SecurityPlus Standard

SecurityPlus201008-1 제정일: 2010 년 8 월 10 일

스마트폰 사용자를 위한 보안 가이드라인 v1.0

SECURITY PLUS

문서 히스토리

2010.7.7. Draft v1.0 공개

2010.7.20 v0.9 Public Beta 공개.

2010.8.10 v1.0 정식 버전 공개

시간과 공간의 제약 없이 다양한 서비스를 이용하고자 하는 사용자의 욕구는 최근 들어 스마트폰의 폭발적인 확산으로 이어져 새로운 IT 세상을 열어 가고 있다. 그러나, 폭발적인 확산과 함께 스마트폰을 목표로 하는 각종 악성 코드와 공격들, 그리고 스마트폰 분실 및 도난으로 인해 개인정보와 데이터의 유출 등 새로운 보안 위협도 마찬가지로 폭발적으로 증가하고 있다. 이러한 시대적 요청에 따라 국내 최대 정보보호 전문 커뮤니티인 SecurityPlus(http://www.securityplus.or.kr)에서는 사용자와 기업을 위한 스마트폰 보안 가이드라인을 기획하고, 그 첫 번째 산출물인 "사용자를 위한 보안 가이드라인"을 발표하였다. 물론, 사용자 입장에서는 보안에 대한 요구가 기업 보다는 약하거나 그런 요구사항이 없을 수도 있다. 그러나, 스마트폰에서의 다양한 금융 서비스의 이용과 개인정보의 저장으로 인해 사용자에 따라서는 오히려 기업보다도 강도가 더 높은 보안에 대한 요구가 있을 수도 있다. 그러한 보안에 대한 요구가 높은 사용자에게 본 가이드라인은 스마트폰의 보안 강도를 자기 스스로 높일 수 있는 지침을 제공한다. 물론, 스마트폰 기기의 종류에 따라 본 가이드라인에 수록된 모든 내용을 적용할 수는 없을 것이다. 그러나, 본 가이드라인에 따라 자신이 보유한 스마트폰에서 할 수 있는 범위까지 적용해 본다면, 보다 보안성 높은 스마트폰의 운영이 가능할 것이다. 아울러, 스마트폰 제조회사에서는 본 가이드라인을 토대로 스마트폰 기기 자체의 보안성을 높이는 데 좋은 참고 자료로 활용하였으면 한다.

본 가이드라인의 기본 열 가지 지침은 아래와 같다.

- USIM PIN 번호 및 장치 비밀번호 등 이용 가능한 비밀번호를 사용하고 관리에 유의하라.
- 중요 데이터는 스마트폰에 저장하지 말고, 불가피한 경우라도 반드시 암호화하라.
- 사용하지 않는 네트워크 서비스(Wi-Fi, 블루투스 등)는 끄고, 필요 시에만 활성화하라.
- 스마트폰의 플랫폼 구조를 임의 변경 말고, 항상 최신 버전을 유지하라.
- 최신 패턴을 유지한 안티 바이러스 소프트웨어를 반드시 사용하라.
- 신뢰할 수 있는 어플리케이션만 다운로드하고 최신 버전을 유지하라.
- 보안이 강화된 웹 브라우저 설정을 유지하고 신뢰할 수 있는 웹 사이트만 방문하라.
- 보안이 강화된 전자메일을 사용하고 메시지는 암호화하라.
- 자신으로부터 스마트폰을 꺼내 놓아야 할 경우에는 반드시 패스워드나 화면 잠금 해제 패턴으로 화면 해제를 할 수 있는 화면 잠금을 사용하라.
- 가능하다면, 원격에서 자신의 스마트폰을 관리할 수 있는 서비스에 가입 및 이용하라.

상기 열 가지 기본 지침에 대한 상세 가이드라인은 아래와 같다.

1. 비밀번호

- USIM PIN 및 장치 비밀번호를 반드시 사용하고, 주기적으로 변경하라.
- 가능하면 USIM PIN 번호와 장치 비밀번호를 다르게 하라.
- USIM PIN 번호와 장치 비밀번호 설정 시, 아래 사항에 주의한다.
  ① 0000 기본 패스워드는 반드시 변경한다.
  ② 전화번호와 연관된 비밀번호를 사용하지 않는다.
  ③ 생일, 자동차 번호 등 개인 정보와 연관된 비밀번호를 사용하지 않는다.
  ④ 1111, 2222와 같이 연속된 번호나, 1234 등 취약한 비밀번호를 사용하지 않는다.
- 자격 증명 저장소의 패스워드는 8자리 이상으로 설정하고, 사용 시 이외에는 응용 프로그램이 보안 인증서 및 다른 자격 증명서에 접근할 수 없도록 해제하라.
- 허용되는 암호 입력 시도 횟수(10회 설정 권장)를 초과할 경우 모든 스마트폰 내 데이터가 삭제되도록 한다.

