<정보 보호를 위한 행동 수칙>

① 중요한 자료는 주기적으로 백업하라

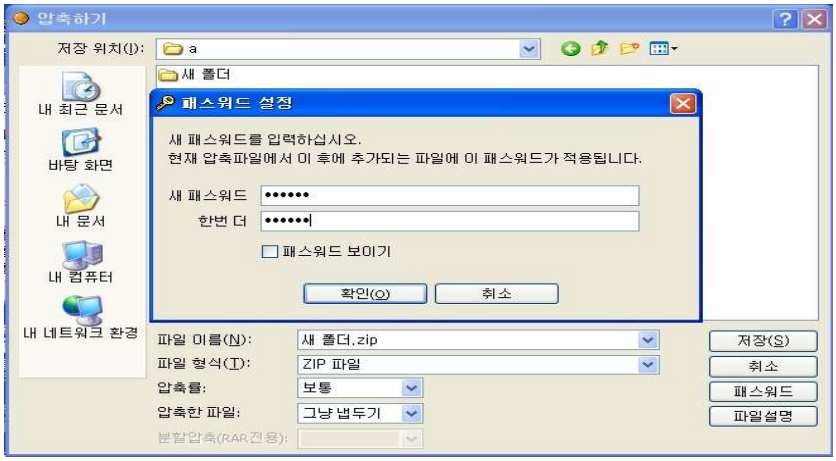
하드웨어 자체가 안전성을 100% 보장하기는 어렵습니다. 파일을 저장하는 장소가 일반적으로 하드디스크 드라이브인데, 하드 디스크는 PC를 켜면 계속 작동하는 장치입니다. 고장과 같은 하드웨어적인 문제도 있을뿐더러, PC를 공격한 해커가 데이터를 다 날려 버릴 수도 있을 것입니다. 따라서 중요한 자료는 다른 하드디스크나 이동 디스크 장치, USB 메모리, CD등에 별도로 저장하여 만일의 사태에 대비할 수 있어야 할 것입니다.

② 주요 정보가 담긴 파일은 암호화해서 보관하라

집에서 사용하는 PC이건 회사에서 사용하는 PC이건 자신에 관련한 또는 업무에 관련한 자료를 PC에 보관하게 되는 경우가 일반적입니다. PC에 침입한 해커는 뭔가 중요한 자료가 없나 시스템을 뒤지게 될 것이고 그런 경우를 대비하기 위해서 중요 데이터나 파일은 암호화 프로그램을 이용하여 저장하는 것이 좋습니다.

별도의 암호화 프로그램을 사용하는 것도 한 방법이지만 간단하게 이용할 수 있는 방법이 압축 프로그램의 암호 기능을 이용하는 것도 한 방법입니다. 압축을 풀 때 패스워드를 물어보게 되고 패스워드를 정확히 입력하지 않으면 압축이 풀리지 않는다는 점을 이용한 것입니다.

다음 그림은 압축 프로그램을 이용하여 압축할 때 패스워드를 지정하는 화면입니다.



<그림a1>

③ 반드시 정품 소프트웨어를 사용하라

정품 소프트웨어에는 대부분 복사 방지 장치나 라이선스에 관련한 기능을 적용하고 있습니다. 불법으로 사용할 수 있도록 프로그램을 깨는 것을 말 그대로 크랙(crack)한다고 합니다. 크랙을 할 수 있는 사람은 프로그래밍에 대한 지식을 가지고 있을 것이고 만일 마음 먹고 악의적인 코드를 집어 넣어 유포한다면 어떤 일이 벌어 질지 자명한 일입니다.

즉 불법 프로그램은 트로이 목마일 확률이 높다고 말 할 수 있는 것입니다. 반드시 정품 소프트웨어를 사용하여야 할 것입니다.

