



안전하고 건전한  
**정보보호**  
**생활가이드**





## 머 리 말

우리는 아침에 일어나서 잠잘 때까지 컴퓨터와 인터넷으로 일하고, 공부하고, 세상과 소통하는 정보화 사회에 살고 있습니다. 인터넷으로 지식을 얻고, 쇼핑과 금융거래를 할 수 있을 뿐만 아니라 지구촌 곳곳을 실시간으로 볼 수 있는 세상입니다.

그러나 컴퓨터와 인터넷은 우리사회를 해킹과 컴퓨터 바이러스 감염, 개인정보 침해, 악성 댓글 등으로 인해 새로운 위험에 빠뜨리고 있습니다. 2003년 1.25 인터넷 대란과 2008년 각종 개인정보 유출 사고 등은 컴퓨터와 인터넷이 얼마나 위험한지를 단적으로 보여준 사례라고 할 수 있겠습니다.

이러한 위험에 슬기롭게 대처하면서 정보화 역기능으로부터 우리의 정보생활을 안전하고 건전하게 보호하기 위해서는 국민 모두의 적극적인 대응이 필요한 시점입니다. 이를 위해서는 컴퓨터와 인터넷 사용에 따른 각종 위험을 정확하게 인식하고 그 예방 및 대응 방법을 제대로 습득하여 이를 실천하는 것이 매우 중요합니다.

행정안전부에서는 각계 전문가와 함께 컴퓨터와 인터넷을 사용하는 데 따른 각종 위험과 그 예방 및 대응 요령을 담은 “정보보호 생활가이드”를 발간하였습니다.

이 책자를 통해 컴퓨터와 인터넷으로 인한 위험을 사전에 예방하여 안전하고 건전한 정보생활에 도움이 될 수 있기를 바랍니다.

행 정 안 전 부



## 목 차

### 안전한 컴퓨터 이용

1. 해킹 차단·대응 방법 / 6
2. 컴퓨터 바이러스 차단·대응 방법 / 8
3. 스파이웨어 차단·대응 방법 / 10
4. 악성 봇 차단·대응 방법 / 12
5. 이메일과 악성바이러스 / 14
6. USB 메모리 관리 방법 / 16
7. 컴퓨터 운영체제 보안 / 18
8. 무선 랜의 정보유출 위험 / 20
9. 컴퓨터 수리·매각·폐기 시 주의 사항 / 22



### 안전한 인터넷 이용

1. 웹브라우저 보안설정의 중요성 / 26
2. 메신저 이용 시 주의 사항 / 28
3. 인터넷 파일공유(P2P)시 주의 사항 / 30
4. 자동설치 프로그램의 위험 / 32
5. 스팸 차단 방법 / 34
6. 안전한 비밀번호 보호 방법 / 36



### 안전한 전자상거래

1. 공인인증서의 중요성 / 40
2. 온라인 금융거래 시 주의 사항 / 42
3. 온라인 쇼핑 시 주의 사항 / 44
4. 인터넷 사기(피싱) 대응 방법 / 46
5. 전화사기(보이스 피싱) 대응 방법 / 48
6. 안전한 온라인 게임 / 50



## IV. 개인정보보호의 중요성

1. 인터넷상의 개인정보보호 방법 / 54
2. 게시판상의 개인정보보호 방법 / 56
3. 개인정보 피해발생 시 신고·구제 절차 / 58
4. 주민등록번호 대신 아이핀 사용 / 60
5. 개인정보 클린 캠페인 / 62



## V. 건강한 정보생활

1. 인터넷 에티켓의 중요성 / 66
2. 악성 댓글의 위험과 대응 방법 / 68
3. 불법·청소년 유해정보 차단 방법 / 70
4. 사이버 성폭력 예방 및 대응 방법 / 72
5. 컴퓨터·인터넷 중독 예방 및 치유 방법 / 74
6. 가족의 건강한 정보생활 가이드 / 76

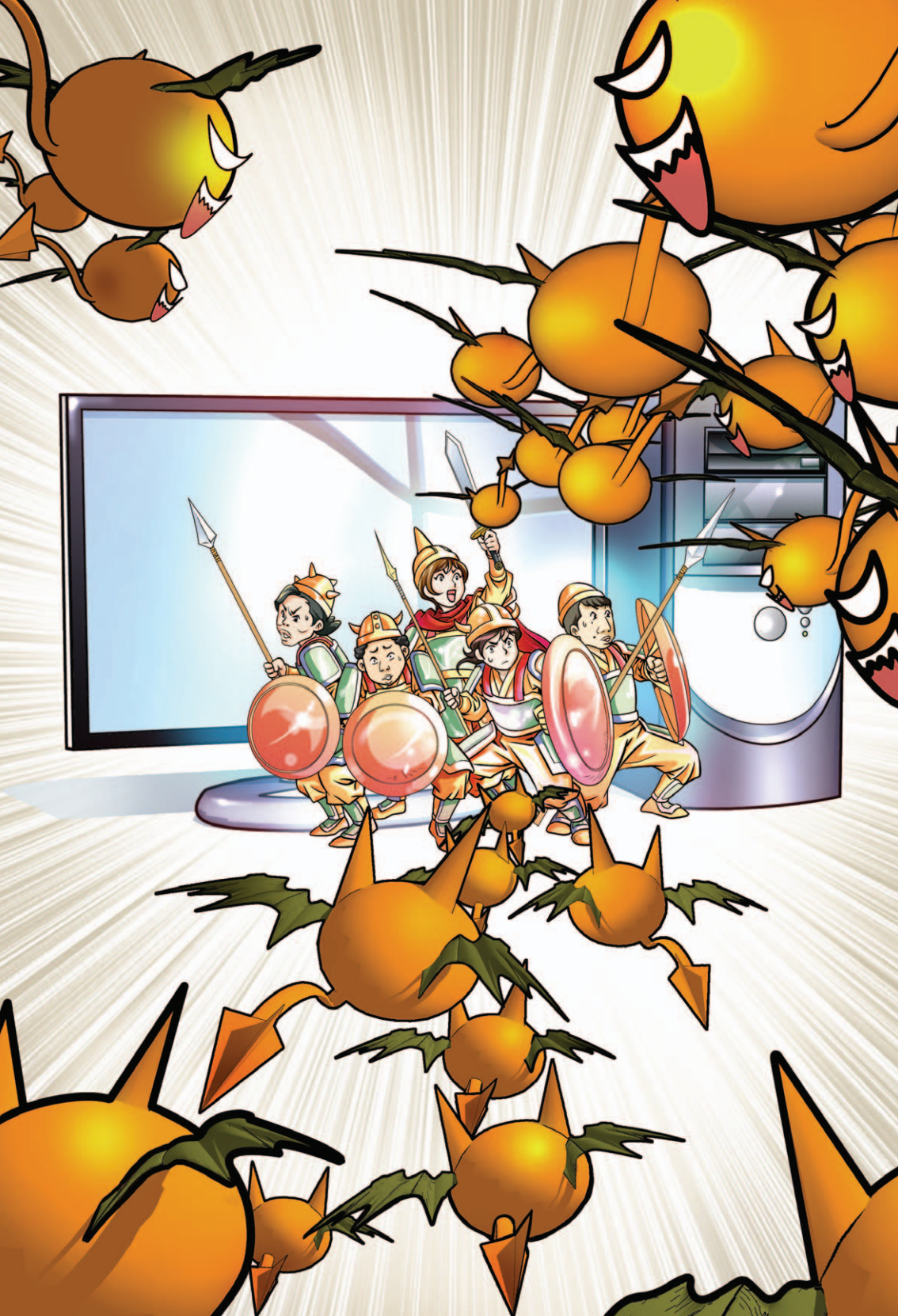


## 부록

1. 상담 및 신고 기관 / 78
2. 알아두면 유용한 웹사이트 / 79
3. 통신사별 스팸 대응 연락처 / 80
4. 컴퓨터 운영체제 보안설정 방법 / 81







안전한 컴퓨터 이용





## 1. 해킹 차단 · 대응 방법



### 해킹이란

사용이 허락되지 않은 컴퓨터에 접근하여 고장을 일으키거나 정보를 도둑질하는 등의 나쁜 행위를 뜻합니다.



2008년 2월 대한민국 최대 규모의 인터넷 상거래 웹사이트가 해킹되어 천만 명 이상의 개인정보가 유출되었습니다.

### 증상 및 피해

- 컴퓨터 내의 중요한 자료가 유출 혹은 변경될 수 있습니다.
- 파일이나 프로그램이 자동으로 생성 · 실행 · 삭제 · 변경됩니다.
- 컴퓨터 환경설정(바탕화면, 해상도 등)이 변경됩니다.
- 정상적으로 실행되던 프로그램이 갑자기 작동이 안 됩니다.
- ※ 윈도우 XP의 경우 '이상 트래픽 경고창'이 나타날 수 있습니다.
- 이유 없이 컴퓨터 속도가 느려지거나 자주 정지됩니다.

### 예방 방법

- 컴퓨터의 보안 업데이트를 '자동'으로 설정합니다.(부록4 참고)  
- (윈도우)[시작]-[설정]-[제어판]-[자동업데이트]를 '자동'으로 설정
- 백신프로그램과 방화벽 등 보안 프로그램을 설치합니다.(부록4 참고)  
- (윈도우)[시작]-[제어판]-[보안센터]-[Windows 방화벽]을 "사용"으로 설정
- 비밀번호는 추측이 어렵게 만들고 자주 변경해야 합니다.(37쪽 참고)

### 해킹 시 대응 방법

- 해킹 피해 발생 시 한국정보보호진흥원, 경찰청 등으로 신고합니다.
- 무료 · 유료 백신프로그램으로 검사 · 치료합니다.  
- 보호나라(<http://www.boho.or.kr>)에서 제공하는 정보 참고
- 백신프로그램으로 치료가 되지 않을 경우 윈도우즈를 재설치합니다.

#### 백신정보

보호나라 ☎ 118, <http://www.boho.or.kr>

#### 상담 · 지원

한국정보보호진흥원 ☎ 118, <http://www.krcert.or.kr>

#### 범죄신고

경찰청 사이버테러대응센터 ☎ (02) 3939-112



## 2. 컴퓨터 바이러스 차단 · 대응 방법



### 컴퓨터 바이러스란

자료를 삭제하는 등 컴퓨터의 정상 작동을 방해하는 악성 프로그램입니다. USB 메모리, 이메일, 메신저 프로그램 등 다양한 방법으로 감염됩니다.

### 증상 및 피해

- 컴퓨터 시작 시 시스템 에러가 나고 윈도우가 작동되지 않습니다.
- 이유 없이 컴퓨터 속도가 저하되고 프로그램이 실행되지 않습니다.
- 컴퓨터 사용 중 비정상적인 그림 · 메시지 · 소리 등이 나타납니다.
- 사용자 명령 없이 프로그램이 실행되거나 주변장치가 작동됩니다.
- 사용자 명령 없이 파일, 아이콘들이 생성 혹은 삭제됩니다.

**사례** 2003년 1월 25일 컴퓨터 바이러스로 인하여 우리나라 인터넷이 4시간 정도 마비되어 약 1,700억 원의 피해가 발생하였습니다.

### 예방 방법

- 컴퓨터의 보안 업데이트를 '자동'으로 설정합니다.(부록4 참고)
  - (윈도우)[시작]-[설정]-[제어판]-[자동업데이트]를 "자동"으로 설정
- 백신프로그램과 방화벽 등 보안 프로그램을 설치합니다.(부록4 참고)
  - 인터넷에서 내려 받거나 이메일에 첨부된 파일 또는 다른 컴퓨터에서 사용한 파일은 백신프로그램으로 검사 후 사용합니다.
  - (윈도우)[시작]-[제어판]-[보안센터]-[Windows 방화벽]을 "사용"으로 설정

### 감염 시 대응 방법

- 무료 · 유료 백신프로그램으로 검사 · 치료합니다.
  - 보호나라(<http://www.boho.or.kr>)에서 제공하는 정보 참고
- 백신프로그램으로 치료가 되지 않을 경우 윈도우즈를 재설치합니다.

