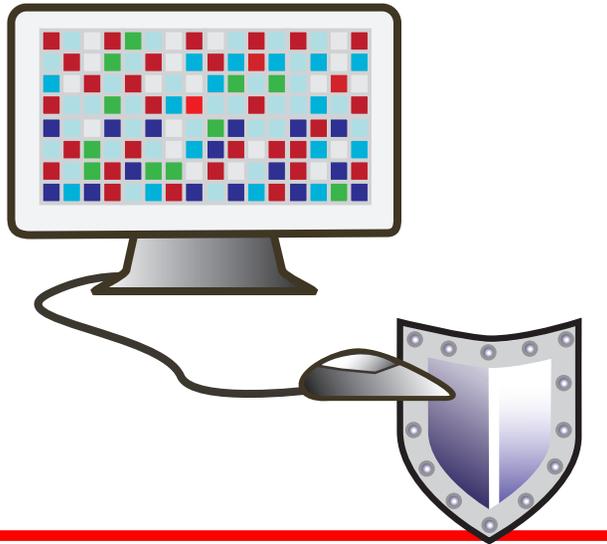


컴퓨터 보안: 모두의 책임

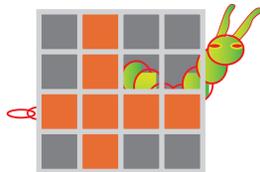
컴퓨터 및 인터넷은 범죄자들이 즐겨 찾는 대상입니다. 이를 보호하지 않는 경우 그들은 귀하의 컴퓨터에 침입하여 신용카드 번호와 은행 계좌 정보 및 기타 민감한 개인 데이터를 도용할 수 있습니다.

모든 컴퓨터 사용자는 보안을 증강하여 귀하 및 귀하의 컴퓨터가 해를 입을 가능성을 줄이는 조치를 취해야 합니다. 다음은 컴퓨터의 안전을 유지하기 위해 흔히 사용되는 컴퓨터 보안 조언입니다.



바이러스 및 웜

컴퓨터 “바이러스”는 귀하의 컴퓨터 상의 프로그램에 붙어서 프로그램 및 정보 또는 하드웨어를 손상시킵니다. 컴퓨터 “웜”은 이와 동일하데 다만 추가로 자신을 복제하는 기능이 있습니다. 이러한 것들은 귀하의 컴퓨터를 손상시키고 다른 사람들의 컴퓨터도 감염시킵니다.

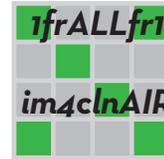


취할 조치:

다음은 시간과 돈이 많이 들지 않는 조치로서 귀하가 당장 취할 수 있는 조치들입니다. 단지 습관만 바꾸면 되는 부분도 있습니다.

패스워드

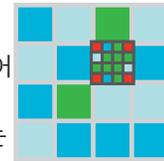
패스워드는 개인 계좌, 문서, 및 신원 정보의 접속 권한 등 귀하의 컴퓨터에 간직된 데이터를 보호합니다.



컴퓨터 침입자 (“해커”) 및 다른 이들이 귀하의 컴퓨터에서 패스워드를 알아내는 것으로부터 컴퓨터를 지키는 방법은 알파벳, 숫자, 기호 (!, @, #, \$, % 등)의 조합을 패스워드로 사용하는 것입니다. 무엇보다 중요한 것은 이 패스워드를 누구와도 공유하지 않는 것입니다. 패스워드를 안전한 장소에 기록하시고 정기적으로 변경하십시오.

패치 및 업데이트

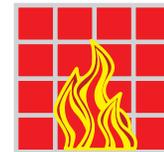
패치 또는 업데이트는 알려진 소프트웨어 문제를 고쳐 주는 작은 컴퓨터 프로그램입니다. 소프트웨어 회사에서는 자주 새로운 패치를 발행하여 귀하가 제품을 등록하신 경우 귀하에게 필요한 업데이트를 웹이나 이메일로 통보합니다.