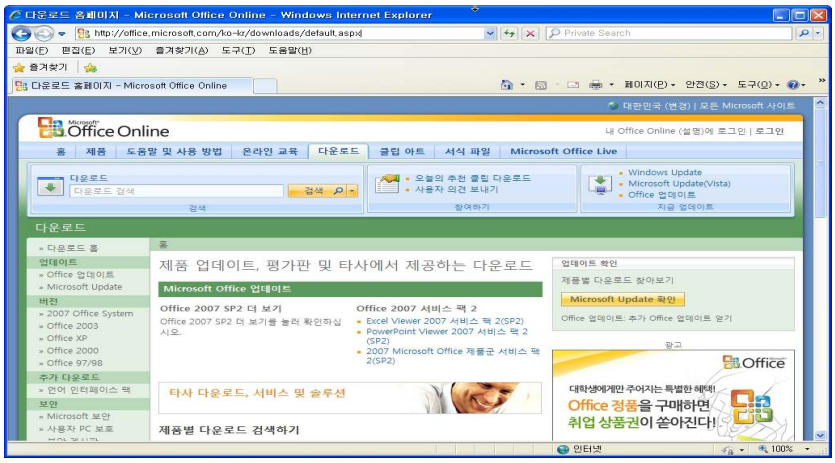
④ 사용하고 있는 소프트웨어에 대한 패치나 보안 관련 업데이트가 나오는 즉시 적용하라

자신의 PC에 설치하여 사용하고 있는 소프트웨어에 보안에 관련한 심각한 문제를 가지고 있다면 어떤 일이 벌어질까요? 버그가 없는 프로그램이 없다라는 말이 있습니다. 문제가 발견되면 그 문제를 고치기 위해서 패치가 나오게 됩니다.

특히 보안 관련한 패치라면 꼭 설치하셔야 하며, 오피스 프로그램의 경우 더욱 더 신경을 써야 할 것입니다. 예로 보고서를 워드 문서로 만들고, 시연을 하기 위해 파워 포인트를, 계산과 통계 등의 작업을 엑셀과 같은 프로그램을 사용할 것입니다. 업무에 관련한 주용 정보를 다루는 프로그램이니 당연히 해당 프로그램의 보안 문제가 발생하였는가 주의를 기울여야겠지요.

다음 그림은 MS 오피스 프로그램의 업데이트와 관련한 정보를 제공하는 사이트의 화면입니다.