**백신 정보** 보호나라 ☎ 118, <http://www.boho.or.kr>  
**상담 · 지원** 한국정보보호진흥원 ☎ 118, <http://www.krcert.or.kr>



## 스파이웨어란

컴퓨터 이용자의 동의 없이 설치되거나 의도와 다르게 작동되어 컴퓨터  
사용에 불편을 끼치거나 정보를 훔쳐가는 악성 프로그램입니다.



## 증상 및 피해

- 컴퓨터 작동의 이상을 유발하거나 중요자료가 유출됩니다.
- 웹브라우저의 '홈페이지 설정'이나 '즐거찾기' 등이 변경됩니다.
- 원하지 않는 광고창이 뜨거나 성인, 광고 웹사이트로 접속됩니다.
- 이용자가 특정 프로그램을 삭제하거나 종료할 수 없습니다.

**사례** 2008년 동영상을 무제한으로 볼 수 있다고 속여 돈을 훔쳐가는 스파이웨어가 등장하였습니다. 사용자가 본인 확인을 위해 휴대폰번호와 주민등록번호를 입력하게 되면 사용자의 동의 없이 3만3천 원이 휴대폰으로 결제되는 피해가 발생하였습니다.

## 예방 방법

- **스파이웨어**는 주로 인터넷 사용 도중 설치되므로 믿을 수 있는 웹사이트만 방문하고 의심되는 광고나 게시물은 클릭하지 않습니다.
- 음란, 도박 등 불건전 웹사이트는 접속하지 않습니다.
- 웹사이트에서 **소프트웨어** 설치를 요구할 경우 주의해야 합니다.

## 대응 방법

- 유료·무료 스파이웨어 치료 프로그램으로 검사·치료합니다.
- 스파이웨어 치료 프로그램은 신뢰할 수 있는 웹사이트(업체 홈페이지 등)에서 요금제도(요금연장 자동결제 등)를 확인한 후 구매하여 사용하시기 바랍니다.

백신 정보

보호나라 ☎ 118, <http://www.boho.or.kr>

상담 · 지원

한국정보보호진흥원 ☎ 118, <http://www.krcert.or.kr>  
한국소비자원 ☎ (02) 3460-3000, <http://www.kca.go.kr>



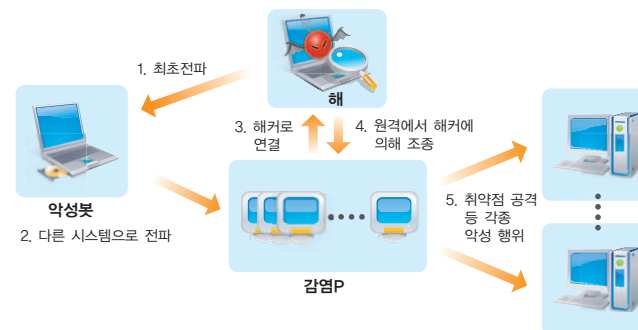


## 4. 악성 봇 차단 · 대응 방법



### 악성 봇이란

악성 로봇(Robot)의 준말로써, 봇에 감염될 경우 해커가 감염된 컴퓨터를 로봇과 같이 마음대로 조종할 수 있습니다.



### 증상 및 피해

- 컴퓨터는 해커가 지시한 일을 수행합니다.  
- 특히 해커가 다른 시스템을 공격하는 데 이용될 수 있습니다.

※ 악성 봇은 특별한 증상이 없는 경우가 많으므로 예방이 매우 중요합니다.

### 예방 방법

- 컴퓨터의 보안 업데이트를 '자동'으로 설정합니다.(부록4 참고)
- 백신프로그램과 방화벽 등 보안 프로그램을 설치합니다.(부록4 참고)
- 비밀번호는 추측이 어렵게 만들고 자주 변경해야 합니다.(37쪽 참고)
- 믿을 수 있는 웹사이트와 프로그램만을 사용합니다.

### 감염 시 대응 방법

- 무료 · 유료 백신프로그램으로 검사 · 치료합니다.  
- 보호나라(<http://www.boho.or.kr>)에서 제공하는 정보 참고
- 백신프로그램으로 치료가 되지 않을 경우 윈도우즈를 재설치합니다.

백신 정보

보호나라 ☎ 118, <http://www.boho.or.kr>

상담 · 지원

한국정보보호진흥원 ☎ 118, <http://www.krcert.or.kr>





## 5. 이메일과 악성바이러스



### 이메일(E-mail)이란

인터넷 상에서 편지나 여러 정보를 주고받을 수 있는 편리한 도구입니다.

### 피해 내용

- 이메일은 컴퓨터 바이러스 등 악성 프로그램 유포나 불법·음란 정보 유포 및 인터넷 사기(피싱)의 수단으로 사용될 수 있습니다.



#### 사례

2008년 말 유명 기업의 크리스마스 이벤트를 가장한 이메일을 통해 컴퓨터 바이러스가 많이 유포되었습니다.

### 안전한 사용 방법

- 출처가 불분명한 이메일이나 첨부파일은 읽지 않고 삭제합니다.

※ **흥미를 유발하는 자극적인 표현·사진은 특히 주의합니다.**

- 첨부파일을 읽거나 저장하기 전에 백신프로그램으로 검사합니다.

- 개인정보를 요구할 경우 홈페이지나 전화를 통하여 확인합니다.

– 이메일 상의 홈페이지 주소·전화번호는 위조될 수 있으므로, 검색사이트나 ☎ 114를 이용하여 연락처를 직접 확인합니다.

- 이메일은 매일 확인하고 중요하지 않은 이메일은 즉시 삭제합니다.

- 이메일 프로그램 또는 서비스 제공자의 차단서비스를 활용합니다.

※ '보호나라' (<http://www.boho.or.kr/>) → 스팸 → 불법스팸 대처방안 → 이메일 내용을 참고합니다.

- 인터넷 게시판 등에 이메일 주소를 남길 때는 신중히 생각합니다.

- 웹사이트 회원가입 시 광고메일 수신 여부를 신중히 결정합니다.

홈쇼핑 쇼핑정보	● 홈쇼핑에서 제공하는 상품과 쇼핑관련 정보(특가상품, 이벤트, 할인쿠폰, 기념일 알림)의 안내를 받으시겠습니까? e-mail 수신거부와 상관없이 주문현황, 결제내역, 배송상태, 무통장 입금내역, 회사의 주요정책 관련 공지메일 등은 발송됩니다.)	
E-MAIL	<input checked="" type="radio"/> 예	<input type="radio"/> 아니오
SMS(문자메세지)	<input checked="" type="radio"/> 예	<input type="radio"/> 아니오
● 쇼핑공감 메일링 서비스	수신하시겠습니까?	<input type="radio"/> 예 <input checked="" type="radio"/> 아니오
● 쇼핑공감 정보공개여부	수신동의 하시면 500 Point 지급됩니다.(지급기준 : 1회)	
	<input checked="" type="radio"/> 공개	<input type="radio"/> 비공개





## 6. USB 메모리 관리방법



### USB 메모리란

USB는 컴퓨터와 주변 기기를 연결하는 표준 가운데 하나로서 컴퓨터에 쉽게 연결하여 정보를 쓰고 읽을 수 있는 도구입니다.

### 피해 내용

- USB 메모리는 여러 컴퓨터에서 사용하는 경우 컴퓨터 바이러스 등에 감염되기 쉬우며 분실·도난 시 대량의 정보가 유출됩니다.

#### 사례



2007년 발표된 통계에 의하면 USB 메모리를 통해 전파되는 악성코드 피해 사례가 월 평균 250여 건씩 발견되고 있습니다.

### 안전한 사용 방법

- USB 메모리를 백신프로그램으로 수시로 검사·치료 합니다.
- USB 메모리 내의 자료는 다음 중 하나의 방법으로 암호화하여 사용합니다.
  - USB 메모리 업체에서 제공하는 암호화 프로그램을 사용합니다.
  - 압축프로그램에서 제공하는 '암호화 압축' 기능을 활용합니다.
  - 문서작성 프로그램의 암호화 저장기능을 사용합니다.

※문서작성 프로그램에 따라 설정방법이 다르므로 도움말 등을 참조합니다.

- 공인인증서는 별도의 USB에 인증서만을 저장하여 사용합니다.



## 7. 컴퓨터 운영체제 보안



### 컴퓨터 운영체제란

컴퓨터의 작동을 직접 제어하고 관리하는 프로그램입니다.

### 피해 내용

- 운영체제의 보안을 설정하지 않으면 해킹 공격에 노출될 수 있으며, 다른 사람이 컴퓨터를 무단으로 사용할 수 있습니다.

### 컴퓨터 운영체제의 보안 설정(부록4 참고)

운영체제의 보안기능을 올바르게 사용하는 것은 정보보호의 첫걸음입니다. 일반적으로 많이 사용하는 윈도우XP를 중심으로 설명 드리겠습니다.

- 사용자 계정의 로그인 암호를 설정하고 "Guest"(손님) 계정을 사용하지 않습니다.
    - 암호가 설정되지 않은 컴퓨터는 누구든지 사용할 수 있습니다.
    - 해커는 Guest 계정을 통하여 시스템에 접근하는 경우가 많습니다.
  - 자리를 비운 동안 다른 사람이 사용할 수 없도록 화면보호기를 설정합니다.
    - [바탕화면] 마우스 오른쪽 버튼 클릭 → [속성] → [화면보호기] 선택 → [화면보호기] 종류 선택, [대기] 시간은 10분 정도로 설정, [다시 시작할 때 암호보호]를 체크하고 [확인] 선택
- ※ 비밀번호는 윈도우 로그인에 사용하는 비밀번호와 동일합니다.
- 컴퓨터의 보안 업데이트를 '자동'으로 설정합니다.
    - 자동 업데이트를 설정하면 새로운 업데이트가 나왔는지 자동으로 확인하여 설치하므로 보안업데이트를 쉽게 할 수 있습니다.

무료 점검 보호나라 ☎ 118, <http://www.boho.or.kr>



## 8. 무선 랜의 정보유출 위험



### 무선 랜(Wireless LAN)이란

물리적인 선 없이 전파를 이용하여 인터넷을 사용하는 방법으로서 이동성과 편리성 때문에 가정과 직장 등에서 널리 사용되고 있습니다.

### 피해 내용

- 무선 랜은 전파를 이용하기 때문에 유선 인터넷에 비해 도청에 매우 취약합니다.



**사례** 2005년 미국 대형 의류할인점에서는 결제 단말기에서 중앙시스템까지의 무선 랜에서 수천만 건의 고객정보가 도난당하는 사고가 발생하였습니다.

### 안전한 사용 방법

- 무선 랜을 사용하여 중요 자료를 전송하지 않습니다.
- 컴퓨터와 무선 랜 기계(무선 공유기 등)에 암호를 설정하여 전송되는 자료를 암호화합니다.
- 무선 공유기에 관리자 암호를 설정합니다.
  - 공유기에 암호를 설정함으로써 권한 없는 사용자의 관리자 페이지 접근을 막도록 합니다.
- ※ 암호의 문자수는 21자 이상으로 충분히 길게 합니다.
- 접속 가능한 기기를 제한합니다.
  - 무선 공유기에서 접속 가능한 기기를 설정합니다. MAC(Media Access Control)이라는 기기별 고유번호를 이용하여 접속 가능한 기기를 선택할 수 있습니다.
- 무선 랜 기계의 자동 로그인 기능을 사용하지 않습니다.



