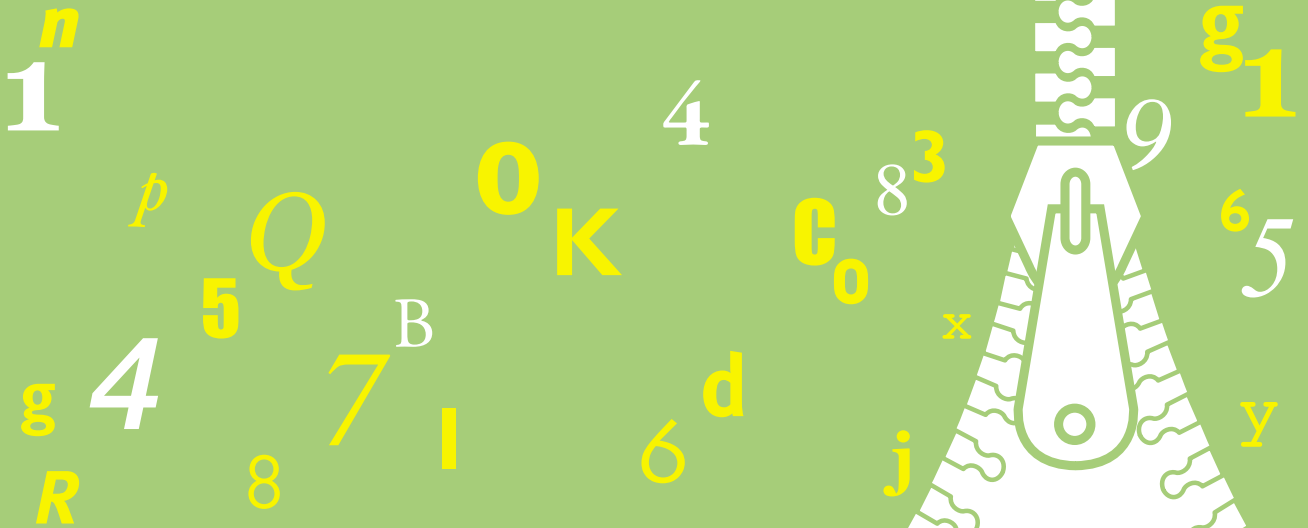


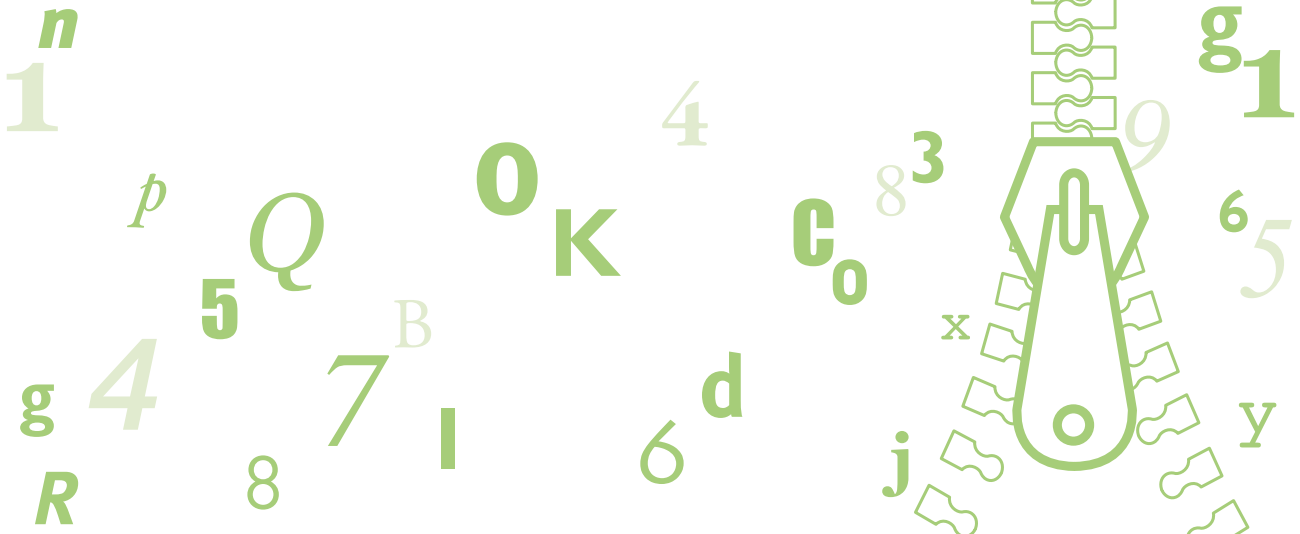
안전한 정보생활을 위한 정보보호 길라잡이

정보보호 가이드북



안전한 정보생활을 위한 정보보호 길라잡이

정보보호 가이드 북







차례




1장 정보보호, 이제는 더 미룰 수 없다! 4

- 1. 인터넷의 안전벨트 ‘정보보호’ 4
- 2. ‘아뭏사’ 할 때는 늦다! 5
- 3. 작은 실천과 습관이 중요 6


2장 정보보호의 첫걸음, 안전한 PC 만들기 8

- 1. 인터넷 익스플로러의 보안 설정을 찾아라 8
 -  쿠키를 막아라 9
 -  ‘자동 완성’ 만 믿으면 안 돼요! 10
 -  ‘내용 관리자’ 를 매만지자 11
- 2. 업데이트하는 것만으로도 PC가 안전해진다! 13
 -  윈도우만 업데이트하면 보안이 저절로! 13

3장 PC를 죽이고 살리는 바이러스와 백신 들여다보기 15

- 1. PC를 위협하는 바이러스 죽이기 15
 - 바이러스, 속 좀 보자 16
 - 바이러스는 어디에서 와서 어떻게 퍼질까? 18
 - 이렇게 하면 자유롭다, “바이러스 꿈짜 마!” 18
- 2. 백신 프로그램 설치하기 19
 -  공개용 백신 프로그램 공짜로 구하자 20
- 3. 바이러스 검사·치료, 인터넷으로 끝낸다고? 22
 -  바이러스 검사, 치료가 공짜! 22
- 4. 개인 정보를 가져가는 스파이웨어를 잡아라 24
 -  Ad-aware로 스파이웨어를 밀어내자 24

4장 한 번 책임지면 영원히 지켜주는 ‘방화벽’ 26

- 1. 방화벽 프로그램으로 PC 보호 출발! 26
 -  방화벽 만들어 꼭꼭 숨겨라 27

5장 백업보다 안전한 게 있을까? 30

1. PC 안의 데이터, 백업으로 안전하게! 30

따라하기 😊 올 테면 오라지! '데이터 백업'으로 정보보호 30

6장 아하, 그렇구나! 이메일 관리 33

1. 아웃룩 익스프레스에서 스팸메일을 받았을 때 33

따라하기 😊 스팸메일을 골라내자 33

2. 웹 메일에서 스팸메일을 받았을 때 35

3. 어딜 들어와? 스팸광고에 수갑을 채우자 36

따라하기 😊 광고 메시지, 필요한 것만 골라받자 37

7장 안전하고 편한 전자상거래 길들이기 38

1. 금융거래, 이렇게 좋을 수가! 38

인터넷뱅킹 얼마나 안전할까? 38

공인인증서 어떻게 이용할까? 39

2. 이것만은 알아두자! 인터넷뱅킹 40

3. 알면 즐겁다! 인터넷쇼핑 41

8장 공공장소에서의 정보보호도 문제없다 42

1. PC방, 사무실, 학교 전산실 PC를 마음껏 쓰자 42

9장 위험할 때 불러주세요! 사이버 도우미 44

1. 사이버 범죄 피해 유형은? 44

오~ 무섭다! 컴퓨터 해킹과 바이러스 44

전자상거래에서 일어나는 사이버 범죄 44

지적재산권 침해 수준 "와, 놀랍다" 44

인터넷에서의 사이버 폭력 45

2. 사이버 범죄 어떻게 대처할까? 45

3. 사이버 도우미 제대로 활용하기 45

정부 및 공공기관에 도움을 요청하자 45

백신 프로그램 회사라서 더더욱 안심! 46

방화벽과 보안 컨설팅 회사에 SOS를 하자 46

민간 도우미에게 도움을 요청하자 46



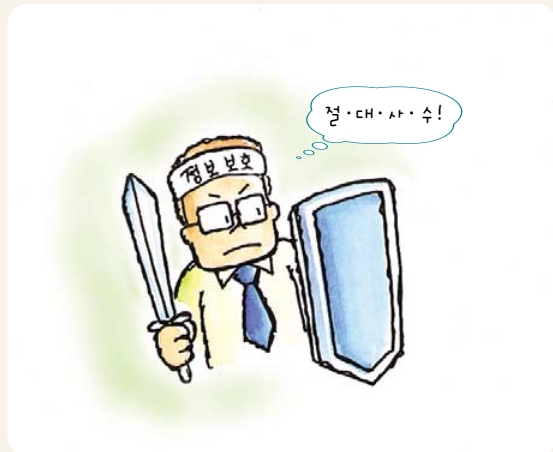
정보보호, 이제는 더 미룰 수 없다!

1 인터넷의 안전벨트 ‘정보보호’

2003년 1월 25일 토요일 오후, 3시간 동안 인터넷 접속이 되지 않았습니다. 어느 한 곳만이 아니라 우리나라 전체에서 인터넷이 ‘떡통’이 되어버렸습니다. ‘정보통신 강국’ 대한민국의 대동맥이라고 할 수 있는 인터넷을 순식간에 마비시킨 이 사건은 말 그대로 ‘인터넷 대란’이었습니다. 그동안 쌓아온 정보통신 최강국의 자부심이 한순간에 무너졌습니다. 사건의 원인은 바로 웜이라는 작은 프로그램 하나였지만, 더 큰 원인은 정보보호에 소홀했던 우리들 모두에게 있었습니다.

우리나라는 세계 최고의 인터넷 환경과 이용률을 자랑하고 있습니다. 바야흐로 1가정 1PC 시대를 살아 가며, 대부분의 사람들이 인터넷을 생활화하고 있습니다. 인터넷 검색, 이메일(e-mail) 주고받기, 커뮤니티 참여 등 사회·문화적 활동부터 인터넷쇼핑, 홈뱅킹 등 다양한 경제 활동에 이르기까지 인터넷을 이용해 정보사회의 혜택을 누리고 있습니다.

그러나 정보통신의 혜택을 누리는 데만 익숙할 뿐 지켜야 할 의무를 너무도 소홀히 하고 있습니다. 정보보호를 가볍게 여겨 1.25 대란과 같은 개인과 기업, 국가적 손실을 초래하게 된 것입니다. 사람에게 더욱 편리한 승용차나 비행기가 한 번 사고가 나면 자전거보다 더 큰 화를 부르듯이, 편하고 좋은 만큼 인터넷이 가지고 있는 잠재적인 위험 또한 어떤 정보통신 매체보다 크고 무섭습니다. 바이러스나 해킹에 대한 예방 없이 PC와 인터넷을 이용하는 것은 안전벨트를 매지 않고 고속으로 달리는 승용차를 탄 것과 같습니다.

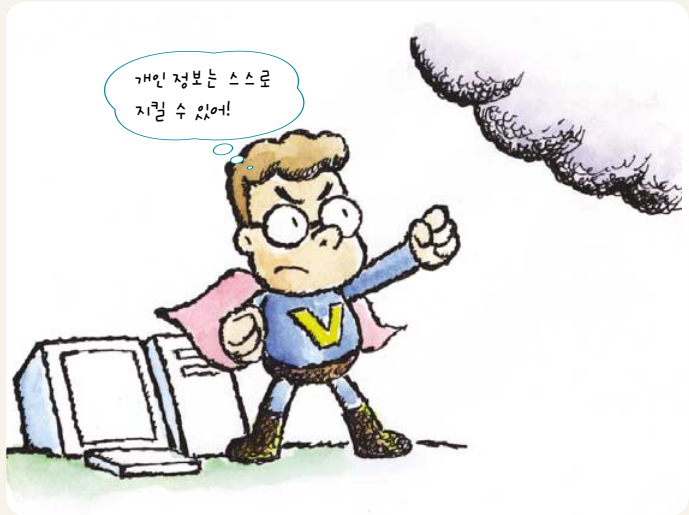


2 ‘아뽀싸’ 할 때는 늦다!

지식정보사회를 살아가는 현대인에게 정보보호는 이제 선택이 아니라 필수입니다. 정보보호에 대한 조치가 전혀 없다면, 돌이킬 수 없는 결과를 초래할 수 있습니다. 자신도 모르는 사이에 소중한 정보들이 유출될 수 있고, 이렇게 유출된 개인 정보는 타인에 의해 악용될 수 있습니다. 또한 바이러스에 의해서 개인의 소중한 자료가 파괴될 수도 있습니다. 이밖에도 정보보호를 소홀히 하였을 경우 사생활 침해, 유해정보 유포, 금융사고, 인터넷 불능 상태 등을 불러일으킬 수 있습니다. 한마디로 도둑에게 인방을 내주는 것과 같습니다.

정보보호란 작게는 개인용 PC에서 쓰는 아이디(ID)와 비밀번호(Password) 보호부터 크게는 기업의 중요한 계약 문서, 국가의 극비 외교 문서의 보호에 이르기까지 포괄적인 의미를 갖고 있습니다. 이러한 정보보호에 소홀히 대처할 경우 개인은 정보유출로 인한 프라이버시 침해와 명예훼손, 금전적인 손해를 볼 수 있고, 기업은 사업의 실패뿐 아니라 기업 자체의 패망을 겪을 수도 있습니다. 국가적으로는 국가의 명예에 먹칠을 하는 것은 물론, 국가 경쟁력을 저하시킬 수도 있습니다. 바로 ‘1.25 인터넷 대란’ 이 국가의 막대한 경제적 손실을 가져오고 명예를 실추한 대표적인 경우입니다.

정보보호에 대한 이해와 조치가 없는 상태에서는 개인과 기업, 나아가 국가에게 치명적인 손실을 입힐 수 있다는 점을 염두에 두고, 개인 정보보호 및 보안에 보다 더 힘써야겠습니다. 소 잃고 외양간 고치는 격이지만 이제라도 바이러스나 해킹 예방에 힘쓰면 안심하고 인터넷 생활을 즐길 수 있을테니까요.



3 작은 실천과 습관이 중요

그렇다면 정보보호를 위해서는 어떻게 해야 할까요? 대부분의 사람들은 정보보호는 어렵고 까다로운 것이라고 생각하고 미리 포기해버립니다. 그러나 정보보호는 우리가 일상적으로 편리하게 이용하는 PC와 인터넷의 일부분이며, 생활화되면 더없이 쉬운 것입니다. 문제는 정보보호가 얼마나 중요한 것인지, 그리고 꼭 필요한 것인지에 대한 이해가 부족하고, 특히 정보보호를 어떻게 해야 하는지 모른다는 데 있습니다.

정보보호를 위한 방법으로 대표적인 예는 PC에 백신 프로그램을 설치하는 것입니다. 우리가 흔히 인터넷과 PC를 사용하면서 얻은 자료와 정보를 바이러스로부터 지키는 것이 바로 백신 프로그램입니다. 혼자서 바이러스나 해킹을 막기 어려울 때는 사이버 도우미에게 SOS를 할 수 있습니다. 정보보호 관련 정부기관이나 정보보호 및 보안 전문회사들이 운영하는 사이버 도우미에게 정보보호에 대한 도움을 청하면 간단합니다.

정보보호를 위한 방법은 많이 있습니다. 그 중에서도 가장 중요한 것은 정보보호를 위한 작은 실천과 습관입니다.



'손쉬운 정보보호 실천수칙 8가지'

정보통신부

- ① 백신 프로그램 설치와 자동 검색, 자동 업데이트 설정하기
- ② 비밀번호는 영문과 숫자를 혼합해 8자리 이상으로 정하고 주기적으로 변경하기
- ③ PC 부팅, 윈도우 로그인, 네트워크 공유 폴더 이용할 때 비밀번호 설정하기
- ④ 일주일에 한 번은 윈도우 등 주요 소프트웨어의 보안 패치 설치하기
- ⑤ 정품 소프트웨어 사용하기
- ⑥ 보낸 사람이 불분명한 이메일은 절대로 열지 않기
- ⑦ 중요한 데이터의 백업(저장)을 생활화하기
- ⑧ 하루에 한 번 PC를 껐다 켜고, 쓰지 않을 때는 전원 끄기

정보보호는 이렇게!