http://office.microsoft.com/ko-kr/downloads/default.aspx



<그림a2>

⑤ 인터넷에서 프로그램이나 파일을 다운로드하는 경우 신뢰할 수 있는 사이트에서만 받고, 파일의 변경 여부를 반드시 확인하라

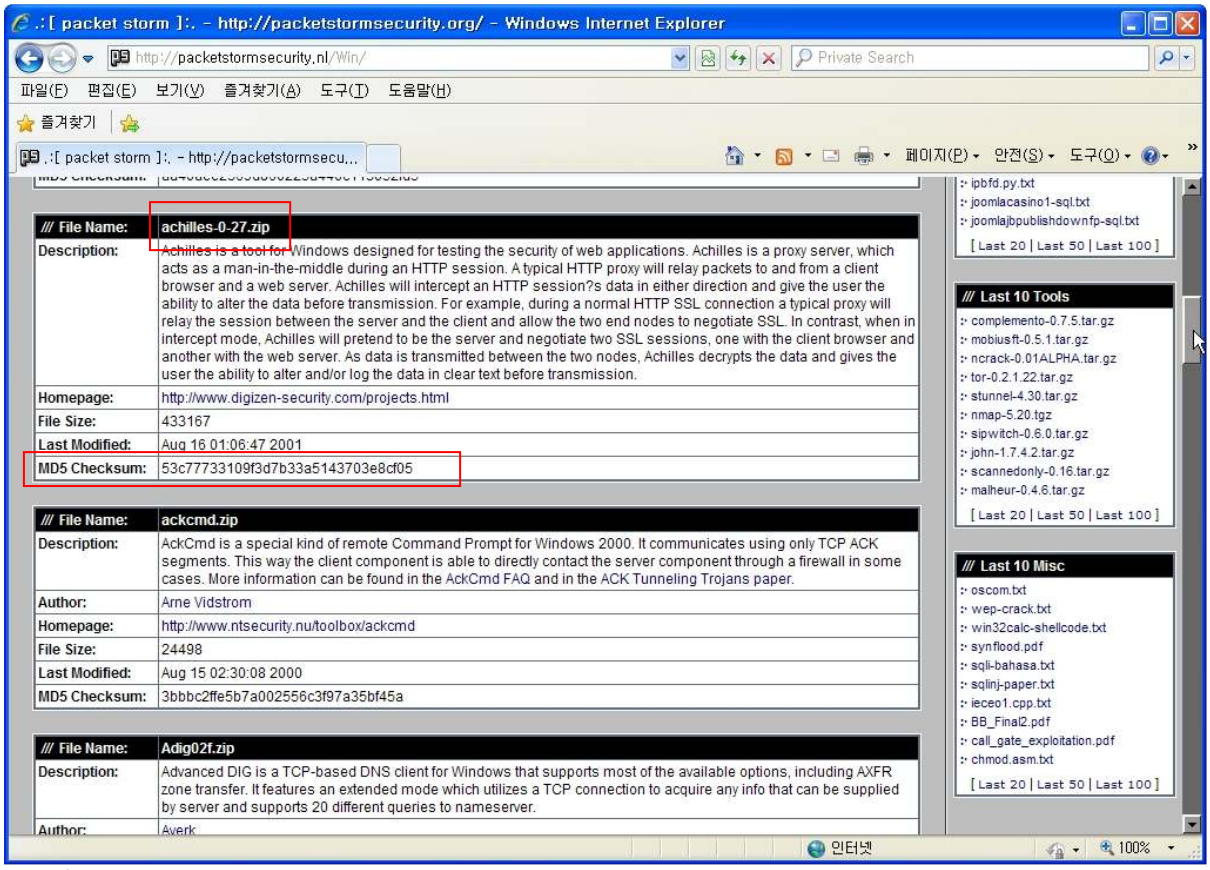
인터넷에서 파일을 제공하는 사이트가 먼저 신뢰할 수 있는지 확인하여야 합니다. 악의를 가지고 해킹하기 위하여 운영되고 있는 사이트가 없다고 장담할 수 없습니다. 또한 믿음이 가는 사이트라고 하더라도 해커가 해킹하여 슬쩍 자신이 만든 악성 프로그램을 올려 놓을 수도 있을 것입니다. 따라서 파일을 다운로드한 경우 파일의 변경 여부를 확인하여야 할 것입니다.

일반적으로 파일의 변경여부를 확인하는 방법으로 공개키를 이용한 방식과 해싱 알고리즘을 이용한 방법이 있습니다. 편리성 때문에 해싱 알고리즘을 이용한 무결성 점검을 많이 하는 편이라 할 수 있는데, 해싱 알고리즘이란 파일의 크기와 상관없이 일정한 크기의 고유값을 계산하는 알고리즘입니다. 파일의 내용이 단 한 글자가 바뀌어도 결과값은 달라지게 됨으로 파일의 변경되었나 안 되었나 쉽게 판단 할 수 있습니다. 많이 사용하는 것이 바로 MD5 해싱 알고리즘을 이용하는 방법입니다.

그림 환경의 프로그램으로 쉽게 사용할 수 있는 것이 "hash my files"라는 프로그램입니다.
다음의 사이트에서 다운로드하여 사용할 수 있습니다.

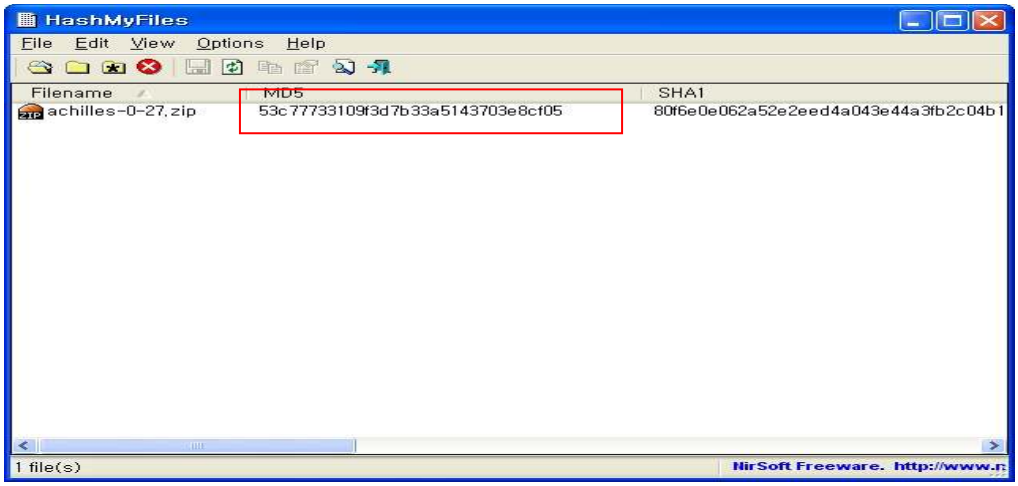
http://www.nirsoft.net/utils/hash_my_files.html

