

교육분야 업무직원 스마트폰 보안대책(안)

< '16. 3. 14(월), 정보보호팀 >

□ 추진배경

- 최근 북한에서 정부 주요 인사를 대상으로 스마트폰을 해킹하는 사례가 발생하여 스마트폰 보안 관리 강화 필요

※ 주요 인사 수십명 스마트폰 해킹해 문자·통화내용 유출('16.3.8, 조선일보)

< 스마트폰 이용 현황 >

- 개인적 이용 : 개인통화, 인터넷 정보검색 등 활용
- 업무적 이용 : 상용서비스(카카오톡, 밴드 등)로 업무 활용
 - ※ 상용서비스를 통해 직원간 업무자료를 사진으로 전송하거나, 문서자료 공유도 다수 파악되고 있음

□ 추진대상

- 대상 : 교육분야 업무를 추진하는 전직원

- 주요해킹 우려 대상자

구분	교육부	대학	교육청	소속·공공기관
대상	과팀장 이상	사무국장* 이상	부교육감 이상	기관장

* 대학은 학무위원회 위원 포함

□ 스마트폰 해킹경로 및 내용

- 스마트폰 해킹경로
 - (문자메시지) 유인하는 문자 메시지 보내고, 이를 선택하면 악성 코드가 설치되어 해킹 가능
 - (앱프로그램) 게임 등의 앱프로그램에 악성코드를 심어두어 앱을 설치하면 악성코드가 설치되어 해킹 가능
 - (사이트접속) 도박 등 신뢰할 수 없는 사이트에 접속하면 악성코드가 설치되어 해킹 가능
- 스마트폰 해킹내용
 - 스마트폰 통화내역, 문자메시지, 음성통화 내용, 전화번호 주소록 등 스마트폰에 있는 대부분의 자료가 해킹 가능

□ 스마트폰 보안관리 강화 방안

- 모바일 백신 설치 <붙임1 설치방법 참조>
 - V3모바일 등 최신 백신 프로그램을 설치하고 수시 점검 실시
- 스마트폰 사용자 보안의식 강화 <붙임2 실천수칙 10가지 참조>
 - (문자메시지) 신뢰할 수 없는 문자 메시지는 읽지 않고 삭제 처리
 - (앱프로그램) 신뢰할 수 없는 앱프로그램은 설치하지 않음
 - (사이트접속) 도박 등 신뢰할 수 없는 사이트는 접속 금지
 - (WiFi접속) 무료로 제공되는(보안에 취약한) WiFi 접속 금지
 - (기타) 불필요한 앱프로그램 삭제 등 핸드폰 관리 강화
- 스마트폰으로 업무목적 사용 금지
 - (문자메시지) 카카오톡 등을 통해 업무용 대화 및 업무자료(사진 등) 전송 금지
 - (모바일게시판) 밴드 등을 이용하여 직원간 업무자료 공유 금지
 - (SNS사용) 페이스북 등 SNS를 통해 업무자료 요구 시 불응
- 보안폰(안전한 스마트폰) 사용 권장
 - 보안폰을 소지하고 있는 교육부 실·국장 이상은 보안폰 이용 활성화

<별첨자료>

[별첨 1] 스마트폰 보안앱 설치 방법





[별첨 2] 정보보호 실천수칙 10가지(스마트폰편)

[별첨 3] 주요 스미싱 사례

[별첨 4] 문자메시지 및 SNS를 통한 업무자료 요구 사례

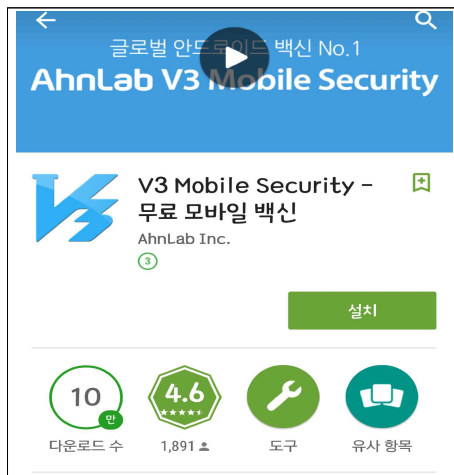
별첨 1 스마트폰 보안앱 설치 방법

□ 최근 가장 많이 사용되고 있는 스마트폰 보안앱 종류 예시

 <p>360 Security - 바이러스 백... 360 Mobile Security Limited 4.6 ★</p>	 <p>CM Security - 무료 바이러스... Cheetah Mobile (AppLock & AntiVir... 4.7 ★</p>
 <p>V3 Mobile Security - 무료... AhnLab Inc. 4.6 ★</p>	 <p>알약 안드로이드 - 폰 속도 향상... ESTsoft Corp. 4.4 ★</p>

□ 보안앱 설치 방법(안드로이드 폰 기준)

- ① 사용자는 핸드폰에서 “Play 스토어” 또는 “App Store”를 실행
- ② 사용자는 핸드폰에서 원하는 보안앱을 검색
- ③ 사용자는 원하는 보안앱을 설치
< V3 모바일앱 설치 화면 예시 >



- ④ 사용자는 정기적으로 보안앱을 실행하여 점검

별첨 2 정보보호 실천수칙 10가지(스마트폰편)