최신 패치를 계속 설치하는 것은 중요합니다. 귀하의 컴퓨터가 이를 자동으로 실행하도록 설정할 수 있습니다. 컴퓨터가 자동으로 소프트웨어 회사와 확인하여 귀하의 운영 체제나 웹 브라우저, 안티-바이러스 프로그램을 고치게 됩니다.

방화벽 및 바이러스/스파이웨어 보호 소프트웨어

방화벽은 네트워크로 연결된 컴퓨터 시스템 간의 정보의 이동을 제한하는 여과 시스템입니다. 방화벽은 개인 정보가 세어 나가거나 원치 않는 프로그램이 잠입해 오는 것을 막습니다.



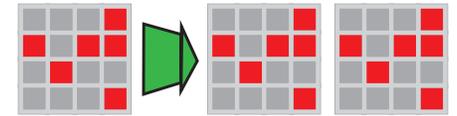
바이러스 보호 소프트웨어나 안티-바이러스 소프트웨어는 악성 소프트웨어를 식별하여 중화시키거나 제거하도록 시도합니다. 이들

프로그램은 귀하의 컴퓨터를 정기적으로 검사하여 바이러스를 “청소” 또는 “제거”하거나 이를 “격리” 또는 “파괴”하려고 노력합니다.

웹 브라우저 설정에서 보안 설정을 높이고 팝업 광고를 차단하십시오.

사용하기 간편한 무료 방화벽 및 안티-바이러스 프로그램을 이용할 수 있습니다. 이들에 대한 정보를 “방화벽 소프트웨어” 또는 “안티-바이러스 프로그램”을 검색함으로써 온라인에서 찾아 보십시오.

복제해 두기



귀하의 컴퓨터의 중요한 파일 및 문서를 복사하는 것은 출생신고서 또는 여권에 대한 추가 사본을 만드는 것만큼 중요합니다. 귀하의 문서 및 파일을 디스크나 USB 메모리 스틱, 웹 저장고 또는 기타 저장 장치 하드웨어에 저장함으로써 이들을 보호하십시오. 이를 정기적으로 시행하십시오.

점검 목록

다음은 가정 사용자가 컴퓨터를 보호하기 위해 취할 수 있는 조치 점검 목록입니다. 다음의 출처는 CERT (컴퓨터 긴급대응팀)의 코디네이션 센터입니다. 더 자세한 사항은 다음의 링크에서 보실 수 있습니다: www.cert.org/tech_tips/home_networks.html.

- 바이러스 보호 소프트웨어를 사용한다.
- 방화벽을 사용한다.
- 모르는 이메일 첨부파일은 열지 않는다.
- 모르는 출처의 프로그램은 실행하지 않는다.
- 숨겨진 파일명 확장자는 비활성화시킨다.
- 모든 응용 프로그램(운영 체제 포함)을 업데이트시켜 둔다.
- 사용하지 않을 때는 컴퓨터를 끄거나 인터넷 연결선을 빼 둔다.

스파이 및 원하지 않는 광고



모두가 자신의 개인 정보를 보호하고자 합니다. 그러나 불행히도 스파이 소프트웨어 (“스파이웨어”) 및 광고 프로그램 (“애드웨어”)는 귀하의 컴퓨터에 허가가 없이도 설치 가능합니다.

귀하는 특정 웹 사이트를 방문하거나 링크를 클릭하거나, 또는 인터넷에서 파일을 다운로드받거나 이메일 메시지의 첨부 파일을 열 때 인식하지도 못한 채 이러한 프로그램들을 설치하는 경우가 있을 수 있습니다.

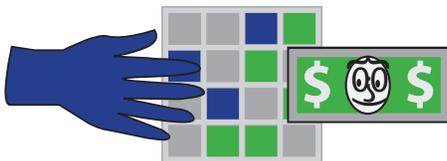
스파이웨어는 개인 정보를 수집하여 이를 범죄자에게 보냅니다. 애드웨어는 팝업 창에 원치 않는 광고를 보이거나 컴퓨터 화면에 광고 바를 만듭니다.