정보보호의 생활화는 자신의 아이디나 비밀번호, 중요한 정보 등 개인 정보의 보호에서부터 기업의 중요한 계약 문서, 국가의 극비 외교 문서를 안전하게 지켜주며, 모두가 안심하고 편리하게 PC와 인터넷을 이용할 수 있게 합니다.



개인 PC 정보보호

- 인터넷 익스플로러 보안 설정하기 ▶ 8쪽
- 윈도우 및 소프트웨어 정기적으로 업데이트하기 ▶ 13쪽
- 정기적으로 자료 백업하기 ▶ 30쪽
- PC 부팅, 로그인, 폴더 공유 시 암호 설정하기
- PC 사용 후 전원 끄기



개인 신상 정보보호

- 방화벽 프로그램 설치하기 ▶ 26쪽
- 인터넷 서비스 제공업체 보안 서비스 이용하기 ▶ 35쪽
- 정기적으로 비밀번호 변경하기 ▶ 40쪽
- 8자리 이상의 비밀번호 사용하기

안전한 정보생활



바이러스로부터 정보보호

- 정품 소프트웨어 사용하기 ▶ 15쪽
- 백신 프로그램 설치하기 ▶ 19쪽
- 정기적으로 백신 프로그램 업데이트하기 ▶ 19쪽
- 온라인 바이러스 검사와 치료하기 ▶ 22쪽
- 개인 정보 빼가는 스파이웨어 제거하기 ▶ 24쪽
- 깨끗한 부팅 디스크 보관하기



해킹으로부터 정보보호

- 발신자가 확실한 이메일만 열기 ▶ 33쪽
- 금융거래 시 공인인증서 사용하기 ▶ 39쪽
- 이메일 보낼 때 전자서명 이용하기 ▶ 42쪽
- 공공장소에서 정보보호 수칙 준수하기 ▶ 42쪽
- 해킹, 정보침해, 불법적인 스팸메일 수신 시 사이버도우미에게 도움 요청하기 ▶ 45쪽



정보 보호의 첫걸음, 안전한 PC 만들기

PC와 인터넷 이용 시간이 많아지고, 정보공유가 활발해지면서 정보보호 및 보안이 점점 더 중요해지고 있습니다. PC와 인터넷을 무분별하게 사용하면 상상할 수 없을 만큼 치명적인 결과를 맞게 됩니다. 따라서 PC와 인터넷을 이용할 때는 정보보호를 위한 예방책을 세워야 합니다. 이러한 정보보호의 시작은 자신의 PC를 안전하게 쓸 수 있게 만드는 것입니다.

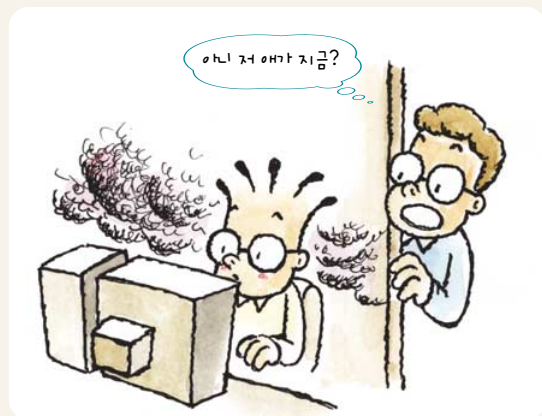
여기에서는 안전한 PC를 만들기 위해 인터넷 익스플로러(Internet Explorer, IE)의 정보보호 설정에 대해 살펴보고, 소프트웨어 업데이트를 통해서 무방비로 노출되어 있는 정보들을 최신 정보로 보완하는 방법에 대해 알아봅니다.

1 인터넷 익스플로러의 보안 설정을 찾아라

인터넷을 통한 정보공유와 활용은 생활의 편리함과 경제적인 이익을 가져다 줍니다. 하지만 인터넷에는 폭력적이고 선정적인 정보들 또한 그대로 노출되어 있습니다. 유해한 정보들과 불법적인 자료들이 우리 아이들을 물들이고 있습니다.

하지만 인터넷 익스플로러 보안 설정을 해놓고, 청소년 유해 정보, 폭력적 정보, 불필요한 스팸 정보 등을 미리 차단한다면 유해한 정보로부터 우리 모두를 보호할 수 있습니다.

여기에서는 인터넷 사용을 제한할 수 있는 방법에 대해 살펴보겠습니다. 우선 '쿠키 설정'으로 인터넷 익스플로러로부터 새어나갈 수 있는 정보의 보안 설정에 대해서 알아봅니다. 또 '자동 완성' 기능을 사용할 때 주의할 점, '내용 관리자'를 통해 불필요한 정보를 차단하는 방법에 대해 살펴봅시다.





쿠키를 막아라

Windows 98 ○ Me ○ 2000 ○ XP ○

쿠키(Cookie)란 인터넷을 이용할 때 입력한 아이디나 전화번호, 주소, 또는 이전에 입력한 정보들을 기억하고 있다가 같은 정보를 다시 입력할 때 자동으로 보여주는 사용정보들을 저장한 작은 크기의 파일입니다. 이런 편리하고 유용한 쿠키는 공동으로 PC를 사용할 경우, 개인 정보 유출에 심각한 피해를 입힐 수 있습니다.

다시 말해서 가정에서 공동으로 사용하는 PC나 여러 사람이 공용으로 사용하는 PC, 또한 PC방이나 공공장소에서 사용하는 PC의 경우 반드시 쿠키 설정을 하여 개인 정보 유출을 막아야 합니다. 꼭 주의하세요.

인터넷 익스플로러는 기본적으로 쿠키를 만들 수 있도록 설정되어 있습니다. 하지만 인터넷 보안 등록 정보를 수정하면, 쿠키를 만들기 전에 확인하도록 지정할 수 있습니다. 또한, 쿠키의 수신을 아예 거부할 수도 있습니다. 그러면 쿠키 삭제를 통한 보안 설정을 실습해 봅시다.

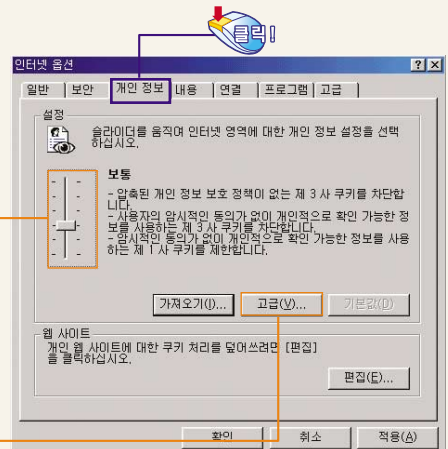


1 인터넷 익스플로러의 [도구] → [인터넷 옵션] 메뉴에서 [개인 정보] 탭을 클릭하면 쿠키에 대한 정보를 변경할 수 있습니다.

쿠키 등급을 설정하기 위해서는 슬라이드 바를 조정하여 보안 등급을 조정합니다.

쿠키를 사용하는 등급을 설정합니다. 아래로 내릴수록 보안 등급이 낮아집니다.

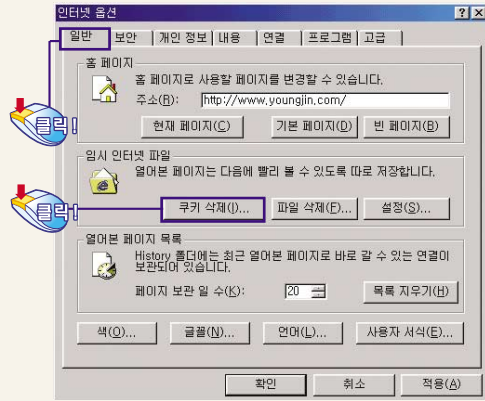
사용자가 직접 보안 등급을 설정할 수 있습니다.



▶ 개인 정보 쿠키 설정하기

2 쿠키를 삭제하려면 [도구] → [인터넷 옵션] 메뉴에서 [일반] 탭을 클릭하세요.

‘임시 인터넷 파일’란의 [쿠키 삭제] 버튼을 클릭하여 현재 저장되어 있는 모든 쿠키를 삭제합니다.



쿠키 삭제하기



회원가입 시 주의할 점

쿠키는 다양한 정보를 저장하는 데 유용하지만, 악의적으로 사용하면 사용자 PC의 정보나 개인 신상정보를 빼가는 것이 가능합니다. 때문에 가족의 생일이나 전화번호, 직장 정보와 같이 너무 많은 사용자 정보를 요구하는 웹 사이트에 가입할 때는 신중해야 합니다.



따라하기

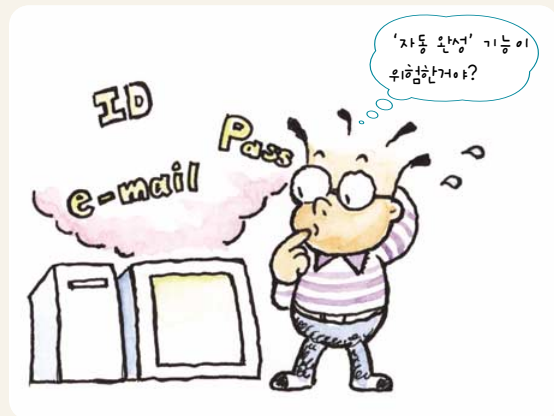
‘자동 완성’ 만 믿으면 안 돼요!

Windows 98 ○ Me ○ 2000 ○ XP ○

인터넷 익스플로러의 ‘자동 완성’ 기능은 웹 사이트의 주소, 사용자의 아이디와 비밀번호, 검색창의 검색 단어, 전화번호, 이메일 주소 등 웹 사이트의 정보를 저장하고 있다가, 사용자가 같은 정보를 다시 입력할 때 입력되어 있는 값들을 보여주고 그 중에서 원하는 값을 선택할 수 있도록 하는 기능입니다.

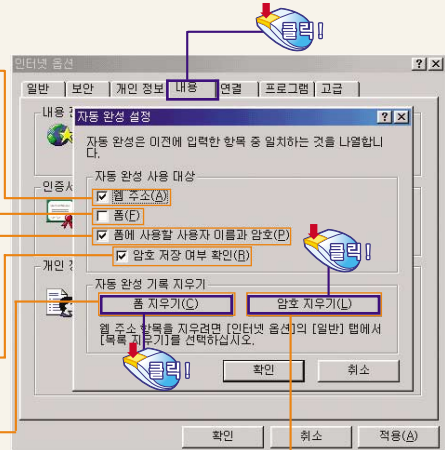
‘자동 완성’ 기능은 혼자 사용하는 PC에서는 매우 편리한 기능이지만, 가족이 함께 사용하거나 PC방과 같이 여러 사람이 공용으로 이용하는 PC에서는 정보가 유출될 위험이 매우 높은 기능입니다.

그럼 ‘자동 완성’의 정보 삭제 및 기능 해제 방법에 대해 살펴봅시다.



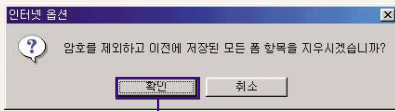
1 인터넷 익스플로러의 [도구] → [인터넷 옵션] 메뉴에서 [내용] 탭을 클릭하세요. ‘개인 정보’란에 있는 [자동 완성] 버튼을 클릭하면 자동 완성 항목을 설정할 수 있습니다. 또한 현재 저장되어 있는 아이디, 전화번호, 메일 주소 등의 정보와 비밀번호 같은 중요한 정보들도 모두 삭제할 수 있습니다.

- 익스플로러의 주소줄에 표시되는 웹 사이트 주소를 저장할 때 사용합니다.
- 방문했던 웹 사이트에서 사용한 사용자의 주소나 전화번호(아이디와 암호 이외의 정보)를 저장할 때 사용합니다(아이디와 암호는 ‘폼’의 선택으로 저장되지 않습니다).
- 방문했던 웹 사이트에서 사용한 아이디와 암호를 저장할 때 사용합니다.
- 현재 웹 사이트에서 사용한 아이디와 암호를 저장해도 되는지 확인합니다.
- 웹 사이트와 관련된 암호를 제외한 나머지 정보를 삭제할 때 사용합니다.
- 웹 사이트와 관련된 암호를 삭제할 때 사용합니다.

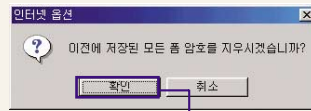


▶ ‘자동 완성’ 기능 설정하기

2 [폼 지우기] 버튼과 [암호 지우기] 버튼을 사용해서 모든 ‘자동 완성’ 정보를 삭제합니다.



▶ 폼 지우기



▶ 암호 지우기

▶▶▶ 따라하기

‘내용 관리자’를 매만지자

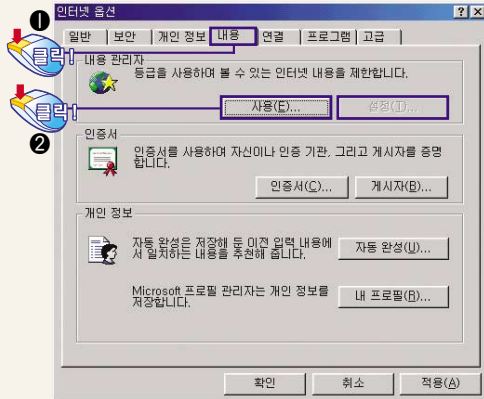
Windows 98 ○ Me ○ 2000 ○ XP ○

인터넷 익스플로러의 기능 중에 ‘내용 관리자’ 기능은 인터넷에서 볼 수 있는 내용을 제한할 수 있습니다. ‘내용 관리자’를 설정해두면 사용자가 지정한 기준에 맞는 등급의 웹 사이트만 보여줍니다. 따라서 음란물이나 폭력물 등 불필요한 정보들을 효과적으로 차단하고, 필요한 경우에만 볼 수 있도록 관리할 수 있습니다.

그럼 ‘내용 관리자’를 설정하여 불필요한 정보에 접근하지 못하도록 제한해 봅시다.

1 인터넷 익스플로러의 [도구] → [인터넷 옵션] 메뉴에서 [내용] 탭을 클릭한 후, [사용] 버튼을 클릭합니다.

이전에 '내용 관리자'를 사용하지 않았다면 [사용] 버튼을 클릭해서 새로 관리자를 시작하고, 이미 사용하고 있다면 [설정] 버튼을 클릭해서 이전의 설정 내용을 변경할 수 있습니다.



'내용 관리자' 설정하기 ▶

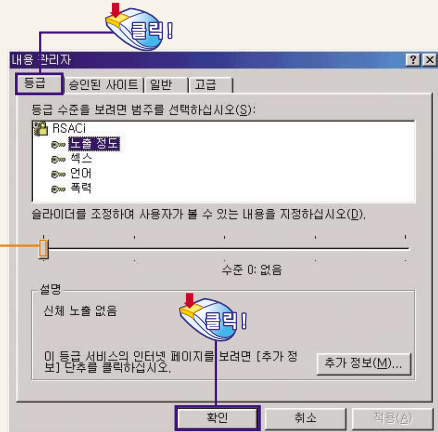
2 [내용 관리자] 대화상자가 나타나면 등급 서비스 를 제공하는 회사에서 정한 항목을 선택합니다. 슬라이더를 조정해서 사용자가 볼 수 있도록 내용을 조정합니다.

슬라이더



'내용 관리자'의 슬라이더 설정

'내용 관리자'의 수준 설정 시 슬라이더는 사용자가 볼 수 있는 정도를 설정합니다. 청소년일수록 슬라이더를 왼쪽으로 설정해 두어야 합니다.