**알림** 무선 랜 관련 설정은 프로그램, 업체별로 다르므로 도움말 등을 참조합니다.



## 9. 컴퓨터 수리 · 매각 · 폐기 시 주의 사항



### 수리의뢰 · 매각 · 폐기 시 정보유출

컴퓨터의 자료를 단순 삭제하는 것은 복구가 가능하므로 완전히 삭제(소거)하여야 합니다.

### 피해 내용

- 컴퓨터나 저장매체를 부적절하게 수리의뢰 · 매각 · 폐기하는 경우 컴퓨터 등에 저장된 정보가 모두 유출될 수 있습니다.

**사례** 2008년 홍콩에서는 컴퓨터 회사직원이 수리 중인 유명 연예인 컴퓨터에 저장된 동영상 유출시켜 커다란 사회적 문제가 되었습니다.

### 안전한 수리 · 매각 · 폐기 방법

- 컴퓨터를 수리의뢰, 매각하는 경우 미리 공인인증서, 개인정보, 작성한 문서나 이메일 등 중요 정보를 완전히 삭제합니다.
- 저장된 자료를 완전히 삭제하는 '소거 프로그램'을 사용합니다.

※ '소거 프로그램' 정보는 인터넷 검색을 통하여 얻으실 수 있습니다.  
 ※ 단순 삭제 혹은 하드디스크 포맷을 하는 경우 탐색기에서는 자료가 안보여도 실제로는 하드 디스크에 자료가 남아 있습니다.

- 컴퓨터나 저장매체를 폐기하는 경우 저장매체(하드디스크 등)를 물리적으로 파괴하여 다시 사용할 수 없도록 합니다.
- 외부 케이스를 파괴하더라도 내부의 장치는 작동될 수 있으므로 내부까지 완전히 파괴합니다.
- 회사에 별도의 정보보호 정책이 있거나 담당 조직이 있는 경우에는 컴퓨터를 폐기하기 전에 담당자와 상담합니다.
- 믿을 수 있는 전문 업체의 수리 · 매각 · 폐기 서비스를 이용합니다.





안전한 인터넷 이용





## 1. 웹브라우저 보안설정의 중요성



### 웹브라우저란

인터넷 상의 정보를 사용자의 컴퓨터에서 볼 수 있도록 해주는 프로그램으로서 인터넷 익스플로러, 파이어폭스 등이 많이 사용됩니다.

### 피해 내용

- 웹브라우저의 보안설정을 하지 않으면 인터넷 이용내역과 컴퓨터에 저장된 웹사이트 아이디와 암호 등이 유출될 수 있습니다.

### 웹브라우저 보안 설정 (인터넷 익스플로러의 경우)

- 보안 수준은 '보통' 이상으로 설정합니다.
  - 메뉴에서 [도구] → [인터넷 옵션] → [보안] → [인터넷]의 보안 수준을 '보통' 이상으로 설정 → [확인]
- ※ [사용자 지정 수준]을 선택하여 세부 설정할 수도 있습니다.
- 이름과 암호는 '자동 완성' 되지 않도록 합니다.
  - 메뉴에서 [도구] → [인터넷 옵션] → [내용] → 자동 완성 [설정] → '자동 완성 사용 대상'에서 '사용자 이름과 암호' 체크 제거 → [확인]
- 사용한 인터넷 파일을 지우도록 설정합니다.
  - 메뉴에서 [도구] → [인터넷 옵션] → [고급] '브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기'를 체크 → [확인]
- 인터넷 사용 도중 각종 정보가 저장되는 '쿠키'는 삭제합니다.
  - [C드라이브] → [Windows] → [Temp] → [Cookies] 폴더에서 index를 제외한 모든 파일을 삭제합니다.



### 공공 컴퓨터 사용 시 주의 사항

- 금융 업무는 공공 컴퓨터를 사용하지 않습니다.
- '아이디 자동 저장'이나 '자동 로그인' 기능은 사용하지 않습니다.
- 웹사이트 이용이 끝났을 때에는 웹브라우저 우측 상단의 창닫기 버튼(✕)을 사용하지 않고 '로그아웃' 버튼을 클릭합니다.





## 2. 메신저 이용 시 주의 사항



### 메신저란

인터넷에서 메시지와 자료를 실시간으로 주고받을 수 있는 프로그램입니다.

### 피해 내용

- 메신저를 잘못 관리하면 아이디를 도용한 사기 피해, 개인정보 유출, 컴퓨터 바이러스 등 악성 프로그램 감염 피해가 발생합니다.

**사례** 2007년 메신저를 해킹하여 대화 도중 긴급히 입금을 요구하는 사기가 발생하였습니다. 피해자들은 친한 사람들에게 갑자기 사고가 발생된 것으로 믿어 입금을 하였습니다.

### 안전한 사용 방법

- 아는 사람이 메신저를 통하여 송금, 개인정보 등을 요구할 경우 대화상대에게 전화를 걸어 사실 여부를 확인합니다.
- 공동 사용하는 컴퓨터는 '자동 로그인' 기능을 사용하지 않습니다.
  - '자동 로그인' 기능을 사용하면 다른 사람이 내 아이디로 로그인하여 사기 및 개인정보 노출 등의 피해가 발생합니다.
- 모르는 사람으로부터의 대화 요청 시 함부로 수락하지 않습니다.
  - 특히 메신저를 통하여 파일을 전송 받거나 모르는 웹사이트에 접속하는 경우 주의가 필요합니다.
- 메신저 대화내용은 다른 사람이 볼 수 있으므로 암호화 기능을 사용합니다.
  - 신용카드 등 중요 정보는 메신저를 통하여 전달하지 않습니다.
- 자리를 잠깐 비우는 경우 메신저 잠금 기능을 사용합니다.
- 비밀번호는 추측이 어렵게 만들고 자주 변경해야 합니다.(37쪽 참고)
- 메신저를 항상 최신 버전으로 업데이트합니다.

### 3. 인터넷 파일공유(P2P) 시 주의 사항



### 인터넷 파일공유(P2P)란

동료 또는 대등한 사람을 뜻하는 P2P(Peer To Peer)는 인터넷에서 용량이 큰 영화나 음악 등 자료를 공유하여 쉽게 받아보는 방법입니다.

### 증상 및 피해

- 공유된 컴퓨터 중 하나가 컴퓨터 바이러스에 감염되면 매우 빠른 속도로 다른 컴퓨터로 확산됩니다.
- 공유된 컴퓨터에 저장된 개인정보 등 중요 정보가 유출됩니다.
- 영화·음악 등 저작권으로 보호되는 자료 공유 시 법적 처벌됩니다.



**사례** 2006년 무료 P2P를 가장한 악성프로그램이 설치된 컴퓨터 약 5만 대가 임의로 조작되어 인터넷 포털 사이트의 광고 검색 순위가 조작되는 사건이 발생하였습니다.

### 안전한 사용 방법

- 중요한 정보가 저장된 컴퓨터에는 P2P 프로그램을 설치하지 않습니다.
- P2P 프로그램 설정에서 공유가 필요한 자료만을 공유하도록 설정합니다.
  - 공유 프로그램 설치 시 문서 전체가 공유되도록 자동 지정되어 컴퓨터의 자료가 모두 공개될 수 있습니다.
- 백신프로그램을 설치하여 컴퓨터 바이러스 등을 차단합니다.
  - 특히 호기심을 유발하는 이름·내용의 자료는 주의가 필요합니다.
- 유명 P2P 프로그램을 가장한 악성 프로그램이 존재하므로 P2P 홈페이지에서 제공하는 프로그램을 이용합니다.
- P2P 프로그램을 사용하지 않을 때는 컴퓨터의 전원을 끕니다.
  - 악성프로그램은 종료 후 하더라도 자동 재실행될 수 있습니다.
- 영화, 음악 등 저작권으로 보호되는 파일을 공유하지 않습니다.
- 자녀가 P2P 프로그램을 사용할 경우 부모의 관심이 필요합니다.
  - P2P는 성인인증을 하지 않고도 각종 음란물을 접할 수 있습니다.



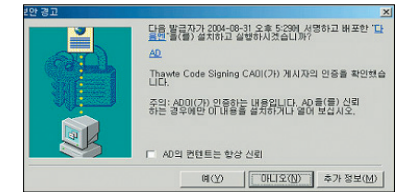


## 4. 자동 설치 프로그램의 위험



### 자동 설치 프로그램이란

인터넷 이용, 이메일 수신 등을 통하여 사용자의 동의 없이 설치되는 프로그램입니다.



### 피해 내용

- 컴퓨터 바이러스, 스파이웨어, 악성 봇 등 각종 악성 프로그램이 자동 설치 프로그램 형태로 배포될 수 있습니다.

### 대응 방법

- 인터넷 사용 중 소프트웨어의 설치 여부를 물어보는 '보안경고창'이 뜨는 경우
  - 믿을 수 있는 웹사이트에서만 '예'를 선택하고
  - 믿을 수 없을 경우 '아니오'를 선택하고 웹사이트에서 빠져 나옵니다.
- 사용자 동의 없이 바탕화면에 생성되는 아이콘을 방지합니다.
  - (인터넷 익스플로러) 메뉴의 [도구] → [인터넷 옵션] → [보안] → 웹 콘텐츠 영역으로 [인터넷] → [사용자 지정 수준] → [바탕 화면 항목 설치] → [설치 안함] 선택 → [확인]

※ 특정 웹사이트의 바탕화면 아이콘 생성을 허락하고자 할 때에는 해당 웹사이트를 신뢰 할 수 있는 웹사이트로 등록합니다.

### 삭제 방법

- 해당 웹사이트의 상·하단에 프로그램 삭제에 관한 설명을 찾아봅니다.
- 인터넷 검색을 통하여 해당 프로그램 삭제 방법을 찾아봅니다.
- 백신프로그램을 이용하여 삭제합니다.
- 치료가 되지 않으면 운영체제 프로그램을 다시 설치합니다.

## 5. 스팸 차단 방법



### 스팸이란

이메일, 휴대폰 등을 이용하여 대량으로 전송되는 불법 정보입니다.

### 피해 내용

- 스팸 처리로 인한 시간 낭비와 음란성 광고메일로 인한 정신적 피해가 발생합니다.

### 예방·대응 방법

- 이메일
  - 광고 등 불필요한 메일은 읽어보거나 응답하지 않고 삭제합니다.
  - 인터넷 게시판 등에 이메일 주소를 남기지 않습니다.
  - 미성년자는 포털 이용 시 청소년 전용계정을 사용합니다.
  - 웹사이트 회원가입 시 광고메일 수신 여부는 신중히 결정합니다.
  - 회원으로 가입한 특정 웹사이트의 메일을 더 이상 받고 싶지 않다면 해당 홈페이지에서 '메일 수신거부'를 설정합니다.
  - 이메일 프로그램·서비스업체의 스팸 차단 기능을 사용합니다.

※ 프로그램, 업체별로 설정방법이 다르므로 도움말 등을 참조합니다.

### 휴대폰

- 스팸전화로 의심되는 경우 응답전화를 하지 않고 무시합니다.

※ 스팸전화번호는 060국번으로 시작되는 경우가 많습니다.

- 웹사이트 회원가입 시 불필요한 전화광고 수신에 동의하지 않습니다.
- 음란사이트, 인터넷 게시판 등에 휴대폰 번호를 남기지 않습니다.
- 이동통신사에 스팸 차단 서비스를 신청합니다.

