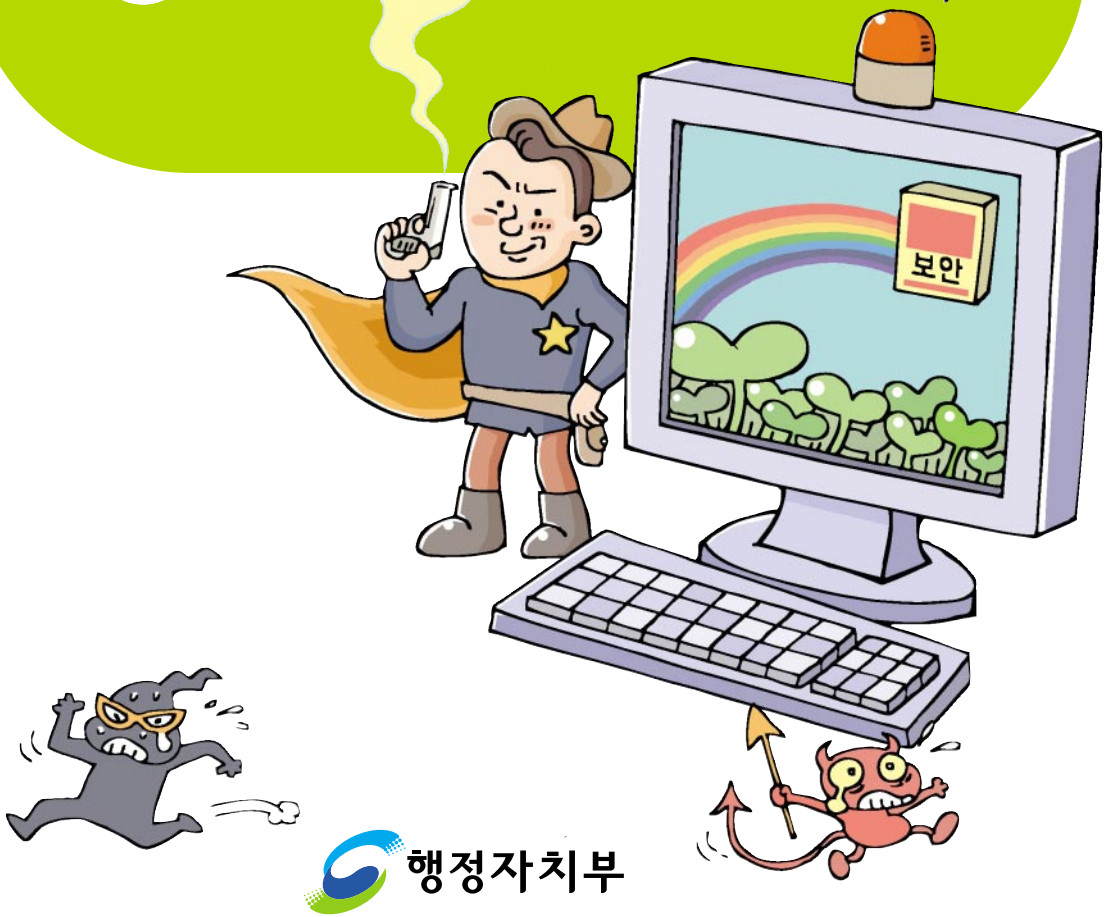
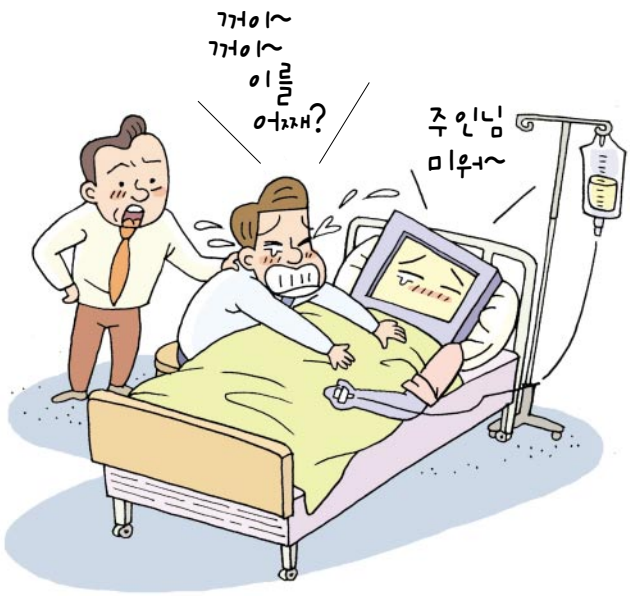
만화로 보는 정보보안 가이드

# 김주사의 정보보안 25시




행정자치부




"당신의 컴퓨터 오늘 하루도 건강한가요?"

꺼이~꺼이~ 이를 어째?

그러게. 처음부터 잘 관리했어야지. 왜 병을 키우나?

다 주인님 때문이에요.

# Contents

## 김주사의 정보보안 블로그

**처음** 컴퓨터를 접한 게 엊그제 같은데 벌써 여러 해가 되었다. 버튼 하나 잘못 누르면 컴퓨터가 잘못되기라도 할까봐 참 조심스러워했다. 그렇게 유리 컵처럼 깨질까 떨어뜨릴까 조심하며 컴퓨터와 함께 한지 어언 수년간.

