로그인 제한 해제

정상 링크주소는
nid.naver.com 으로 시작

비정상 링크주소
car*sion.com/nayaboard/...**

○ 카카오(다음)



안녕하세요. Daum 입니다.

회원님의 비밀번호와 계정을 보호하기 위해 로그인 제한을 걸었습니다.

회원님의 계정에 접근해 로그인 시도를 차단하고 있습니다.

회원님의 비밀번호가 노출되었습니다.

계정정보 보호를 위한 조치입니다.

회원님의 소중한 정보를 보호하기 위해 비밀번호를 변경하고 로그인 제한을 해제하세요.

지금 비밀번호 변경하기

비밀번호를 변경하고 로그인 제한을 해제하면 계정을 안전하게 사용할 수 있습니다.


감사합니다.

정상 링크주소는
accounts.kakao.com

비정상 링크주소
car*sion.com/nayaboard/...**

④ 로그인 화면 주소 확인

○ 식별방법

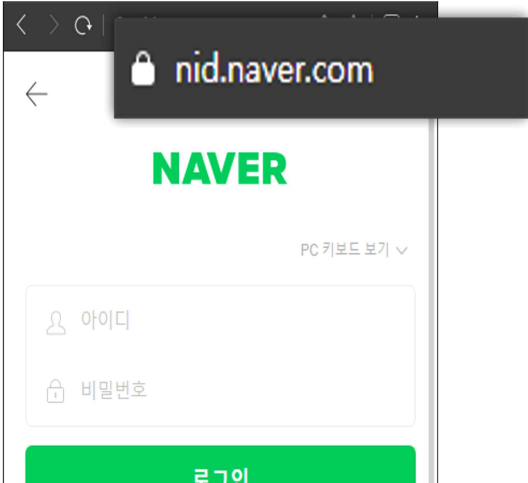


해킹메일 식별방법 ④ 로그인 화면 주소 확인

혹시 메일에 있는 링크를 클릭했더라도 주소를 확인하면 피해를 막을 수 있습니다.

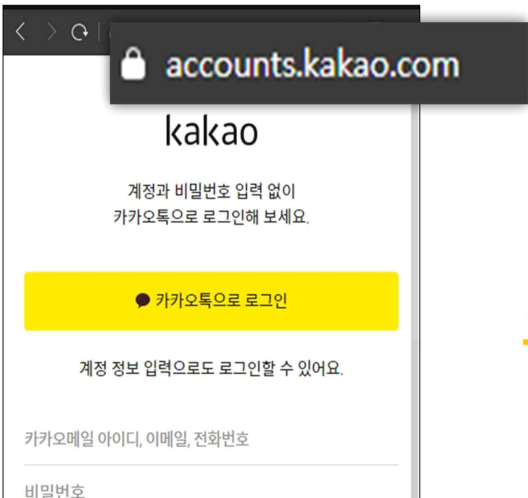
- 보안접속 : "https://..." 로 시작
- 로그인 접속 URL : "**nid.naver.com**/..." "**accounts.kakao.com**/..."
- 주소 왼쪽에 자물쇠 마크 또는 공식 로고 포함

○ 네이버



! 네이버 로그인 화면
● **nid.naver.com** 확인

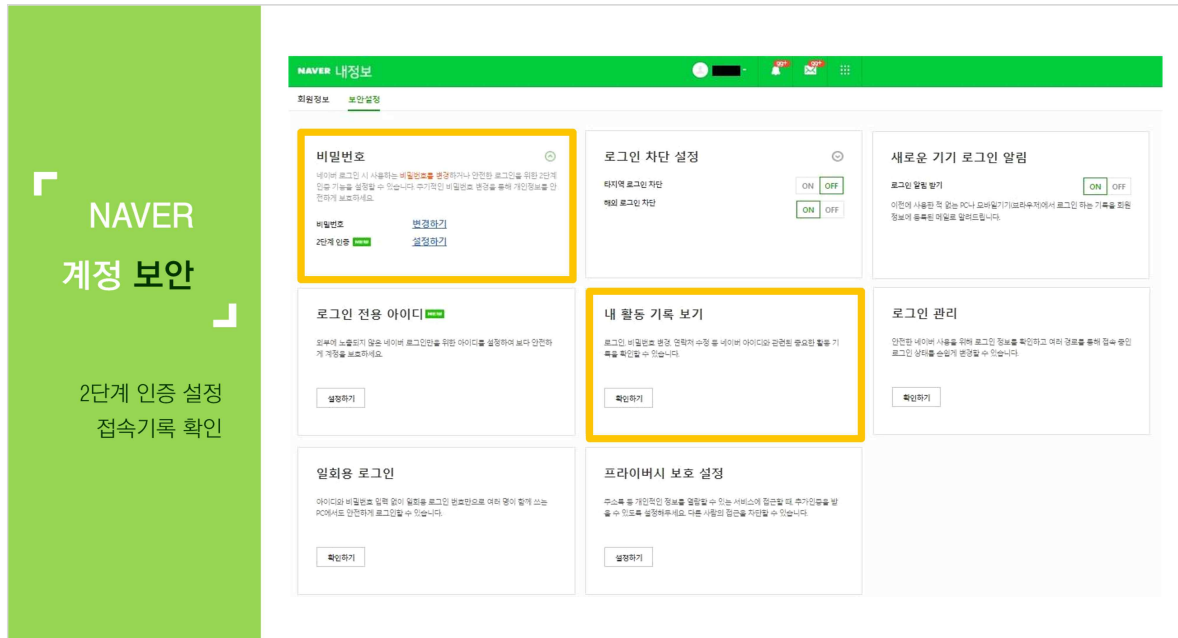
○ 카카오(다음)



! 다음 로그인 화면
● **accounts.kakao.com** 확인

⑤ 메일 무단열람 방지를 위한 2단계 인증 설정

o 네이버



o 카카오(다음)