※ 이동통신사 고객센터(휴대폰으로 국번없이 114)로 신청(무료)

- 휴대폰 사용설명서를 확인하여 스팸차단 기능을 설정합니다.

### ■ 윈도우XP 팝업(경고창)

- 바탕화면 [내컴퓨터]에서 오른쪽 마우스를 클릭 → [관리] → [컴퓨터관리] → [서비스 및 응용프로그램] → [서비스] → [메신저(Messenger)] → [시작유형]을 '사용 안함' → [확인]

상담·신고 한국정보보호진흥원 불법스팸대응센터 ☎ 1336, <http://www.spamcop.or.kr>



## 6. 안전한 비밀번호 보호방법



### 비밀번호란

인터넷 사이트 이용, 금융거래, 컴퓨터 로그인 등에 본인확인을 위해 사용되는 정보입니다.

### 피해 내용

- 다른 사람이 비밀번호를 알게 될 경우 금전 피해, 정보 유출 및 사기 등 불법행위에 사용될 수 있습니다.

### 설정 방법

- 다른 사람이 추측할 수 없도록 숫자·특수문자를 섞어 8자 이상으로 구성합니다.  
(예 : 10H+20Min, !!Can&9lt)
- 본인·가족의 이름, 생일, 주민등록번호 등은 사용하지 않습니다.
- 익숙한 명칭·제목·속담 등을 활용하여 기억하기 쉽게 합니다.

※ “행복주식회사” → 홀수 번째 글자 : “행주회” → 영문입력 : “Godwnghl”  
 ※ “This May Be One Way To Remember” → 단어 첫째 문자 : “TmB1w2R”  
 ※ “백설공주와 일곱 난장이” → “백설+7난장” → 영문입력 : “QorTjt+7SksWkd”

- 비밀번호는 웹사이트별로 다르게 설정합니다.
- 기본 비밀번호에 웹사이트별 규칙을 추가하여 비밀번호로 사용합니다.
- 금융거래에 사용하는 비밀번호는 일반 비밀번호와 다르게 설정합니다.

※ 기본 비밀번호 “486\*+”에 웹사이트 이름의 짝수 번째 문자 추가  
 (yahoo.com : “486\*+ao.o”, google.co.kr : “486\*+tgeo.r”)

### 관리 방법

- 비밀번호가 타인에게 노출되지 않도록 합니다.
- ※ 기록이 불가피하다면 본인이 휴대하거나 안전하게 보관합니다.
- 타인에게 비밀번호와 관련된 정보 및 힌트를 알려주지 않습니다.
- 비밀번호는 최소한 3개월마다 변경합니다.
- 비밀번호가 타인에게 노출되면 즉시 변경합니다.
- ※ 변경된 비밀번호는 이전 비밀번호와 연관성이 없어야 합니다.





안전한 전자상거래





## 1. 공인인증서의 중요성



### 공인인증서란

인터넷에서 상거래 또는 민원신청 시 신원확인을 위해 사용하는 디지털 증명서(디지털인감)로서 다음과 같이 사용됩니다.

- 전자상거래 : 인터넷쇼핑, 전자계약, 전자무역 등
- 인터넷금융 : 은행업무, 증권거래, 보험거래 등
- 전자민원 : 각종 민원서류 발급, 세금 납부 등 민원 신청

공인인증서를 사용하지 않으면 상거래나 계약 등에 있어 법적 효과가 인정되지 않아 분쟁 발생 시 대응이 곤란할 수 있습니다.

### 발급 방법

- ① 은행, 증권사, 우체국, 공인인증기관 등에 신분증을 지참하고 직접 방문하여 인증서 발급 신청서를 제출합니다.
- ② 방문한 기관에서 제공하는 설명서에 따라 인터넷에서 인증서 파일을 내려 받습니다.

### 안전한 사용 방법

- 공인인증서는 별도의 USB 메모리에 저장하여 사용합니다.
  - 공인인증서를 컴퓨터에 저장하면 다른 사람이 복사할 수 있고, 해킹·컴퓨터 바이러스 등의 공격발생 시 유출될 수 있습니다.
- 비밀번호는 추측이 어렵게 만들고 자주 변경해야 합니다.(37쪽 참고)

※ 해킹한 이메일·쇼핑몰 계정 비밀번호를 사용할 수 있으므로 이메일·쇼핑몰 계정 비밀번호와 다른 비밀번호를 사용합니다.

- 서비스를 이용하는 금융 사이트 등에서 제공하는 키보드해킹 방지 프로그램, 피싱 방지 프로그램 등을 설치합니다.
- 보안서버를 갖춘 안전한 웹사이트(웹브라우저 화면 우측 하단에 자물쇠 아이콘 이 보임을 이용합니다.
- 피싱방 등 여러 사람이 사용하는 컴퓨터에서는 공인인증서를 이용한 금융거래 등을 하지 않습니다.

## 2. 온라인 금융거래 시 주의 사항



### 피해 내용

- 온라인 금융거래 시 정보보호가 되지 않을 경우 의도하지 않은 예금 인출, 송금과 같은 금전적인 손해가 발생합니다.

### 안전한 온라인 금융거래 방법

- 금융기관 웹사이트 이용 시 제공되는 보안프로그램을 설치합니다.  
- 윈도우 자동 업데이트, 백신프로그램, 방화벽 등도 설치하여야 합니다.
- 보안카드, 비밀번호 등의 정보는 다른 사람이 볼 수 있는 곳에 기록하지 않고 알려 주지도 않습니다.
- 금융계좌, 공인인증서 등의 비밀번호는 일반 홈페이지 비밀번호와 다르게 설정 하고 자주 변경합니다.
- 금융기관 웹사이트는 유사 웹사이트가 많으므로 즐겨찾기를 이용하거나, 직접 정확한 주소를 입력하고 이용합니다.
- 전자금융거래 이용을 휴대폰으로 알려주는 은행서비스를 이용합니다.
- 공인인증서는 USB 메모리 등 이동식 저장매체에 저장합니다.
- 피시방 등 공용 컴퓨터에서는 금융거래를 하지 않습니다.
- 의심되는 이메일이나 게시판의 글은 열어보지 말고, 첨부파일은 읽기·저장하기 전에 백신프로그램으로 검사합니다.
- 선수금 입금 요구, 상식수준 이상의 대출 조건을 제시하는 경우 해당 금융회사에 사실 여부를 직접 확인합니다.

상담 · 신고 금융감독원 전자민원창구 ☎ [02]1332, <http://minwon.fss.or.kr>

범 죄 신고 경찰청 사이버테러대응센터 ☎ [02]3939-112, <http://www.netan.go.kr>



### 3. 온라인 쇼핑 시 주의 사항



#### 피해 내용

- 온라인 쇼핑 시 사기 등에 의한 금전적 피해가 발생할 수 있습니다.

#### 안전한 온라인 쇼핑 방법

- 사이버 안전을 위한 기본조치를 하는 웹사이트인지 확인합니다.
  - 웹사이트 주소가 'https'로 시작하거나 웹브라우저 화면 우측 하단 등에 자물쇠 (🔒)가 보이면 기본적인 안전 조치를 하는 웹사이트라고 판단할 수 있습니다.
  - 한국정보통신산업협회와 한국전자거래진흥원 인증마크를 획득한 온라인 쇼핑몰 인지 확인합니다.
- 웹사이트에서 실명확인이나 배송지 등 반드시 필요한 정보 외에 불필요하게 많은 개인정보를 요구하면 일단 의심합니다.
- 온라인 결제 화면, 이메일로 제공되는 거래내역, 영수증 등을 저장·출력해 두면, 분쟁 발생 시 증거 자료로 활용할 수 있습니다.
- 현금보다는 피해보상을 받을 수 있는 신용카드를 사용합니다.

#### 온라인 쇼핑 시 사기 예방 요령

- 신용카드 대신 현금거래를 유도하는 사람은 일단 의심합니다.
  - 급한 이유가 있어 싸게 파는 대신 현금거래를 요구하는 경우
- '특가 할인상품' 등 과장된 광고 이메일을 조심합니다.
- 게시판 등에 '쉽게 돈 버는 법' 등을 쓰는 사람은 조심합니다.
- 신뢰할 수 있는 쇼핑몰만 이용하고, 다음 사항을 확인합니다.
  - 거래조건(상품정보, 보증기간, 배송기간, 반품조건 등)
  - 회사정보(회사신뢰도, 매출실적, 약도, 주소, 연락처 등)
  - 게시판(고객게시판 유무, 배송지연, 항의 글 내용 등)
  - 해당 쇼핑몰·판매자 대상의 피해자 모임·카페
- 유명 쇼핑몰이더라도 개인 판매자는 주의가 필요합니다.
- 직거래가 불가하다면 아는 사람과 동행하여 공개된 장소에서 합니다.

상담·신고 한국소비자원 ☎ (02) 3460-3000, <http://www.kca.go.kr>

범 죄 신고 경찰청 사이버테러대응센터 ☎ (02) 3939-112, <http://www.netan.go.kr>

III. 안전한 전자상거래 46 | 47





## 5. 전화사기(보이스 피싱) 대응 방법



### 피해 내용

■ 전화로 유명기관·인물을 사칭하여 사기를 벌이는 행위입니다.

- 수법
- 수업 등 자녀와 연락되지 않는 시간에 납치되었다고 부모에게 연락
  - 경찰을 사칭하여 범죄확인을 위한 개인정보 및 금융정보 확인
  - 세금 등을 환불해준다고 전화하여 현금지급기 조작을 요구

### 예방 방법

- 주위의 노인 분들에게 전화사기에 속지 않도록 말씀드립니다.
- 가족의 친구나 선생님 등의 비상연락망을 확보합니다.
- 동창회, 종친회 웹사이트에 주소록 등 연락처를 게시하지 않습니다.
- 동창생·친척이라고 하면서 입금 요구 시 반드시 사실관계를 확인합니다.
- 은행계좌, 신용카드, 주민등록번호 등을 알려주지 않습니다.

※ 금융기관, 공공기관, 경찰서 등에서는 개인·금융 정보를 전화·이메일·메신저·전화자동응답시스템(ARS) 등으로 물어보지 않습니다.  
※ 게시판 등에 전화번호, 계좌번호 등의 정보를 게시하지 않습니다.

- 세금·보험료·등록금 등을 환불하여 준다는 전화에 속지 않습니다.

※ 금융기관, 경찰서, 공공기관 등은 현금지급기로 환불하지 않습니다.

- 전화사기는 추적을 피하기 위해 발신자 표시가 없거나 국제전화번호를 사용하는 경우가 많으므로 이상한 발신자 번호는 주의합니다.
- 전자금융거래 이용을 휴대폰으로 알려주는 은행서비스를 이용합니다.

### 대응 방법

- 전화사기 발생 즉시 은행에 신고하여 돈이 인출되지 않도록 합니다.
- 신분증 분실 시 금융감독원이나 거래 은행·카드사에 본인확인 강화를 요청합니다.

상당·신고	개인정보침해신고센터 ☎ 국번없이 1336, <a href="http://www.1336.or.kr">http://www.1336.or.kr</a>
금융·신고	금융감독원 ☎ (02) 3786-8576, <a href="http://minwon.fss.or.kr">http://minwon.fss.or.kr</a> 거래 은행이나 카드사 등 금융기관
범·죄·신고	경찰청 ☎ 국번없이 1379, <a href="http://www.police.go.kr">http://www.police.go.kr</a> 검찰청 ☎ 국번없이 1301, <a href="http://www.spo.go.kr">http://www.spo.go.kr</a>



## 6. 안전한 온라인 게임



### 피해 내용

온라인 게임 이용자를 속여 아이디·비밀번호 등을 알아낸 후 캐릭터를 삭제하거나 게임 아이템을 가로채는 일이 많습니다. 또한, 욕설이나 음란 메시지를 보내거나 컴퓨터 바이러스에 감염시키는 경우가 많습니다.