**나는** 어느덧 컴퓨터 속의 세상, 사이버 세상을 항해하는 선장이 되었다.

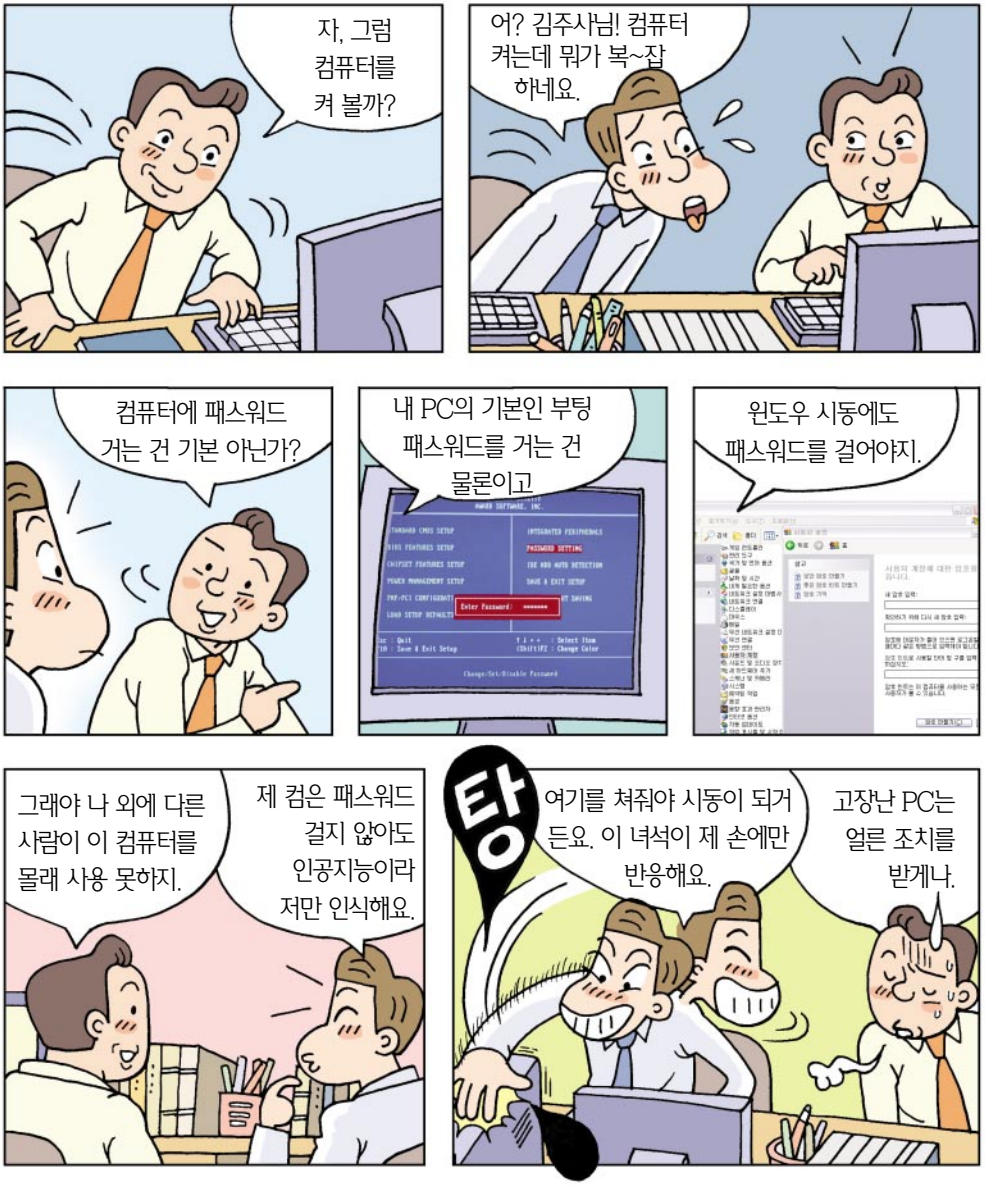
**현재** 나는 거의 하루를 컴퓨터와 함께 일하고 있다.

**내가** 사용하는 PC가 세상 모두와 소통하듯이 세상 모든 것이 내 PC에 접근할 수 있음을 결코 잊지 않는다. 작은 정보라 해도 그게 모두 국민과 직접적으로 연결되는 대한민국 자산이다. 세상에 완벽한 것은 없다지만, 정말 완벽해야 할 게 단 하나 있다면 그건 **정보보안**일 것이다.

**동료** 직원들은 나보고 걱정이 많아 탈이라고 하는데, 나는 동료 직원들 때문에 걱정이다. 후우, 보안을 잘 해야하는데…….

2006. 0월 0일 김주사

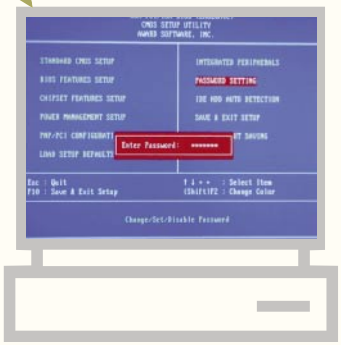
# 9시 자, 컴퓨터를 켜 볼까?


자, 그럼 컴퓨터를 켜 볼까?
어? 김주사님! 컴퓨터 켜는데 뭐가 복~잡하네요.
컴퓨터에 패스워드 거는 건 기본 아닌가?
내 PC의 기본인 부팅 패스워드를 거는 건 물론이고
윈도우 시동에도 패스워드를 걸어야지.
그래야 나 외에 다른 사람이 이 컴퓨터를 몰래 사용 못하지.
제 컴은 패스워드 걸지 않아도 인공지능이라 저만 인식해요.
탕
여기를 쳐줘야 시동이 되거든요. 이 녀석이 제 손에만 반응해요.
고장난 PC는 얼른 조치를 받게나.

