컨수머 액션 출판물

자물쇠를 채우세요

온라인 개인 정보 보호

인터넷은 개인이나 가족들에게 사실상 언제 어디서나 컴퓨터나 모바일 장치를 이용해 친목, 쇼핑, 은행 업무, 직장 업무, 학습, 오락 등을 할 수 있게 해 줍니다. 이러한 인터넷의 기능들을 수용하는 것은 많은 이득을 가져다 주며 대부분의 경우 안전합니다. 이러한 점은 대부분의 업체들이 이용자들의 개인 정보 보안 유지를 위한 최신 기술을 우선적으로 적용해 이용자들의 온라인 보안에 큰 비중을 두기 때문입니다.

그러나 온라인상의 개인 정보와 보안은 공동책임입니다. 원하는 수준의 개인 정보 보호와 가장 높은 수준의 보안 유지를 위해 컴퓨터와 모바일 사용자들은 기본적인 상식과 구글이나 마이크로 소프트와 같은 대형 기술 업체들이 무료로 제공하는 도구들을 포함 사용 가능한 모든 보안 도구들을 활용해 자신의 개인 정보 보호에 대한 책임을 져야 합니다. 적극적인 참여는 안전하고 건전한 디지털 방식의 생활을 즐길 수 있도록 도와 줍니다.

계좌 잠그기

기술은 끊임없이 진화하고 있으며 다른사람이 여러분의 계좌와 개인정보에 접근할 수 없도록 하는 더 좋은 방법들을 제공하고 있습니다. 온라인 뱅킹에서부터 소셜 미디어까지 민감한 개인 정보를 처리하는 웹사이트들은 훔쳐보려는 눈들로 부터 개인 정보의 안전을 지킬 수 있는 도구들을 제공합니다. 복잡한 암호는 개인 정보를 보호하는 좋은 방법중 하나이며 이중 인증은 더 더욱 좋습니다.

암호 보호: 암호는 첫번째 방어선이며 가장 기본적이고 광범위하게 이용되는 계좌 보호 방법입니다. 다음은 계좌 보호를 위해 암호를 효과적으로 이용하는 방법들 입니다.

◆ 최소한 8자리의 무작위 문자, 숫자 및 부호의 혼합으로 된 암호를 만드십시오. Google (*bit.ly/1MoNVfk*), Microsoft (*bit.ly/1JnLHbp*) 또는 ConnectSafely (*bit.ly/1Kyu2i2*)에서 복잡한 암호 생성에 관한 자세한 정보를 얻을 수 있습니다. 또한 Passwords-Generator.net과 같은 온라인 도구를이용해 암호 생성에 대한 도움을 받을수 있습니다.

◆ 암호는 비밀로 간직해야만 합니다. 적어두는 것 보다는 모든 암호를 한곳에 저장하고 하나의 암호만 기억하면 되는 도구를 이용하십시오. PCMag.com (*bit.ly/1Otbirr*) 이나 Lifehacker (*bit.ly/1QXEc1b*)에서 암호 관리에 관한 도구들에 대해 알아볼 수 있습니다.

◆ 다양한 계좌에 대해 각각 다른 암호들을 사용하십시오. 필요에 따라 - 예를들어 누군가가 여러분의 암호를 알아 냈거나 정보 침해(많은 양의 사용자 정보 노출 또는 도난)가 발생한 경우 - 자주 암호를 변경하십시오.

◆ 타인이 답을 알아내기 힘든 보안 질문들을 선택하십시오. “어머니의 결혼 전 성함이 무엇입니까?” 혹은 “애완 동물의 이름이 무엇입니까?” 같은 타인이 쉽게 답을 알아낼 수 있는 질문들을 피하십시오. (보안 질문들은 본인이 암호를 기억하지 못하거나 등록되어 있지 않은 컴퓨터 혹은 기타 장치에서 신분검증을 하기 위해 일부 계좌들이 사용합니다.)