- 수법**
- 게임 아이템을 복사해 줄 테니 바닥에 잠시 놓아두라고 한다.
  - 게임 캐릭터를 잠시 빌려달라며 아이디·비밀번호를 요구한다.
  - 게임 운영자를 사칭하며 개인정보를 요구한다.

### 대응 방법

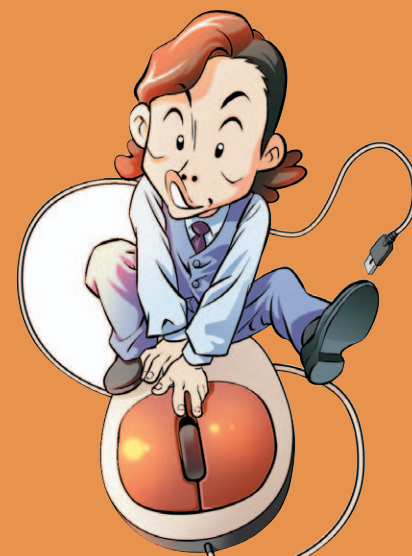
- 온라인 게임 운영자를 사칭하여 개인정보를 요구할 경우 거부합니다.
  - 실제 온라인 게임 운영자는 절대로 이용자의 개인정보(아이디·비밀번호 등)를 요구하지 않습니다.
  - 아이디·비밀번호 유출 시 게임 캐릭터 삭제나 아이템 탈취 등의 피해가 발생됩니다.
- 누군가 욕설이나 음란 메시지를 보낼 경우 대응하거나 직접 만나서 해결하지 않습니다.
  - 해당 메시지를 보낸 사람의 아이디와 메시지가 담긴 화면을 저장하거나 사진을 찍어 게임업체 고객센터로 신고합니다.
- 게임 머니와 아이템을 현금으로 구매하거나 다른 사람과 현금 거래를 하지 않습니다.
- 아이디와 비밀번호를 잊어버린 경우 이용하는 게임의 고객센터에서만 찾아볼 수 있으므로 고객센터에 방문하여 신고를 하거나 상담을 받습니다.
- 게임 중 컴퓨터에서 소리가 나지 않으면서 'Generic Host Process for Win32 Services' 관련 에러 메시지가 나타날 경우 바이러스에 감염되었을 수 있습니다.
  - 윈도우 보안 업데이트를 하고 백신프로그램으로 컴퓨터를 검사합니다.
  - 백신프로그램으로 치료가 되지 않을 경우 윈도우즈를 재설치합니다.

**범 죄 신고** 경찰청 사이버테러대응센터 ☎ (02)3939-112, <http://www.netan.go.kr>





## 개인정보 보호의 중요성



# 1. 인터넷상의 개인정보보호 방법



## 개인정보란

이름, 주민등록번호, 주소, 전화번호, 영상 등 개인에 관한 정보입니다.

## 피해 내용

- 개인정보가 노출될 경우에는 사기 등 범죄에 사용될 수 있습니다.

## 보호 방법

- 개인정보를 제공할 때는 개인정보취급방침과 약관을 자세히 확인합니다.
- 인터넷에 올리는 자료에 개인정보가 포함되지 않도록 하며, 공용폴더에 개인정보 파일이 저장되지 않도록 합니다.
- 아이디 · 비밀번호 · 주민등록번호 등은 다른 사람에게 알려주지 않습니다.
- 회원가입 시 주민등록번호 대체수단(아이핀 : i-PIN)을 이용하고, 반드시 필요하지 않은 개인정보는 입력하지 않습니다.
- 다른 사람이 자신의 주민등록번호를 이용한 회원가입 시 통지받을 수 있도록 '명의도용 확인서비스'를 신청합니다.
- 타인이 자신 명의로 회원가입 시 개인정보침해신고센터에 신고합니다.
- 인터넷에 개인정보 유출시 해당 웹사이트에 삭제를 요청하고, 삭제되지 않을 경우 개인정보침해신고센터에 신고합니다.

## 부모님이 알아두어야 할 유의사항

- 자녀가 방문한 홈페이지를 확인하고 아이디 · 비밀번호를 알아둡니다.
- 웹사이트에서 만14세 미만 어린이의 개인정보를 수집하기 위해서는 반드시 부모님의 동의를 받아야 합니다.
  - ① 자녀가 가입한 웹사이트의 개인정보취급방침 및 약관을 확인합니다.
  - ② 웹사이트가 자녀의 개인정보를 수집하도록 허락할지 결정합니다.
  - ③ 자녀가 제공한 개인정보를 확인하고, 필요하다면 회원탈퇴 혹은 개인정보 삭제를 요청합니다.

상담 · 신고	개인정보침해신고센터 ☎ 국번없이 1336, <a href="http://www.1336.or.kr">http://www.1336.or.kr</a>
범 죄 신고	검찰청 ☎ 국번없이 1301, <a href="http://www.spo.go.kr">http://www.spo.go.kr</a> 경찰청 사이버테러대응센터 ☎ 국번없이 (02)3939-112, <a href="http://www.netan.go.kr">www.netan.go.kr</a>



IV. 개인정보보호의 중요성 56 | 57

### 3. 개인정보 피해발생 시 신고·구제 절차



#### 개인정보침해신고센터

- 개인정보보호에 관한 문의사항이 있거나, 침해당한 경우에는 한국정보보호진흥원 개인정보침해신고센터에 상담 또는 피해구제를 신청할 수 있습니다.
- 접수된 내용에 대해서는 사실 확인을 거친 후, 법률위반 사업자에 대한 재발방지 조치, 관계기관에 위법사실 통보, 경제적·정신적 피해에 대한 구제조치 등을 시행하고 있습니다.
- 처리절차는 모두 무료이며, 홈페이지와 전화 등을 통하여 간편하게 민원을 신청하실 수 있습니다.

#### 상담 및 신고 사항

- 홈페이지 회원탈퇴 요청 시 처리 거부
- 개인정보의 훼손, 침해, 도용
- 본인 동의 없는 개인정보 수집
- 부모 동의 없는 자녀의 개인정보 수집
- 개인정보의 유출 및 제3자 제공
- 개인정보의 열람·정정 요구 시 불응

#### 상담 및 신고 방법

- 홈페이지 : <http://www.1336.or.kr>
- 이메일 : [privacy@kisa.or.kr](mailto:privacy@kisa.or.kr)
- 전 화 : 국번없이 1336
- 팩 스 : ☎ (02) 405-4729
- 우편·방문 : 서울특별시 송파구 중대로 135 IT벤처타워 서관 4층  
한국정보보호진흥원 개인정보침해신고센터



## 4. 주민등록번호 대신 아이핀 사용



## 아이핀(i-PIN : Internet Personal Identification Number)이란

인터넷 사용자들이 주민등록번호를 사용하지 않고도 본인확인을 할 수 있도록 만들어진 무료서비스입니다. 주민등록번호를 사용하지 않으므로 개인정보 침해로 인한 피해를 줄일 수 있습니다.

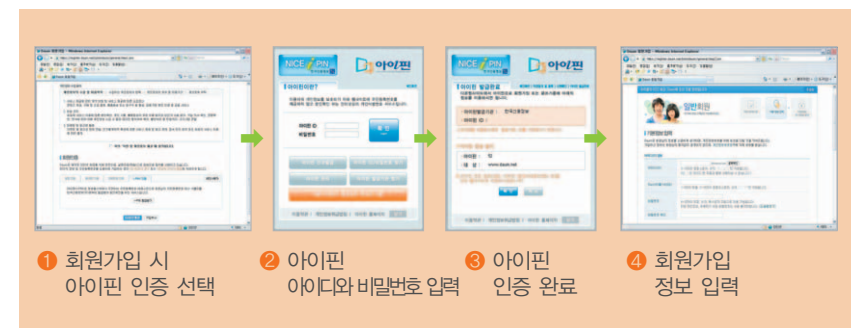
### 발급 방법

■ 다음 기관에서 아이핀을 발급 받습니다.

본인확인기관	서비스명	발급 사이트	연락처
행정안전부	공공 아이핀	<a href="http://www.gpin.go.kr">http://www.gpin.go.kr</a>	2100-3399
한국정보인증	원패스	<a href="http://www.signgate.com">http://www.signgate.com</a>	1577-8787
한국신용정보	나이스 아이핀	<a href="http://www.nuguya.com">http://www.nuguya.com</a>	1588-2486
한국신용평가정보	가상주민번호	<a href="http://www.vno.co.kr">http://www.vno.co.kr</a>	1600-1522
서울신용평가정보	Siren24 아이핀	<a href="http://www.siren24.com">http://www.siren24.com</a>	846-5000

### 사용 방법 (예 : 본인 확인 후 회원 가입)

■ 웹사이트에서 제공하는 본인확인방법 중 “아이핀 인증”을 선택하고, 아이핀 아이디와 비밀번호를 입력하여 본인확인을 받습니다.













## 1. 인터넷 에티켓의 중요성



### 인터넷 에티켓(네티켓)이란

네트워크(Network)와 에티켓(Etiquette)의 합성어로 인터넷 예절입니다. 네티켓을 지키지 않으면 경우에 따라서는 욕설 및 명예훼손으로 인한 법적처벌 및 손해배상책임을 질 수 있습니다.

### 이메일 네티켓

- 제목은 메일 내용을 함축하여 간략하게 쓰고, 본문은 읽기 편하게 요점만 작성합니다.
- 본인이 누구인지 분명하게 밝히고 행운의 편지, 스팸 등을 보내지 않습니다.
- 발송취소가 불가능하므로 내용 및 수신자는 정확하게 입력합니다.
- 흥분한 상태에서는 작성하지 않고 욕설 등을 하지 않습니다.
- 받은 메일은 보낸 사람의 허락 없이 다른 사람에게 전달하지 않습니다.
- 첨부 파일의 용량을 줄여 수신자가 쉽게 열어볼 수 있게 합니다.

### 대화방(채팅) 네티켓

- 직접 만나는 마음가짐으로 임하며 존칭(00님)을 사용합니다.
- 인사는 정중히 하고 자기 자신을 먼저 소개하고 대화에 참여합니다.
- 중간에 참여시 진행 중인 대화의 내용·분위기를 파악하고 참여합니다.
- 초보자를 무시하지 않으며 모르는 사항은 친절하게 가르쳐 줍니다.
- 같은 내용의 말을 한꺼번에 반복해서 작성하지 않습니다.
- 여러 사람과 동시에 대화할 때에는 상대방을 혼동하지 않습니다.
- 정치, 종교 등에 있어서 지극히 개인적인 주장은 자제합니다.

### 온라인 게임 네티켓

- 게이머도 일종의 스포츠맨이므로 스포츠맨십을 가집니다.
- 이겼을 때는 상대를 위로하고 졌을 때는 깨끗하게 인정합니다.
- 상대방에게 높임말을 사용하며 게임 중에 일방적으로 퇴장하지 않습니다.
- 게임에 너무 집착하지 않으며 단순한 오락으로 즐깁니다.



## 2. 악성 댓글의 위험과 대응 방법



### 악성 댓글이란

댓글은 한 게시물 바로 밑에 자신의 의견을 남기는 짧은 글입니다. 악성 댓글은 욕설, 비방, 유언비어 등을 내용으로 하는 댓글로서, 댓글의 상대방 뿐만 아니라 사회에 큰 피해를 줍니다.