▶ '내용 관리자' 등급 정하기



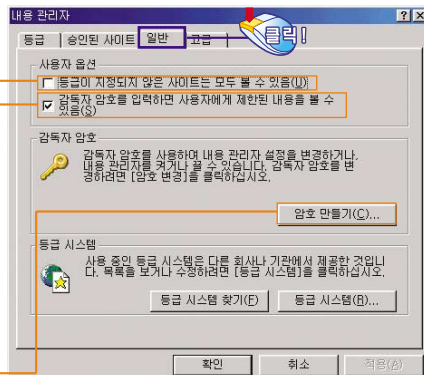
'내용 관리자'의 중요한 옵션

'내용 관리자'의 [일반] 탭에는 사용자가 지정할 수 있는 중요한 옵션이 3가지 있습니다.

선택하면 등급 시스템에 의해서 지정되지 않은 모든 웹 사이트를 표시합니다. 모든 웹 사이트가 등급 시스템에 등록되어 있는 것이 아니므로 등급이 지정되지 않은 일반 웹 사이트들을 보려면 반드시 선택합니다. 선택하지 않으면 국내외의 많은 일반 웹 사이트를 볼 수 없습니다.

부모가 등급이 제한된 웹 사이트를 아이들에게 일시적으로 보여줄 때 설정한 암호를 입력하면 해당 웹 사이트를 볼 수 있습니다.

제한이 걸린 등급의 웹 사이트를 일시적으로 보이게 하거나 '내용 관리자'의 설정을 변경하려고 할 때 사용할 암호를 지정합니다.



▶ '내용 관리자'의 중요한 옵션 설정하기

2 업데이트하는 것만으로도 PC가 안전해진다!

소프트웨어의 특성상 사용 중에 프로그램의 버그나 오류 등의 잘못된 부분, 또는 정보보호에서의 허점 등은 자주 발생합니다. 때문에 프로그램 제작사에서는 프로그램의 잘못된 부분을 고치도록 제작사의 홈페이지를 통해서 일종의 업그레이드된 소프트웨어를 제공합니다. 소프트웨어의 버그나 오류를 그대로 방치하면 이를 악용한 해킹(인터넷 등 여러 침입 가능한 경로를 통해서 발생하는 컴퓨터 침입 사고)이나 바이러스 등의 공격으로부터 피해를 입을 가능성이 매우 높습니다.

윈도우를 비롯하여 사용하고 있는 소프트웨어 제조업체 홈페이지를 수시로 방문하여 최소 일주일에 한 번은 업데이트를 하세요. 그럼 보다 안전한 PC를 만들기 위해서 필요한 윈도우 업데이트 방법에 대하여 살펴봅시다.




따라하기

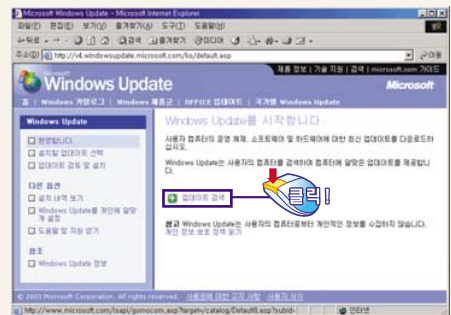
윈도우만 업데이트하면 보안이 저절로!

Windows 98 ○ Me ○ 2000 ○ XP ○

윈도우는 정기적으로 업데이트를 해주어야 합니다. 왜냐하면 업데이트를 통해 프로그램의 버그나 오류 등을 수정할 수 있을 뿐만 아니라, 정보보호를 위한 각종 문제점들을 패치하여 보완할 수 있기 때문입니다. 최소 일주일에 한 번은 업데이트 사이트를 방문하여 최신 버전으로 업그레이드하세요. 그럼 윈도우 업데이트하는 방법을 살펴봅시다.

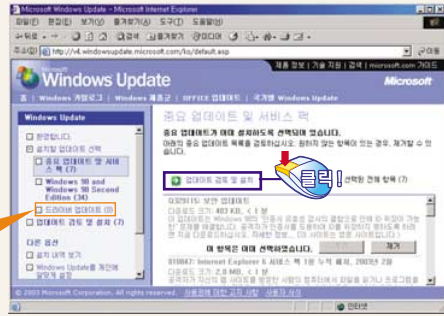
1 인터넷 익스플로러에서 windowsupdate.microsoft.com 사이트를 직접 방문하거나, 윈도우에서 [시작] 버튼을 누른 후 메뉴에서 [Windows Update]를 클릭합니다. '업데이트 검색'을 클릭해서 사용하는 PC의 업데이트가 있는지 검사합니다.

윈도우 업데이트 검색하기 



2 업데이트 검사가 끝나고 업데이트할 항목이 있으면 업데이트 항목이 나타납니다.

‘업데이트 검토 및 설치’를 클릭한 후 다음 웹 사이트에서 ‘지금 설치’를 클릭하여 업데이트를 시작합니다.



드라이버 업데이트 (0)

업데이트 검토 및 설치하기

3 업데이트가 완료되어 설치가 종료되면 메시지에 따라 시스템을 재부팅합니다. 시스템을 재부팅하면 업데이트된 항목들의 설치가 완료됩니다.

마이크로소프트 사의 메일 서비스에 가입하면 제품 소식을 비롯하여 최신 프로그램 다운로드 등 업데이트 및 기술 정보에 관련된 내용들을 이메일로 받아볼 수 있습니다(www.microsoft.com/korea/newsletter/guide).



드라이버 업데이트할 때 주의사항

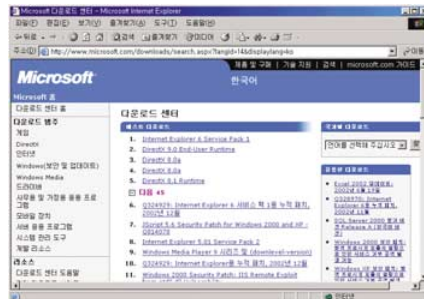
‘드라이버 업데이트’에 있는 설치된 드라이버들을 업데이트할 때는 주의해야 합니다. 디바이스 드라이버에 대해서는 업데이트 검사가 제대로 이루어지지 않아, 마이크로소프트사에서 제공하는 드라이버 버전이 현재 사용하고 있는 버전보다 낮은 버전임에도 불구하고 업데이트 항목에 선택되는 경우가 있습니다. 이러한 상황에서 업데이트를 진행하면 현재 사용하고 있는 장치와의 충돌로 인해 장치가 제대로 동작하지 않을 수 있습니다. 반드시 정확한 드라이버 버전을 확인하고 업데이트를 해야 합니다.



마이크로소프트 사의 다운로드 센터

www.microsoft.com/korea/download/default.asp 웹 사이트로 가면 마이크로소프트 사의 여러 가지 소프트웨어를 업데이트할 수 있습니다.

윈도우 이외의 백신 프로그램이나 워드프로세서 등 사용 중인 프로그램들도 해당 웹 사이트를 정기적으로 방문해서 반드시 업데이트하세요.

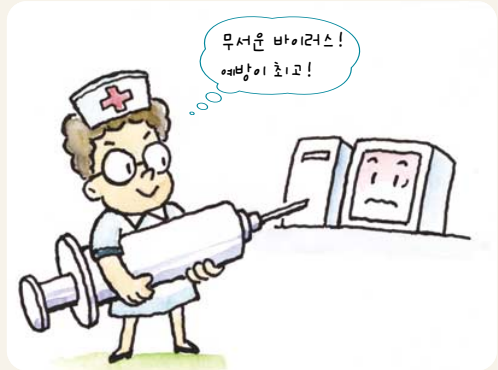


다운로드 센터



PC를 죽이고 살리는 바이러스와 백신 들여다보기

컴퓨터에 이상이 생기는 가장 큰 이유는 바이러스 때문입니다. 흔히 컴퓨터가 바이러스에 걸렸다고 말하는데, 어떻게 컴퓨터에 사람이 걸리는 감기 바이러스와 같은 것이 감염되는 걸까요? 사람은 몸이 약해지면 감기에 걸리기 쉽습니다. 컴퓨터를 사용하면서 정보보호와 보안의 경계심을 늦추면 컴퓨터도 바이러스에 감염되기 쉽습니다.



바이러스는 인터넷 사용을 할 때 무분별하게 데이터를 다운로드하거나 이메일을 사용하면서 걸리게 됩니다. 또 불법 소프트웨어에 침투해서 전파되기도 합니다. 플로피디스크나 인터넷으로 데이터를 공유할 때는 항상 실행하기 전에 백신 프로그램을 이용해 바이러스 검사를 해야 합니다. 그렇지 않은 상태에서 사용할 경우 바이러스에 감염될 수도 있습니다. 감염되면 데이터가 파괴될 수 있으며, 인터넷 접속 불능 상태에 빠져 개인과 기업에게 치명적인 손실을 가져올 수 있습니다.

이 장에서는 이러한 바이러스란 도대체 무엇이고, 바이러스 유형에는 어떤 것이 있으며, PC가 바이러스에 걸리지 않도록 대처하는 방법을 알아봅니다. 또한 바이러스에 감염되었을 때 백신 프로그램을 이용해서 바이러스를 치료하는 방법과 백신 프로그램을 최신 버전으로 업데이트하는 방법도 짚어보겠습니다. 마지막으로 소프트웨어에 포함되어 개인 정보를 마음대로 가져가는 스파이웨어를 완벽하게 삭제하는 방법을 꼼꼼히 살펴봅시다.

1 PC를 위협하는 바이러스 죽이기

컴퓨터 바이러스는 컴퓨터 작동에 피해를 주는 일종의 프로그램입니다. 프로그램의 실행 가능한 영역을 감염시키거나, 메모리에 머무르면서 파일을 감염시켜 프로그램이 실행되지 못하게 만듭니다. 대부분의 바이러스 프로그램들은 컴퓨터에 저장되어 있는 자료를 파괴하거나 자기 자신 또는 자신의 변형을 복사합니다. 일단 바이러스에 감염되면 PC의 실행 속도가 현저히 줄어듭니다. PC 속도가 눈에 띄게 저하되면 일단

바이러스에 감염된 것이 아닌지 의심해보고 점검해보아야 합니다.

그럼 바이러스의 종류에는 무엇이 있는지 알아보고, 바이러스에 걸리지 않기 위한 예방법에 대해 살펴봅시다.



1 | 바이러스, 속 좀 보자

자기복제 능력을 가지고 다른 컴퓨터와 파일로 전염되는 바이러스는 웜, 트로이목마, 일반 바이러스로 구분할 수 있습니다. 모두 악의적인 코드를 실행해서 자료나 PC의 손실을 가져옵니다. 각 바이러스의 특징은 다음과 같습니다.

1 웜

웜은 감염 대상이 정해져 있지 않고 불특정 다수를 목표로 활동하는, 자기복제가 가능한 프로그램을 말합니다. 특징은 빠른 전파 속도와 엄청난 자기복제 능력입니다. 특히 보안상 취약한 곳을 공격해서 자기복제를 하여 매우 짧은 시간에 많은 컴퓨터를 전염시킬 수 있습니다. 또한 네트워크를 통해서 복제본이 돌아다니기 때문에, 전체 네트워크의 용량 초과로 인터넷 접속 불가라는 부수적인 결과도 초래하게 됩니다.

2003년 1월 25일의 인터넷 대란도 수백 바이트 크기의 작은 인터넷 웜 때문에 전체 네트워크가 마비되었던 것입니다. 이 경우 개인이 사용하는 PC가 바이러스의 중간 경유지로 사용될 수 있기 때문에 개인 PC의 정보보호가 공공 PC에 대한 보안 못지 않게 중요합니다.



웜, 접근 불가

PC와 인터넷을 안전하게 사용하기 위해서는 사용자들이 정보보호에 관심과 노력을 기울여야 할 것입니다. 취약점이 있는 보안 사항들을 수시로 패치해야 하고, 백신 프로그램을 이용하여 바이러스를 자동 검색하며, 최신 버전으로 백신 프로그램을 업데이트해야 합니다. 또 PC나 서버 구성을 자신의 용도에 맞게 설정해주어야 합니다.



님다 바이러스

웜은 자기복제 능력은 있지만 다른 파일을 감염시키지는 않고 주로 이메일이나 인터넷을 통해서 특정 조건이 일치하는 다른 PC를 감염시킵니다. 2001년 9월에 발생한 님다 바이러스가 대표적인 웜입니다.

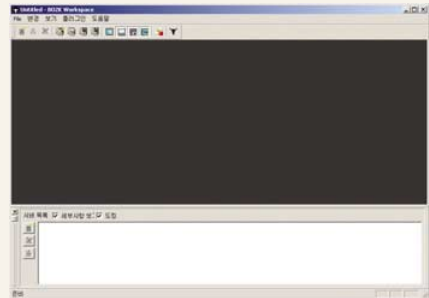
2 트로이목마

트로이목마는 자기복제 기능보다는 주로 해당 컴퓨터의 정보를 빼내거나 웬과 같은 악성 코드를 전염시키기 위한 매개체로 많이 이용되는 백 오리피스와 같은 유형의 프로그램입니다. 백 오리피스는 강력한 해킹 프로그램으로, 이메일의 첨부 파일 혹은 인터넷에서 유용한 프로그램인 것처럼 위장해서 사용자가 실행하는 순간 감염됩니다. 감염되면 컴퓨터에 침입해 사용자가 작업하는 모든 것을 감시하고 중요한 정보(신용카드 정보나 아이디, 은행 계좌번호와 비밀번호 등)를 훔쳐내서 개인에게 큰 해를 입힐 수 있습니다.

프로그램 설치 시 항상 주의하기

트로이목마는 일반적으로 '연말정산 계산 프로그램'과 같이 사람들이 한번쯤 실행하고 싶은 이름을 가지고 있어 방심하기 쉽습니다. 그 때문에 트로이목마라는 이름이 붙었습니다.

따라서 공개 소프트웨어를 사용할 때는 반드시 많이 알려진 웹 사이트에 접속해서 프로그램을 다운로드받는 것이 안전합니다. 개인이 운영하는 웹 사이트나 공공 게시판과 같이 보안이 취약한 곳에서 프로그램을 다운로드받는 것은 피하는 것이 좋습니다.



백 오리피스 2000



대표적인 트로이목마, 백 오리피스 2000

1999년 7월에 발견된 백 오리피스 2000이 대표적인 트로이목마입니다. 백 오리피스 2000은 그래픽이나 게임 또는 유틸리티와 같은 유용한 프로그램에 첨부된 형태로 전파되기 때문에 사용자에게 쉽게 설치될 수 있습니다. 원격지에서 감염된 컴퓨터의 모든 작업(파일 복사, 삭제, 키보드 입력 가로채기, 현재 화면 보기 등)이 가능하기 때문에, 사용자의 정보나 파일들이 쉽게 외부로 유출됩니다.

트로이목마에 감염되면!

- ① 접속한 시스템의 모든 파일을 실행할 수 있으며 읽고 쓰기도 가능합니다.
- ② 인터넷 익스플로러 등 임의의 프로그램을 실행시키거나, 현재 실행하고 있는 임의의 프로그램에 대한 실행 취소가 가능합니다.
- ③ 사용자가 입력하는 모든 키보드 입력을 가로채서 사용하는 은행 계좌의 아이디와 비밀번호를 알아내는 것은 물론이고, 보안카드의 비밀번호마저 쉽게 가로채서 저장한 후 지정된 장소로 보냅니다.
- ④ 현재 실행 중인 화면의 캡처도 가능해서 사용자가 무엇을 하고 있는지 확인할 수 있습니다.
- ⑤ 인터넷 웬과 같은 임의의 프로그램을 인스톨하고 실행해서 자신이 원하는 바이러스를 유포시킬 수 있습니다.



일반 바이러스

일반 바이러스는 웬, 트로이목마의 특성과는 달리 시스템에 직접적인 영향을 끼칩니다. Win32/YAI, Win32/Weird 바이러스는 파일을 삭제하며, CIH 바이러스는 바이오스(BIOS)를 파괴하여 PC를 전혀 사용할 수 없게 합니다. 또한, 마이크로소프트 사의 오피스 프로그램을 감염시키는 X97M_Morx와 같은 매크로 바이러스, 공유 폴더를 통해 악의적인 목적으로 유포되는 VBS/JumpBot도 일반 바이러스 범주에 포함됩니다.