1. 단문 문자(또는 SNS) 메시지에 포함된 URL 클릭하지 않기
2. 최신 스마트폰 백신을 설치하고 정기적으로 점검하기
3. 스마트폰 보안 잠금(비밀번호 또는 화면 패턴)을 설정하여 이용하기
4. 공식 앱 마켓이 아닌 다른 출처(출처를 알 수 없는 앱)의 앱 설치 제한하기
5. 스마트폰 운영체제를 항상 최신으로 업데이트하기
6. 공인인증서는 USIM 등 안전한 저장장소에 보관하기
7. 루팅, 탈옥 등 스마트폰 구조를 임의로 변경하지 않기
* 루팅, 탈옥 : 보안상의 문제로 일반적으로 허용하지 않는 수정권한을 획득
8. 스마트폰 앱 설치시 과도한 권한을 요구하는 앱은 설치하지 않기
9. 스마트폰 WiFi 연결시 제공자 불분명한 공유기 이용하지 않기
10. 스마트폰에 중요정보 정리하기
- 매일 양치질하는 것처럼 매일 보안 소프트웨어 실행하여 PC, 스마트폰의 바이러스도 없애주세요.
- 주민등록증, 보안카드가 찍힌 사진 등은 보관하지 말고 깨끗하게 삭제하세요.

※ 출처 : 한국인터넷진흥원 보호나라(www.boho.or.kr)

별첨 3 주요 스미싱 사례

대표유형	사례이미지	
개인 사칭 유형	★돌★잔★치★조★대★장★ 보냈습니다 "co*y.c*m/xM*E*PvLfgSeg's"	토요일z결혼식(및q지o알고w축복하러와주 세요k웨딩z사진첩 "t.c*/R*/twTv*w"
	모바일s창첩y장eqDr착하y였습니가다 tw*.k*/yo'e!5*81'h	(죽y하,췌해u주)세요.^^ b**ds.co*
택배 사칭 유형	고객님의 택배가 부자중으로 발송되었습 니다. i*.g*/Lu*Lno"	(로전택배) 1/15 고객님의택배 발송처리/주소불 주소지확인(변경요망) < 1**k*/u*o* >
	[현대택배]고객님 택배가 도착하였습니다. 확인하여주세요"ur*.c*/Z***a"	12_15고객님배송불가 주소불명 주소확인 변경요망 n*a*.c*.dte*k*.net-우체국
공공기관 사칭 유형	민원24 중간소속으로 민원접수되어 안내드 립니다. 확인하기 http://o.g*sh*pl*.om	검찰로 사진 송지되었습니다 b*t*/1G*71*d
	[법칙금고지서] 교통법규 위반으로 고지서 가 발부되었습니다 my.m*fi*e.k*r	(민방위) 소집훈련통보서 수령하세요. http://d*.d*/8**e
사회적이슈 유형	[연합뉴스] 여객선(세월호) 침몰사고 구조현황 동영상 http://g*o*/jv*ir*	"2014브라질 월드컵 거리응원장소 어디 일까요? 응원장소 확인 http://*a.*o/*C*3
	실남애 찾아보아야하는데 영상으로남아 인사 드립니다 열심히 달려왔습니다 z*y.k*/0e*	추석물량 증가로 배송이 지연되고있습니다. 배송일정확인하세요http://oo*/l*b*1x*
기타 유형	고객님의 자동차 일은 5일입니다. 통장 잔액확인 부탁드립니다.http://b*e.*m/Nd**	고객님 네이버계정은 신고접수 상태입 니다 해제하세요>http://b*t.d*/nave*y*
	(주)현대캐피탈-본인인증절차 go*al/A*1y*4 설치후즉발기버튼인증확인바랍니다.	[쿠팡]롯데리아 이벤트 불고기버거 세트 70%할인 www.gr*p.k*/Sj*7

1) 스미싱 : '무료쿠폰 제공', '돌잔치 초대장' 등을 내용으로 하는 문자메시지내 인터넷주소를 클릭하면 악성코드가 설치되어 해커가 원하는 개인·각종정보 탈취하는 수법

별첨 4 문자메시지 및 SNS를 통한 업무자료 요구 사례



<KBS 보도, '16.3.12>

국정원은 11일 국회 정보위원회 보고를 통해 **북한이 300명 정도의 외교 안보 라인 인사들에게 문자를 보내, 이 가운데 40명 정도의 스마트폰을 해킹했다고** 밝혔다. 특히 국정원은 정보위 보고 과정에서 해킹 당한 스마트폰 음성 내용을 공개했는데, "사령관님 들어왔습니다" 등의 음성이 담겨 있었던 것으로 전해졌다.

이에 따라 북한이 군 수뇌부의 동선까지 면밀히 파악했을 가능성이 대두되고 있다.

국정원은 또 해킹과 관련해 특정인의 해킹 여부에 대해서는 명확하게 확인하지 않았으나, "김관진 안보실장의 스마트폰을 교체했느냐"는 정보위원의 질의에 "바꿨을 겁니다"라고 답해 북한의 잇따른 해킹 공격이 외교안보라인 주요 인사들에게 집중됐음을 시사했다. 북한은 특히 외교안보라인 인사들에게 청와대와 외교부, 통일부 등을 사칭한 문자를 보내 해킹을 시도한 것으로 알려졌다.

주호영 국회 정보위원장은 국정원 보고에 따르면 **북한이 페이스북상에 가상의 연구단체 계정을 만들고는 미모의 여성 사진을 올린 뒤 전·현직 공직자들과 친구를 맺었으며, 이후 연구활동 명목으로 민감한 정책 자료를 요구하는 등 새로운 방식의 사이버 공격도 전개했다고** 밝혔다.

< 이하 생략 >

2) SNS(Social Network Service) : 특정한 관심·활동 등을 공유하는 사람들 사이에 관계망을 구축해 주는 온라인 서비스로써 페이스북(Facebook), 트위터(Twitter), 인스타그램(Instagram) 등이 있다.