〈악성 댓글의 유형 및 내용〉

유 형	내 용
욕설·비방(명예훼손)	특정인(연예인, 정치인 등) 또는 불특정 다수에게 나쁜 말을 하는 행위
도 배	같은 내용의 욕설이나 의미 없는 글들을 연속해서 게시하여 정상적인 의견 공유를 방해하는 것
성적 욕설	성에 대한 노골적인 표현으로 불쾌감과 수치심을 주는 것
유언비어	거짓을 인터넷상에 퍼뜨려 피해를 입히는 행위

### 예방 및 대응 방법

- 악성 댓글을 예방하기 위해서는 올바른 인터넷 언어를 사용합니다.
  - 이름·얼굴이 보이지 않는다고 욕설이나 비방을 하지 않습니다.

※ 내가 욕을 들었을 때 기분이 나쁘고 불쾌하다면 상대방도 나와 같은 기분일 것입니다.

- 주장은 사실과 논리적 사고에 의해서만 타당성을 인정받을 수 있습니다.

※ 자기주장에 집착하게 되면 욕설이나 비방을 하기 쉽습니다. 욕설과 비방은 호소력이 없으며, 자신의 인격만 욕되게 할 뿐입니다.

- 악성 댓글에 대해서는 욕설·비방 등으로 대응하지 않습니다.
  - 한두 명이 욕을 하고, 사람들이 따라 하기 시작하면 인터넷이 욕으로 가득 차게 될 것입니다.

### 악성 댓글에 대한 제재와 피해구제

- 악성 댓글 작성자에 대해서는 모욕, 명예훼손 등으로 법적 처벌과 손해배상책임이 부과될 수 있습니다.
- 피해자는 악성 댓글 작성자를 형사고소하거나 손해배상을 청구할 수 있습니다.

범 죄 신 고 경찰청 사이버테러대응센터 ☎ (02) 3939-112, [www.netan.go.kr](http://www.netan.go.kr)

### 3. 불법 · 청소년 유해정보 차단 방법



#### 불법 · 청소년 유해정보란

불법정보는 법률을 위반하여 개인 · 사회 · 국가적 이익을 침해하는 정보이며, 청소년 유해정보는 청소년에게 유해한 영향을 줄 수 있는 정보입니다.

#### 피해 내용

- 불법 · 청소년 유해정보를 자주 접하게 되면 건전한 정보생활을 할 수 없게 되며, 유해정보를 유포한 자는 법적 처벌됩니다.

유 형	내 용
불법정보	음란통신, 명예훼손 정보, 해킹 · 바이러스 정보, 청소년 유해 매체물 표시의무 위반 정보, 도박 등 사행행위 정보, 국가기밀 누설정보, 국가보안법 위반 정보, 범죄 관련 정보
청소년유해정보	신음소리, 괴성 등 음성, 음란 · 폭력 화상 및 동영상 또는 문자

#### 차단 방법

- 이메일을 통해 전달되는 청소년 유해 스팸은 차단 소프트웨어를 사용하여 차단합니다.  
- 다운로드 : 스팸체커(<http://spam.kiscom.or.kr>)
- 불법 · 청소년유해정보를 제공하는 웹사이트는 '내용 선별 소프트웨어'를 사용하여 차단합니다.  
- 상세 정보 : 인터넷내용등급서비스(<http://www.safenet.ne.kr>)

#### 신고 방법

- 인터넷119 홈페이지(<http://www.singo.or.kr>) → [신고] 메뉴 클릭 → 실명인증 → 이름과 연락처, 제목, 신고내용 등 필요 정보를 입력 → 증거자료 첨부

※ 인터넷119 홈페이지(<http://www.singo.or.kr>)에서 제공하는 '인터넷 파랑새' 프로그램을 이용하면 더욱 쉽게 신고할 수 있습니다.

상담 · 신고	인터넷119 ☎ 국번없이 1377, <a href="http://www.singo.or.kr">http://www.singo.or.kr</a>
범 죄 신고	경찰청 사이버테러대응센터 ☎ (02) 3939-112, <a href="http://www.netan.go.kr">http://www.netan.go.kr</a>



## 4. 사이버 성폭력 예방 및 대응 방법



### 사이버 성폭력이란

사이버 공간에서 상대방에게 성적인 괴롭힘을 주는 행위로서, 성과 관련된 언어폭력, 특정인의 성적 정보 공개, 스토킹, 음란물 전송 등이 해당됩니다. 사이버 성폭력으로 인해 피해자가 자살하는 등 큰 피해가 발생할 수 있으며, 가해자는 법적 처벌 및 손해배상책임을 지게 됩니다.

**사례** 2000년 인터넷 음란 사이트 자유게시판에 '남성 파트너 구함' 등의 글이 특정 여성의 연락처와 함께 게재되었습니다. 개인 정보가 도용된 해당 여성은 남성들의 메일과 전화공세에 시달리는 피해를 당했습니다.

### 사이버 성폭력 예방 및 대응

- 사이버 성폭력의 대상이 되는 여성 아이디를 사용하지 않습니다.
- 비밀번호는 추측이 어렵게 만들고 자주 변경해야 합니다.(37쪽 참고)
- 개인정보는 '최소한의 것만 기입'하거나 '비공개'로 합니다.
- 상대방이 불쾌한 행동을 한다면 대화를 즉시 중단합니다.
  - 사이버 성폭력 시 반응을 보이면 상대방은 관심이 있다는 뜻으로 받아들일 수 있습니다.
- 원하지 않는 메일을 받았다면 답장을 보내지 않습니다.
- 온라인상에서 만난 사람을 직접 만나는 일은 신중해야 합니다.
  - 어디서 누구와 만나는지 주위 사람에게 알리고, 친구 등 다른 사람과 함께 공공 장소에서 만납니다.
- 부모님은 자녀들의 인터넷 사용에 관심을 기울입니다.
- 쪽지/메일 수신 거부, 특정 내용/발신기가 보낸 이메일 자동 삭제 등의 기능을 이용하여 성폭력을 예방합니다.
- 가해자는 주로 컴퓨터에 자신이 없고, 기술이 부족한 초보자를 대상으로 성폭력을 행사하므로 컴퓨터에 관한 기초 지식을 습득합니다.
- 성폭력 피해를 입거나 목격했을 때 즉시 인터넷119에 신고합니다.
  - 신고하지 않고 그냥 넘어가면 가해자는 계속해서 많은 사람들에게 피해를 입힐 수 있습니다.

**상담 · 신고** 인터넷119 ☎ 국번없이 1377, <http://www.singo.or.kr>

**범 죄 신고** 경찰청 사이버테러대응센터 ☎ (02) 3939-112 <http://www.netan.go.kr>

## 5. 컴퓨터 · 인터넷 중독 예방 및 치유 방법



### 컴퓨터 · 인터넷 중독이란

컴퓨터 · 인터넷의 과다 사용으로 일상생활의 장애가 유발되는 상태입니다. 컴퓨터 · 인터넷 중독이 심하면 다음과 같은 피해가 발생할 수 있습니다.

- 직장 또는 학교생활에 충실하지 못하고 다른 사람과 관계가 원만하지 않음
- 심한 경우 다른 사람에게 폭력을 휘두르거나 자살할 수 있음

**사례** 2007년 폭력 성향의 인터넷 게임에 중독된 중학생이 “공부는 안 하고 왜 집을 나갔느냐, 돈을 훔쳐 어디다 썼느냐?”며 꾸짖는 할머니를 찾김에 살해하는 사고가 발생했습니다.

### 인터넷 중독 예방법

#### 청 소 년

- 숙제 · 청소 등 할 일을 먼저 한 후에 컴퓨터를 사용합니다.
- 학습이나 숙제 수행을 위한 컴퓨터 활용을 늘립니다.
- 하루에 사용하는 컴퓨터 시간을 미리 정해 둡니다.
- 특별한 목적 없이 인터넷을 1시간 이상 사용하지 않습니다.
- 컴퓨터 사용시간과 내용을 컴퓨터 사용일지에 기록합니다.
- 인터넷을 하면서 식사나 군것질을 하지 않습니다.
- 인터넷 때문에 취침시간을 넘기지 않습니다.
- 인터넷 이외의 취미생활, 운동, 문화 활동을 즐깁니다.

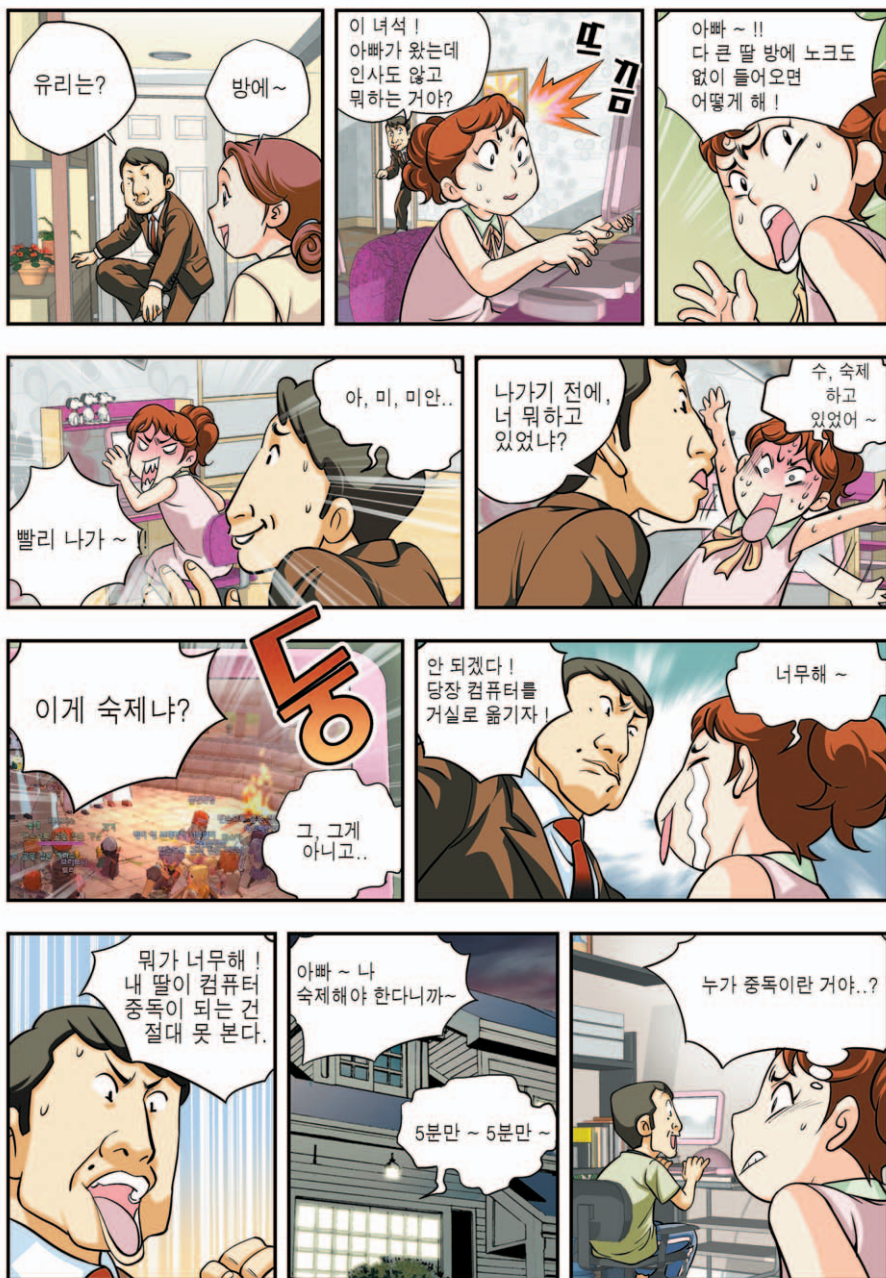
#### 부 모

- 컴퓨터는 거실 등 가족이 함께 사용하는 장소에 둡니다.
- 컴퓨터 사용은 강압적 통제보다는 자녀와 협의하여 결정합니다.
- 부모님도 컴퓨터 · 인터넷을 사용할 수 있도록 합니다.
- 자녀의 학습을 돕는 긍정적인 인터넷 사용을 격려합니다.
- 자녀가 운동, 문화 등의 취미 활동을 할 수 있도록 유도합니다.
- 자녀의 인터넷 사용에 대한 일관된 태도를 보여 줍니다.
- 필요시 컴퓨터 사용시간 관리 소프트웨어를 설치합니다.
- 자녀의 평소 생각이나 고민에 대해 관심을 보여 줍니다.
- 문제가 심각하면 전문상담기관의 도움을 받습니다.