예로 다음의 사이트에서 다음의 파일을 다운로드 하였습니다.



<그림a3>

MD5 Checksum의 값을 확인하여야 합니다.
다운로드한 파일의 해싱값을 해싱 프로그램을 이용하여 추출한 후 확인합니다.



<그림a4>

만일 계산된 값이 다운로드한 페이지의 값과 틀린다면 사용하여서는 안됩니다.

⑥ 이슈가 되는 보안 사고나 보안 정보를 반드시 확인하라

인터넷의 특성상 한 곳에서 발생한 보안 사고는 거의 실시간에 가깝게 다른 곳에서 발생하게 됩니다. 따라서 이슈가 되는 보안 사고나 정보를 알고 있다면 보안을 높일 수 있을 것입니다. 예

로 2009년의 7.7 대란 때 사고를 일으키는 좀비 PC가 가정에서 사용하고 있는 것이 많았다고 합니다. 관련 정보를 입수하여 가정의 PC를 백신과 진단 툴을 이용하여 점검함으로써 해킹에 이용당하는 것을 막을 수 있었습니다.

⑦ 반드시 최신으로 업데이트된 백신 프로그램을 사용하라

업데이트되지 않은 백신은 아무런 가치가 없습니다. 오히려 사용자가 오래된 백신 프로그램을 설치하여 이용하면서도 자신은 안전하다고 생각하게 된다면 더 큰 문제입니다. 알려지지 않은 바이러스는 100% 예방하기 어렵습니다. 알려진 바이러스라고 하더라도 업데이트되지 않은 백신 프로그램은 해당 바이러스를 잡아내지 못할 것입니다.

⑧ 백신 프로그램의 실시간 감시 기능을 꼭 사용하고, 주기적으로 바이러스 감염 여부를 확인하라

실시간 감시를 백신 프로그램이 한다고 하더라도 잡아내지 않도록 예외 처리된 프로그램이 있을 수 있습니다. 주로 원격에서 접근하여 PC를 관리할 수 있도록 해주는 프로그램들이 예외로 처리되어 잡아내지 않는데, 해커가 당연히 악용할 수 있을 것입니다.
따라서 주기적으로 바이러스 백신 프로그램을 이용하여 바이러스 검사를 해주어야만 할 것입니다.
실시간 감시 기능이 모든 바이러스를 탐지하고 막아내는 것이 아니라는 생각을 꼭 가져야만 할 것입니다.

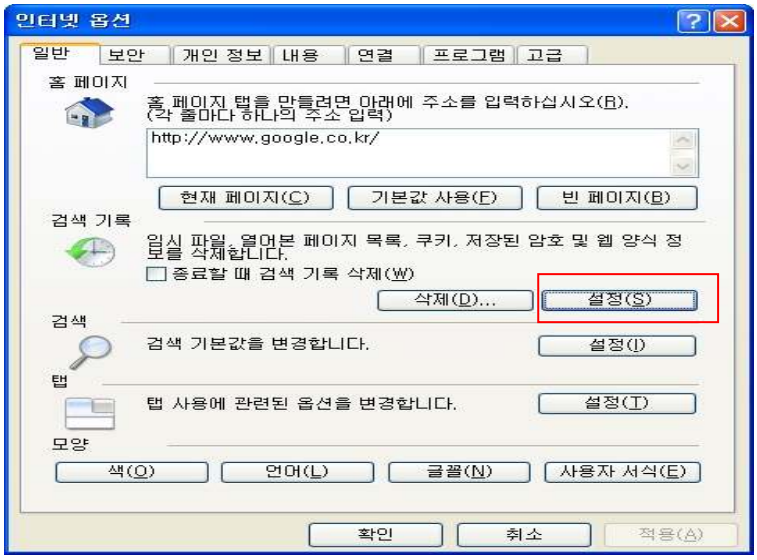
⑨ 이메일에 첨부된 파일이나, P2P 사이트 등에서 다운로드한 파일은 반드시 백신으로 검사한 후 사용하라