귀하의 금전을 요구하는 혐오 이메일 및 스킴

정크 이메일에 답장을 보내지 마시고 삭제하십시오!
귀하가 알고 신뢰하는 사람에게서 온 이메일만 여시고 그 링크를 클릭하십시오.

“스팸”은 귀하가 절대 원한 바가 없는 정크 이메일입니다. 답장을 하지 마시고, 바로 삭제하십시오.

“피싱”은 스팸이나 팝업 메시지를 사용하여 교묘하게 귀하로 하여금 개인 정보나 사회보장번호 또는 패스워드 등을 공유하게 하는 온라인 사기입니다. “피셔”들은 자신의 이메일과 웹 사이트를 마치 은행 또는 기타 신뢰받는 기관인 것처럼 변장합니다. 이들은 교묘한 술수로 귀하로 하여금 자신들에게 계좌 번호 및 패스워드를 내주게끔 합니다. 개인 정보를 요청하는 링크에 답신을 보내거나 링크를 클릭하지 마십시오. 삭제하십시오!



시애틀 정보 보안 웹 사이트도 방문해 보십시오:
www.seattle.gov/informationsecurity.

마이크로소프트 사의 보안 사이트를 방문하시면 여러 다른 언어로 된 정보도 참조하실 수 있습니다. 이곳을 방문하십시오: <http://www.microsoft.com/protect> 에서 “worldwide sites (전 세계 사이트)”를 클릭하셔서 귀하의 언어를 선택하십시오.

도움받을 수 있는 곳

이 정보의 인쇄본을 원하시면 (206) 233-7877로 전화 또는 PO Box 94709, Seattle, WA, 98124-4709로 우편 연락을 주십시오.

귀하의 지역 공공 도서관 및 지역사회 기술 센터 또한 더 상세한 정보를 얻을 수 있는 훌륭한 자원입니다. 다음을 참조하십시오:
www.seattle.gov/tech/techmap

도움말은 컴퓨터 기술 지원 회사 및 온라인 포럼에서도 참조하실 수 있습니다. 소비자 보고서, 컴퓨터 잡지, 컴퓨터 상점, 제조업체 또는 소프트웨어 업체 역시 유용한 정보를 제공해 드립니다.

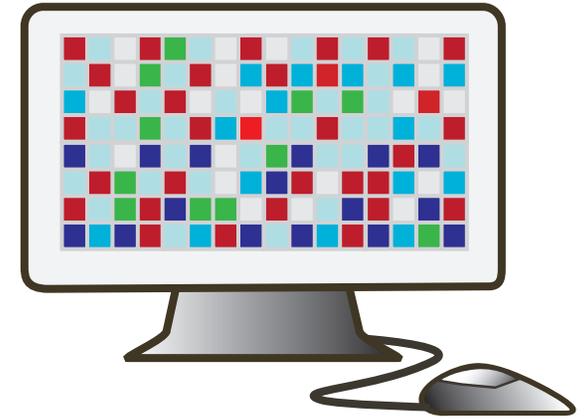
이 안내 책자는 시애틀 시, 정보기술과의 커뮤니티 기술 프로그램 및 정보보안실(Department of Information Technology's Community Technology Program and Office of Information Security)에서 제공합니다.
www.seattle.gov/tech
www.seattle.gov/informationsecurity

이 정보는 대중의 교육 및 인식 제고를 위해 제공됩니다. 가능한 정확한 정보를 전달하기 위해 노력했습니다만, 모든 정보가 정확하다는 보장은 드리지 못하며 오류나 누락에 대한 책임은 지지 않습니다.

귀하 스스로가 추가 조사를 실시하시고, 신뢰받는 컴퓨터 보안 전문가의 상담을 받으시기를 권장하는 바입니다.



귀하의 컴퓨터는 안전한가요?



귀하의 컴퓨터 보호 및 보안을 위한 팁