# 김주사의 클릭보안 따라하기 ①

출입문 단속은 기본

## 컴퓨터 부팅용 패스워드 설정



PC를 켠 후, ❶ Delete 또는 F2 키를 눌러 **CMOS SETUP UTILITY** 화면이 나오게 한 후, ❷**CMOS SETUP UTILITY** 화면에서 **USER PASSWORD** 항목을 선택한 후, ❸**SUPERVISOR PASSWORD** 항목에서 **BOOTING PASSWORD**를 설정한다.

*본 설정 방법은 컴퓨터 종류에 따라서 차이가 날 수 있습니다.

내 컴퓨터에는 열쇠가 있다

## 사용자용 패스워드 설정

❶**시작**의 **제어판**으로 들어간 후, ❷**사용자 계정**을 클릭한다. ❸사용자 계정 화면에서 변경할 **사용자 계정**을 선택하고 **내 암호 변경**을 선택하여 ❹**암호**를 설정한다.

*사용자 계정이 만들어지지 않은 경우에는 사용자 계정 화면에서 변경할 사용자 계정을 선택할 수 없으므로, 먼저 사용자 계정을 만든 후에 설정해야 한다.


## 보안의 중심, 김주사의 패스워드 관리법

① 패스워드가 노출되지 않도록 조심하기
② 숫자만으로 이루어지거나, 영어 단어 또는 길이가 짧은 패스워드 등 다른 사람이 추측하기 쉬운 패스워드 사용하지 않기
③ 다른 사람이 볼 수 있는 곳에 패스워드를 기록하거나 방치하지 않기
④ 최소 분기 1회 주기적으로 패스워드 변경하기
⑤ 패스워드는 8자 이상, 영문자, 숫자 및 특수문자의 조합으로 구성하기

*본 가이드의 컴퓨터 설정은 윈도우즈 XP를 기준으로 한 것이며, 운영체제 사양에 따라서 다를 수 있습니다.

9시 10분

# 오, 이메일이 많이 왔네

# 김주사의 클릭보안 따라하기 2

무심코 클릭, 바이러스 우글우글

## 이메일 프로그램의 보안기능 사용하기

**바이러스 등 악성 프로그램이 이메일로 배달되어서 내 컴퓨터에 큰 피해를 줄 수 있으므로 다음과 같이 이메일 볼 때 주의하자.**

- 보낸 사람이 불분명한 메일이나 메일 제목이 흥미를 유발하는 스팸메일 등은 열어보지 않고 바로 삭제하기
- 첨부 파일은 저장하여 바이러스 검사 후 열기
- 이메일 프로그램에서 제공하는 바이러스 방지 설정하기
- 바이러스 백신 프로그램 기능 중에서 메일 감시 기능 사용하기

**이메일은 내용이 암호화되어서 보내는 것이 아니므로 다음 사항에 주의하자.**

- 중요문서, 개인정보 등이 담긴 내용은 되도록이면 이메일로 보내지 말고, 부득이 할 경우에는 이메일 프로그램의 보안 기능을 사용하기
- 문서를 이메일로 보낼 필요가 있을 때에는 문서를 암호화해서 전달하기
- 업무와 관련된 내용을 개인적으로 사용하는 웹메일을 사용해서 보내지 말기


### 이메일 안전하게 사용하는 방법

① 발신자가 불명확한 메일은 열어보지 말고 삭제하기
② 'exe, pif, scr' 등의 확장자가 붙은 첨부파일은 일단 저장하여 바이러스 검사 후 열어 보기
③ 개인정보, 계좌정보 등을 요구하는 수상한 이메일의 경우 링크된 사이트를 방문하거나 요구정보를 입력하지 말고, 관련 기관에 확인하는 등 각별히 주의하기
④ 이메일 프로그램에서 제공하는 스팸메일, 바이러스 차단 기능 적극 활용하기

# 11시 보남씨는 손님과 회의 중

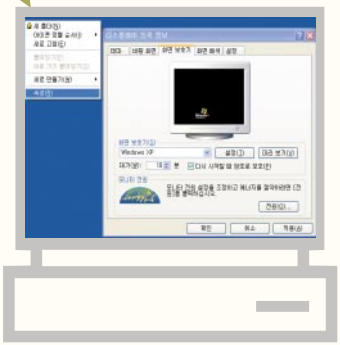
# 김주사의 클릭보안 따라하기 3

내 PC의 맨얼굴은 살짝 가려놓자

## 화면보호 설정

❶**시작**의 **제어판** 선택 ❷**디스플레이** 클릭하여 상단 메뉴 중 ❸**화면보호기** 항목을 선택한 후, 화면보호기 화면을 '없음'이 아닌 다른 것으로 설정한다. 화면보호기 대기시간은 10분 이내로 설정 ❹**다시 시작할 때 암호로 보호**(P)를 ☑