악성 바이러스와 같은 파일뿐만 아니라 다른 시스템을 공격하는 프로그램이 이메일에 첨부되어 유포되거나, P2P 통하여 유포가 많이 되고 있습니다. 따라서 부득이하게 파일을 사용하여야 하는 경우 반드시 최신으로 업데이트된 백신 프로그램을 이용하여 검사한 후 사용하여야 합니다.

⑩ 웹 사이트에 접속 시 Active X와 같은 추가 설치 프로그램의 설치 여부를 묻는 경우 무조건 설치하지 말고 확인하고 설치하라

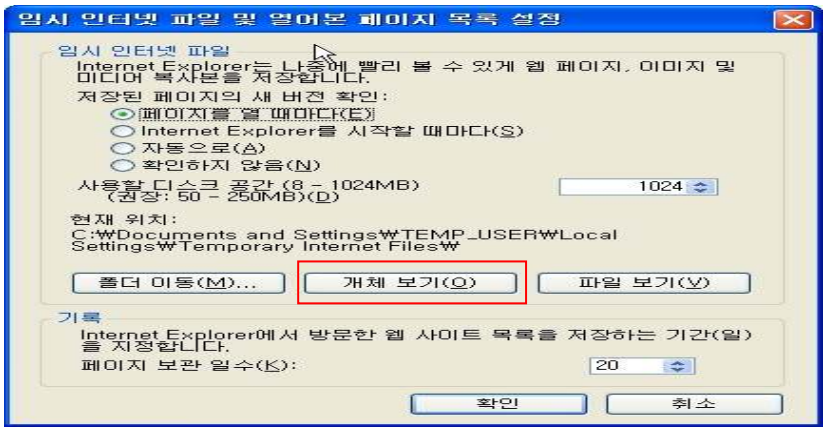
웹 서버에 방문한 사용자에게 추가 서비스나 기능을 제공하기 위하여 사이트에 접속할 때 프로그램을 설치하는 경우가 많습니다. 대부분 보안에 관련한 추가 기능을 제공하는 경우가 많은데 신뢰할 수 없는 사이트에서 설치 여부를 묻는 경우 절대로 설치하여서는 안됩니다.
또한 보안이 취약한 웹 서버를 해커가 해킹한 후 해당 사이트를 방문하는 사용자의 PC에 DOS용 공격 툴을 설치하도록 하여 대단위 서비스 거부 공격에 악용하는 경우도 종종 있습니다. 따라서 아무 생각 없이 프로그램을 설치 및 실행하여서는 안됩니다.

설치된 Active X와 같은 파일들은 사용하지 않는다면 제거해 주는 것이 좋습니다.
임시 파일을 확인하려면 인터넷 익스플로러의 "도구"탭을 클릭하여 "인터넷 옵션"을 선택합니다.



<그림a5>

검색 기록의 "설정"을 클릭하면 다음의 화면이 나옵니다.



<그림a6>

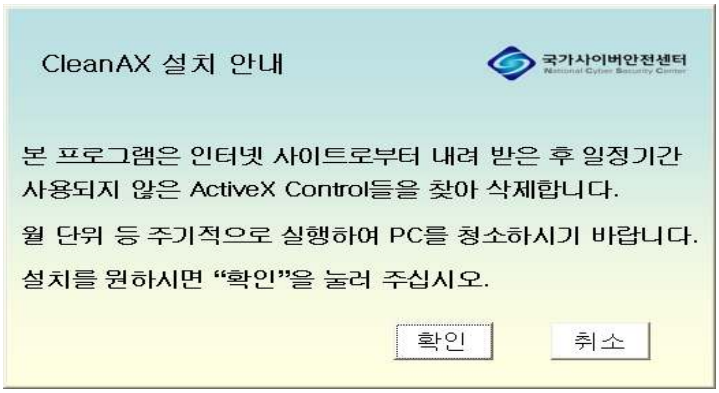
"개체 보기"를 클릭하면 다음과 같이 관련 파일을 확인할 수 있습니다.