하지만, 현재 많이 발견되는 바이러스는 웬과 트로이목마가 지닌 특징뿐만 아니라, 일반 바이러스가 지닌 특징도 복합적으로 포함하고 있기 때문에, 특별히 어떤 종류인지 분류하기가 어려운 것이 현재 바이러스의 추세입니다.

2 | 바이러스는 어디에서 와서 어떻게 퍼질까?

바이러스의 감염 경로는 다음과 같습니다.

❶ 이메일의 첨부 파일을 통해 바이러스에 감염됩니다.

일반적으로 사용자의 이목을 끌 만한 내용의 이메일 첨부 파일을 위장해서 사용자가 해당 파일을 실행하도록 만듭니다.

❷ 오래된 소프트웨어의 취약점을 이용해서 바이러스가 침투합니다.

최신 보안 패치가 적용되지 않은 시스템을 찾아 보안의 허점을 이용해 바이러스를 감염시킵니다.

❸ 관리 목적으로 공유된 폴더를 통해 바이러스에 감염됩니다.

주로 윈도우 NT, 윈도우 2000, 윈도우 XP 계열에서 관리 목적으로 공유된 C\$, IPC\$의 허점을 파고들어 바이러스를 감염시킵니다.

❹ PC방과 같이 공공장소에서 사용자가 잠시 자리를 비운 사이 바이러스의 감염이 이루어집니다.

PC방에서 공용 PC를 사용하다가 잠시 자리를 비운 사이 악의적인 사람에 의해 바이러스가 감염되기도 합니다.

❺ 세어웨어나 프리웨어를 통해 바이러스 감염이 이루어집니다.

누구나 자유롭게 사용할 수 있는 프리웨어나 세어웨어를 통해서 바이러스에 감염됩니다.

3 | 이렇게 하면 자유롭다, “바이러스 꼼짝 마!”

바이러스로부터 자신의 PC를 안전하게 지킬 수 있는 방법은 다음과 같습니다.

❶ 백신 프로그램과 방화벽 프로그램을 설치하면 바이러스의 위협으로부터 안전합니다.

❷ 사용하는 윈도우나 백신 프로그램의 해당 웹 사이트를 정기적으로 방문해서 최신 바이러스 정보와 백신 프로그램 엔진을 업데이트합니다.

❸ 바이러스에 의한 감염으로 PC가 부팅되지 않을 때를 대비해서 깨끗한 부팅 디스크를 준비해 두도록 합니다.

❹ PC 통신이나 인터넷을 이용하여 자료를 다운로드할 때 반드시 신뢰할 수 있는 웹 사이트를 이용하고, 설치 전 백신 프로그램으로 바이러스 검사를 합니다.

❺ 발신자가 표시되어 있지 않거나 전혀 모르는 곳으로부터 온 메일 또는 음란물 등 호기심을 자극하는 메일은 열어볼 때 주의하고 특히 첨부 파일은 신중하게 실행 여부를 결정합니다.

❻ 맬리사, 워드 및 엑셀 매크로 등의 바이러스는 주로 마이크로소프트 사 제품 사용자를 대상으로 공격합니다. 해당 제품을 사용하는 경우에는 수시로 바이러스 점검을 합니다.

❼ 여러 명이 공동으로 사용하는 PC(게임방, 학교, 공공기관 등)나 공유 디스크, CD-ROM은 항상 최신 버전의 백신 프로그램으로 검사합니다.

❽ 백업 프로그램을 이용해서 필요한 데이터 파일이나 실행 파일(확장자가 exe, com인 파일)을 백업할 때는 반드시 백업 전에 백신 프로그램으로 바이러스 검사를 진행한 후 바이러스가 없을 경우에만 백업을 합니다(바이러스에 감염된 상태로 백업하면 나중에 해당 파일을 실행할 때 바이러스에 재감염되는 경우가 있습니다).



정기적으로 백신 프로그램 업데이트하기

새로운 바이러스가 계속 발견되고 있기 때문에 지속적인 바이러스 검색과 치료 엔진의 업데이트가 필요합니다. 백신 프로그램별로 다양한 업그레이드 방법을 살펴봅시다.

- 1 | 안철수 연구소의 V3 업데이트 | home.ahnlab.com/customer/download_engineup.html
안철수 연구소에서는 매주 수요일마다 바이러스 백신 엔진을 업데이트하고 있습니다.
- 2 | 하우리의 바이로봇 업데이트 | www.hauri.co.kr/down/dwn_engine.html
바이러스 백신 엔진을 수작업으로 업데이트할 수 있으며, 비정기적으로 백신의 엔진을 업데이트하고 있습니다.
| www.hauri.co.kr/down/dwn_update.html
자동 바이러스 업데이트 기능을 이용합니다. 즉, 자동으로 온라인을 통해 가장 최신의 바이러스 백신 엔진으로 업데이트해주는 곳입니다. 바이로봇이 PC에 설치되어 있어야 업데이트할 수 있습니다.
- 3 | 에브리존의 터보백신 | www.everyzone.co.kr
터보백신은 매주 목요일마다 정기적으로 바이러스 백신 엔진을 업데이트하고 있습니다.

2 백신 프로그램 설치하기

앞에서 살펴보았듯이 바이러스의 위협으로부터 벗어나기 위해서는 새로운 프로그램을 사용하기 전에 항상 백신 프로그램으로 검사해야 합니다. 또한 윈도우나 백신 프로그램의 해당 웹 사이트를 통해 최신 바이러스 정보와 백신 프로그램으로 업데이트해야 합니다.

현재 국내에서 구입할 수 있는 백신 프로그램으로는 안철수 연구소의 V3 시리즈와 하우리의 바이로봇, 에브리존의 터보백신 등의 국산 백신 제품이 있고, 시만텍의 노턴 안티바이러스, 트렌드 마이크로의 PC-cillin 등의 외국 제품이 있습니다.

어떤 백신 제품을 사용하든지 적어도 일주일에 한 번씩은 정기적으로 업데이트를 해주는 것이 좋습니다. 또한 요즘은 바이러스가 더 많이, 더 빨리 퍼지기 때문에 백신 엔진은 늘 최신의 상태를 유지해야 합니다. 특히 코드레드나 님다 바이러스 또는 미켈란젤로 바이러스와 같이 개인이 사용하는 PC에 치명적인 위협을 가할 수 있는 바이러스의 변종이 계속해서 등장하기 때문에, 백신 프로그램 없이는 대처하기 어렵습니다.

백신 프로그램의 종류

제조사	제품명	사이트 주소
안철수 연구소	V3	home.ahnlab.com
하우리	바이로봇	www.hauri.co.kr
에브리존	터보백신	www.everyzone.co.kr
시만텍	노턴 안티바이러스	www.symantec.co.kr
트렌드 마이크로	PC-cillin	www.trendmicro.co.kr

따라하기 

공개용 백신 프로그램 공짜로 구하자

Windows 98 ○ Me ○ 2000 ○ XP ○

1 | 안철수 연구소의 V3Pro

우선 국내에서 많이 사용하고 있는 안철수 연구소의 V3Pro를 설치해 봅시다. V3Pro는 유료 프로그램이지만 30일 동안 무료로 사용할 수 있는 평가판을 제공하고 있습니다.

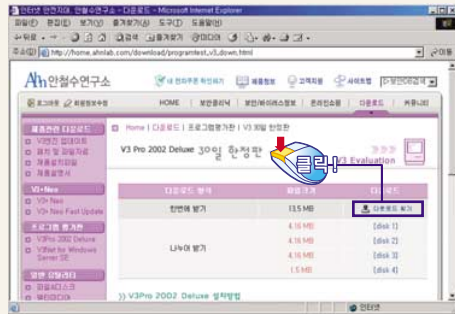
1 안철수 연구소 웹 사이트(home.ahnlab.com)에서 30일 평가판을 다운로드받기 위해서는 우선 회원가입을 해야 합니다. 가입 후에 로그인을 합니다. '평가판 다운로드' 항목을 클릭하면 30일 평가판을 다운로드할 수 있는 웹 사이트로 이동합니다.

안철수 연구소 웹 사이트 ▶



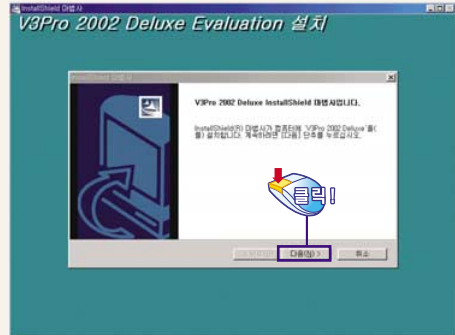
2 '다운로드 받기'를 클릭해서 V3Pro 평가판을 다운로드합니다.

평가판 다운로드하기 ▶



3 다운로드받은 V3Pro 평가판을 설치합니다.

평가판 설치하기 ▶



4 설치가 완료되면 화면 오른쪽 하단(윈도우 트레이)에 그림과 같은 아이콘이 나타나서 현재 V3Pro가 실행 중임을 보여줍니다.



▶ V3Pro 실행 아이콘

5 V3Pro 아이콘을 더블클릭하면 바이러스 검사 창이 나타납니다. 검사할 디렉터리를 선택하고 [검사 실행] 버튼을 클릭하여 바이러스 검사를 수행합니다.

V3Pro로 바이러스 검사하기

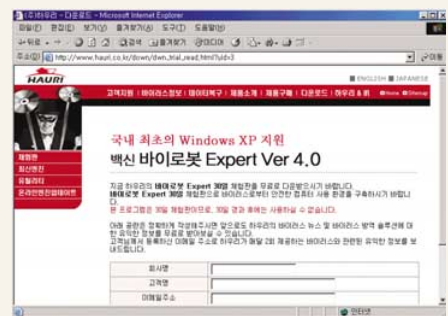


2 | 하우리의 바이로봇

하우리 웹 사이트에서 바이로봇의 30일 체험판을 제공합니다. 다운로드하여 설치해 봅시다.

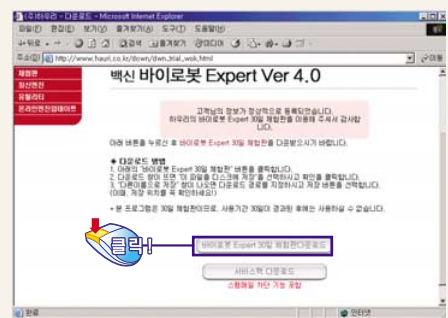
1 하우리의 30일 체험판 다운로드 사이트(www.hauri.co.kr/down/dwn_trial_read.html?uid=3)에서 체험판을 이용하려면 간단한 신상 정보를 입력해야 합니다. 회사명, 고객명, 이메일 주소를 입력하고 현재 사용하고 있는 백신이 있다면 해당 백신을 선택합니다.

하우리 웹 사이트



2 그리고 나서 [확인] 버튼을 클릭하면 다운로드 웹 사이트로 이동합니다. [바이로봇 Expert 30일 체험판다운로드] 버튼을 클릭하여 나타나는 메시지에 따라 체험판을 저장합니다.

하우리 백신 다운로드하기



3 다운로드받은 압축 파일을 풀면 바이로봇을 설치할 수 있는 실행 파일이 나타납니다. 설치 프로그램을 실행시킵니다.

하우리 백신 설치하기

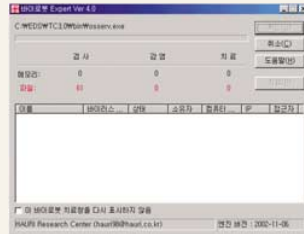


4 설치 프로그램의 실행이 완료되면 바이로봇 아이콘이 화면의 오른쪽 아래(윈도우 트레이)에 나타나 현재 바이로봇이 실행 중임을 보여줍니다.



바이로봇 실행 아이콘

5 하우리 바이로봇 아이콘을 더블클릭하면 바이러스 검사창이 나타납니다. 검사할 파일을 선택하고 [검사 시작] 버튼을 클릭하여 바이러스 검사를 시작합니다.



바이로봇으로 바이러스 검사하기

3 바이러스 검사 · 치료, 인터넷으로 끝낸다고?

앞에서 살펴본 바와 같이 바이러스를 검사하려면 PC에 백신 프로그램을 설치하는 것이 일반적입니다. 하지만 이런 방법 이외에도 온라인에서 무료로 바이러스를 검색할 수 있는 유용한 방법들이 있습니다. 상용 바이러스 백신 프로그램의 설치가 부담스럽거나 바이러스가 의심되지만 백신 프로그램이 없어 검사를 할 수 없다면, 온라인에서 이용 가능한 바이러스 검사 사이트를 찾아가 보세요.



바이러스 검사, 치료가 공짜!

Windows 98 ○ Me ○ 2000 ○ XP ○

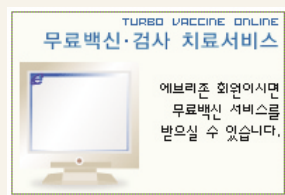
에브리존의 터보백신 온라인 사이트(www.everyzone.com)에서는 회원가입을 하면 무료로 바이러스를 검사, 치료할 수 있는 기능을 제공하고 있습니다. 백신 프로그램을 설치하지 않고도 바이러스를 찾아 치료할 수 있는 것입니다.

1 에브리존의 터보백신 온라인을 사용하기 위해서는 먼저 회원가입을 해야 합니다. www.everyzone.com에서 회원가입을 합니다.



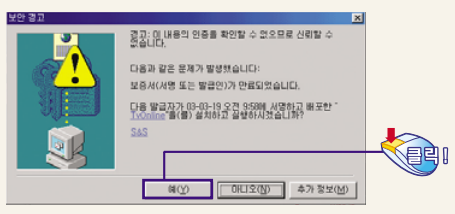
에브리존 회원가입하기

2 로그인을 하면 '무료 온라인 바이러스 백신 검사/치료 서비스'를 이용할 수 있습니다. 해당 사이트에서 다음 그림의 이미지를 클릭합니다.



무료 바이러스 검사와 치료 서비스 ▶

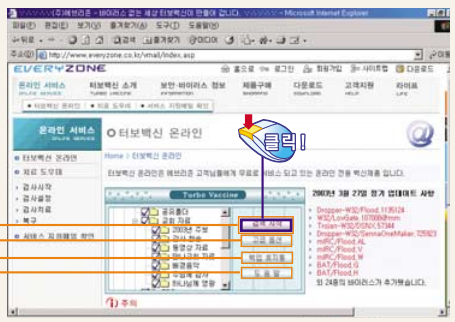
3 프로그램이 설치되면서 '보안 경고'가 나타나는데, [예] 버튼을 클릭합니다.



보안 경고 메시지 ▶

4 프로그램이 설치되면 바이러스 검사창이 나타납니다. 검사할 폴더(디렉터리)를 선택하고, [검사 시작] 버튼을 클릭하면 검사를 시작합니다.

- 바이러스 검색을 시작합니다.
- 바이러스 검사 및 치료에 사용할 옵션을 설정합니다.
- 바이러스 치료 전의 파일들을 보관하고 있습니다.
- 도움말 화면으로 이동합니다.



▶ 검사 시작하기

5 바이러스가 발견되면 바이러스에 대한 치료를 시작합니다.



바이러스 치료하기 ▶



하우리의 라이브콜

하우리에서도 라이브콜(LiveCall)이라는 이름으로 온라인 바이러스 검사와 치료 서비스를 제공합니다(www.livecall.co.kr/livecall/index.html). 단, 바이러스 검사는 무료이지만 치료하려면 비용을 지불해야 합니다.



하우리의 라이브콜 ▶

4 개인 정보를 가져가는 스파이웨어를 잡아라

스파이웨어는 컴퓨터 사용자의 정보(사용자의 이름이나 인터넷 접속 기록, URL 리스트, 다운로드한 파일의 정보 등)를 수집하여 광고업체나 개인 정보를 필요로 하는 사람에게 전달하기 위해서 컴퓨터에 설치되는 프로그램을 말합니다. 즉, 어떤 사람이나 조직에 관한 정보를 수집할 목적으로 프리웨어, 셰어웨어 또는 애드웨어(광고를 보는 대가로 무료로 사용할 수 있는 프리웨어)에 포함되어 배포되는 프로그램을 말합니다.