*사용자 계정에서 설정된 암호와 화면보호기 암호는 같은 것이므로, 우선 사용자 계정 암호 설정을 해야 함



알면 약, 모르면 독

## 공유폴더 확인 및 해지

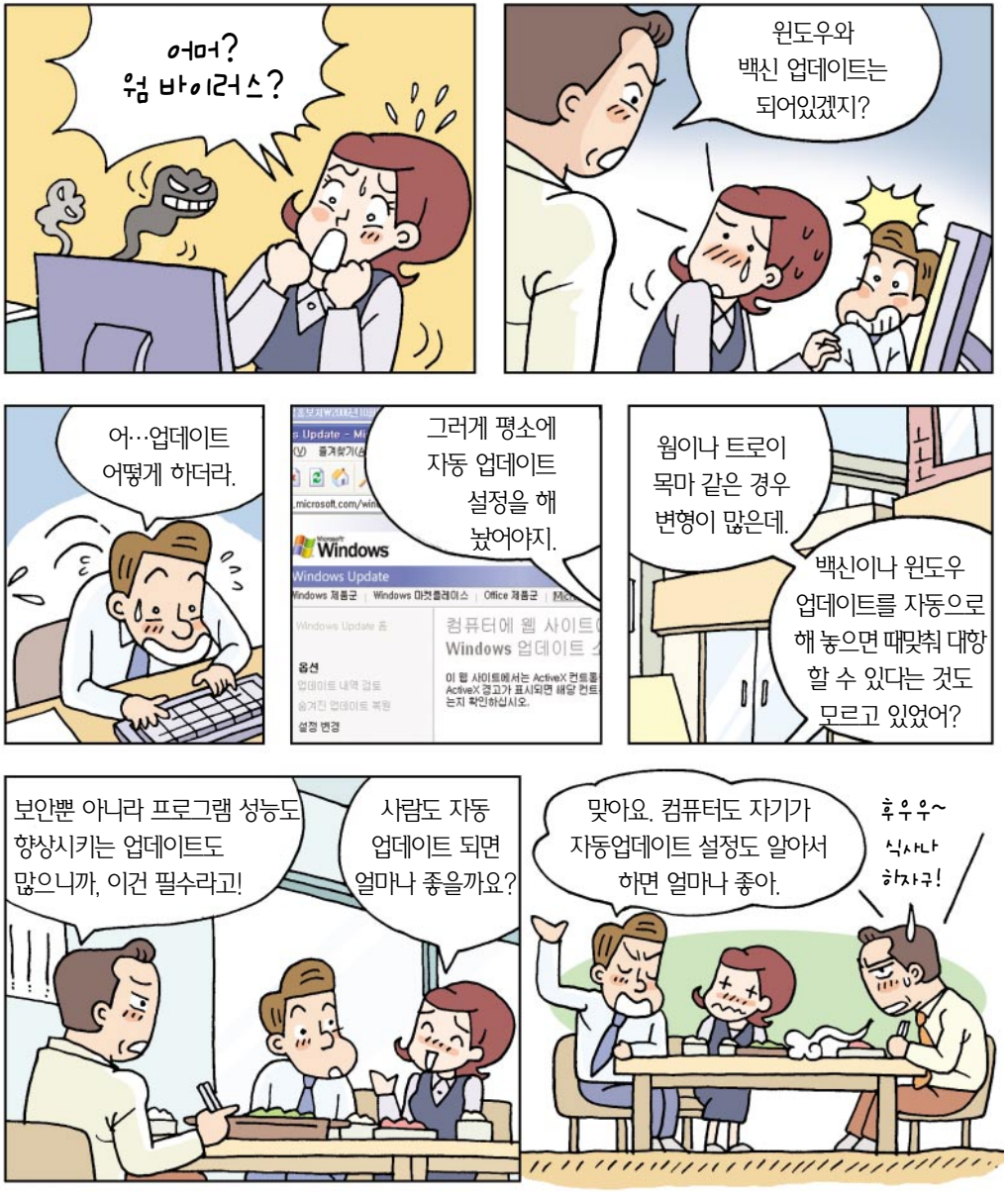
공유 폴더를 통한 악성 프로그램의 감염 가능성도 높지만, 중요 문서를 공유함으로써 내부 중요 자료의 유출 가능성도 있으므로, 공유 폴더 사용을 자제해야 함. 내 PC에 설정되어 있는 공유 폴더를 찾아서 해지하는 방법은 ❶**시작**의 **제어판** 선택 ❷관리 도구에서 **컴퓨터 관리(로컬)** 선택 ❸공유 폴더 클릭 후, 공유 선택 ❹오른쪽 창에 보이는 공유 폴더 리스트를 확인한 후, 해당 폴더로 이동하여, 폴더에 마우스 오른쪽 버튼을 클릭 ❺공유 및 보안 클릭 ❻**이 폴더를 공유함**의 ☑ 를 해제하면 된다.

*Windows XP에서는 관리를 목적으로 ADMIN$, C$, D$ 등이 기본적으로 공유되어 있으나, 이를 악용한 바이러스 감염 사례가 증가하고 있어, 이들 모두 공유 해지하는 것이 바람직하다.


## 내가 만든 정보 보호 방법

① 부팅·윈도우·화면보호기 패스워드 설정으로 다른 사람이 내 컴퓨터를 사용하지 못 하도록 하기
② 주요 문서는 내 컴퓨터에 저장할 때에도 암호화해서 저장하기
③ 업무관리시스템 이용시, 중요 문서는 비공개로 설정하여 외부 노출 방지하기
④ 바이러스 백신S/W를 이용하여 바이러스, 스파이웨어 등을 수시로 확인하기

# 12시 앗싸, 점심이다


어머?
웜 바이러스?
윈도우와
백신 업데이트는
되어있겠지?
어…업데이트
어떻게 하더라.
그러게 평소에
자동 업데이트
설정을 해
놨어야지.
Windows
Windows Update
웜이나 트로이
목마 같은 경우
변형이 많은데.
백신이나 윈도우
업데이트를 자동으로
해 놓으면 때맞춰 대항
할 수 있다는 것도
모르고 있었어?
보안뿐 아니라 프로그램 성능도
향상시키는 업데이트도
많으니까, 이건 필수라고!
사람도 자동
업데이트 되면
얼마나 좋을까요?
맞아요. 컴퓨터도 자기가
자동업데이트 설정도 알아서
하면 얼마나 좋아.
후우우~
식사나
하자구!

