방송통신위원회
KOREA COMMUNICATIONS COMMISSION

2010.6.29.(화)

보도자료

2010년 6월 29일(화) 배포 시점부터 보도하여 주시기 바랍니다.

문의 : 네트워크정책국 네트워크정보보호팀 박철순 팀장(☎750-2750)
네트워크정보보호팀 구교영 사무관(☎750-2755) eaglefree@kcc.go.kr

스마트폰 보안위협, 민·관이 함께 적극 대응한다

- 「이용자 10대 안전수칙」에 이어, 「스마트폰 정보보호 주체별 역할」 정립·발표 -

방송통신위원회(위원장 최시중)는 '스마트폰 정보보호 민·관 합동대응반' 및 '모바일 시큐리티 포럼'을 통해 스마트폰 정보보호 주체인 이동통신사, 스마트폰 제조사, 백신사, 보안솔루션사 및 정부 등의 「스마트폰 정보보호 주체별 역할」을 정립하여 발표하였다.

최근 국내 스마트폰 이용자수가 급증하고 이와 관련된 보안위협 가능성이 대두됨에 따라, 스마트폰 침해사고 예방 및 대응을 위한 대책 및 관련기관 간 협력체계 구축 필요성이 제기되고 있다. 이에 따라 방통위는 지난 1월부터 '스마트폰 정보보호 민·관 합동대응반'을 구성·운영해 오면서, 이용자 스스로가 보안위협을 사전 예방하고 유사시 피해를 최소화할 수 있도록 「이용자 10대 안전수칙」을 만들어 발표한 바 있다.

그러나 스마트폰 보안위협은 정부나 이용자 등 어느 한 주체의 노력만으로는 효과적인 대응에 한계가 있음을 공감하고, 그 후속조치로 이동통신사, 스마트폰 제조사, 백신사, 보안솔루션사 등 사업자와 정부 등 각 주체별 선제적이고 체계적인 공동 대응이 가능하도록 민·관 합동대응반과 시큐리티 포럼 연석회의를 통해 스마트폰 정보보호 주체별로 필요한 상세 역할을 정립하였다.

「스마트폰 정보보호 주체별 역할」의 주요 내용은 아래와 같다.

(이동통신사의 역할) ▲ 모바일 악성코드 대응방안 수립 및 이행 ▲ 스마트폰 정보보호 침해사고 접수 및 처리절차 수립 ▲ 악성코드 조기경보 서비스 제공 ▲ 중요 S/W 패치 및 업데이트 서비스 지원 ▲ 스마트폰 원격 제어 서비스 제공 ▲ 단말기 보안설정 정보 제공

(스마트폰 제조사의 역할) ▲ 단말기 잠금 기능 강화 ▲ 데이터 암호화 기능 탑재 ▲ 데이터 및 시스템 백업 · 복구 기능 탑재 ▲ 데이터 및 시스템 접근제어 기능 제공 ▲ 단말기 안전성 검사 강화 ▲ 단말기 보안설정 매뉴얼 제공 ▲ 악성코드 샘플 확보 협력 등

(모바일 백신사 및 보안솔루션사의 역할) ▲ 신속한 악성코드 샘플 확보 체계 마련 ▲ 모바일 환경을 고려한 백신 개발 ▲ 신속한 백신 업데이트 제공 ▲ 악성코드 정보의 제공 ▲ 다양한 보안 솔루션 연구 · 개발 추진 등

(방통위/ KISA의 역할) ▲ 민·관 협의체 구성 및 지원 ▲ 이용자 보안 인식 제고 ▲ 모바일 위협정보 수집 및 분석기술 개발 ▲ 발생 가능한 침해사고에 대한 예측 및 대응방안 연구 ▲ 모바일 시큐리티 전문인력 양성 및 교육 강화 ▲ 모바일 서비스용 웹사이트 침해예방 및 대응 체계 구축 등 스마트폰 정보보호 침해사고 예방 및 대응활동 강화

향후 상기 스마트폰 정보보호 주체들은 각각의 역할을 충실히 수행하고 공동 협력을 긴밀히 펼쳐 나가기로 하였다. 이를 위해 보다 상세한 역할 및 대응 안내서를 제작하여 각 주체들에게 배포하여 활용토록 할 예정이다. 아울러 정부차원에서도 모바일 악성코드 유포 의심사이트에 대한 모니터링을 강화하는 한편, 민·관 합동대응반 및 모바일 시큐리티 포럼 등 기 구축된 민·관 협력 체계를 통해 안전한 스마트폰 이용환경을 조성하는데 주력해 나갈 계획이다.