◆ 사용이 끝났을 때에는 계좌에서 로그아웃 하고 브라우저 로그인 정보를 저장하지 못하도록 하십시오. (브라우저의 암호 저장 여부를 묻는 메시지가 표시되었을 때 “Not now,” “Never for this site” 또는 비슷한 옵션을 클릭하거나 브라우저 설정 또는 기본 설정의 보안, 암호, 동기화 혹은 자동 완성의 해당 박스들을 체크 또는 언체크 하십시오.)

◆ 컴퓨터를 켜거나 “깨우기” 위한 암호를 요구하도록 설정 하십시오. 이것은 누군가가 여러분의 컴퓨터로 여러분의 계좌에 접근하는 것을 한층 더 어렵게 만듭니다. 애플 컴퓨터(Mac) (*apple.co/1V9p5Yt*)와 PC (*abt.cm/1Wiy72s*)에서 이러한 암호를 설정하는 방법을 알아 두십시오. (모바일 장치들도 암호, PIN 또는 지문 등을 요구하도록 설정하십시오.)

이중 인증(Two-factor authentication,2FA): 이것은 단일 암호보다 훨씬 강한 보호 수단입니다. 이중 인증은 계좌 접속을 위해 두가지 정보를 요구합니다(예를 들어 암호와 여러분이 선택한 화면 상의 사진이나 그래픽의 확인, 암호와 지문 인식, 또는 암호와 문자 메시지나 이메일로 받은 또 다른 암호). 이는 식료품 가게에서 직불 카드를 긁은 후 PIN을 입력해야 하는 것과 같습니다. Stop.Think.Connect. (*bit.ly/1DQlzpY*)에서 이중 인증에 관한 상세한 정보를 얻을 수 있습니다.

가능하면 모든 웹사이트에서 이중 인증을 사용하도록 설정합니다. 모든 웹사이트가 이를 제공하지는 않지만 구글, 애플, 페이스북, 트위터 그리고 페이팔 등을 포함한 많은 웹사이트들이 이중 인증을 제공합니다. 웹

사이트 bit.ly/1JpGz6w 에서는 다수의 이중 인증을 제공하는 웹사이트들과 제공하지 않는 웹사이트들의 목록을 보여 줍니다. (여러분이 사용하는 웹사이트들 중 이중 인증을 제공하지 않는 웹사이트들에게 이중 인증을 제공해 줄 것을 요청 하십시오.) 웹사이트들 마다 이중 인증 설정 방법은 다릅니다. 먼저 설정을 확인 후 찾을 수 없을 경우 해당 웹사이트의 고객 지원팀에 연락 하십시오.

안전한 온라인 및 모바일 거래

온라인 쇼핑과 뱅킹은 여러분의 시간과 돈을 절약해 줄 수 있으며 온라인으로 돈을 지출하고 관리하는 가장 큰 두가지 이유입니다. 그리고 본인의 지갑을 보관 하듯 간단하고 효과적인 주의 사항을 지킴으로서 여러분의 모든 계좌를 안전하게 관리 할 수 있습니다. 아래와 같은 강력한 보안 도구들도 준비되어 있으니 안심 하십시오.

암호화(Encryption): 이것은 사이버 공간을 통해 보내지는 전산 정보를 암호화해 해커들이 여러분의 활동을 추적하고 정보를 훔치는 것을 훨씬 더 어렵게 만드는 기술입니다.

방문하는 웹사이트에서 여러분이 주고 받는 정보를 보호하기 위한 암호화의 사용여부를 확인 하시려면 웹사이트 주소(URL)에 “보안(secure)”을 뜻하는 “s”(http:// 대신에 https://)가 있는지 확인하십시오. 또한 보안 웹사이트에 들어 갔을 때 자물쇠 표시가 보이거나 웹사이트 주소 표시 줄 자체가 녹색으로 바뀔 수 있습니다. 구매, 금융 계좌 조회 또는 기타 거래 등을 하기 전에 한가지 이상의 위와같은 보증 표시가 있는지 찾아 보십시오.

일부 일반 이메일과 문자 메시지는 암호화 되지 않음을 유의하시고 계좌번호, 사회보장번호 또는 그 밖의 민감한 정보는 이러한 방법으로 보내지 마십시오.