# 김주사의 클릭보안 따라하기 4

업데이트 착착, 바이러스 싹싹

## 윈도우 O/S 자동업데이트 설정

자동업데이트 설정은 ❶**시작**의 **제어판**에서 ❷**자동업데이트**를 클릭한 후, ❸**자동(권장)항목**을 클릭하면 된다.

*수동업데이트 설정은 시작의 윈도우 업데이트 항목을 클릭한 후, 업데이트 항목을 검사한다. 빠른 설치 항목을 클릭하면 업데이트 항목이 자동으로 설치 된다.

내 PC에도 '보약'이 필요하다

## 바이러스 백신 S/W 업데이트

① 바이러스 백신 S/W가 설치되어 있는지 확인
② 바이러스 백신 S/W 설정 내용에 실시간으로 바이러스 감시 기능 설정
③ 바이러스 백신 S/W 환경 설정 내용에 자동으로 백신 업데이트 기능 설정


## 김주사의 바이러스 미리 막는 법칙

① 백신 프로그램과 PC 방화벽 프로그램 설치하기
② 최신 바이러스 정보 수집과 프로그램 엔진 업데이트하기
③ 자료를 다운로드할 때는 신뢰할 수 있는 웹사이트를 이용하고 실행하기 전에 바이러스 백신S/W로 바이러스 검사하기
④ 바이러스 감염으로 PC가 부팅되지 않을 때를 대비해서 부팅 디스크 준비하기
⑤ 발신자 표시가 없거나 불분명한 메일 등은 열어볼 때 주의하고 특히 첨부파일은 저장하여 바이러스 검사후 실행하기
⑥ 멜리사, 워드 및 엑셀 매크로 등의 바이러스는 주로 마이크로소프트사 제품 사용자를 대상으로 공격하니, 해당제품을 사용하는 경우 수시로 바이러스 점검하기
⑦ 여러 명이 쓰는 PC나 공유디스크, CD-ROM은 최신버전의 백신 프로그램으로 검사하기
⑧ 백업 프로그램을 이용, 필요한 데이터 파일이나 실행파일(확장자가 exe, com인 파일)을 백업할 때는 반드시 백업 전에 바이러스 검사 후 백업하기

# 1시 좋은 거 있는데 볼래요?



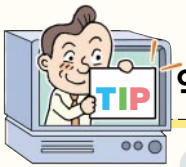



# 김주사의 클릭보안 따라하기 5

스포츠의 페어플레이, 컴퓨터에도 있죠

## '불법·유해 사이트' 방문 금지

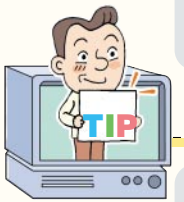
불법 동영상, 불법 S/W를 다운 받을 수 있는 불법 사이트는 저작권 위배는 물론, 악성 프로그램 및 바이러스에 쉽게 노출 될 수 있고, 악성 프로그램 감염을 통한 정보 유출 가능성이 높다. 또한 게임, 성인 관련 '유해 사이트'도 바이러스 유포 가능성이 높다.
즉 이런 사이트는 접속을 하지 않는 것이 좋으며 부득이 하게 다운받은 프로그램은 항상 백신 검사 후 사용해야 한다.


## 악성프로그램 감염 경로

① 이메일에 첨부된 악성 프로그램을 모르고 실행했을 때
② 알 수 없는 사람이 보낸 파일을 확인하지 않고 실행했을 때
③ P2P등을 이용하여 다운받은 확실하지 않은 파일을 실행했을 때
④ 믿을 수 없는 사이트의 자료실에서 파일을 다운로드 받았을 때

※이런 경우 항상 자신의 바이러스 백신 S/W로 검사한 후 실행하여야 한다.




## 악성 프로그램 설치를 막는 방법

① 알 수 없는 광고성 스팸메일을 열었을 때 보안경보창이 뜰 경우 절대 '확인'이나 '예' 또는 '아니오'를 누르지 말고 창 닫기 버튼을 눌러 설치하지 않기
② 인터넷에서 무료프로그램을 다운받아 설치시에는 '사용자 계약서'를 꼭 읽어 보고 설치하기
③ 윈도우 보안 패치를 주기적으로 하기
④ 인터넷 보안수준 설정은 ❶ **인터넷 익스플로어** 실행 후, ❷ **도구** 메뉴 선택, ❸ **인터넷 옵션** 선택 ❹ **보안**에서 **신뢰할 수 있는 사이트(보통) 이상**으로 설정하기

# 2시 으아, 자료가 위험해!


어머, 어떡해?
무슨 일이에요? 쥐 나왔어요?
난 몰라~ 저장해 둔 자료가 날아갔어요.
바이러스 검사를 해보는 게 좋겠군.
백업은 해뒀겠지?
그게… 그러니까!
저런.
파일 백업하는 건 기본이지. 정전이나 바이러스에 대비하는건 물론이고.
PC가 고장났을 때를 대비해서 미리미리 백업을 해 둬야죠.
잘 알고 있군. 정보남씨는 자료를 잘 백업해 뒀겠지?
물론이죠. 하드디스크에 다른 이름으로 폴더를 만들었죠.
CD나 백업용 디스크 같은 다른 독립된 저장공간에 해야지.
이젠 입이 아프다.