붙 임 : '스마트폰 정보보호 주체별 역할 주요 내용' 1부.

※ '스마트폰 이용자 10대 안전수칙' 포함

〔붙임〕

스마트폰 정보보호 주체별 역할 개요

□ 이동통신서비스 사업자

① 모바일 악성코드 대응방안 수립 및 이행

- 모바일 악성코드의 감염으로 인한 사용자 피해를 최소화하고 서비스에 영향을 미치지 않도록 침해대응체계 수립 및 이행 필요

② 사고접수 및 처리절차 수립

- 스마트폰 분실 및 도난 사고, 악성코드에 의한 침해사고 접수 · 처리를 위한 고객 대응 매뉴얼 마련 및 효과적 대응을 위한 유관기관으로의 정보 전파 · 공유

③ 악성코드 조기경보 서비스 제공

- 신규 모바일 악성코드의 출현 및 악성코드에 의한 피해 접수 시, 정보보호알림이 서비스(KISA 및 이통사 공동 제공)에 가입한 고객을 대상으로 악성코드 증상, 대처방안 등의 관련 내용 통보

④ 악성코드 감염 사용자 대상 서비스 이용 제한 기준 마련

- 스마트폰 악성코드 감염 사용자 대상 서비스 이용 제한 기준(본인 동의 절차 포함) 및 대응 프로세스를 마련하고 해당 사항을 이용 약관에 반영

⑤ 중요 S/W 패치 및 업데이트 서비스 지원

- 국가적·사회적 이슈가 되어 선제적 대응이 필요하다고 판단되는 스마트폰 악성코드에 대해서는 정부와 협의하여 이통사 포털 또는 앱스토어를 통한 전용백신 무료 배포

⑥ 안티스팸 서비스 제공

- 공개되거나 자체 분석한 스팸 발송번호에 대해 서버차원의 근원적 차단을 지원하고, 스팸메시지를 통해 전달되는 모바일 악성코드의 특성을 고려, 메시지 패턴분석을 통한 스팸 발송현황 탐지 서비스 지원을 고려하는 한편, 신고·접수된 스팸발송 번호 등을 등록하여 관리하는 방안 마련

⑦ 스마트폰 원격 제어 서비스 제공

- 단말기 제조사와의 협력을 통해 분실 및 도난당한 스마트폰에 대해 중요한 정보를 원격으로 삭제하거나 사용을 불가능하게 할 수 있는 서비스제공 방안 검토

⑧ 단말기 보안설정 정보 제공

- 스마트폰 개통 시 가입축하 및 공지 메시지에 '스마트폰의 안전한 이용에 관한 내용 또는 관련 홈페이지 주소(URL)' 제공 방안 검토(관련 홈페이지는 방통위·KISA가 제공)

⑨ 네트워크 및 서버 관리

- 외부 공격으로부터 이통사 네트워크와 서버를 보호하기 위한 보안시스템 구축 및 발생 가능한 공격 정보의 사전 파악을 통한 원활한 운용성 확보

⑩ 모바일 악성코드 테스트 망 지원

- 국내 모바일 정보보호 분야 발전 및 관련업체의 효과적인 보안 솔루션 개발 지원을 위해 테스트용 연구실 및 실험 장비 지원 고려

⑪ WAP Push 서비스 관리

- 스마트폰 단말기 사용자를 보호하기 위하여 가급적 특수한(관리적) 용도로만 WAP Push 서비스(Service Loading)를 제공하거나 Service Indication(Callback URL) 형태로 대체하는 방안 고려