가정에서 무선 인터넷 통신망(Wi-Fi)을 사용한다는 것은 무선 라우터(wireless router)를 소유하고 있다는 뜻입니다. 무선 네트워크를 통해 여러분이 인터넷으로 보내는 정보에 가까이 있는 누군가가 접근하는 것을 방지하기 위해 무선 라우터의 암호화 기능이 켜져 있는지 확인하십시오.(대부분 구입 시 꺼져 있습니다.) 이와 동시에 여러분의 무선 인터넷 통신망 접속 범위 내에 있는 침입자가 여러분의 통신망에 연결하는 것을 막기 위해 강력한 네트워크 암호(최소 14자리의 무작위 문자들)를 만드십시오. OnGuardOnline.gov (1.usa.gov/1G2Eiya)에서 무선 네트워크 보안에 대한 상세한 정보를 얻을 수 있습니다.

외부 네트워크의 암호화 여부는 항상 확인할 수 없음으로, 집에서 멀리 떨어져 있을 경우 쇼핑이나 은행업무를 위해 공공 무선 인터넷 통신망을 사용하기 보다는 휴대폰 업체의 네트워크를 사용하는 것이 가장 안전합니다. 공용으로 사용되는 컴퓨터 또는 기타 장치를 사용할 경우 여러분이 자리를 떠난 후 다른 사람이 여러분의 계좌에 접근하는 것을 방지 하기 위해 은행업무나 쇼핑을 마친 후 항상 로그아웃을 해야 합니다. 연방 통상 위원회(the Federal Trade Commission, FTC) (1.usa.gov/1L62Nlr)로 부터 공공 무선 인터넷 통신망의 안전한 사용법에 대한 상세한 정보를 얻을 수 있습니다.

방화벽(Firewalls): 대부분의 컴퓨터 운영 체제(operating system)는 방화벽-외부와 여러분의 컴퓨터 사이에 있는 장벽-을 내장하고 있습니다. 내장 방화벽이 항상 “켜져” 있는 것은 아닙니다. 컴퓨터의 보안 설정(대부분의 경우 “Preferences” 아래 에서 찾을 수 있음)에서 방화벽이 켜져 있는지 확인하십시오. 이러한 보안 설정을 찾기 힘든 경우 “firewall”이라는 단어와 여러분 컴퓨터 운영 체제의 이름을 함께 이용해 온라인 검색을 통한 보안 설정 방법을 찾아 보십시오.

모바일 장치의 안전성

스마트폰이나 태블릿은 인터넷의 모든 기능을 어디에서나 이용 가능하게 합니다. 편리한 휴대성과 위와 같은 장치들을 사용 가능하게 하는 기술은 사용자들에게 큰 장점을 가져다 주지만, 이러한 모바일 장치들 특유의 개인 정보 보호 및 보안에 대한 문제가 발생합니다. 이러한 문제들이 위와 같은 장치들을 여러분이 원하는 모든 방법으로 사용해서는 않된다는 뜻은 아니며 단지 아주 조금 추가적인 혹은 조금 다른 몇 단계의 조치가 여러분의 사생활 와 개인 정보를 보호할 수 있다는 뜻입니다.

모바일 장치의 보안: 모바일 장치의 편리한 휴대성 때문에 데스크탑 컴퓨터 등에 비해 분실 또는 도난의 위험성이 더 많이 자리하고 있습니다. 모바일 장치를 잘 보관하는 방법 이외에도 모바일 장치와 모바일 장치 내의 정보 안전을 위해 특별히 설계된 기술 도구를 이용할 수 있습니다.

암호(또는 종류에 따라 지문 등) 혹은 PIN을 이용해 모바일 장치를 잠그는 것부터 시작하십시오. 사용을 멈춘 몇분 안에 잠기도록 설정하십시오. 이와 함께 Find My iPhone (Apple) 또는 Android Device Manager와 같은 원격 위치추적/잠금/삭제 프로그램에 등록하십시오. 이 프로그램은 모바일 장치를 어디에 두었는지 기억나지 않을 경우 위치를 알려주거나, 분실 또는 도난시 원격으로 모바일 장치를 잠그거나 저장된 것들을 삭제할 수 있게 해줍니다.