# 김주사의 클릭보안 따라하기 6

데이터의 안전 위한 예방주사

## 데이터 백업

① PC안에 데이터를 백업하기

**❶시작**의 **프로그램**에서 **❷보조프로그램 ❸시스템도구**로 이동 후, **백업**을 클릭한다. **❹백업 및 복원 마법사 시작**화면에서 '**다음(N)**' 클릭 **❺파일 및 설정 백업**을 선택하고 '**다음(N)**'을 클릭 **❻**백업할 내용 선택 **❼**백업종류, 대상 및 이름을 선택하고 백업을 시작한다.

이후 데이터 손실이 생겼을 경우, **❽시스템 도구**에서 **백업**을 선택, **백업된 파일 복원**을 선택한다.

② 백업파일은 외장형 하드디스크나 CD 등 별도의 저장매체에 저장하고, 안전한 장소에 보관한다.


안전을 공유하자

## 메신저 보안

메신저는 해킹 등의 방법으로 자신의 주요 정보 및 개인정보가 유출 될 수 있다. 따라서 **업무 내용에 관한 메신저 사용은 금지**해야 한다. 꼭 사용해야 할 때는 다음 사항을 명심하자.

- 대화 상대방으로부터 갑자기 전송되어온 파일이나 링크는 상대방 확인 후 실행
- 모르는 사람이 보내온 실행파일은 함부로 실행하지 말고, 필요시 최신 업데이트 된 백신으로 검사 후 실행

※첨부된 악성 프로그램의 확장자는 주로 'exe' 'pif' 'scr' 등 실행파일 임


## 김주사의 백업의 중요성 엿보기

사용자의 실수나 바이러스 등의 악성 프로그램에 의해 컴퓨터에 저장되어 있는 사용자의 중요 데이터가 손상되었을 경우, 주기적으로 백업된 복사본이 없다면 중요한 데이터를 복구할 수 없게 된다.

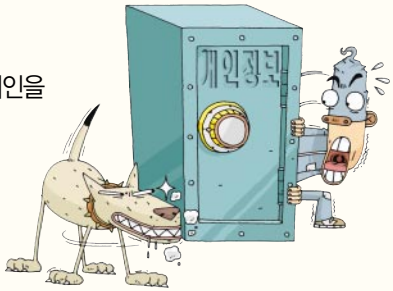
컴퓨터 수명이 다해서 폐기할 때에는 하드디스크를 포맷 등으로 저장된 정보가 외부에 노출되지 않도록 해야 한다.

# 5시 개인정보가 보이면 어떡하나?

# 김주사의 클릭보안 따라하기 7

정보사회의 가장 중요한 의무

## 개인정보보호

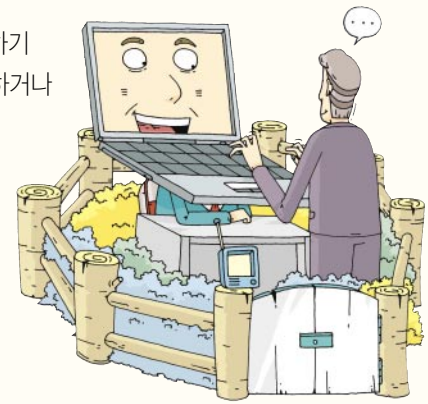



① 개인정보란?

생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 개인을 식별할 수 있는 정보로, 다른 정보와 결합하여 개인을 식별할 수 있는 정보도 포함한다.

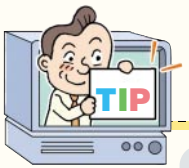
② 업무상 필요한 개인정보의 관리

- 홈페이지 등에 정보를 게시할 때에는 개인정보나 중요 정보가 담겨 있는지 다시 한번 확인하고 게시하기
- 개인정보는 최소한으로 수집, 이용하고 반드시 개인정보 제공자에게 알리기
- 이용 목적이 다한 개인정보는 즉시 삭제하기
- 개인정보를 PC에 보관할 때는 반드시 암호화해서 보관하기
- 직무상 알게 된 개인정보를 누설 또는 권한없이 처리하거나 타인에게 제공 금지하기



③ 주민등록번호 도용은 이제 그만!

- 개정된 주민등록법에 따라서 타인의 주민등록번호로 인터넷 회원으로 가입하는 등 주민등록번호를 도용하면, 3년 이하의 징역 또는 1천만원 이하의 벌금이 부과됨




### 내 개인정보는 내가 지킨다

① 개인정보의 제공은 신뢰도가 높은 사이트에서 필요한 경우에만 허용하기
② 미니홈피, 블로그, 공개게시판 등에 함부로 자신의 개인정보를 알리지 말기
③ 포털 검색 등을 통해 자신의 개인정보 노출 여부를 정기적으로 점검하기
④ 개인정보 제공시 개인정보보호방침을 반드시 확인하기
⑤ 개인정보 노출 사실을 발견할 경우 해당 웹사이트에 삭제 요청 등의 조치 요구하기

# 7시 집에 가서 마무리해야겠군

# 김주사의 클릭보안 따라하기 8


밖에서도 안전하게 일하자

## 정부원격근무전산망서비스(GVPN)

① 정부원격근무전산망서비스란?

정부원격근무전산망서비스는 가정이나 출장지 등에서 인터넷을 통해 전자결재 및 각종 행정정보시스템에 안전한 접속을 지원하는 시스템으로 행정전자서명(GPKI) 인증서를 발급 받아야 사용 가능하다.

② 이용방법

행정자치부 행정전자서명인증센터 홈페이지(www.gpki.go.kr)에서 신청서를 다운 받아 작성한 후, 행정자치부(전자정부본부 전자정부보안팀)에 이용자 등록 신청을 하면 공문 접수 후 다음 날부터 사용이 가능하다.