해킹이 특정 시스템을 파괴하거나 비밀을 알아내는 것이 목적이라면, 스파이웨어는 주로 마케팅과 관련된 정보 수집에 목적을 두고 있습니다. 스파이웨어를 효율적으로 제거하려면 스파이웨어를 전문적으로 찾아서 지워주는 프로그램을 이용해야 합니다. 여기에서는 널리 이용되고 있는 Ad-aware 스파이웨어 제거 프로그램을 사용해 봅시다.



Ad-aware로 스파이웨어를 밀어내자

Windows 98 ○ Me ○ 2000 ○ XP ○

Ad-aware는 스파이웨어를 검색하여 제거해주는 대표적인 프로그램입니다. 사용하기 편리한 인터페이스로 구성되어 있고, 몇 번의 클릭으로 스파이웨어를 쉽게 검색해서 제거할 수 있습니다.

1 Ad-aware 프로그램은 라바소프트(Lavasoft)의 웹 사이트(www.lavasoft.de/support/download)에서 다운로드할 수 있습니다. Ad-aware는 프리웨어입니다.

Ad-aware 다운로드하기



2 Ad-aware 6.0 표준판(Standard Edition)을 다운로드받아서 실행합니다. Ad-aware가 설치되면 Ad-aware를 실행시킵니다. 스파이웨어를 검사하기 위해서 [Scan Now] 버튼을 클릭합니다.

Ad-aware 실행하기



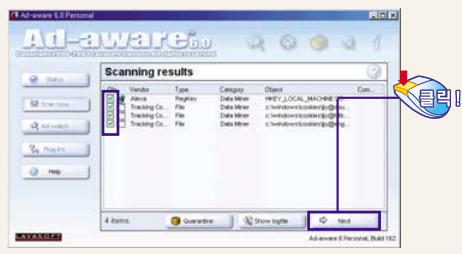
3 그러면 스파이웨어 검사를 수행할 수 있습니다. 만약 검사를 중단하고자 한다면 [Abort] 버튼을 클릭합니다.

스파이웨어 검사하기



4 스파이웨어가 발견되면 제거할 스파이웨어를 선택하고 [Next] 버튼을 클릭하여 스파이웨어를 삭제합니다.

스파이웨어 제거하기



개인 정보의 유출

스파이웨어 프로그램은 사용자의 필요에 의해 다운로드 후 사용됩니다. 현재의 스파이웨어는 단순한 정보는 물론, 유료 콘텐츠를 이용할 때 필요한 비밀번호까지 빼낼 수 있어 개인 정보에 심각한 피해를 줄 수도 있습니다. 인터넷 사용자가 많이 이용하는 다운로드 관리 프로그램인 고질라(GoZilla)를 비롯하여 마우스 커서 그림을 관리하는 콧대 커서(Comet Cursor), 유명한 파일 전송 프로그램인 CuteFTP 등이 대표적인 스파이웨어 프로그램입니다.



한번 책임지면 영원히 지켜주는 '방화벽'

내가 하는 모든 일을 다른 사람이 전부 알고 있다면 어떤 기분이 들까요? 인터넷뱅킹을 사용할 때나 신용카드를 인터넷쇼핑을 할 때 누군가가 내가 입력하는 비밀번호나 카드번호를 그대로 보고 있다면 어떨까요?

최근의 개인 정보 피해 사례를 살펴보면 백 오리 피스나 워 등에 의해 중요한 정보가 차단·유출되는 경우가 많습니다. 또 네트워크 용량 초과로 인한 인터넷 접속 불능 상태가 개인 또는 기업에 막대한 피해를 유발시키고 있습니다.



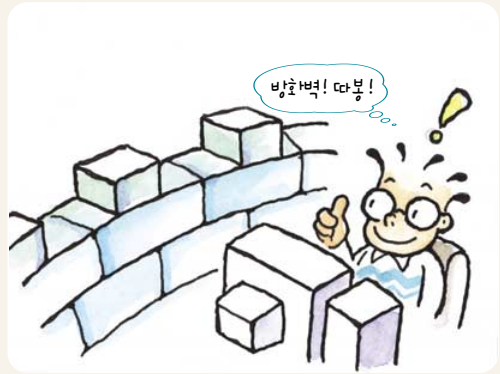
사용자의 컴퓨터를 마음대로 조종하고 필요한 정보들을 몰래 수집할 수 있는 트로이목마와 인터넷을 불능 상태로 만드는 웜과 같은 바이러스가 컴퓨터에 침투했을 때는 백신 프로그램으로 치료하면 됩니다. 하지만 컴퓨터가 바이러스에 걸리지 않게 하는 보다 적극적인 방법은 사전에 방화벽 프로그램을 설치하여 자신의 컴퓨터를 안전하게 보호하는 것입니다.

이 장에서는 방화벽 프로그램을 이용해 개인 정보를 보호하는 방법에 대해서 꼼꼼히 살펴봅시다.

1 방화벽 프로그램으로 PC 보호 출발!

방화벽 프로그램은 침입을 시도하는 각종 바이러스로부터 PC를 안전하게 보호하기 위해 만들어진 침입 차단 시스템입니다.

방화벽 프로그램은 인터넷을 통해 사용자의 PC로 접근을 시도하는 각종 해킹 툴이나 바이러스를 방어하고, 허가를 받지 않으면 외부로의 정보 전송도 자동으로 차단됩니다. PC 작업 속도가 느려지거나 인터넷 접속이 느려지는 문제도 없으므로 가장 확실한 정보보호 방법이라 할 수 있습니다.



따라하기

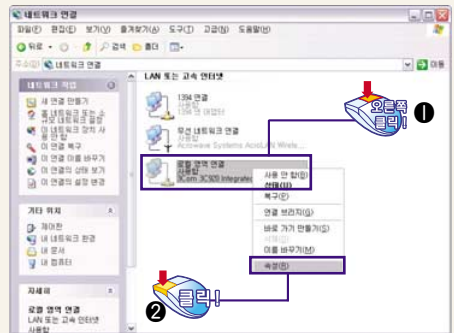
방화벽 만들어 꼭꼭 숨겨라

Windows 98 × Me × 2000 × XP ○

윈도우 XP에는 별도의 프로그램을 인스톨하거나 새로운 방화벽 프로그램을 구입하지 않고도 사용할 수 있는 기본 방화벽 기능이 있습니다. 기능에서도 상용 프로그램에 뒤지지 않고, 운영체제에 통합되어 있기 때문에 쉽게 사용할 수 있습니다. 단, 인터넷에 접속할 때 필요한 프로그램에서 사용하는 포트를 명시해야 하기 때문에 세밀한 제어는 불가능합니다. 그러나 일반 사용자들이 쉽게 사용할 수 있다는 장점이 있습니다. 만약 윈도우 XP의 기본 방화벽 기능을 사용하지 않는다면 상용 방화벽 프로그램을 사용할 수 있습니다.

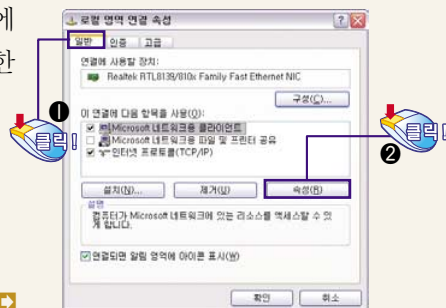
- 1 [제어판]에서 [네트워크 연결]을 더블클릭합니다. 그러면 사용자의 PC에 설치되어 있는 네트워크 상태가 나타납니다. 마우스 오른쪽 버튼으로 [로컬 영역 연결]을 선택한 다음, [속성] 메뉴를 선택하세요.

[속성] 메뉴 선택 ▶

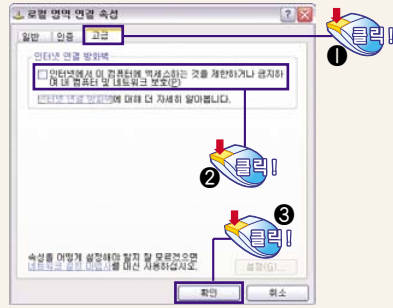


- 2 [로컬 영역 연결 속성] 대화상자의 [일반] 탭에서 [속성] 버튼을 클릭하여 네트워크의 세밀한 속성을 설정합니다.

네트워크 속성 설정하기 ▶

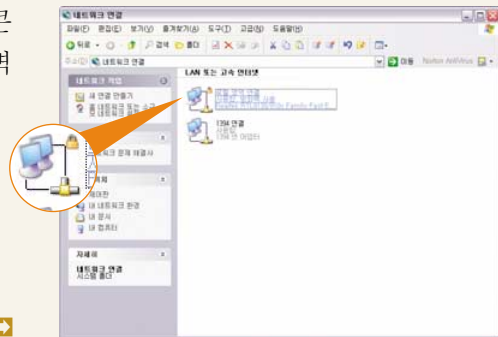


3 [고급] 탭을 선택한 후 ‘인터넷에서 이 컴퓨터...’를 선택하면 방화벽 기능을 사용할 수 있습니다.



인터넷 연결 방화벽 사용하기

4 방화벽 기능을 사용하면 네트워크 연결 아이콘에 열쇠 모양의 그림이 첨부되어 현재 방화벽 기능이 작동하고 있음을 알려줍니다.



변경된 아이콘



다양한 방화벽 프로그램

방화벽 프로그램의 종류는 매우 다양합니다. 하지만 방화벽 프로그램 사용 시 무엇보다 중요한 점은 사용자가 이용하기 쉽고, 또한 검증된 프로그램이어야 합니다.

- 1 | 안철수 연구소의 MyFirewall (home.ahnlab.com/webclinic)
TCP/IP 혹은 다른 프로토콜을 통하여 외부로 전송하거나 외부로부터의 접속이 있을 경우, 이를 모니터링하고 차단 경고하는 기능을 제공하는 온라인 PC파이어월입니다. 사용자의 PC에서 인터넷뱅킹과 같은 특정 웹 사이트를 이용할 때 방화벽 기능이 작동해서 안심하고 웹 사이트를 이용할 수 있습니다.
- 2 | 안철수 연구소의 Personal Firewall (home.ahnlab.com/pouductinfo/apf.html)
네트워크를 통한 외부 침입자로부터 데이터를 보호하고, 정보의 유출을 차단할 수 있는 개인용 침입 차단 솔루션입니다. 특히 최근 급증하고 있는 트로이목마 및 해커의 침입으로부터 PC를 안전하게 보호할 수 있습니다. 트로이목마에 대한 차단과 응용 프로그램, 네트워크 접속이나 공유 등에 대한 규칙을 설정하는 기능을 가지고 있습니다.
- 3 | 하우리의 Personal Security Suite (www.hauri.co.kr/pouduct/hpss.html)
바이러스 백신 기능과 해킹 차단, 데이터 복구 기술이 통합된 솔루션입니다. 백신 프로그램으로 바이로봇을 탑재하고 강력한 인터넷 감시 기능으로 각종 악성 코드 유입을 차단합니다. 더불어 손상된 엑셀 문서의 복구 기능을 지원합니다.

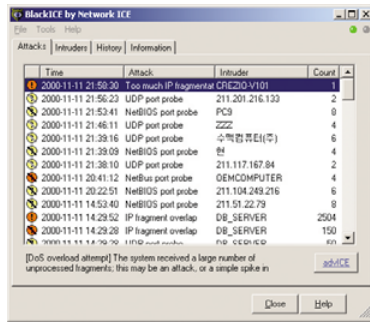


실시간으로 침입자를 잡아내자

상용 프로그램을 사용하면 인터넷을 통해 외부에서 접근하는 기록을 실시간으로 확인할 수 있습니다. 불법적인 접근을 시도하는 사용자의 IP 자체를 차단할 수 있으며, IP를 모르는 경우에는 해당 사용자의 컴퓨터 이름으로도 막을 수 있습니다. 반대로 해당 사용자의 자세한 정보를 얻어서 기록으로 보관해두면 사이버 범죄를 신고할 때도 유용하게 쓰입니다.

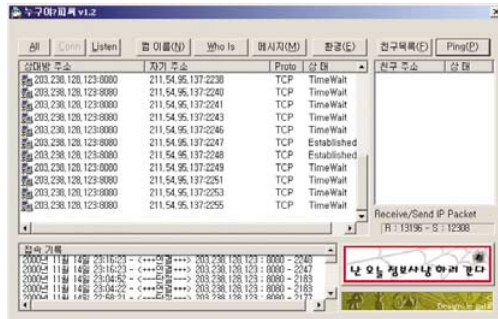
다음의 예는 BlackICE, 누구야? PC, 윈도우 XP 등의 침입자 탐지 화면을 보여주고 있습니다. 참고하여 개인 정보보호에 활용합니다.

1 | 'BlackICE'의 침입자 정보 탐지 화면



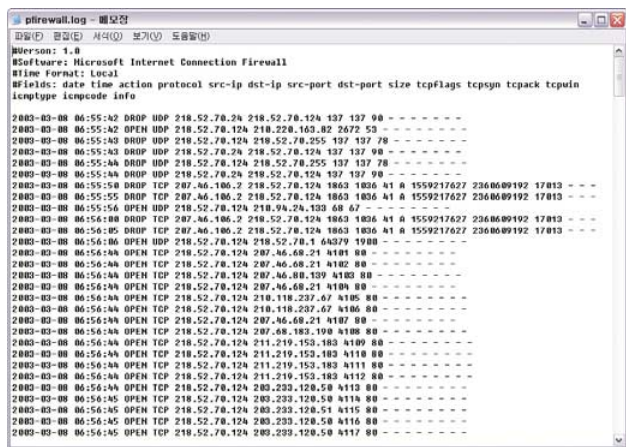
BlackICE의 (Attacks) 탭

2 | '누구야? PC'의 침입자 정보 탐지 화면



현재 연결된 포트 상태 표시

3 | '윈도우 XP'의 침입자 정보 탐지 화면



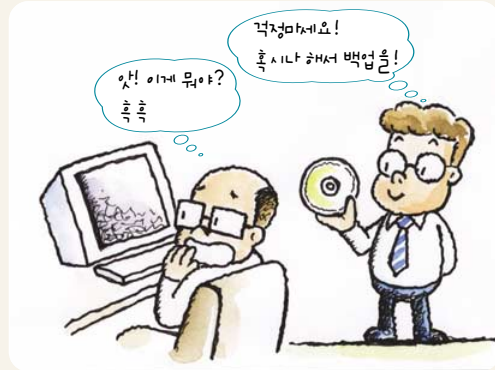
윈도우 XP 탐지 로그



백업보다 안전한 게 있을까?

아무리 정보보호와 보안을 철저히 한다고 해도 만일의 사태는 일어납니다. 갑자기 컴퓨터가 다운되거나 해킹의 위협에 노출되어도 걱정 없이 데이터를 지키는 방법은 없을까요? 혹시 일어날지 모를 데이터 손실에 대비해 데이터를 안전하게 보관하는 방법을 백업이라고 합니다.

PC에서 기본으로 제공하는 백업 기능을 이용해서 바이러스나 해킹에 의해 중요한 데이터가 손실되지 않도록, 데이터를 잃어버려도 다시 복구할 수 있도록 대처하는 방법을 알아봅시다.



1 PC 안의 데이터, 백업으로 안전하게!

백업이란 컴퓨터에 있는 파일들을 복사하여 플로피디스크나, CD 콤팩트디스크 등과 같은 미디어에 저장하는 것을 말합니다. 데이터 손실 및 파괴에 대비한 완벽한 데이터 복구 방법입니다.



따라하기

Windows 98 ○ Me ○ 2000 ○ XP ○

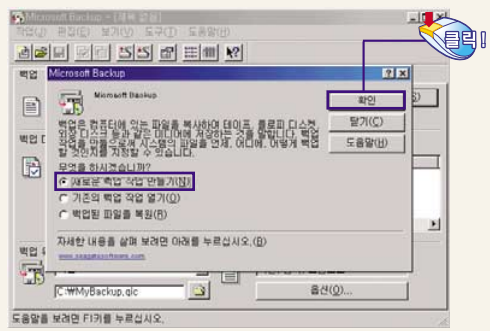
올 테면 오라지! '데이터 백업'으로 정보보호

윈도우는 기본적으로 중요한 데이터들을 백업할 수 있는 기능을 제공합니다. 이 기능을 이용해서 PC에 있는 중요 데이터들을 백업해두면 필요할 때 언제든지 사용할 수 있습니다.