모바일 장치의 판매, 기부 혹은 폐기처분에 앞서 저장된 정보를 반드시 전부 삭제해 아무도 여러분의 개인 정보에 접근하지 못하도록 하십시오. CTIA-The Wireless Association은 특정 모바일 장치의 정보 삭제에 관한 유용한 정보와 설명에 관한 웹사이트 링크를 제공합니다 (bit.ly/1jeEDZN).

AARP (bit.ly/1FfksoF)에서 사이버 보강(cyberproofing)에 대한 상세한 정보를 얻을 수 있습니다.

앱(Apps): “앱”은 모바일 장치들을 위해 특별히 설계된 소프트웨어 응용 프로그램입니다. 스마트폰이나 태블릿의 기능 대부분은 다운로드 받은 앱들에서 오며 여러분의 신체건강 관리, “셀피(selfie)” 올리기, 친구들 에게 내 저녁식사 장소 알려주기, 투자 관리, 친구들과 단어 맞추는 게임하기 등과 같이 아주 많은 것들을 가능하게 합니다. 이러한 강력한 소프트웨어들이 여러분이 원하는 방향의 반대가 아닌 여러분이 원하는 방향으로 사용되게 하십시오.

◆ 앱을 검사해 보십시오. 믿을 수 있는 곳에서만 앱을 다운 받으십시오. 사용자 경험담을 읽어 보시고 다운 받기 전에 개발자가 합법적인지도 알아 보십시오.

◆ 여러분이 원하는 만큼의 개인 정보 보호 수준을 앱에 설정하십시오. 많은 앱들이 여러분의 연락처나 일정표, 그리고 위치와 같은 사용자의 개인 정보를 검색하고 공유하는 기능

에 의존하고 있습니다. 앱의 수집 및 공유 기능을 조정하려면 앱 자체 설정(모바일 장치 설정이 아닌)을 체크해 보십시오. 해당 앱이 여러분이 안전하다고 생각하는 것보다 더 많은 개인 정보를 수집할 경우 다운 받지 마십시오. 가능할 경우 해당 앱의 개인 정보 보호 방침에 대해서도 알아 보십시오. 만약 이러한 정보 방침을 알아 볼 수 없을 경우 다른 앱의 선택을 고려해 보십시오.

◆ 여러분의 위치를 다른 사람들에게 알려 주는 앱은 피하거나 가능할 경우 그 기능을 꺼두십시오. 여러분의 실질적인 위치를 타인과 공유하는 것은 집에 강도가 침입 할 수 있는 위험에 빠질수 있으며 그렇지 않다 하더라도 여러분의 안전과 개인 정보 보호에 해가 됩니다. (지도 제공이나 길안내와 같은 일부 앱들은 서비스 제공을 위해 여러분의 위치를 이용하지만 공개하지는 않습니다.)

◆ 소프트웨어 업데이트가 나올때마다 설치해 항상 최신 버전의 앱을 사용하도록 하십시오.

◆ 여러분이 허락 하고자 하는 것보다 더 많은 양의 개인 정보를 수집하거나 공유할 계획일 경우 앱을 제거할 수 있도록 앱의 사용약관이나 개인 정보 보호 방침 변경 통지서들을 읽어 보십시오. 앱과 변경 내용의 중요성에 따라 직접 통지(일반적으로 이메일이나 "푸시 알림(push notification)"으로 알려진 해당 앱 내에서 받을수도 있습니다.)를 받을 수도 있습니다. 그 밖의 경우 변경 사항을 알 수 있는 유일한 방법은 앱 내의 해당 부분을 찾아 보거나 앱의 웹사이트를 방문해 찾아 보는 것입니다.

안전한 소셜 미디어

많은 사람들에게 소셜 미디어를 이용하는 것은 일상생활의 일부분입니다. 여러분이 선택한 사람들만을 상대로 자신이 원하는 것들만 공개한다면 공유는 좋은 것일 수 있습니다. 필요이상의 공유에 의한 잠재적인 문제를 피하기 위해 게시물, 트윗(tweet) 혹은 다른 개인 정보를 밝힐수 있는 행동을 취하기 전 다시한번 생각해 보시고, 다른 사람들이 볼수 있는 내용들을 제한 시킬 수 있는 도구들을 이용 하십시오.