<그림a7>

불필요한 Active X를 쉽게 삭제해주는 프로그램은 많은데, 국가 사이버 안전센터에서 개발하여 무료로 배포하고 있는 "CleanAX"라는 프로그램을 소개합니다.

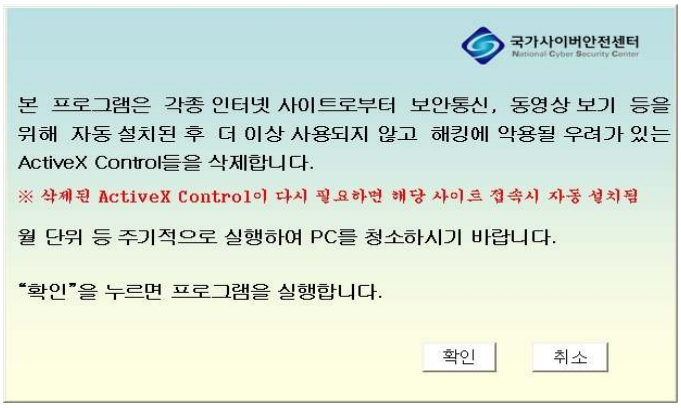
http://www.ncsc.go.kr

다음은 CleanAX 설치 프로그램을 더블 클릭하여 실행한 화면입니다.



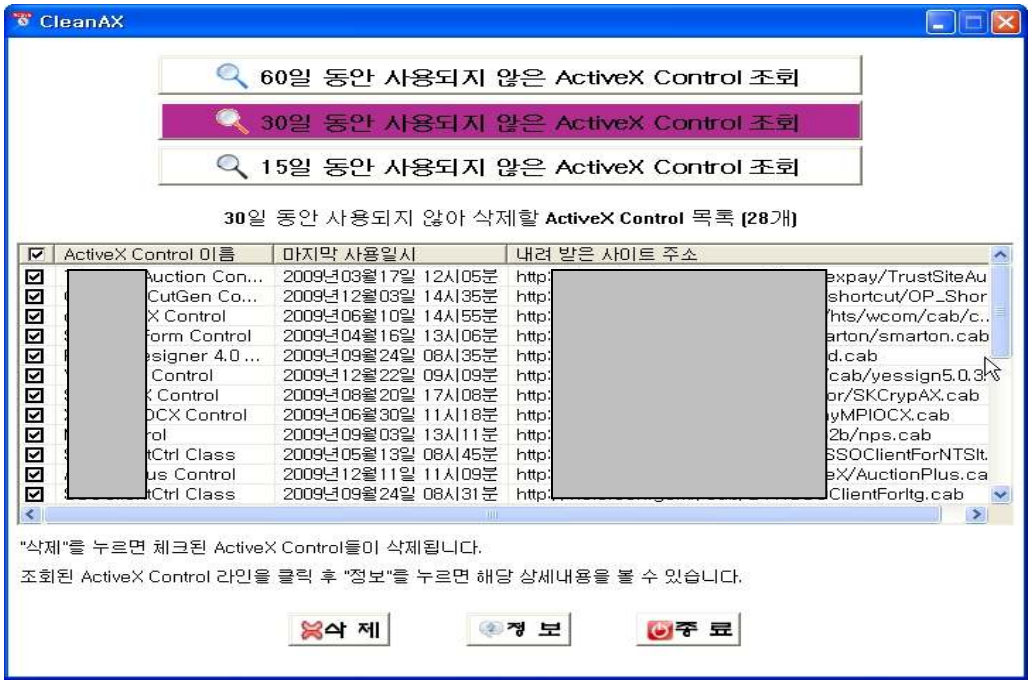
<그림a8>

확인을 클릭하면 다음의 화면이 나옵니다.



<그림a8>

확인을 클릭하면 프로그램이 설치가 끝나고, 다음 그림은 실행한 화면으로 사용하지 않는 Active X를 쉽게 제거할 수 있습니다.



<그림a8>

이상으로 내 PC는 내가 지키자는 특명을 완수하기 위한 지침을 확인하였습니다^^