⑫ 공조체제 유지

- 동종업체, 백신사, 단말기 제조사 및 정부기관과 긴밀한 협력 관계를 유지하여 모바일 악성코드와 관련한 정보 공유 및 침해사고 발생 시의 효과적 대응책 마련 필요

□ 스마트폰 단말기 제조사

① 단말기 잠금 기능 강화

- 이용자의 피해를 최소한으로 줄이기 위해 스마트폰 단말기 잠금 기능을 강화(ex, 4자리이상 패스워드 자리 수 설정, 특수문자 및 영문자 사용 등)하는 방안 고려

② 블루투스 연결 가능 목록 관리 기능 제공

- 많은 이용자들이 블루투스 기능을 미사용할 시에도 활성화 상태를 유지하는 경우가 많기 때문에 블루투스 기능 활성화 상태에서 사용자가 사전에 연결 가능 목록에 등록한 단말기만 연결이 가능하도록 하는 기능 제공

③ 데이터 암호화 제공

- 이용자 정보보호 차원에서 개인 프라이버시와 관계가 있는 중요 파일(전화번호, 이메일, SMS 등)에 대한 데이터 암호화 모듈의 탑재 고려

④ 데이터 및 시스템 백업·복구 기능 제공

- 스마트폰 분실 및 손상으로 인한 신규제품 구입 시 이용자의 애플리케이션 재설치, 데이터 복구 등에 소요되는 시간을 절약할 수 있도록 스마트폰에 저장된 시스템 및 사용자 데이터 손실시 이전 상태로 복원할 수 있는 백업 및 복구 기능 제공 고려

⑤ 데이터 및 시스템 접근 제어

- 스마트폰 내에 저장된 민감한 정보를 별도의 저장 영역에 보관하고, 패스워드 등 사용자 인증을 통해 접근을 허용하는 파일 접근 제어기능 구현 필요

⑥ 안티스팸 기능 제공

- 전화번호를 숨기거나 변조하며, 메시지 필터링을 우회하기 위해 특정 문자를 삽입하여 전송하는 우회적인 스팸에 대한 차단 및 제거 기능 검토

⑦ 안전성 검사 강화

- 스마트폰 침해사고로 인한 피해를 최소화할 수 있도록 단말기 출시 전, 다양한 응용 애플리케이션을 설치한 상태에서 다각적인 방법으로 단말기의 안전성을 검증하는 방안 마련

⑧ 단말기 보안설정 매뉴얼 제공

- 단말기 매뉴얼을 통해 기본 기능에 포함된 보안 기능에 대한 정보를 제공하고, 필요시 이용자가 손쉽게 단말기 보안설정 정보를 이용할 수 있도록 홈페이지를 통해 분실·도난, 악성코드 피해사례와 그에 대한 대처방법 등을 안내

⑨ 악성코드 샘플 확보 협력

- 악성코드로 인한 감염이 의심되는 스마트폰의 A/S 접수 시, 샘플 확보를 위해 백신사와 협력하고, 관련내용을 즉시 유관기관에 전파

⑩ 신속한 보안패치 및 업데이트 제공

- 스마트폰 OS 및 기본 프로그램의 취약점 발견 및 인지 시, 이에 대한 패치를 신속히 확보하고 S/W 업데이트 제공 방안 마련

⑪ 공조체제 유지

- 동종업체, 백신사, 이동통신사 및 정부기관과 긴밀한 협력 관계를 유지하여 모바일 악성코드와 관련한 정보 공유 및 침해사고 발생 시의 효과적 대응책 마련 필요

□ 모바일 백신 및 보안솔루션 사업자

① 신속한 악성코드 샘플 확보

- 이동통신사, 단말기 제조사 등과의 유기적 협력 관계 구축을 통한 신속한 악성코드 샘플 확보

② 모바일 환경을 고려한 백신 개발

- 다양한 스마트폰 운영체제를 감안하여야 하며, 저전력 · 저용량의 모바일 환경에 최적화 할 수 있도록 백신 연구 및 개발

③ 신속한 백신 업데이트

- 스마트폰 이용자 보호를 위해 신규 악성코드에 대한 신속한 백신 업데이트를 제공해야 하며, 업데이트는 PC 동기화, 무선망 및 이통망 등 다양한 인터페이스를 통해 가능하도록 지원(비상시 이용자가 이통망을 사용할 수 밖에 없는 상황을 고려하여 이통사와의 협력을 통해 이용자 보호방안 마련)