**상 답** 인터넷중독예방상담센터 ☎ 1599-0075, <http://www.kado.or.kr/APC>  
(인터넷 중독 및 게임 중독 진단 서비스도 제공)



## 6. 가족의 건전한 정보생활 가이드



### 부모와 자녀가 함께 할 일

- 컴퓨터는 거실 등 개방된 장소에 두고 가족들이 함께 이용합니다.
- 인터넷에서 하는 활동에 대해 항상 대화하고 도움을 줍니다.
- 게임 아이템 거래, 인터넷을 통한 원조결제 등 컴퓨터와 인터넷 사용과 관련된 사회문제에 관심을 가집니다.
- 온라인 게임 이용시간 등 인터넷 사용 규칙을 정해서 이용하도록 합니다.

### 부모가 자녀를 위해 할 일

- 자녀가 가입한 웹사이트 · 인터넷카페와 아이디 · 비밀번호를 알아둡니다.
- 부모의 주민등록번호, 신용카드번호 및 기타 비밀번호를 자녀에게 알려주지 않습니다.
- 자녀에게 올바른 인터넷 사용방법, 네티켓 등을 알려주고 가족들의 컴퓨터 사용에 일관된 원칙을 적용합니다.
  - 인터넷 사용 시 이름, 주소, 학교 등 개인정보를 알려주지 않도록 합니다.
  - 부모의 허락 없이 인터넷을 통해 알게 된 사람을 직접 만나지 않도록 합니다.
  - 부모의 허락 없이 부가적인 요금을 내야 하는 정보나 게임 등을 이용하지 않도록 합니다.
  - 인터넷 게시판에 글을 쓸 때는 에티켓을 갖추도록 합니다.
  - 영화 · 음악 파일 등 다른 사람의 저작물을 인터넷에 올려 저작권을 침해하지 않도록 합니다.



## 1. 상담 및 신고 기관

항 목	상담 · 신고 기관
개인정보	개인정보침해신고센터(한국정보보호진흥원) ☎ 1336 <a href="http://www.1336.or.kr">http://www.1336.or.kr</a> ※ 범죄신고 : 경찰청 사이버테러대응센터 <a href="http://www.netan.go.kr">http://www.netan.go.kr</a>
스팸	불법스팸대응센터(한국정보보호진흥원) ☎ 1336 <a href="http://www.spamcop.or.kr">http://www.spamcop.or.kr</a>
공인인증서 (전자서명)	전자서명인증관리센터(한국정보보호진흥원) <a href="http://www.rootca.or.kr/kcac.html">http://www.rootca.or.kr/kcac.html</a> ※ 공인인증기관 한국정보인증(주) ☎ 1577-8787 <a href="http://www.signgate.com">http://www.signgate.com</a> (주)코스콤 ☎ 1577-7337 <a href="http://www.signkorea.com">http://www.signkorea.com</a> 금융결제원 ☎ 1577-5500 <a href="http://www.yessign.or.kr">http://www.yessign.or.kr</a> 한국전자인증(주) ☎ 1566-0566 <a href="http://www.crosscert.com">http://www.crosscert.com</a> 한국무역정보통신 ☎ 1566-2119 <a href="http://www.tradesign.net">http://www.tradesign.net</a>
해킹, 컴퓨터 바이러스	인터넷침해사고대응지원센터(한국정보보호진흥원) ☎ 118 <a href="http://www.krcert.or.kr">http://www.krcert.or.kr</a> ※ 범죄신고 : 경찰청 사이버테러대응센터 <a href="http://www.netan.go.kr">http://www.netan.go.kr</a>
피싱	인터넷침해사고대응지원센터(한국정보보호진흥원) ☎ 118 <a href="http://www.krcert.or.kr">http://www.krcert.or.kr</a> ※ 범죄신고 : 경찰청 사이버테러대응센터 <a href="http://www.netan.go.kr">http://www.netan.go.kr</a>
사기	금융감독원 전자민원창구 ☎ 02-1332 <a href="http://minwon.fss.or.kr">http://minwon.fss.or.kr</a> 한국소비자원 ☎ 02-3460-3000 <a href="http://www.kca.go.kr">http://www.kca.go.kr</a> ※ 범죄신고 : 경찰청 사이버테러대응센터 <a href="http://www.netan.go.kr">http://www.netan.go.kr</a>
사이버성폭력 · 명예훼손	방송통신심의위원회 명예훼손분쟁조정부 ☎ 1377 <a href="http://www.cyberhumanrights.or.kr">www.cyberhumanrights.or.kr</a> 한국성폭력상담소 ☎ 02-338-5801~2 <a href="http://www.sisters.or.kr">http://www.sisters.or.kr</a> 한국여성민우회 성폭력상담소 ☎ 02-739-8858 <a href="http://www.womenlink.or.kr">http://www.womenlink.or.kr</a> ※ 범죄신고 : 경찰청 사이버테러대응센터 <a href="http://www.netan.go.kr">http://www.netan.go.kr</a>
불법 · 청소년유해정보	방송통신심의위원회 불법 · 청소년유해정보 신고센터 ☎ 1377 <a href="http://www.internet119.or.kr">http://www.internet119.or.kr</a> 학부모정보감시단(청소년 유해정보) ☎ 02-706-4452 <a href="http://www.cyberparents.or.kr">www.cyberparents.or.kr</a> ※ 범죄신고 : 경찰청 사이버테러대응센터 <a href="http://www.netan.go.kr">http://www.netan.go.kr</a>
인터넷 중독	인터넷중독예방상담센터(한국정보문화진흥원) ☎ 1599-0075 <a href="http://www.kado.or.kr/iapc">http://www.kado.or.kr/iapc</a>

## 2. 알아두면 유용한 웹사이트

웹사이트	서비스 내용
보호나라 <a href="http://www.boho.or.kr">http://www.boho.or.kr</a>	해킹, 바이러스, 스팸, 개인정보 등 정보보호에 관한 종합적인 정보 제공
인터넷중독예방상담센터 <a href="https://www.kado.or.kr/iapc">https://www.kado.or.kr/iapc</a>	인터넷 중독 및 게임 중독의 상담 및 예방 서비스 제공
인터넷내용등급서비스(SafeNet) <a href="http://www.safenet.net">http://www.safenet.net</a>	등급 표시 정보 중에서 자기 수준에 맞는 정보를 선택할 수 있는 내용선별 프로그램 제공
장애인 정보화 교육사이트 <a href="https://able.kado.or.kr">https://able.kado.or.kr</a>	장애인을 위한 정보화교육과 컴퓨터 사용 관련 문제를 전화 및 온라인 상담 제공
배움나라 <a href="https://www.estudy.or.kr">https://www.estudy.or.kr</a>	전 국민 정보화교육을 위한 온라인 정보화교육 제공 (일반인, 시각장애인, 교사를 구분)
청소년권장사이트 아이틴넷 <a href="http://www.iteennet.or.kr">http://www.iteennet.or.kr</a>	청소년에게 건전하고 유익한 정보를 제공하는 사이트 정보 제공
어르신나라 <a href="https://www.aged.or.kr">https://www.aged.or.kr</a>	고령층을 위한 정보화교육, 어르신IT봉사단 운영 및 어르신 정보화 행사 개최
컴사랑 글사랑 <a href="https://www.ganada.or.kr">https://www.ganada.or.kr</a>	한글을 해독하지 못하는 성인과 여성결혼이민자에게 정보화 소양 교육 및 문자 교육 제공
국가지식포털 <a href="https://www.knowledge.go.kr">https://www.knowledge.go.kr</a>	각 기관별로 전산화된 국가지식 자료를 통합 검색하여 제공





### 3. 통신사별 스팸 대응 연락처

기관	연락처
KT	대상 : 060-700, 080, 1588, 1577, 0502 스팸차단 전화 : 국번없이 100 (일반전화), 080-2580-016, 018 (무료) 홈페이지 : <a href="http://www.kt.co.kr">http://www.kt.co.kr</a>
LG 데이콤	대상 : 0505, (0303), 1544, 080(850~869), 060-600 스팸차단 전화 : 1544-0001 (일반전화), 080-850-8572 (무료) 홈페이지 : <a href="http://www.dacom.net">http://www.dacom.net</a>
온세통신	대상 : 060-900, 080-(870~889) 스팸차단 전화 : 1688-1000, 1688-2000 (일반전화) (유료) / 083-100 (무료) 홈페이지 : <a href="http://www.onse.net">http://www.onse.net</a>
SK브로드 밴드 (구 : 하나로텔레콤)	대상 : 060-700, 080, 1588, 1577, 0502 스팸차단 전화 : 국번없이 106 (일반전화), 080-8282-106 (무료) 홈페이지 : <a href="http://www.sk broadband.com">http://www.sk broadband.com</a>
SKT	대상 : 030, 060, SMS 스팸차단 전화 : 1566-0011 (일반전화) (유료) / 011-114(휴대폰) (무료) 홈페이지 : <a href="http://www.tworld.co.kr">http://www.tworld.co.kr</a>

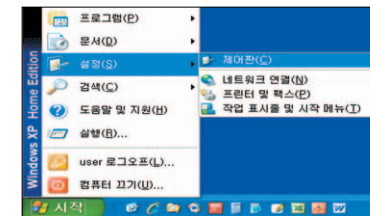
### 4. 컴퓨터 운영체제(윈도우XP) 보안설정 방법

#### 로그인 암호 설정

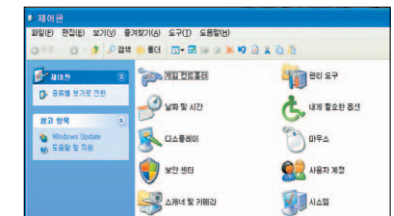
- 로그인 암호가 설정되지 않은 컴퓨터는 누구나 사용가능하므로 로그인 암호를 반드시 설정합니다.
- [시작] → [설정] → [제어판] → [사용자 계정] → 계정 선택 후 [암호 만들기] → 암호 · 힌트 입력 후 [암호 만들기] 클릭

※ 안전한 암호를 만드는 방법은 본문 37쪽을 참고하세요.

