개인정보 오남용 피해예방 10계명

계명 1. 회원가입을 하거나 개인정보를 제공할 때에는 개인정보취급방침 및 약관을 꼼꼼히 살핍니다.

사업자는 [정보통신망 이용촉진 및 정보보호 등에 관한 법률]에 따라 회원가입 등의 방법으로 개인정보를 수집하고자할 경우, 개인정보 수집 및 이용목적, 보유 및 이용기간, 위탁 업무의 내용 및 수탁자 등 개인정보 취급 관련 내용을 개인정보취급방침에 포함하여 공개하도록 하고 있습니다. (제27조의 2) 따라서 이용자는 회원가입을 하거나 개인정보를 제공할 경우 사업자의 개인정보 수집 및 이용목적 등을 자세히 검토한 후 가입/제공 하여야 합니다. 개인정보침해 신고센터 (privacy.kisa.or.kr) 개인정보취급방침 동영상 : "개인정보취급방침 동영상-이렇게 작성/제공 하세요" 개인정보취급방침 작성요령 : 개인정보 취급방침 작성 안내문 download [자료실] → 개인정보 취급방침 작성 예시

계명 2. 회원가입시 비밀번호를 타인이 유추하기 어렵도록 영문/숫자 등을 조합하여 8자리 이상으로 설정합니다.

안전한 패스워드란 제3자가 쉽게 추측할 수 없으며, 인터넷을 통해 전송되는 정보를 해킹하여 이용자 패스워드를 알 수 없거나 알 수 있어도 많은 시간이 요구되는 패스워드를 말합니다. 개인정보침해 신고센터 접속 → [공지사항] → "패스워드 선택/이용 가이드 및 암호이용 가이드라인"

계명 3. 가급적 안전성이 높은 주민번호 대체수단(아이핀;i-PIN)으로 회원가입을 하고, 꼭 필요하지 않은 개인정보는 입력하지 않습니다.

아이핀(i-PIN)은 인터넷상 개인식별번호(Internet Personal Identification Number)로써, 대면확인이 어려운 온라인에서 본인확인을 할 수 있는 수단의 하나입니다. 인터넷이용자가 주민등록번호를 제공하지 않으면서 본인확인을 할 수 있는 방법 이므로 개인정보(주민등록번호)의 오/남용을 줄일 수 있습니다. i-PIN은 이용자가 인터넷 사이트 회원가입이나 성인인증 등을 위해 자신의 신원정보를 본인확인기관에 제공하고 본인확인이 필요할 때마다 식별ID와 비밀번호를 이용하여 본인확인을 받는 방법으로, 다수의 본인확인기관이 서비스를 제공하고 있습니다. 개인정보침해 신고센터 (privacy.kisa.or.kr) [주요사업] → [아이핀] → [자료실] → 안내책자 "개인정보보호와 i-PIN", "사례를 통해 알아보는 i-PIN", "이용자를 위한 아이핀 안내리플릿"

계명 4. 자신이 가입한 사이트에 타인이 자신인 것처럼 로그인하기 어렵도록 비밀번호를 주기적으로 변경합니다.

권장하는 패스워드 변경주기는 6개월 이며 패스워드 변경 시 이전에 사용하지 않은 새로운 패

스워드를 사용하고 변경된 패스워드는 예전의 패스워드와 연관성이 없어야 합니다. 개인정보침해 신고센터 접속 →[공지사항]→ "패스워드 선택/이용 가이드 및 암호이용 가이드라인"

계명 5. 타인이 자신의 명의로 신규 회원가입 시 즉각 차단하고, 이를 통지받을 수 있도록 명의도용 확인서비스를 이용합니다.
명의도용 확인 서비스 사이트 크레딧뱅크(http://www.creditbank.co.kr), 사이렌24(http://www.siren24.com), 마이크레딧(http://www.mycredit.co.kr) 자신의 개인정보가 노출되어 타인이 자신의 명의로 자신도 모르게 회원가입이 되어있는 경우가 있으므로 명의도용확인 서비스를 이용하여 인터넷 가입정보 확인, 정보도용 차단, 실명인증기록 조회 등을 확인할 수 있습니다.