관련 프로그램은 행정자치부 행정전자서명인증센터 홈페이지(www.gpki.go.kr)에 접속하여, ❶자료실 메뉴 ❷GVPN 자료실 ❸「GVPN 접속프로그램(해당기관용)」을 다운로드 받아 실행하면 된다.

※정부원격근무전산망서비스 관련문의: 행정자치부 전자정부보안팀, 02)2100-3644, 3655

행정전자서명인증서 발급

## 행정전자서명(GPKI) 인증서 발급

행정자치부 행정전자서명인증센터 홈페이지(www.gpki.go.kr)에서 행정전자서명 인증서 신청 양식을 다운 받아 작성한 후 각 중앙행정기관 및 16개 시도에 공문으로 신청하면 된다.

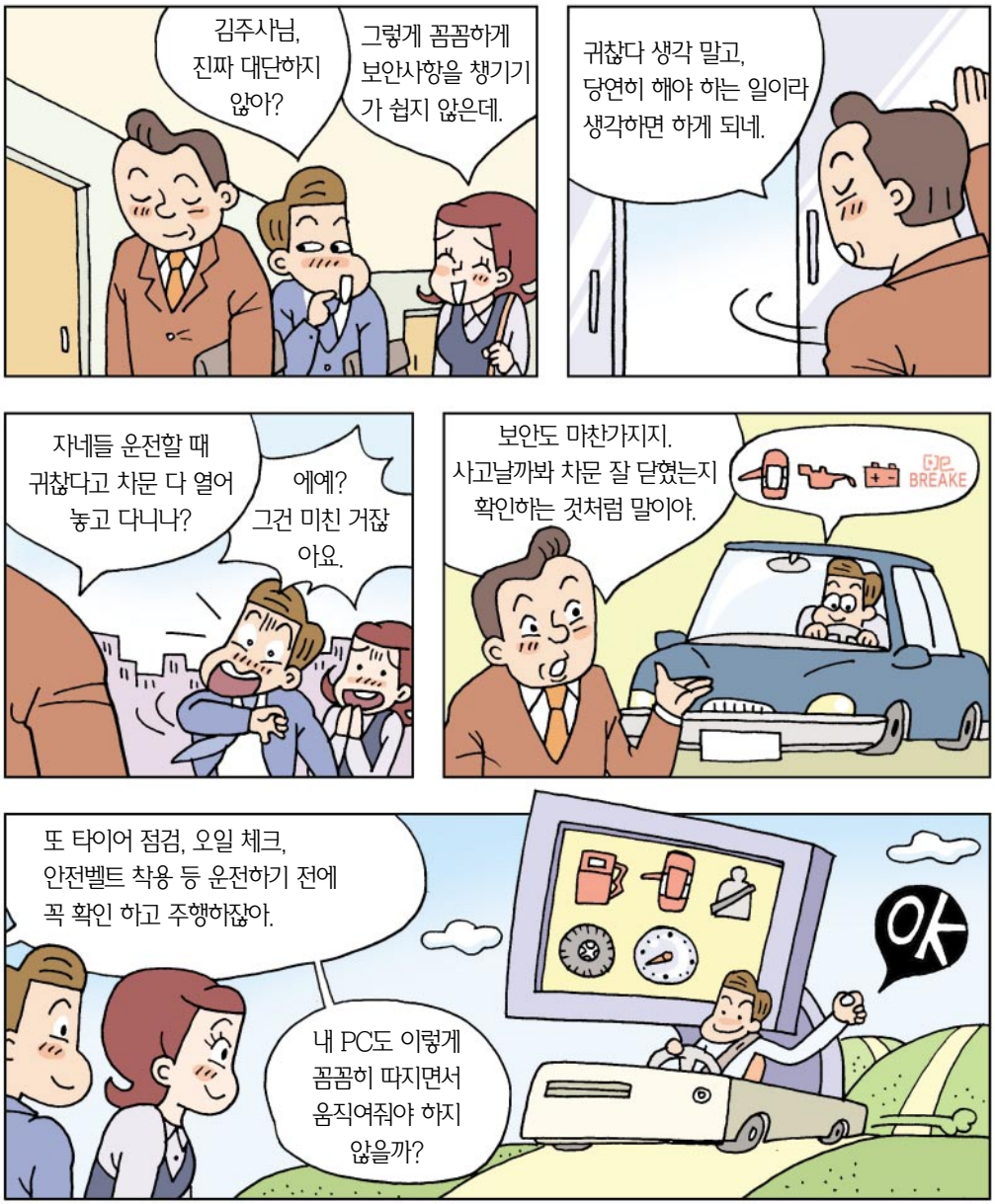
또한 신청 내용이 접수되면, 이메일로 발급 상황을 안내하고, 안내 받은 이메일에 따라 행정전자서명 인증서를 발급 받으면 된다.