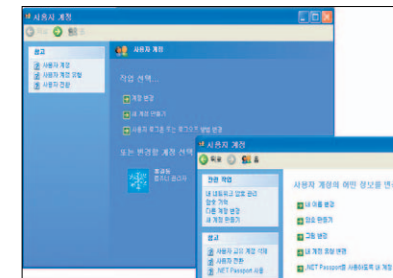
#### ① [시작] → [설정] → [제어판]



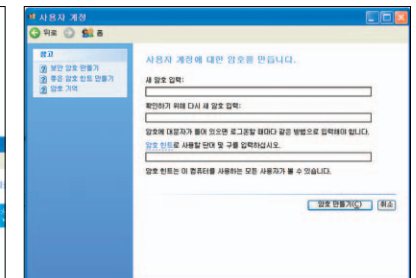
#### ② [사용자 계정]



#### ③ 사용하는 계정 → [암호 만들기]



#### ④ 정보 입력 후 [암호 만들기]

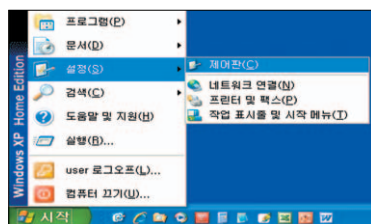




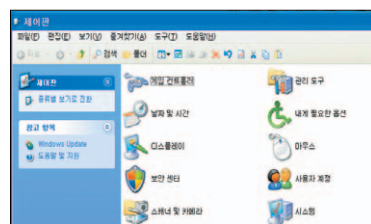
## Guest(손님) 계정은 사용하지 않음

- 해커는 Guest 계정을 통하여 시스템에 접근하는 경우가 많으므로 Guest 계정은 사용하지 않도록 설정합니다.
- [시작] → [설정] → [제어판] → [사용자 계정] → [Guest] → [Guest 계정 끄기]

① [시작] → [설정] → [제어판]



② [사용자 계정]



③ [Guest] 계정 선택



④ [Guest 계정 끄기]



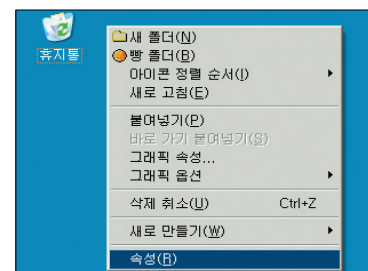
## 화면보호기 설정

- 자리를 비운 동안 다른 사람이 사용할 수 없도록 화면보호기를 설정합니다.
- [바탕화면] 마우스 오른쪽 버튼 클릭 → [속성] → [화면보호기] 선택 → [화면보호기] 종류 선택, [대기] 시간은 10분 정도로 설정, [다시 시작할 때 암호로 보호]를 체크 → [확인] 선택

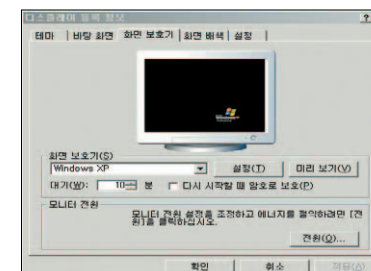
※ 서비스 팩3 이상에서는 [화면보호기] 선택 화면에서 [전원]버튼을 선택 → [전원 옵션 등록 정보] 화면에서 [고급]선택 → [컴퓨터가 대기 모드에서 나올 때 암호 묻기]를 체크 → [확인] 선택

※ 비밀번호는 윈도우 로그인에 사용하는 비밀번호와 동일합니다.

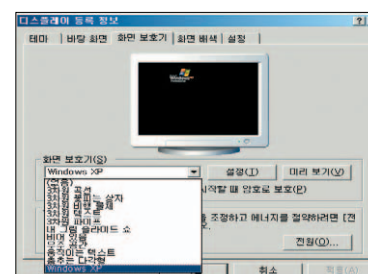
① [바탕화면]마우스오른쪽버튼→[속성]



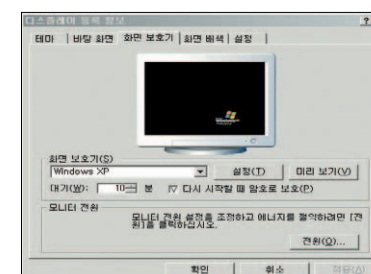
② [화면보호기] 선택



③ [화면보호기 종류], [대기] 시간 설정, [다시 시작할 때 암호로 보호] 체크 → [확인]



④ 서비스 팩3에선 [컴퓨터가 대기 모드에서 나올 때 암호 묻기] 체크 → [확인]







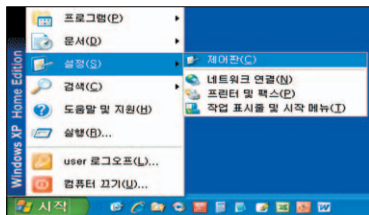
## 운영체제의 자동 업데이트 설정

- 새로운 운영체제 업데이트가 나왔는지 자동으로 확인하여 설치하는 '자동 업데이트 기능'을 설정합니다.
  - 자동 업데이트를 설정하면 보안 관련 업데이트도 자동으로 수행되므로 컴퓨터의 보안이 강화됩니다.
- 설정 : [시작] → [설정] → [제어판] → [성능 및 유지 관리] → [시스템] → [자동 업데이트]

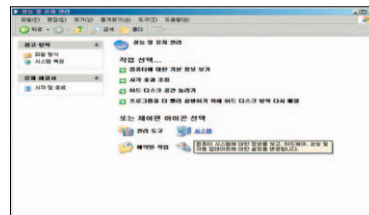
※ 업데이트 방법 중 “자동(권장)”을 권장하며 시간은 자신이 컴퓨터를 자주 사용하는 시간으로 설정합니다.

- 수행 : 업데이트 요청 메시지가 나타나면 업데이트 실시

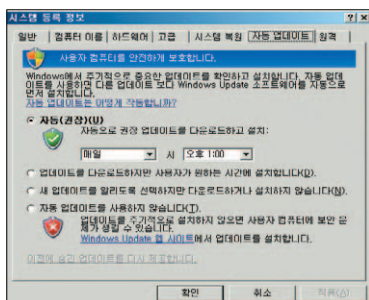
### ① [시작] → [설정] → [제어판]



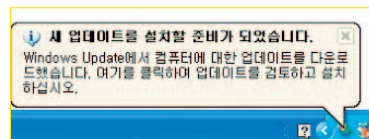
### ② [성능 및 유지 관리] → [시스템]



### ③ [자동 업데이트]



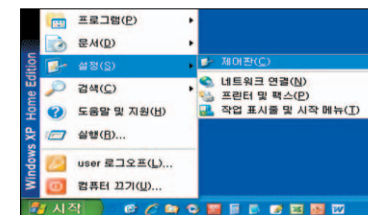
- ④ 컴퓨터 사용 중 화면 오른쪽 하단에 “새 업데이트 설치 준비” 메시지가 나타나면 아이콘을 더블클릭하여 업데이트합니다.



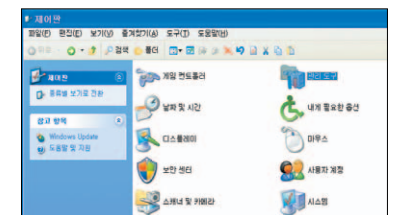
## 공유 폴더 관리

- 공유 폴더란 여러 대의 컴퓨터들이 자료를 네트워크를 통해 서로 주고받을 수 있도록 설정한 폴더를 말합니다.
  - 공유된 폴더는 해커의 주요 공격 대상이 되므로 반드시 필요한 경우만 공유하고, 자료의 공유가 끝나면 즉시 공유를 중지합니다.
- [시작] → [제어판] → [관리도구] → [컴퓨터 관리] → [시스템 도구] → [공유 폴더] → [공유]를 선택하여 공유 리스트 확인 → 공유 중지 대상을 마우스 오른쪽 버튼으로 클릭하여 [공유중지] 선택

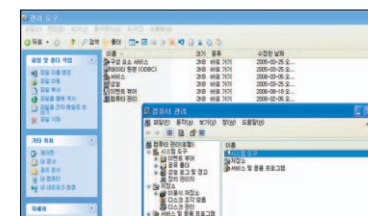
### ① [시작] → [설정] → [제어판]



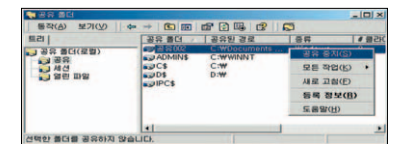
### ② [관리 도구]



### ③ [컴퓨터 관리] → [시스템 도구]



- ④ [공유 폴더] → [공유] → 공유 중지 대상을 마우스 오른쪽 버튼으로 클릭하여 [공유중지] 선택





### 레지스트리 수정과 공유문서 공유기능 해제

- [관리도구]에서 공유를 제거하더라도 컴퓨터를 다시 켜면 재공유가 되기 때문에 레지스트리 키를 수정합니다.

- ① [시작] → [실행] → “regedit”를 입력하고 [엔터] 키
- ② 왼쪽 창에서 KEY\_LOCAL\_MACHINE을 선택하여  
KEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\  
Serviceslanmanserver\parameters로 이동
- ③ 오른쪽 창에서 다음 항목을 더블클릭하여 설정 후 종료  
Value Name : AutoShareWks  
Type : REG\_DWORD  
Value : 0

- [컴퓨터\$]의 경우는 제거가 되지 않으므로 널(Null) 세션을 제거하는 방법을 이용합니다.

- ① [시작] → [실행] → “regedit”를 입력하고 [엔터]
- ② 왼쪽 창에서 KEY\_LOCAL\_MACHINE을 선택하여  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\  
LSA로 이동
- ③ 오른쪽 창에서 다음 항목을 더블클릭하여 설정 후 종료  
Value Name : RestrictAnonymous  
Data Type : REG\_DWORD  
Value : 1  
※ 기본값은 0 으로 되어 있으며, 1로 변경

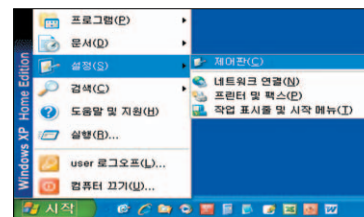
- 윈도우XP 는 기본적으로 “공유문서(ShardDocs)” 폴더에 공유 기능을 부여하고 있으므로 공유기능을 해제하여야 합니다.

[탐색기] → [내 컴퓨터] → [공유문서] → 마우스 오른쪽 버튼 클릭 후  
[속성] 선택 → [공유] 에서 네트워크 공유가 되지 않도록 해제

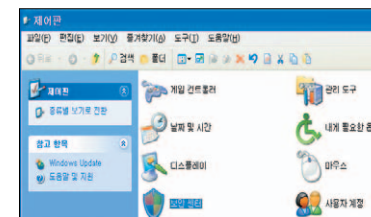
### 윈도우즈 방화벽 설치

- 외부에서 네트워크를 통하여 사용자 컴퓨터로 들어오는 것을 제한하여 컴퓨터를 보호할 수 있도록 윈도우즈 방화벽을 설정합니다.
- [시작] → [설정] → [제어판] → [보안센터] → [Windows 방화벽] → [일반]에서 ‘사용(권장)’을 선택 → [확인]

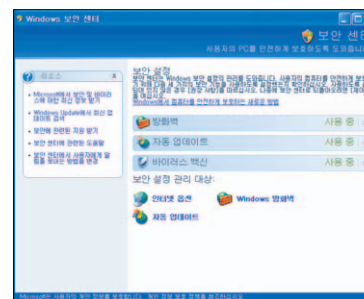
① [시작] → [설정] → [제어판]



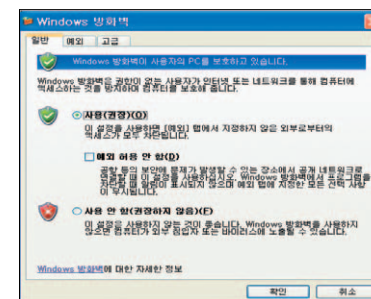
② [보안 센터]



③ [Windows 방화벽]



④ [일반] ‘사용(권장)’ 선택 → [확인]





- 발행처      행정안전부 <http://www.mopas.go.kr>  
                한국정보보호진흥원 <http://www.kisa.or.kr>
- 발행부      행정안전부 정보보호정책과 | (02)2100-3634
- 편    집      박    영    우
- 만    화      박    영    민
- 디자인 인쇄    신생보훈복지인쇄조합 | (02)2269-0127