④ 악성코드 정보 제공

- 백신 프로그램은 악성코드 탐지 및 치료뿐만 아니라 악성행위(정보유출, MMS 무단 전송 등)에 대한 상세 정보 제공을 통해 사용자 스스로 피해여부를 확인하고 추가피해를 예방할 수 있도록 지원

⑤ 다양한 보안 솔루션의 연구·개발

- 일반 사용자를 위한 안티스팸, 안티바이러스, 방화벽 등의 솔루션은 물론, 비즈니스 업무 수행자를 위한 VPN, 인증, DRM 등의 보안 솔루션에 대한 지속적 연구 개발을 통해 스마트폰 서비스의 확산 · 발전에 노력

⑥ 공조체제 유지

- 동종업체, 이동통신사, 단말기 제조사 및 정부기관과 긴밀한 협력 관계를 유지하여 모바일 악성코드와 관련한 정보 공유 및 침해사고 발생 시의 효과적 대응책 마련 필요

□ 방송통신위원회 및 KISA

① 민·관 협의체 구성 및 지원

- 모바일 악성코드에 대한 정보 공유 및 침해사고 대응을 위한 민·관 협의체 구성·지원 및 정기적인 협력 회의를 통한 모바일 악성코드 관련 정보 공유 및 협력체계 구축

② 사용자 보안인식 제고

- 스마트폰 이용자가 모바일 악성코드를 인지하고 대응할 수 있도록 인터넷을 포함한 각종 매체와 오프라인의 세미나를 통해 다양한 정보 및 자료를 제공하여 사용자 보안인식 제고

③ 모바일 위협정보 수집 및 악성코드 분석 · 채집기술 개발

- 국내 · 외 주요 해킹 · 보안 관련 기관들과 정보 공유를 통해 모바일 위협정보를 조기 감지하여 전파 및 데이터베이스화하고 이용자가 스마트폰 악성코드 감염여부를 인지할 수 있는 기술적 판단방법 마련 및 악성코드 분석 · 채집기술 개발 필요

④ 모바일 콘텐츠 안전성 확보 방안 검토

- 모바일 콘텐츠 시장의 활성화를 유지하면서 사용자 보호할 수 있는 모바일 콘텐츠 안전성 검증체계 구축 필요

⑤ 발생 가능한 모바일 침해사고에 대한 예측 및 대응방안 연구

- 악성코드 및 해커의 공격이 점차 지능화되고 있으므로 미래의 발생 가능한 다양한 공격에 대한 예측 및 대응 방안 마련 필요

⑥ 모바일 인터넷 고충 처리

- 무선인터넷 이용에서 개개인이 겪을 수 있는 개인정보침해 및 해킹으로 인한 고충 처리를 위한 창구를 마련하고 문제 상담, 민원 처리, 정책적 지원

⑦ 모바일 시큐리티 전문 인력 양성 및 교육 강화

- 모바일 보안 분야의 국내 기술력을 확보하기 위해 기존 인력의 심화 교육 및 재교육을 통한 전문 인력 양성과 대학 정보보호 동아리, 취약점 분석·악성코드 분석 등을 상시 훈련할 수 있도록 온라인 학습장 등을 조성하여 신규 보안 전문가 양성

⑧ 모바일 인터넷 환경에서의 보안강화 법제 개선

- 해킹, 이용자 개인정보 유출 등 모바일 인터넷 정보보호 이슈에 대응하기 위한 구체적인 조치 마련과 법·제도 체계 정비

⑨ 안전한 이용을 위한 모바일 단말·인프라·서비스 보안 기술 개발

- 스마트폰 등 모바일 단말 및 플랫폼 보호 기술 개발, 모바일 인터넷 침해사고 대응 기술 개발, 콘텐츠 보호기술 개발, 모바일 사용자 프라이버시 보호 기술 개발 등 지원