2. 데이터

- 가능하다면 기밀성이 요구되는 데이터는 스마트폰 내에 저장하지 않고 인터넷으로 이용 가능한 원격 저장소에 보관한다. 만일 불가피하게 스마트폰 내에 저장해야 한다면, 미디어 카드 및 스마트폰에 저장된 데이터는 반드시 일정 수준 이상의 암호화를 적용하여야 한다.
- 전자 금융과 관련된 정보는 이미지(그림 파일) 형태이든, 어플리케이션에 제공하는 저장 기능을 통해서든 스마트폰 내에 저장되지 않도록 하고, 사용 후 캐쉬되거나 저장된 정보(임시 파일 등)는 반드시 삭제한다.
- 저장 매체인 메모리 카드를 공유해서 사용하지 않는다.
- 데이터 동기화를 위한 PC나 노트북에 대한 보안 관리에 유의한다.

3. 네트워크 서비스

- Wi-Fi, 블루투스, 적외선 장치 기능 등 무선 인터페이스는 사용 시에만 켜 놓는다.
- 가능하다면, SSL 혹은 VPN 원격 접속을 통해서 인증 정보 및 자료 전달 또는 자료 동기화를 수행한다.
- 신뢰할 수 없는 개방형 Wi-Fi 네트워크의 사용을 자제하고, 불가피하게 사용할 시에는 개인 정보 등 중요 정보를 전송하지 않는다.
- 블루투스 탐색이 불가능하도록 설정(짝 장치와만 연결)한다.
- 블루투스를 통한 데이터 전달 시 암호화 채널을 사용한다.
- 국제전화, 070, 060 통화에 대한 제한 혹은 금지 설정을 사용한다.

4. 운영체제

- 제일브레이크(Jail Break) 혹은 루팅(Rooting)과 같이 스마트폰의 플랫폼 구조를 임의로 변경하지 않는다.
- 스마트폰의 운영 체제를 항상 최신 버전으로 업데이트 및 유지한다.
- 장시간 사용하지 않거나, 스마트폰을 잠갔을 때, 중요 데이터에 대해 메모리 상의 임시 데이터를 삭제한다.

5. 어플리케이션
- 안티 바이러스 소프트웨어를 반드시 설치하고 사용한다.
- 어플리케이션 및 안티 바이러스 소프트웨어를 항상 최신 버전으로 업데이트 및 유지한다.
- 이상 증상이 지속될 경우 백신 프로그램을 통해 악성코드 감염 여부를 확인한다.
- 의심스러운 애플리케이션은 다운로드하지 않고, 다운로드한 파일은 악성코드 감염 여부를 확인한 후 사용한다.

6. 인터넷
- 보안이 강화되도록 웹 브라우저를 설정한다.
  * 아래 사항은 반드시 설정해야 할 권고사항이다.
  ① SSL 또는 TLS를 이용하고 암호화 강도는 가능하다면 128비트 암호화로 설정한다.
  ② 이용한 웹 사이트에 대한 입력 패스워드의 자동 저장 기능을 사용하지 않는다.
  ③ 팝업을 차단한다.
  ④ 잠재적으로 위조된 웹 사이트 방문 시 경고를 받도록 한다.
  ⑤ 비보안 페이지로 변경할 때 경고 표시 한다.
  * 아래 사항 설정 시 웹 페이지가 올바로 표시되지 않을 수 있습니다.
  ⑥ 쿠키를 허용하지 않는다.
  ⑦ 이용할 웹 서비스에 자바스크립트를 사용하지 않는다면 비활성화한다.
  ⑧ 이용할 웹 서비스에 멀티미디어 자료의 이용을 원하지 않는다면, 플러그인(Flash 등)을 비활성화한다.
- 신뢰할 수 없는 사이트나 링크는 방문하지 않으며, 신뢰할 수 없는 RSS는 등록하지 않는다.

7. 전자메일
- 보안이 강화되도록 전자메일을 설정하고 사용한다.
  ① 전자메일 계정 설정 시, 보안 연결을 제공하는 전자메일인 경우, 보안 연결을 사용하고, SSL 인증서를 수락하도록 설정한다.
  ② 개인 인증서를 활용하고, PGP 혹은 S/MIME으로 메시지에 대한 서명 및 암호화

를 통해 사용한다.

③ 수신자와 공유된 암호 구문을 이용해 메시지를 암호화하여 전달한다.

- 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제한다.

8. 화면 잠금

- 충전이나 자료 동기화 등 자신으로부터 떨어지는 경우, 반드시 화면 잠금을 수행하며, 화면 해제 시 반드시 패스워드 혹은 화면 잠금 해제 패턴을 입력하도록 설정한다.

9. 원격 관리

- 가능하다면, 원격에서 스마트폰 기기를 관리할 수 있는 서비스(위치 탐색, 원격 메시지 전송, 원격 데이터 삭제 등)를 이용한다.

상기와 같은 SecurityPlus의 “사용자를 위한 스마트폰 보안 가이드라인”에 따라 보다 안전하게 스마트폰을 사용하시기 바랍니다. 끝.