1 윈도우에서 [시작] → [프로그램] → [보조프로그램] → [시스템 도구]에서 [백업]을 선택하여 백업 프로그램을 실행합니다.

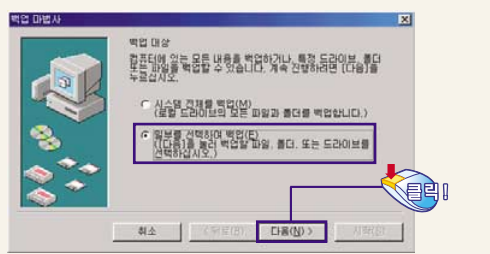
[Microsoft Backup] 대화상자에서 '새로운 백업 작업 만들기'를 선택하고, [확인] 버튼을 클릭하세요.

새로운 백업 작업 만들기



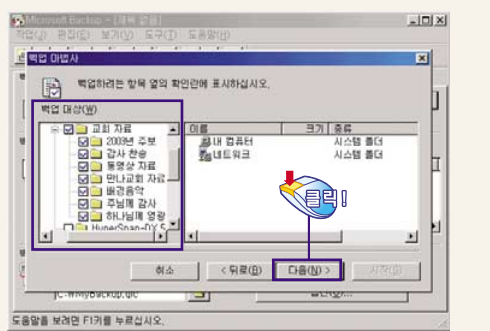
2 백업할 대상을 선택할 수 있는 대화상자가 나타납니다. 여기에서는 '일부를 선택하여 백업'을 선택하여 특정 데이터 파일을 백업하도록 합니다. [다음] 버튼을 클릭합니다.

백업 대상 선택하기



3 '백업 대상' 항목에서 백업할 폴더(디렉터리)나 파일을 선택한 후, [다음] 버튼을 클릭하세요. 다음에 나타나는 대화상자에서 '선택한 모든 파일'을 선택하고, [다음] 버튼을 클릭합니다.

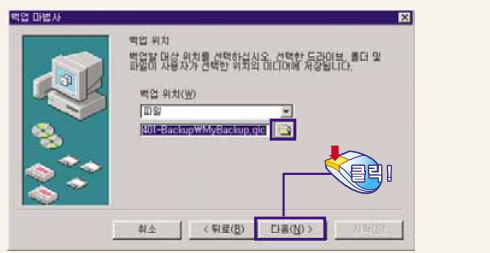
백업할 때는 백업할 폴더(예를 들면, C:\Temp\20030401-Backup)를 따로 만들고, 그 폴더에 백업할 파일들을 선택해서 복사한 후 백업합니다. 원본이 있는 폴더를 그대로 선택해서 백업하면 복원할 때 원본에 덮어쓸 가능성이 있어서 파일을 관리하기 어렵습니다. 따라서 백업할 폴더를 새로 만들어서 백업하도록 합니다.



백업할 항목 선택하기

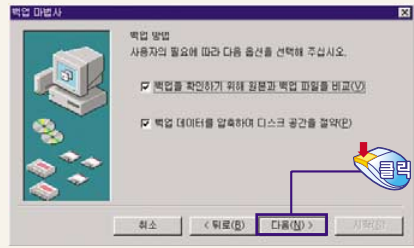
4 아이콘을 클릭하여 백업할 대상 위치를 선택하고, 백업 파일의 이름을 입력한 후 [다음] 버튼을 클릭합니다.

백업할 파일의 위치와 이름 지정하기



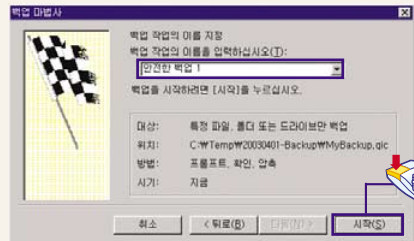
5 백업 방법을 그림과 같이 선택한 후 [다음] 버튼을 클릭하여 계속 진행합니다.

백업 선택 옵션 설정하기



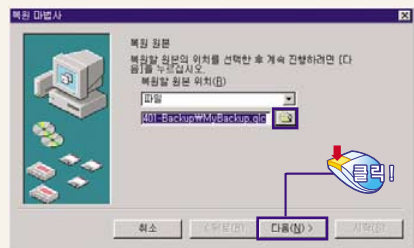
6 백업 작업의 이름을 지정한 다음, [시작] 버튼을 클릭하여 백업을 진행하도록 합니다.

백업 작업의 이름 지정하기



7 파일을 다시 복원하려면 [시작] → [프로그램] → [보조프로그램] → [시스템 도구]에서 [백업]을 선택하여 백업 프로그램을 실행합니다.

‘백업된 파일을 복원’을 선택하여 이전에 저장한 파일 및 데이터를 복원할 수 있습니다. 복원할 데이터를 선택하면 데이터에 대한 복원이 이루어집니다.



복원할 파일 선택하기



아하, 그렇구나! 이메일 관리

이메일(e-mail)을 주고받는 것은 이제 생활의 일부가 되었습니다. 많은 사람들의 생활을 보다 편리하고 윤택하게 해주는 이메일, 하지만 무분별하고 일방적인 스팸메일이 판치고 있는 상황에서 이메일도 바이러스와 해킹으로부터 안전하지 않습니다. 게다가 악의적인 바이러스와 스팸광고가 들어 있는 메일은 개인과 기업에 상당한 피해를 입힙니다.



이 장에서는 이메일의 정보보호와 보안을 위해서 이메일을 안전하게 주고받는 방법과 불필요한 메일을 미리 차단하는 방법을 살펴봅니다.

1 아웃룩 익스프레스에서 스팸메일을 받았을 때

자신과 아무런 관계가 없는 사람들에게 허락도 받지 않고 임의로 발송하는 메일을 스팸메일이라고 합니다. 발송에 사용되는 주소는 주로 게시판이나 스팸 전용 프로그램을 이용해서 수집하거나, 이메일 주소를 구입해서 사용하기도 합니다. 여기에서는 아웃룩 익스프레스를 이용하여 스팸메일을 사전에 차단하는 방법에 대해서 알아보시다.



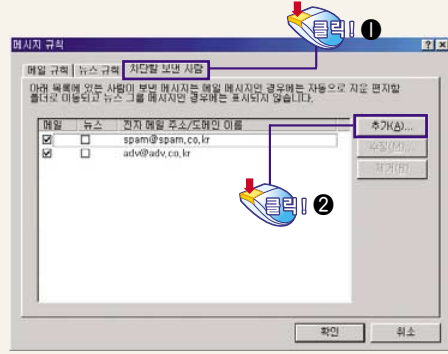
따라하기 스팸메일을 골라내자

Windows 98 ○ Me ○ 2000 ○ XP ○

‘광고 메일을 받지 않으려면 회신을 하세요’ 라거나 ‘아래 버튼을 클릭하면 됩니다’ 등의 스팸메일의 문구를 자주 보았을 것입니다. 이 경우 실제로 메일 리스트에서 삭제해주시기도 하지만, 때로는 또 다른 용도로 이용될 수 있습니다. 때문에 직접 스팸메일을 분류하는 것이 정보보호를 위한 효과적인 방법입니다. 아웃룩 익스프레스를 이용하여 원천적으로 스팸메일을 차단할 수 있습니다.

1 아웃룩 익스프레스를 실행하여 [도구] → [메시지 규칙]에서 [차단할 보낸 사람 목록] 메뉴를 선택합니다.

[추가] 버튼을 클릭하면 차단할 메일 주소를 입력할 수 있습니다. 차단하고자 하는 메일 주소를 입력하면 등록된 목록에 있는 사람이 보낸 메시지는 자동으로 '지운 편지함'으로 이동됩니다.



☞ 차단할 보낸 사람 등록하기

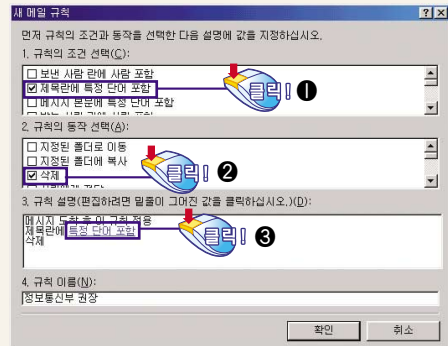


스팸메일의 분류

정보통신부는 스팸메일에 대해서는 메일의 제목에 지정된 (광고) 혹은 (홍보) 등의 문구를 의무적으로 표시하도록 하였습니다. 메일의 제목을 기준으로 스팸메일을 분류할 수 있습니다.

2 [도구] → [메시지 규칙]에서 [메일] 메뉴를 선택하면 메일 규칙을 새로 만들 수 있습니다. [메시지 규칙] 대화상자에서 [새로 만들기] 버튼을 클릭하여 [새 메일 규칙] 대화상자를 실행합니다.

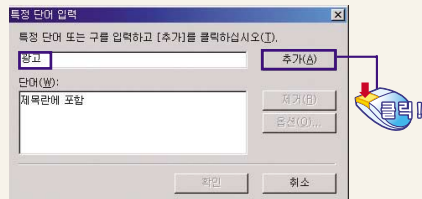
대화상자의 '1. 규칙의 조건 선택' 항목에서는 메일의 제목에서 '광고'라는 단어가 들어가는 메일을 삭제할 것이므로, '제목란에 특정 단어 포함'을 선택합니다. '2. 규칙의 동작 선택' 항목에서는 지정된 광고 메일이 왔을 때 바로 삭제할 것이므로 '삭제'를 선택하고, '3. 규칙 설명'에서 '특정 단어 포함'을 클릭합니다.



☞ 새 메일 규칙 설정하기

3 [특정 단어 입력] 대화상자에서 '광고'라고 입력하고, [추가] 버튼을 클릭합니다.

메일 중에서 '광고'라는 단어가 포함된 메일은 삭제될 것입니다. [확인] 버튼을 눌러 대화상자를 닫아 마무리합니다.



☞ (특정 단어 입력) 대화상자



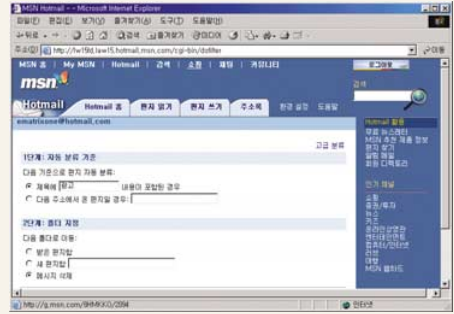
백신 프로그램을 이용하여 실시간으로 이메일 검사하기

기본적으로 거의 모든 백신 프로그램들은 이메일에 대한 바이러스 검사와 치료 기능을 가지고 있으며, 이메일을 쓰거나 읽을 때 자동으로 실시간 바이러스 검사를 진행합니다. 백신 프로그램은 일반적으로 많이 사용하는 아웃룩 익스프레스나 아웃룩과 같은 이메일 클라이언트 프로그램과의 통합이 지원되기 때문에 이메일을 주고받을 때 쉽게 바이러스의 검색과 치료가 가능합니다.

2 웹 메일에서 스팸메일을 받았을 때

다음, 드림위즈, 핫메일, 한메일처럼 웹에서만 이용할 수 있는 이메일 계정에서는 스팸메일을 어떻게 분류할까요?

웹에서만 이용할 수 있는 대부분의 이메일 계정은 해당 사이트에서 아웃룩 익스프레스와 비슷한 기능을 제공합니다. 수신 거부, 스팸메일 관리 등과 같은 메뉴로 스팸 메일을 분류하는 기능을 제공하기 때문에, 웹 메일에서도 쉽게 스팸메일을 분류할 수 있습니다.



▶ 웹 스팸메일 분류하기



웹 메일로 들어오는 스팸메일을 막아라

한국통신이나 하나로통신 등 인터넷 서비스 업체에서 제공하는 'PC보안 프로그램'을 이용하면, 일방적이고 무분별하게 보내지는 스팸메일을 사전에 차단하여 정보보호를 강화할 수 있습니다.

'스팸메일 차단 서비스'를 제공하는 대표적인 인터넷 서비스를 살펴봅시다.

1 한국통신 (pcsec.megapass.net)

'메가패스 PC보안 서비스'는 키보드 입력에 대한 암호화로 정보의 유출을 방지할 수 있는 서비스를 제공합니다.

메가패스 PC보안 서비스 ▶



2 하나로통신 (pcsafe.hanafos.com)

'하나포스 PC보안 서비스'는 바이러스 검사와 치료, 스팸메일 차단, 파일의 암호화 저장, PC 방화벽 기능, 백도어 탐지 및 제거 기능, 원격 장애처리 기능 등을 하나의 패키지로 묶어서 유료로 제공되고 있습니다.

하나포스 PC보안 서비스 ▶



3 두루넷 (product.thrunet.com/addfree_v3.asp)

'보안 클리닉 서비스'를 안철수 연구소와 손잡고 제공합니다. V3를 이용한 바이러스의 무료 검사와 유료 치료, My Firewall을 통한 무료 방화벽 기능이 제공됩니다.



두루넷 보안 클리닉 서비스 ▶



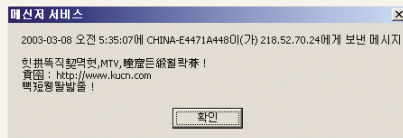
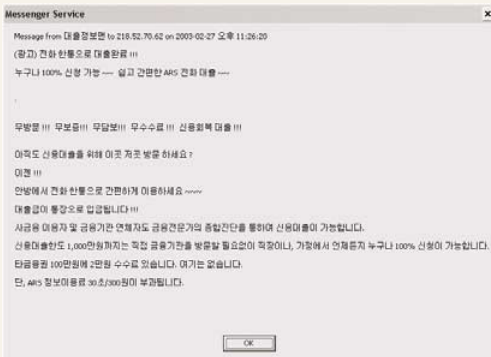
스팸메일 차단 프로그램

아웃룩이나 아웃룩 익스프레스에 플러그인(Plug-In) 형식으로 추가되어, 스팸메일에 대한 차단을 도와주는 차단 프로그램을 '스팸 메일 차단 프로그램'이라고 합니다. 음란성 메일을 차단하거나 다양한 개인 필터링 기능을 통해서 강력한 차단 기능을 제공합니다. 서어웨어인 CleanSpam, 프리웨어인 MailWasher 등 다양한 프로그램이 나와 있습니다.

3 어딜 들어와? 스팸광고에 수감을 채우자

컴퓨터 사용 중 가끔 광고 팝업창이 갑자기 나타나는 것을 경험해본 적이 있습니까? 러시아어, 중국어, 일어, 영어, 한국어까지 다양한 국어로 여러 가지 내용을 담고 있는 광고들입니다. 아무리 유용한 내용이라도 이렇게 불쑥불쑥 나타나면 성가시고 귀찮은 일입니다.

이런 경우 'Messenger' 서비스를 설정하여 더 이상 팝업창이 나타나지 않게 할 수 있습니다. 불필요한 정보로 더 이상 시간을 소비하지 마세요.



메신저 광고



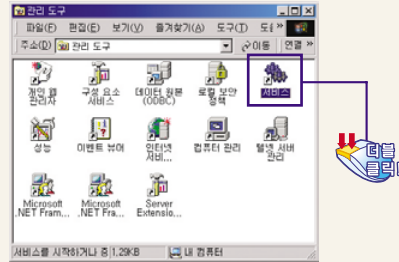
광고 메시지, 필요한 것만 골라받자

Windows 98 X Me X 2000 O XP O

‘Messenger’ 서비스를 이용하면, 컴퓨터 모니터에 갑자기 나타나는 광고 메시지를 원천적으로 차단할 수 있습니다. 여기에서는 윈도우 2000에서 지원되는 ‘Messenger’ 서비스를 이용하여 불필요한 정보를 차단할 수 있는 방법을 알아봅시다. 하루에도 수십 번씩 나타나는 광고 메시지는 이젠 옛날 이야기가 될 것입니다.