⑩ 모바일 서비스 이용 및 운용 가이드라인 마련·보급

- 스마트폰, 모바일 웹서비스 등 모바일 기기 및 인터넷 환경의 취약점을 분석하여 대상별 보안 수칙 및 대응 가이드라인을 개발하여 보급

⑪ 모바일 서비스용 웹사이트 침해예방 및 대응체계 구축

- 유선인터넷에서와 마찬가지로 모바일 웹 취약점에 대한 공격 및 침해 위협이 증가할 것으로 예상되므로 모바일 웹사이트 취약점 점검 및 사회공학적인 방법을 이용한 악성코드 유포 및 피싱 등의 공격 조기 탐지 및 차단

⑫ 모바일 보안위협 국제 대응 공조체제 마련

- 글로벌화되고 있는 사이버 위협에 대해 모바일 환경 차원에서도 긴밀한 국가간 대응 체계 마련이 필요하므로, 국가간 협력 채널을 마련하고 OECD, ITU 등 주요 국제기구를 통한 협력 강화 및 국제사회 정보보호 대응 선도

□ 스마트폰 이용자 (10대 안전수칙 기 발표, 10.2.8)

① 의심스러운 애플리케이션 다운로드하지 않기

- 스마트폰용 악성코드는 위·변조된 애플리케이션에 의해 유포 될 가능성이 있으므로 의심스러운 애플리케이션의 다운로드 자제

② 신뢰할 수 없는 사이트 방문하지 않기

- 의심스럽거나 알려지지 않은 사이트를 방문할 경우 정상 프로그램으로 가장한 악성프로그램이 사용자 몰래 설치될 수 있으므로. 신뢰할 수 없는 사이트 방문 자제

③ 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기

- 멀티미디어메세지(MMS)와 이메일의 첨부파일 기능은 악성코드 유포 수단으로 사용되는 경우가 많으므로 발신인이 불명확하거나 의심스러운 메시지 및 메일은 열어보지 말고 즉시 삭제 필요

④ 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기

- 단말기를 분실 혹은 도난당했을 경우 개인정보 유출 및 악성코드 설치 방지를 위하여 단말기 비밀번호 설정 필요

⑤ 블루투스 기능 등 무선 인터페이스는 사용시에만 켜놓기

- 악성코드 감염 가능성을 줄일 뿐만 아니라 단말기의 불필요한 배터리 소모를 막기 위해서는 블루투스 등 무선 인터페이스는 사용 시에만 활성화

⑥ 이상증상이 지속될 경우 악성코드 감염여부 확인하기

- 이상증상 발생 시 스마트폰 매뉴얼에 따라 조치하며 조치 후에도 이상증상이 지속될 경우 악성코드에 의한 감염 가능성이 있으므로 백신 프로그램을 통한 단말기 진단 및 치료 필요

⑦ 다운로드한 파일은 바이러스 유무를 검사한 후 사용하기

- 스마트폰용 악성프로그램은 특정 프로그램이나 파일에 숨겨져 유포될 수 있으므로, 프로그램 및 파일 다운로드 · 실행 시 스마트폰용 백신프로그램으로 바이러스 유무 검사 후 사용

⑧ PC에도 백신프로그램을 설치하고 정기적으로 바이러스 검사하기

- 스마트폰과 PC간 데이터 백업, 복사, 전송 등의 작업수행 과정에서 PC에 숨어있는 악성코드가 스마트폰으로 옮겨질 수 있으므로 PC에 대한 백신 프로그램 설치 및 정기점검 필요

⑨ 스마트폰 플랫폼의 구조를 임의로 변경하지 않기

- 스마트폰 플랫폼 구조를 변경(예: Jailbreak) 사용할 경우, 기본적인 보안기능 등에 영향을 주어 문제가 발생할 수 있으므로 이용자 스스로 구조 변경 자제

⑩ 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트 하기

- 해커들은 보안 취약점을 이용하고 다양한 공격기법을 사용하고 있으므로 이용자는 자신이 사용하는 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트하여 사용