개인정보 보호: 소셜미디어를 이용하는 모든 사람이 여러분의 이익을 최우선으로 생각하지는 않습니다. 여러분의 개인 정보가 의도하지 않은 방법으로 이용되지 않도록 누구와 무엇을 공유할지에 대해 현명한 선택을 하는 것이 중요합니다.

아무와도 공유하지 않음, 친구들만과 공유 또는 일반 대중과 공유 등과 같이 소셜 미디어 네트워크의 개인 정보 보호 설정을 본인이 원하는 수준으로 조정하는 것부터 시작하십시오. 먼저 본인의 계좌에 로그인 한 다음 "Privacy(개인 정보)," "Privacy Controls(개인정보 조정)," "Privacy Settings(개인정보 설정)," "Account Settings(계좌 설정)" 또는 "Preferences(환경 설정)"과 같은 식별표나 제목을 찾으십시오. 이들을 찾기 힘들 경우 해당 웹사이트의 "도움" 기능을 이용하거나 웹사이트의 고객 지원팀에 이메일을 보내십시오.

신분 증명 목적(그리고 신분 도용)으로 이용될 수 있는 이름, 주소, 전화번호, 어머니의 결혼 전 성함 또는 생일 등과 같은 개인 정보를 공유하지 마십시오. 그리고 여러분 자신과 재산을 위험에 빠뜨릴 수 있는 현재 위치나 여행 계획 같은 내용의 공유는 삼가해야 합니다.

모르는 사람으로 부터의 초대 또는 "친구" 제의는 받아들이지 않는 것이 좋습니다.

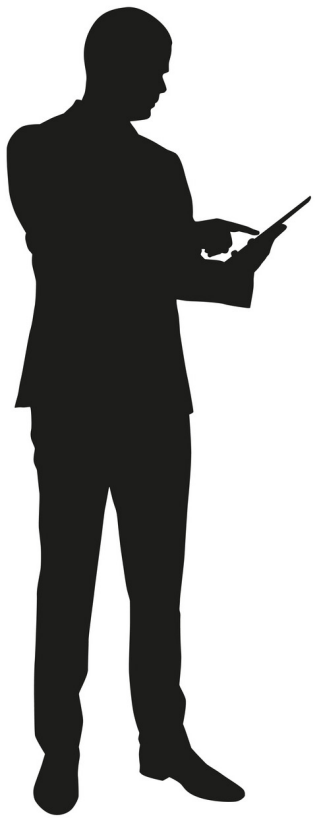
소비자 보호단체의 출판물인 '소셜 미디어 이용자들을 위한 개인 정보 보호와 관리' (*bit.ly/1xPC8PO*)에서 상세한 정보를 얻을 수 있습니다.

여러분의 온라인 평판(e-reputation) **보호하기:** 사진, 동영상, 활동 내용, 의견 등과 같이 여러분이 공유하는 내용들은 여러분 자신에 관한 것들을 밝힙니다. 온라인 평판을 보호하고 관리하는 것은 여러분 자신이 곤경에 빠질수 있는 경우을 방지하며 나쁜 인상으로 인한 잠재적인 문제를 피할 수 있도록 합니다. 다음은 소셜 미디어로 인한 문제들로부터 자신을 보호하는 가장 좋은 "습관들"입니다.

◆ 고용주, 채용담당자, 대학 입학 사정관, 대출 기관, 집주인, 고객/의뢰인, 정부 기관, 보험 회사 또는 그 밖의 의사 결정권자가 여러분이 공유하는 것들에 대해 어떻게 생각할지 고려해 보십시오. 여러분이 개인적으로 모르는 많은 사람들이 여러분에 대해 알아보기 위해 소셜 미디어를 이용할 수 있다는 점을 깨달아야 합니다.