‘Messenger’ 서비스는 윈도우 2000 이상 버전에서만 지원됩니다. 윈도우 98에서는 지원되지 않습니다.

1 윈도우 2000에서 ‘제어판’을 실행하여 ‘관리 도구’ → ‘서비스’ → ‘Messenger’를 차례대로 더블클릭합니다.

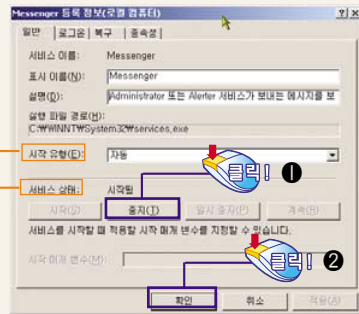


‘서비스’ 실행하기

2 [메신저 등록 정보] 대화상자에서 광고 메시지를 차단하기 위해서는 [중지] 버튼을 클릭하세요.

서비스가 실행되는 유형을 설정합니다. ‘자동’은 PC를 시작할 때 서비스가 자동으로 시작되고, ‘수동’은 사용자가 일일이 [시작] 버튼을 클릭해서 서비스를 시작해야 합니다. ‘사용 안 함’은 어떠한 일이 있어도 해당 서비스를 사용하지 않습니다.

서비스의 현재 시작 상태를 나타냅니다. 서비스가 시작되면 ‘시작됨’으로 나타납니다.



[메신저 등록 정보] 대화상자

3 [확인] 버튼을 클릭하면 변경한 사항이 적용됩니다.



스팸메일 신고하기

정보통신부의 개인정보보호지침고시에 어긋나는 스팸메일은 불법스팸대응센터(www.spamcop.or.kr)에 신고할 수 있습니다. 스팸메일을 신고할 때는 신고자가 누구인지 정확히 밝히고, 처리 결과를 받을 연락처와 신고 이유, 스팸메일을 발송하는 사람의 메일 주소, 스팸메일 파일(eml, html) 또는 스팸메일을 캡처한 이미지 등의 증거자료를 첨부해야 합니다.

스팸메일 신고하기





안전하고 편한 전자상거래 길들이기

인터넷을 이용하면 앉아서도 은행 업무를 볼 수 있다는 것은 누구나 알고 있는 사실입니다. 하지만 인터넷뱅킹을 이용하는 것이 과연 안전할까요?

이 장에서는 은행에 가지 않고도 안전하게 은행 업무를 볼 수 있는 방법과 인터넷뱅킹 이용 시 주의할 점에 대해 알아봅니다. 또 인터넷쇼핑에서 반드시 지켜야 할 사항들도 알아봅니다.



1 금융거래, 이렇게 좋을 수가!

인터넷뱅킹을 이용하기 위해서는 일단 은행을 방문하여 인터넷뱅킹을 신청해야 합니다. 그런 다음 해당 은행 홈페이지를 방문하여 회원가입 후 인터넷뱅킹에 필요한 내용들을 등록합니다. 인터넷뱅킹을 할 때에는 안전한 금융거래를 위해서 공인인증서(Certificate), 즉 사이버 거래 인감증명서를 사용합니다. 공인인증서는 정부가 지정한 공인인증기관(Certification Authority)에서 발행하는데, 안전한 인터넷뱅킹을 위해 법률 효력이 인정되는 보안 방법이 적용되므로, 안심하고 사용할 수 있습니다.

1 | 인터넷뱅킹 얼마나 안전할까?

가입자는 공인인증서를 발급받아 모든 은행의 인터넷뱅킹과 전자상거래를 할 수 있습니다. 사이버 상에서 사용하는 인감도장, 즉 공인인증서에는 인증서 버전, 인증서 일련번호, 인증서의 유효기간, 발급기관명 및 전자서명 알고리즘 정보, 가입자 이름 등과 같은 개인 정보가 암호화되어 있습니다. 따라서 고객은 보다 안전하고 편리하게 금융거래를 할 수 있습니다. 공인인증서를 이용한 거래는 법적 효력이 있는 객관적 자료를 확보함으로써, 사고발생 시 손해배상 혜택을 받을 수 있습니다.

1 인터넷뱅킹의 이중 안전장치, 보안카드

인터넷뱅킹을 이용할 때는 일반 공인인증서를 이용한 로그인 이외에 본인을 확인할 수 있는 부가적인 방안으로 보안카드를 사용합니다. 거래 시 보안카드의 특정 번호를 입력하도록 요구하기 때문에 정말로 본인이 맞는지 확인하는 이중 절차를 거치게 됩니다.

2 암호화된 비밀키, 전자서명

전자서명은 개인만이 가지고 있는 비밀키를 사용하여 원본 문서를 암호화된 숫자들로 변환한 것을 말합니다. 전자서명의 장점은 다음과 같습니다.

- ❶ 인터넷쇼핑이나 중요 문서의 수신·발신 시 거래 상대방에 대한 인증을 받을 수 있습니다.
- ❷ 타인이 보낸 문서를 신뢰할 수 있습니다.
- ❸ 본인이 가지고 있는 비밀키는 공개키에서 역으로 추출하거나 만들 수 없고, 인증기관에 사본도 없기 때문에 전자서명의 위·변조가 불가능합니다.
- ❹ 전자서명된 문서에 대한 법적 보증을 받을 수 있어 원본 문서의 증명에 사용될 수 있습니다.
- ❺ 각종 민원서류의 온라인 서비스에 대해서 전자서명으로, 본인임을 증명할 수 있기 때문에 온라인으로 민원을 신청·처리할 수 있습니다.

2 | 공인인증서 어떻게 이용할까?

공인인증서는 공인인증기관(Certificate Authority: CA)에서 발급받을 수 있습니다. 발급받은 공인인증서는 전자서명법에 의하여 법적인 효력을 가지므로, 모든 전자상거래에서 실질적인 오프라인 거래와 똑같이 사용될 수 있습니다. 즉, 공인인증기관의 인증서를 이용해서 처리한 행위는 법적으로 완전히 보장받을 수 있습니다. 또한 발급받은 공인인증서는 다음과 같이 활용할 수 있습니다.

- ❶ 인터넷뱅킹 서비스 | 예금조회, 계좌이체, 대출, 카드 등의 은행 업무를 할 수 있습니다.
- ❷ 인터넷증권 서비스 | 계좌와 연동한 안전한 증권거래, 증권계좌 관리를 할 수 있습니다.
- ❸ 보험가입/대출 서비스 | 인터넷을 통한 보험가입 및 대출 서비스에서 본인임을 확인할 수 있습니다.
- ❹ 인터넷빌링 서비스 | 각종 생활요금을 인터넷으로 납부할 수 있습니다.
- ❺ 전자화폐 서비스 | 온라인에서 전자화폐를 사용할 수 있습니다. 전자화폐의 지불이나 거래에서 인증서를 사용해서 안전하게 거래할 수 있습니다.
- ❻ 인터넷쇼핑 | 인터넷쇼핑몰에 대해서 안심하고 이용할 수 있는 신뢰성을 확보할 수 있습니다.
- ❼ 인터넷을 통한 각종 예약 | 항공권, 열차권, 공연의 입장권 및 호텔 예약 시 일일이 확인하지 않아도 쉽게 본인임을 알릴 수 있습니다.
- ❽ 이메일의 송·수신 | 이메일에 인증서를 사용하기 때문에 보낸 메일이 어떠한 변경도 없는 원본임을 보증할 수 있습니다.

**공인인증 서비스 제공**

현재 공인인증 서비스는 한국정보인증, 한국증권전산, 금융결제원, 한국전산원, 한국전자인증, 한국무역정보통신 등 6개 기관에서 제공하고 있습니다.

2 이것만은 알아두자! 인터넷뱅킹

인터넷뱅킹은 이용 가능한 모든 금융거래를 보다 편리하고, 안전하게 사용할 수 있도록 합니다. 하지만 사용상의 부주의 및 정보보호의 부족으로 인하여 개인 정보가 쉽게 유출될 수 있습니다. 개인 정보의 유출을 막기 위해서는 다음 사항들을 꼼꼼히 점검해보고 항상 숙지해야 합니다. 보다 안전하고 편리한 사용을 위한 필수 점검사항입니다.

1 공인인증서는 스마트 카드나 USB 드라이버와 같은 안전한 장소에 보관합니다.

가족 공동으로 사용하는 PC나 PC방에서 인증서를 사용할 때는 PC에 인증서를 복사하지 말고 반드시 스마트 카드나 USB 드라이버를 사용해서 인증서를 사용합니다.

2 아이디와 비밀번호는 따로 보관합니다.

잊어버리기 쉽고 각종 아이디나 비밀번호를 수첩에 같이 적어놓는 것은 대단히 위험합니다.

3 비밀번호를 자주 변경합니다.

공인인증서는 유효기간이 보통 발급 후 1년입니다. 하지만 최소 3개월에 한 번 정도는 비밀번호를 변경해서 새로 발급받습니다.

4 보안 관련 프로그램을 적극 활용합니다.

인터넷뱅킹에 접속할 때 은행이 제공하는 해킹 방지 프로그램을 구동해 제대로 작동하는지 확인한 후 사용합니다.

5 보안카드를 잘 보관합니다.

보안카드는 본인만이 알고 있는 곳에 따로 보관합니다.

6 이체한도를 정해놓습니다.

은행에서 인터넷뱅킹을 신청할 때 1회 이체한도나 1일 이체한도를 적정선에서 설정해 놓아야 합니다. 왜냐하면 개인 이 한꺼번에 많은 금액을 인터넷뱅킹에서 사용할 일은 거의 없기 때문입니다.



인터넷뱅킹의 보상 기준

현행 '전자금융거래 표준약관'에 따르면 고객의 과실이 아닌 사고나 원인이 불분명한 사고, 은행과 고객 모두에게 과실이 없는 사고의 경우에는 은행이 위험을 부담하도록 되어 있습니다. 즉, 은행 직원의 범죄나 제3자의 해킹으로 피해를 본 고객은 얼마든지 보상받을 수 있습니다. 하지만 비밀번호가 타인에게 유출되어 사고가 났다든가 사용자 PC에 대한 정보보호를 제대로 하지 않아서 해킹을 당한 경우에는 명백한 고객의 과실이므로 보상받기가 어렵습니다. 그러므로 정보보호에 더욱 신경을 써야 할 것입니다.

3 알면 즐겁다! 인터넷쇼핑

바쁜 시대를 살아가는 현대인이 쇼핑하러 가는 것도 시간 낭비일 수 있습니다. 따라서 언제 어디서나 원하는 물건을 쉽고, 빠르게 구입할 수 있는 인터넷쇼핑은 이제 현대인들에게 꼭 필요한 것이 되었습니다. 하지만 인터넷쇼핑에서 꼭 지켜야 할 사항들이 있습니다. 안전하고 유익한 쇼핑이 되도록 다음 사항들을 꼭 점검해 보시다.



- ❶ 신용카드 결제 시 비밀번호 4자리를 모두 입력하라고 요구하는 곳은 피합니다.
- ❷ 인터넷쇼핑몰 사이트에 나와 있는 사업자 정보, 회사 전화번호, 메일 주소, 대표자 성명, 사업자 등록번호 등을 꼼꼼히 메모하고, 이용약관도 자세히 읽어보아야 합니다.
- ❸ 주문 결과를 확인한 후 신용카드 결제 시 나오는 영수증을 반드시 출력합니다.
- ❹ 쇼핑물을 이용하기 전에 고객 게시판이나 방명록을 읽어보아 다른 사람들이 어떻게 평가하고 있는지도 살펴봅니다.
- ❺ 배송이 잘 이루어지는지 확인합니다.
- ❻ 물건이 제대로 구비되어 있는지 확인합니다.
- ❼ 너무 작은 쇼핑물보다는 대규모 쇼핑물을 이용하고 자주 가는 사이트를 선택해서 이용합니다.
- ❽ 쇼핑물 이용 시 암호화(SSL)가 제대로 지원되는지 확인합니다.
- ❾ 문제가 발생하면 소비자보호원(www.cpb.or.kr) 또는 소비자 단체에 적극적으로 구제를 요청합니다.
- ❿ 결제가 이루어졌는지 반드시 확인합니다.



전자화폐란 무엇일까?

전자화폐는 카드, 컴퓨터에 화폐가치를 저장한 새로운 개념의 화폐입니다. 기존 동전, 지폐 등의 화폐는 제조 비용, 보관에 불편하여 정보화사회가 진전됨에 따라 등장한 새로운 개념의 화폐입니다. 전자화폐는 카드에 화폐가치를 저장하는 IC카드형 전자화폐와 PC에 화폐가치를 저장하는 네트워크형 전자화폐가 있으며 다음과 같은 특징을 갖고 있습니다.

- 1 | 전자화폐는 휴대가 편리합니다.
전자화폐는 카드, 컴퓨터에 화폐가치를 저장하여 지폐, 동전을 소지할 필요가 없어 편리합니다.
- 2 | 위·변조가 어렵습니다.
전자화폐는 위·변조가 어려워 전자상거래에서 안전하게 사용할 수 있습니다.

이러한 전자화폐는 은행의 창구, 인터넷뱅킹, 충전소 등을 통해 먼저 이용금액을 충전한 후 충전금액 범위 내에서 자유롭게 사용할 수 있습니다.



공공장소에서의 정보보호도 문제없다

공항, 커피숍, 극장, 서점, 공공기관 등 인터넷을 이용할 수 있는 공공장소가 점점 늘어나고 있습니다. 언제 어디서나 손쉽게 인터넷을 이용할 수 있어서 매우 편리하지만 위험이 따르는 곳이 공공장소이기도 합니다. 정보보호와 보안의 사각지대라고 할 수 있는 공공장소에서의 PC와 인터넷 이용 시에는 주의가 필요합니다.

여기에서는 공공장소에서 인터넷을 이용할 때 꼭 알아두어야 할 사항에 대해 살펴봅시다.



1 PC방, 사무실, 학교 전산실 PC를 마음껏 쓰자

공항이나 철도역사, 극장가 같은 공공장소에 설치되어 있는 PC에서의 개인 정보 유출은 매우 심각한 상태입니다. 더욱이 해당 PC에 트로이목마가 있다면 사용자의 키보드 입력을 가로채서 아이디와 비밀번호, 신용카드 번호 등을 해킹당할 수도 있습니다. 공공장소에서의 정보보호를 위해서는 다음과 같은 사항을 반드시 지켜야 합니다.

1 아이디와 비밀번호는 '저장하지 않음'을 선택합니다.

사용한 아이디와 비밀번호, 쿠키까지 모두 지웁니다.

2 이메일 사용 시 반드시 전자서명을 이용합니다.

전자서명은 해당 이메일이 원본 그대로임을 알려주는 좋은 수단입니다. 중요한 이메일을 보낼 때는 전자서명을 사용해서 상대방에게 원본 그대로임을 알려줍니다.

3 공인인증서를 사용할 때는 휴대 장치를 이용합니다.

스마트 카드나 USB 드라이버와 같이 본인이 직접 휴대할 수 있는 장치에 보관한 후 이용할 때 해당 인증서를 휴대한 장치에서 가져오도록 사용하는 것이 안전합니다.

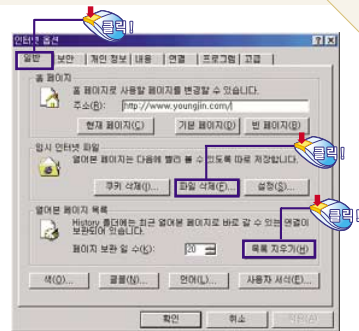
- 4 휴대 장치를 이용하지 않은 상태에서 공인인증서를 사용한 후에는 반드시 해당 PC에 저장된 공인인증서 파일을 완전히 삭제합니다. 공인인증서를 사용하고 난 후 공인인증서 관리 항목으로 가서 해당 공인인증서를 PC에서 삭제합니다. 공인인증서를 사용하고 나면 자동으로 없어진다고 생각하는데 절대 그렇지 않습니다.
- 5 사용 전에 온라인 백신 프로그램을 이용하여 바이러스 검사를 수행한 후 사용합니다. 무료로 제공되는 온라인 백신 프로그램이나 방화벽 프로그램을 이용해서 PC 사용 전에 바이러스가 있는지 반드시 확인하고, 사용 중에는 방화벽 프로그램으로 보호하도록 합니다.
- 6 사용 후 시스템 종료 및 재시동을 합니다. PC의 사용이 끝나면 반드시 '시스템 종료'를 선택해서 PC를 끄거나, '다시 시작'을 선택해서 PC를 재시동합니다.
- 7 임시 인터넷 파일과 열어본 페이지의 목록을 삭제합니다. 인터넷에서 이용했던 홈페이지 데이터 및 주소 목록을 삭제하여 사용 흔적을 지우도록 합니다.