계명 6. 자신의 아이디와 비밀번호, 주민번호 등 개인정보가 공개되지 않도록 주의하여 관리하며 친구나 다른 사람에게 알려주지 않습니다.

주위의 친구나 가족에게 자신의 아이디나 비밀번호, 개인정보를 공개하여 타인이 본인의 정보를 악용하기도 하므로 가능한한 자신의 개인정보는 접근 권한을 제한하거나 주의하여 관리하여 본인의 개인정보 오/남용을 최대한 막아야 합니다.

계명 7. 인터넷에 올리는 데이터에 개인정보가 포함되지 않도록 하며, P2P로 제공하는 자신의 공유폴더에 개인정보 파일이 저장되지 않도록 합니다.

P2P(peer to peer)서비스는 인터넷에 연결된 모든 개인 PC로부터 직접 정보를 제공받고 검색은물론 내려 받기까지 할 수 있는 서비스로 웹사이트에 한정되어 있던 정보추출 경로를 개인, 회사가 운영하는 DB까지 확대할 수 있습니다. 따라서 자신의 개인정보 또는 다른 사람의 개인정보를 공유폴더에 저장하여 P2P 사이트에 올리는 것은 개인정보 노출 및 오/남용을 극대화 하는 것이라 볼 수 있으므로, 개인정보가 포함된 파일은 홈페이지나 공유폴더에 게시하지 않고 개인 메일로 전송하거나 오프라인에서 배포하여야 합니다. [관련사례] 인터넷P2P 사이트를 통해 주민등록번호를 수집하여 중국에서 가짜 주민등록증을 만들어 국내로 들여온 뒤 이를 대포폰, 대포통장을 개설 및 고급 승용차 구입 등에 악용

계명 8. 금융거래 시 신용카드 번호와 같은 금융 정보 등을 저장할 경우 암호화 하여 저장하고, 되도록 PC방 등 개방 환경을 이용하지 않습니다.

신용카드 번호와 같은 금융정보 등의 중요한 개인정보들을 문서에 작성하여 저장할 경우 암호화기능을 제공하는 문서프로그램(한글,MS 오피스 등)을 사용해야 합니다. 개인정보가 담긴 문서를 프린트하여 다른 사람들이 볼 수 있는 곳에 두거나, 문서파일을 PC방 등 개방 환경에서 사용 및 복사를 자제하고, 복사 시 반드시 삭제하여야 합니다. 이용자가 개인 PC에 파일을 저장할 경우 암호화 저장 방법은 다음과 같이 할 수 있습니다. 한글 : 상단 탭에서 파일 → 문서암호 워드2003 : 상단 탭에서 도구 → 옵션 → 보안 탭 → 이 문서의 파일 암호화 옵션

계명 9. 인터넷에서 아무 자료나 함부로 다운로드 하지 않습니다.

인터넷상에서 정확히 모르는 파일을 다운로드 하게 되면 그 파일이 개인정보를 유출하는 프로그램일 경우도 있고 해킹 프로그램일수도 있어 파일을 다운로드 시행 했을 시 이용자 개인 PC에 있는 개인정보를 유/노출 시킬 수 있으므로 파일 내역을 잘 모르거나 의심이 가는 자료는 다운로드 하지 않습니다.

계명 10. 개인정보가 유출된 경우 해당 사이트 관리자에게 삭제를 요청하고, 처리되지 않는 경우 즉시 개인정보침해신고센터 (국번없이 118, privacy.kisa.or.kr)에 신고합니다.

개인정보침해신고센터는 신속한 신고 접수 및 대처 요령에 대해 상담을 하고 있습니다.

발췌 : privacy.kisa.or.kr