◆ 여러분이 선택한 사람들과만 공유했다고 짐작하는 것들을 "친구"가 재 게시, 재 트윗 혹은 다른방법으로 드러낼 수 있다는 점을 유의해야 합니다. 그리고 만약 여러분이 다른 사람의 프로파일에 게시물을 등록했다면, 여러분은 누가 그 게시물을 볼수 있는지에 대한 제한권이 전혀 없습니다.

◆ 필요할 경우 되짚어 보십시오. 과거에 공유했던 것들을 더이상 미래의 사용자들에게는 보이지 않도록 몇몇 소셜 미디어 사이트들은 게시물 삭제, 사진 제거, 공유자 변경 등을 가능케 합니다. (물론 이미 공유했던 것들을 본 사람들에 대해서는 아무런 도리가 없습니다.)



◆ "구글"로 자신의 이름을 검색했을 때 어떤 것들이 나오는지 확인해 보십시오. 다른 사람들에게 여러분이 포함된 원치 않은 사진, 동영상 또는 게시물들을 제거해 줄 것을 요청하십시오.

◆ 여러분의 계좌가 해킹을 통해 본인에게 불리하게 사용되지 않도록 계좌 보안을 확실히 하십시오.

구글의 안전 센터(*bit.ly/1FunANi*)에서 온라인 평판 관리에 대한 상세한 정보를 얻을 수 있습니다.

가족 친화적인 인터넷

인터넷은 성인들에게 뿐만아니라 모든 연령의 어린이들에게 풍부한 고품질정보를 제공합니다. 여러분의 가족이 부적절한 내용은 피하면서 인터넷이 제공하는 것들을 최대한 즐길수 있도록 여러분이 취할수 있는 보호 장치와 예방책들이 있습니다.

부적절한 정보 차단: 어린이들의 연령에 적합하고 우수한 정보들은 아주 많습니다. 또한 부적절한 정보들도 많습니다. 정보가 제공되는 많은 업체-광대역 서비스 제공업체 부터 소셜 미디어 업체-들은 온라

인 이용 가능 시간부터 특정 웹사이트 방문 제한, 특정 동영상 시청 제한, 특정 게시판 및 대화방 제한 등과 같이 모든 것을 부모님들이 관리할 수 있도록 하고 있습니다.

가족 온라인 안전 연구소(the Family Online Safety Institute (*bit.ly/1L63Emf*)) 와 구글 안전 센터 (*bit.ly/1G2F7XP*)에서 자녀 보호(parental controls)에 대한 상세한 정보를 얻을 수 있습니다.

의사소통 관찰: 모든 정보가 어린이들을 위해 적절치 않은 것처럼 소셜 미디어를 이용하는 모든 사람들이 여러분의 자녀 보호에 대해 고려하지는 않습니다. 부모로써 여러분 자신이 온라인상에서 자녀분들의 관계를 위한 가장 큰 역할을 맡은 사람입니다.

자녀들에게 온라인에서 어떻게 안전하고 책임감을 가질수 있는 지에 대해 얘기해 보십시오. 방문이 허락되는 웹사이트들과 온라인에서 대화가 허락되는 상대들에 대한 규칙을 명확히 정해 주십시오. 자녀들과 온라인 "친구"가 되어 소셜 미디어에서 자녀들이 공유하는 정보를 볼 수 있도록하고 또한 다른 사람들이 자녀들과 공유하는 정보도 볼 수 있도록 하십시오. 인터넷에서 "만난" 누군가를 보러 혼자 나가서는 안된다는 것을 명확히 알리십시오. 자녀들이 부적절한 온라인 대화에 대해 말했을 경우 벌을 주거나 인터넷 이용을 금지시키지 않겠다는 약속을 하십시오. OnGuardOnline.gov (*http://bit.ly/2eewlAl*)에서 유용한 정보를 확인해 보십시오.

학교 관계자들, 지역 경찰 또는 CyberTipline (*bit.ly/1NMiQDY* 또는 800-843-5678)과 같은 적절한 기관에 괴롭히거나 약탈적 행동들을 행할 경우 신고하십시오.