'임시 인터넷 파일' 삭제하기

'임시 인터넷 파일'은 인터넷을 사용하면서 생기는 이미지나 사운드 등의 데이터를 임시로 저장하는 곳입니다. 이전에 방문했던 웹 사이트를 가면 이곳에서 미리 저장된 이미지와 사운드를 가져와서 사용자에게 빨리 화면을 보여주는 것입니다.

익스플로러의 [도구] → [인터넷 옵션] 메뉴에서 [일반] 탭의 '임시 인터넷 파일' 항목에서 [파일 삭제] 버튼을 누르면 임시 인터넷 파일을 삭제할 수 있습니다.



'임시 인터넷 파일' 및 '열어본 페이지 목록' 지우기

'열어본 페이지 목록' 삭제하기

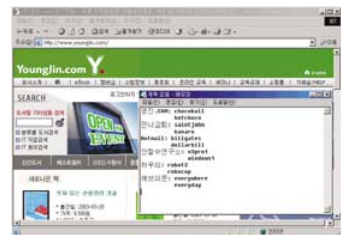
'열어본 페이지 목록'을 삭제하려면 인터넷 익스플로러의 [도구] → [인터넷 옵션] 메뉴에서 [일반] 탭을 클릭하고, '열어본 페이지 목록' 영역에서 (목록 지우기) 버튼을 클릭합니다. 여기서 모든 목록을 지우거나 주소 입력창의 사이트 주소를 입력하는 부분에서 자동 입력이 되지 않고 더 이상 목록도 나오지 않습니다.



PC방에서 보다 안전하게 PC를 사용하려면?

앞에서 다룬 공공장소에서의 주의할 점 이외에 몇 가지 사항을 더 살펴봅시다.

- 1 | 아이디와 비밀번호는 '메모장'을 이용하여 입력합니다. 윈도우에서 [시작] → [프로그램] → [보조프로그램] → [메모장]을 클릭하여 메모장을 실행합니다. 메모장에 사용할 아이디와 비밀번호를 미리 적어놓은 다음, '복사' 한 후 아이디와 비밀번호 입력을 요구하는 곳에 '붙여넣기'로 입력합니다. 이때 메모장은 열어만 놓고 사용하고 절대 파일로 저장해서는 안 됩니다.
- 2 | 다운로드받은 파일은 반드시 백신 프로그램으로 검사한 후 실행합니다. PC를 처음 이용할 때 바이러스 백신으로 검사했다고 해서 안심해서는 안 됩니다. 실행하기 전에 반드시 다운로드받은 파일에 대한 바이러스 검사를 해서 안전한지 확인해야 합니다.
- 3 | 자리를 비울 때는 반드시 화면 보호기를 실행시킵니다. PC를 이용하는 중간에 잠시 자리를 비울 때에는 반드시 화면 보호기를 실행시켜서 다른 사람이 이용하지 못하도록 해야 합니다.



메모장에서 아이디와 비밀번호 복사하기



위험할 때 불러주세요! 사이버 도우미

인터넷을 이용하는 사람들이 많아지면서 인터넷 범죄 또한 꾸준하고 다양하게 증가하고 있습니다. 사이버 범죄는 그 영향과 파급 효과가 매우 큼니다. 개인 정보가 유출되어 사생활이 침해당하고, 경제적·정신적 손해를 입는다면 어떻게 해야 할까요?

이 장에서는 사이버 범죄의 피해 사례를 알아보고 대처하는 방법을 살펴봅니다.

1 사이버 범죄 피해 유형은?

사이버 범죄는 각종 해킹이나 스팸메일의 발송, 음란·폭력물 게시 또는 판매, 인터넷 사기, 전자상거래 사기, 컴퓨터 바이러스 유포 등과 같은 인터넷에서 일어날 수 있는 모든 범죄 행위를 일컫는 말입니다. 여기에서는 인터넷을 사용하면서 발생할 수 있는 사이버 범죄의 유형을 살펴봅니다. 사이버 범죄로 인한 피해 사례는 바로 자신의 이야기일 수 있습니다. 다음 사항들을 유념하여 개인 정보가 침해당하지 않도록 사이버 범죄에 대한 경계심을 늦춰서는 안될 것입니다.

1 오~ 무섭다! 컴퓨터 해킹과 바이러스

가장 일반적인 사이버 범죄의 유형입니다. 전산망에 대한 해킹으로 데이터를 파괴, 혹은 특정 정보를 유출하거나 바이러스를 유포해서 전체 네트워크를 마비시킵니다. 특히 개인 정보를 마음대로 가져가고, 은행에서 쉽게 돈을 인출하거나 중요한 회사 기밀 문서를 제한 없이 가져가서 이용할 수 있습니다. PC와 인터넷을 이용할 때는 항상 정보보호에 유념하는 것을 잊지마세요.

2 전자상거래에서 일어나는 사이버 범죄

인터넷을 이용하는 각종 전자거래에서 게시판을 이용한 물품 사기 행각, 개인 정보를 몰래 빼내서 타사에 넘기는 행위, 해킹을 통한 개인 아이디와 비밀번호 도용 등을 들 수 있습니다. 현재 가장 문제되고 있는 물품 사기 행각은 물품의 대금 지급이 먼저 이루어진 후 배송이 이루어진다는 점을 악용합니다. 따라서 짧은 기간에 많은 주문을 받아 물품 대금을 챙기고 바로 잠적하는 방법을 사용해서 금전적 손실을 입고 있습니다.

3 지적재산권 침해 수준 “와, 놀랍다”

인터넷에 존재하는 파일들은 일반적으로 쉽게 복사할 수 있습니다. 그래서 저작물들에 대한 지적재산권 문제가 많이 발생합니다. 특히 개인 웹 사이트에 있는 많은 정보들이 저작자의 허락을 받지 않고 무단으로 사용되는 경우가 많습니다. 모든 저작물들은 원문 그대로 가져갈 때 반드시 저작자의 허락을 받도록 법률로 정하고 있으므로, 불법적인 저작

권의 침해로 인한 민·형사상의 소송에 말려들지 않도록 조심해야 합니다.

4 인터넷에서의 사이버 폭력

특정 또는 불특정 다수를 대상으로 인터넷에서 이루어지는 음란하거나 폭력적인 내용의 글 또는 영상물을 통한 범죄를 말합니다. 특히 게시판이나 이메일 등을 통해 특정인과 접촉하려고 지속적으로 시도하는 사이버 스토킹이 꾸준히 증가하고 있습니다. 사이버 스토킹은 인터넷의 익명성으로 인해서 밝혀내는 것 또한 쉽지 않습니다. 사이버 스토킹이나 게시판에서의 개인 인신 공격은 개인 모독죄로 민·형사상 고소 및 고발을 통한 법적 제재를 받을 수 있는 심각한 불법행위임을 알아야 합니다.

2 사이버 범죄 어떻게 대처할까?

사이버 범죄가 발생한다면 어떻게 해야 할까요? 다음 사항들을 통해 사이버 범죄에 대처하는 방법을 살펴봅시다.

- 1 **사이버 범죄가 일어나면 일단 증거를 확보해야 합니다.** | 해킹을 당한 경우 해당 화면을 캡처해서 보관합니다. 게시판에 음란·폭력물이 게재된 경우에는 게시물을 증거물로 보관합니다.
- 2 **실제로 신고하기 전에 각 경찰서의 사이버 범죄를 전담하는 담당 부서에 전화하거나 방문해서 미리 상담하도록 합니다.** | 확보한 증거물을 제시하고 6차 원칙에 따라서 정확하게 사건을 기술해야 합니다. 또 필요에 따라서 담당자가 요구하는 증거물을 더 확보해야 합니다. 때로는 실제로 수사하기가 어려운 부분도 있기 때문에 미리 충분한 상담을 하는 것이 비용과 시간을 절약하는 길입니다.
- 3 **모든 증거가 갖추어졌으면 실제 신고합니다.** | 사이버 경찰청이나 각 경찰서의 사이버 범죄전담반에 공식적인 신고를 하면 그 이후에 수사가 진행됩니다. 수사가 진행되는 동안에는 적극적으로 협조해서 신속하고 정확한 수사가 되도록 돕습니다.

3 사이버 도우미 제대로 활용하기

인터넷에서 실제로 도움을 받을 수 있는 사이트를 알아봅시다.

1 | 정부 및 공공기관에 도움을 요청하자

1 정보통신부 (www.mic.go.kr)

정보통신·전파관리·우편업무 등에 관한 사무를 관장하는 중앙행정기관 / 국가의 정보화 정책 수립 및 조정 / 초고속 정보통신망의 정보보호 및 구축·정보보호 전반에 걸친 지원

2 한국정보보호진흥원 (www.kisa.or.kr)

정보보호 전반에 대한 정책 및 제도 연구 / 정보보호 기술 개발, 정보보호 시스템의 연구·개발·시험·평가 / 정보보호에 대한 홍보·교육·기술지원·자문 / 해킹 및 바이러스상담지원센터 운영 (www.certcc.or.kr) / 개인정보침해 신고센터 운영 (www.cyberprivacy.or.kr) / 불법스팸신고센터 운영 (www.spamcop.or.kr)

3 한국정보문화진흥원 (www.kado.or.kr)

정보격차 해소를 위한 전담기관 / 생산적인 정보활용 촉진 및 오·남용 예방 / 정보화 역기능 예방을 위한 인터넷 중독 예방상담센터 운영 / 정보윤리 교육을 통한 건전한 정보이용 교육 홍보 / 국민에 대한 정보화 교육 및 홍보 / 국가간 정보격차 해소를 위한 국제협력 업무

4 정보통신 윤리위원회 (www.icec.or.kr)

불법 청소년유해정보신고센터 운영 (www.internet119.or.kr) / 사이버상의 명예훼손, 성폭력, 스토킹 신고 상담센터 운영 (www.cyberhumanrights.or.kr)

2 | 백신 프로그램 회사라서 더더욱 안심!**1 안철수연구소 (home.ahnlab.com)**

바이러스 백신 프로그램 업체 / V3 등 바이러스 백신 판매

2 하우리 (www.hauri.co.kr)

바이러스 백신 프로그램 업체 / 바이로봇으로 대표되는 바이러스 백신 판매 / 온라인 바이러스 진단 사이트 운영

3 에브리존 (www.everyzone.co.kr)

바이러스 백신 프로그램 업체 / 터보백신으로 대표되는 바이러스 백신 판매 / 온라인 바이러스 진단과 치료 사이트 운영

3 | 방화벽과 보안 컨설팅 회사에 SOS를 하자**1 시큐어소프트 (www.securesoft.com)**

보안 컨설팅 업체 / 기업 정보시스템의 보호, 진단, 분석 등 보안 컨설팅 사업 운영 / 침입 차단·탐지, 기상사설망, 바이러스 차단, 유해 사이트 차단 등의 기능 제공하는 하드웨어 일체형 통합보안 시스템 제공

2 지란지교소프트 (www.jiran.com)

하드웨어 일체형의 스팸메일 차단 시스템과 메일 보안 프로그램 제공 / 암호화를 통한 파일 보호 시스템 제공 / 웹 전송 데이터를 암호화해 보호하는 웹 트랜잭션 데이터 보호 솔루션 제공

4 | 민간 도우미에게 도움을 요청하자**1 안전한온라인을위한민간네트워크 (www.safeonline.or.kr)****2 학부모정보감시단 (www.cyberparents.or.kr)****3 한국사이버감시단 (www.wwwcap.or.kr)****4 안전한가정지킴이 (www.safefamily.co.kr)**



‘손쉬운 정보보호 실천수칙 8 가지’



- ① 백신 프로그램 설치와 자동 검색, 자동 업데이트 설정하기
- ② 비밀번호는 영문과 숫자를 혼합해 8자리 이상으로 정하고 주기적으로 변경하기
- ③ PC 부팅, 윈도우 로그인, 네트워크 공유 폴더 이용할 때 비밀번호 설정하기
- ④ 일주일에 한 번은 윈도우 등 주요 소프트웨어의 보안 패치 설치하기
- ⑤ 정품 소프트웨어 사용하기
- ⑥ 보낸 사람이 불분명한 이메일은 절대로 열지 않기
- ⑦ 중요한 데이터의 백업(저장)을 생활화하기
- ⑧ 하루에 한 번 PC를 껐다 켜고, 쓰지 않을 때는 전원 끄기

‘정보보호 사이버 도우미’



기 관	정보보호 도우미
정보통신부 www.mic.go.kr	민원종합처리센터 02) 750-2917
한국정보보호진흥원 www.kisa.or.kr	정보보호상담실 02) 4055-114 해킹 및 바이러스상담지원센터 www.certcc.or.kr 개인정보침해신고센터 www.cyberprivacy.or.kr 불법스팸신고센터 www.spamcop.or.kr 사이버 118 www.cyber118.or.kr
한국정보문화진흥원 www.kado.or.kr	정보윤리사업부 02) 3660-2582 인터넷중독예방상담센터 www.iapc.or.kr(02-3660-2580) 배움나라 www.estudy.or.kr
정보통신윤리위원회 www.icec.or.kr	불법 청소년유해정보신고센터 www.internet119.or.kr 사이버 명예훼손·성폭력상담센터 www.cyberhumanrights.or.kr
사이버경찰청 www.npa.go.kr	사이버테러 대응센터 www.ctrc.go.kr
민간 도우미	안전한온라인을위한민간네트워크 www.safeonline.or.kr 학부모정보감시단 www.cyberparents.or.kr 한국사이버감시단 www.wwwcap.or.kr 안전한가정지킴이 www.safefamily.co.kr

정보보호 가이드북



(157-715) 서울특별시 강서구 등촌1동 645-11

발행일 : 2003. 4. 30

발행인 : 손 연 기

발행처 : 한국정보문화진흥원

전 화 : 02)3660-2500

(이 책자는 비매품입니다)

모두가 참여 하는 정보세상, 한국정보문화진흥원이 함께합니다



www.kado.or.kr

한국정보문화진흥원은 국내외 정보격차해소 전담기관으로 모든 국민이 정보화의 혜택을 함께 누리는 디지털 참여복지사회 건설을 위해 끊임없이 노력하고 있습니다.

- | | |
|-----------------|---|
| 정보접근지원 | 지역정보접근센터구축, 사랑의PC보내기 운동, 콘텐츠개발·보급(도움나라), |
| 국민정보화교육 | 정보화교육강사지원단, e-Korean교육, 여성 e-Biz교육, 우체국정보교육센터, 온라인정보화교육(배움나라), 국민·공무원정보이용능력평가, 정보문화홍보관, 정보화선도교사양성, 장애인정보화교육, 노인정보화교육, 타부처 정보화교육지원 |
| 정보생활촉진 | 정보문화상, 정보가족, 우수사이버빌리지선발대회, 실버온라인바둑대회, 정보올림픽아이드, 대학생프로그래밍경시대회, 아름다운 e세상 발간, 가정정보화네트워크, 한국정보문화운동협의회 |
| 국제협력 | 해외인터넷청년봉사단, 개도국정보접근센터구축·지원, 해외IT전문가중장기양성, 해외연론인IT투어, 신국제규범대응전략연구 |
| 정보화역기능예방 | 건전정보이용교육, 인터넷중독예방상담, 사이버범죄예방·교화 |
| 조사연구 | 정보격차해소정책개발지원, 국민정보화실태조사·연구, 정보접근성향상표준화포럼 |
| IT World | 미래정보사회 체험관 운영 (과천 서울대공원 소재) |



한국정보문화진흥원
KOREA AGENCY FOR DIGITAL OPPORTUNITY & PROMOTION