스마트폰 정보보호 '이용자 10대 안전수칙'

① 의심스러운 애플리케이션 다운로드하지 않기

② 신뢰할 수 없는 사이트 방문하지 않기

③ 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기

④ 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기

⑤ 블루투스 기능 등 무선 인터페이스는 사용시에만 켜놓기

⑥ 이상증상이 지속될 경우 악성코드 감염여부 확인하기

⑦ 다운로드한 파일은 바이러스 유무를 검사한 후 사용하기

⑧ PC에도 백신프로그램을 설치하고 정기적으로 바이러스 검사하기

⑨ 스마트폰 플랫폼의 구조를 임의로 변경하지 않기

⑩ 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트 하기

붙 임 스마트폰 보안 관련 '이용자 10대 안전수칙' 설명자료 1부.

'이용자 10대 안전수칙' 설명자료

□ 배경

스마트폰 이용이 확대됨에 따라 스마트폰에서도 PC에서처럼 악성코드에 감염될 수 있습니다.

스마트폰이 악성코드에 감염될 경우 개인정보 유출, 데이터 변조, 금전적 피해, 기기 오작동, 사생활 침해 등의 피해를 입을 수 있으며, 단말기가 좀비 스마트폰이 되어 자신도 모르게 해커에 의해 조종되거나 DDoS 등의 공격 도구로 악용될 수 있습니다. 따라서, 방통위, KISA, ETRI, 이통사, 제조사, 백신 업체 전문가로 구성된 '스마트폰 정보보호 민·관 합동대응반'은 악성코드로 인한 피해를 사전에 예방하기 위해 스마트폰 이용자 스스로 평소에 실천할 수 있는 안전 수칙을 제시합니다.

□ 스마트폰 이용자 안전 수칙

o 의심스러운 애플리케이션 다운로드하지 않기

스마트폰용 악성코드는 위·변조된 애플리케이션에 의해 유포 될 가능성이 있습니다. 따라서 의심스러운 애플리케이션의 다운로드를 자제하시기 바랍니다.

o 신뢰할 수 없는 사이트 방문하지 않기

의심스럽거나 알려지지 않은 사이트를 방문할 경우 정상 프로그램으로 가장한 악성 프로그램이 사용자 몰래 설치될 수 있습니다. 인터넷을 통해 단말기가 악성코드에 감염되는 것을 예방하기 위해서 신뢰할 수 없는 사이트에는 방문하지 않도록 합니다.

o 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기

멀티미디어메세지(MMS)와 이메일은 첨부파일 기능을 제공하기 때문에 스마트폰 악성코드를 유포하기 위한 좋은 수단으로 사용되고 있습니다. 해커들은 게임이나 공짜 경품지급, 혹은 유명인의 사생활에 대한 이야기 등 자극적이거나 흥미로운 내용을 전달하여 사용자를 현혹하는 방법으로 악성코드를 유포하고 있습니다. 발신인이 불명확하거나 의심스러운 메시지 및 메일은 열어보지 마시고 즉시 삭제하시기 바랍니다.

o 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기

단말기를 분실 혹은 도난당했을 경우 개인정보가 유출되는 것을 방지하기 위하여 단말기 비밀번호를 설정하여야 합니다. 또한 단말기를 되찾은 경우라도 악의를 가진 누군가에 의해 악성코드가 설치될 수 있기 때문에 비밀번호 설정은 중요합니다. 제품출시 시 기본으로 제공되는 비밀번호(예 : "0000")를 반드시 변경하여 사용하시기 바라며, 비밀번호를 설정할 때에는 유추하기 쉬운 비밀번호(예 : "1111", "1234" 등)는 사용하지 않도록 합니다.

o 블루투스 등 무선인터페이스는 사용 시에만 켜놓기

지금까지 국외에서 발생한 스마트폰 악성코드의 상당수가 무선인터페이스의 일종인 블루투스(Bluetooth) 기능을 통해 유포된 것으로 조사되고 있습니다. 따라서 블루투스나 무선랜을 사용하지 않을 경우에는 해당 기능을 비활성화(꺼놓음) 하는 것이 필요합니다. 이로써 악성코드 감염 가능성을 줄일 뿐만 아니라 단말기의 불필요한 배터리 소모를 막을 수 있습니다.

o 이상증상이 지속될 경우 악성코드 감염여부 확인하기

웹 사이트 접속 또는 애플리케이션 실행 후 스마트폰이 오작동하거나, 바탕화면 변조 및 저장된 개인정보가 삭제되는 등 이상증상이 발생하면 스마트폰 매뉴얼에 따라 조치하여야 합니다. 그럼에도 이상증상이 지속될 경우 스마트폰 악성코드에 의한 감염일 가능성이 있으므로 백신 프로그램을 통해 단말기를 진단하고 치료하여야 합니다. 또한 악성코드 감염이 확인된 경우 한국인터넷진흥원(KISA), 이통사, 제조사, 백신업체 등에 신고하여 악성코드의 확산이 방지될 수 있도록 시민의식을 발휘해 주시는 것이 필요합니다.

o 다운로드한 파일은 바이러스 유무를 검사한 후 사용하기

스마트폰용 악성프로그램은 인터넷을 통해 특정 프로그램이나 파일에 숨겨져 유포될 수 있으므로, 프로그램이나 파일을 다운로드하여 실행하고자 할 경우 가급적 스마트폰용 백신프로그램으로 바이러스 유무를 검사한 후 사용하는 것이 좋습니다.

o PC에도 백신 프로그램을 설치하고 정기적으로 바이러스 검사하기

동기화 프로그램을 통해 스마트폰과 PC간 데이터 백업 및 복사, 음악파일 전송, 운영체제 패치 등의 작업을 수행할 수 있습니다. 이러한 과정에서 PC에 숨어있는 악성코드가 스마트폰으로 옮겨질 수 있으므로 스마트폰은 물론 PC에서의 백신 프로그램 설치 및 정기점검이 꼭 필요합니다.

o 스마트폰 플랫폼의 구조를 임의로 변경하지 않기

스마트폰 플랫폼 구조를 변경(예: Jailbreak)하여 사용할 경우, 기본적인 보안기능 등에 영향을 주어 문제가 발생할 수 있으므로 이용자 스스로 스마트폰 플랫폼의 구조를 변경하지 않도록 합니다.

o 운영체제 및 백신 프로그램을 항상 최신 버전으로 업데이트 하기

해커들은 스마트폰 플랫폼의 보안 취약점을 이용해 악성코드를 유포하고 백신프로그램의 탐지를 회피하기 위한 다양한 공격기법을 사용하고 있습니다. 따라서 자신이 사용하는 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트하여 사용하여야 합니다.

※ 스마트폰 보안 관련 궁금한 사항은 한국인터넷진흥원(KISA, ☏118)으로 문의하시면 친절하게 안내해 드립니다.

- 이용중인 통신사나 제조업체, 백신업체에 문의해도 자세한 안내를 받으실 수 있습니다.