원치 않는 마케팅 방지: 많은 온라인 업체들이 이용자들의 개인 정보를 수집 합니다. 일부 업체들은 선호 할 만한 영화 및 책을 추천하는 것과 같은 사용자 경험 향상과 최적화를 위해 이러한 개인 정보를 이용하며 다른 업체들은 비슷한 관심사를 가진 사람들의 흥미를 끌기 위한 마케팅 메시지 제작에 이용합니다. 데이터 브로커로 알려진 또다른 업체들은 소비자 정보를 수집해 제삼자 마케팅 업체나 그 밖의 광고와 이벤트 목적으로 수집된 정보를 이용하는 업체에게 판매 합니다. 믿을 만한 회사들은 소비자 정보 이용에 대한 투명성을 유지하며 소비자들에게 정보 공유 여부에 대한 결정권을 제공 합니다.

여러분의 개인 정보가 어떻게 사용될지 그리고 여러분의 개인 정보에 대한 관리 능력을 배울 수 있는 방법들이 있습니다.

◆ 해당 사이트가 언제 어떻게 개인 정보를 수집, 이용 그리고 공유하는지 알수 있도록 해당 업체의 "개인 정보 보호 방침" 또는 "정보 이용 방침"을 읽어 보십시오. 해당 업체의 방침에 만족하지 못할 경우 사용자에게 더 많은 권한을 부여하는 다른 웹사이트를 찾아보십시오.

◆ 자녀가 있을 경우 방문하는 웹사이트에서 개인정보를 공개하지 말것을 당부 하십시오. 어린이 온라인 개인 정보 보호법(the Children's Online Privacy Protection Act, COPPA)에 따르면 웹사이트들이 13세 미만의 어린이로부터 개인 정보를 수집 또는 이용하려면 부모의 동의를 받을 것을 규정하고 있습니다. 위반 사항은 연방 통상위원회(*www.ftccomplaintassistant.gov* 또는 877-FTC-HELP)로 신고하십시오.

◆ 적절할 경우 인터넷 브라우저가 여러분이 방문한 웹사이트와 페이지 정보를 저장하지 않고 원치 않는 광고창이 뜨는 것을 막아주는 팝업창 차단 기능을 사용하는 인터넷 브라우저의 "개인보호 브라우징(Private browsing)"을 사용 하십시오. (팝업창 차단은 판매 웹사이트의 "쇼핑 카트" 또는 "쇼핑백"에 있는 물건들을 기억하는 것과 같은 바람직한 기능을 방해할 수도 있습니다.)

◆ 해당 서비스에 등록하거나 이를 이용하기 위해 요구되는 최소한의 정보(대부분 별표로 표시됨)보다 더 많은 정보를 제공할만한 합당한 이유가 있는지 생각해 보십시오. 가능한한 가장 적은 양의 개인정보만 제공 하십시오.

◆ 순순해 보이는 단순한 퀴즈나 게임에 참가하는 경우와 같이 겉으로는 문제가 없어 보이지만 검증되지 않은 웹사이트에 개인정보를 제공할 경우 언제든 의도하지 않은 목적으로 사용될수 있다는 점을 이해해야 합니다.

기술은 의사소통, 업무 수행, 학습, 창조, 공유 그리고 즐거움 등을 위한 새로운 방법을 끊임없이 제공합니다. 이러한 기회를 놓치지 마십시오. 하지만 조심해야만 합니다. 여러분과 여러분 가족의 온라인 안전 유지를 위한 모두의 노력에 동참 하십시오. ■

컨수머 액션(Consumer Action)에 관하여

www.consumer-action.org

소비자 보호단체는 다양한 언어의 교육 출판물, 지역 사회 봉사 활동 그리고 문제에 초점을 맞춘 옹호 등을 통해 전국의 소수 소비자들이 시장에서 자신의 권리를 주장하고 경제적으로 번영할 수 있도록 돕습니다.

소비자 보호단체의 조언 및 추천 핫라인으로 소비자 불만을 신고하십시오: *http://www.consumer-action.org/hotline/complaint_form* 또는 415-777-9635.

중국어, 영어 그리고 스페인어로 상담 가능

이 출판물은 구글과 제휴해 만들었습니다.