※행정전자서명인증서 관련 문의: 행정자치부 행정전자서명인증센터 홈페이지(www.gpki.go.kr) 안내 참조


### 김주사의 행정전자서명 인증서 안전하게 관리하는 방법

① 행정전자서명인증서는 USB 메모리 또는 이동·외장형 하드디스크에 저장
② 비밀번호는 외부에 노출되지 않도록 안전하게 관리
③ 비밀번호는 영문자, 숫자 및 특수 문자의 조합으로 8자리 이상 구성

# 믿음직한 김주사


김주사님, 진짜 대단하지 않아?
그렇게 꼼꼼하게 보안사항을 챙기기가 쉽지 않은데.
귀찮다 생각 말고, 당연히 해야 하는 일이라 생각하면 하게 되네.
자네들 운전할 때 귀찮다고 차문 다 열어 놓고 다니나?
에엑? 그건 미친 거잖아요.
보안도 마찬가지지. 사고날까봐 차문 잘 닫혔는지 확인하는 것처럼 말이야.
BREAKE
또 타이어 점검, 오일 체크, 안전벨트 착용 등 운전하기 전에 꼭 확인 하고 주행하잖아.
내 PC도 이렇게 꼼꼼히 따지면서 움직여줘야 하지 않을까?
OK


게다가 해킹은 갈수록
지능화 되고 있고,
보안은 아무리 강조해도
지나치지 않아.
꽉
자동차의 안전벨트가
생명을 지켜주듯, 보안 습관은
우리 정보를 지켜 주는 것이지.
철컥!
보안
조심히…
후우~
버튼 한번 눌러드
렸드니 말씀이 끝
나질 않네.
그래도 존경스
럽지 않아요?
저렇게 철저하
시니.
저렇게 믿음직한 분과
사시는 사모님은 아무
걱정 없으실거야.
그건
동감.
정말 걱정되네요.
아니…
이게 아닌데.
이상하네.
아침에 당신이 보안
어쩌구 하면서 암호
바꿨잖아요.

# 나의 정보보안 수준은?

앞에서 나온 여러 가지 보호 방법은 잘 숙지하셨나요? 그럼, 나의 보안 수준은 어느 정도 인지 한번 체크해 봅시다.

| 보안내용 | 체크 |
|---|---|
| ① 윈도우 자동업데이트를 설정함 | |
| ② 바이러스 백신 S/W 자동업데이트를 설정함 | |
| ③ 자료를 정기적으로 백업하고 안전하게 보관함 | |
| ④ 출처가 불분명한 이메일·첨부파일은 바로 삭제함 | |
| ⑤ PC 방화벽을 설치, 실시간 감시 기능을 설정함 | |
| ⑥ PC 부팅용 패스워드와 로그인 패스워드를 설정함 | |
| ⑦ 화면보호기를 설정함 | |
| ⑧ 수상한 사이트를 방문하거나 불법 프로그램을 다운받지 않음 | |
| ⑨ 메신저 사용을 자제하고, 메신저로 교환한 자료는 백신으로 검사함 | |
| ⑩ 개인정보나 주요 정보가 담긴 파일은 암호화해서 보관함 | |
| ⑪ 패스워드는 영문, 숫자, 특수문자 조합으로 8자리 이상임 | |
| ⑫ 패스워드를 다른 사람에게 알려주거나 공유하지 않음 | |
| ⑬ 공유 폴더는 필요할 때만 최소한으로 사용함 | |
| ⑭ 바이러스 백신 S/W는 실시간 감시 기능을 설정하고, 주기적으로 검사함 | |
| ⑮ 행정전자서명인증서는 USB 메모리 또는 CD와 같은 안전한 곳에 보관함 | |

## 체크 갯수

**11개~15개** **축하합니다.**

김주사의 잔소리에서 당신은 곧 해방 되실 수 있겠군요.

**6개~10개** **아직 부족하군요.**

저기 어딘가에서 김주사가 당신을 지켜보고 있습니다.

**1개~5개** **김주사는 안보이고, 보남씨가 당신과 맞먹으려고 하는군요.**

설마 이대로 둘 생각은 아니신 거죠?

# 김주사의 알면 '보안' 모르면 '불안'

## 1 정부보안정보공유분석센터(www.gisac.go.kr)

행정자치부에서 운영 중인 정부보안정보공유분석센터는 최신의 PC보안 점검 및 악성코드 제거 프로그램을 이용할 수 있도록 지원하고, 해킹, 바이러스 등 사이버 위협에 대해 적시에 대응할 수 있도록 실시간으로 모니터링하고 있다.


## 2 행정전자서명 인증관리센터(www.gpki.go.kr)

행정전자서명 인증관리센터는 사이버 상에서 행정기관 및 공무원에 대한 신원 확인과 전자 문서의 위·변조 방지를 위해 각 행정기관에게는 전자관인과 컴퓨터 서버용 인증서를, 공무원 개인에게는 개인용 인증서를 발급해 주고 있다.

## 3 국가사이버안전센터(www.ncsc.go.kr)

국가사이버안전센터는 해킹, 바이러스 등 사이버 위협 상황을 직접 모니터링하고 '전자정부 보안관제센터', '인터넷침해사고 대응지원센터', '국방정보전대응센터' 등 국내·외로부터의 각종 위협 정보를 종합 분석하여, 공격징후를 탐지해 각급기관에 안전대책을 지원하며, 긴급상황 발생 시에는 예·경보를 발령해 주고 있다.


정보남씨, 지난번 지시 사항 마무리됐습니까?
아직, 보안 좀 신경 쓰느라~
아까 점심 먹고 꾸벅꾸벅 존 건 뭡니까?
Z Z
!!!
헉
너무 보안에 신경썼더니, 피로가 쌓여서 그만
으이그, 말이나 못하면.
이 사람 머리 속에 든 바이러스는 어떻게 해야 하는 건지… 원!
'보안의 생활화' 잊지 마세요!

행정자치부

●**발행처** 행정자치부 ●**발행일** 2006년 12월 ●**내용 및 배포문의** 전자정부본부 전자정부보안팀
●**전화** 02)2100-3640, 3639 ●**주소** (우)110-760 서울시 종로구 세종로 55 정부중앙청사