전자금융 이용자 정보보호 수칙

1. 금융회사에서 제공하는 보안프로그램을 반드시 설치하기

전자금융거래를 위해 금융회사의 홈페이지에 접속하면 해당 금융회사에서 제공하는 보안프로그램이 자동적으로 설치됩니다. 이 때, 임의로 설치를 중단하거나 설치된 보안프로그램의 실행을 중지시키지 않아야 합니다. 또한 자동적으로 설치가 되지 않을 경우에는 설치 안내에 따라 수동으로 보안프로그램을 꼭 설치한 후에 전자금융거래를 해야 합니다. 이는 금융거래 내용을 타인에게 노출되지 않도록 하기 위함입니다.

2. 전자금융에 필요한 정보는 수첩, 지갑 등 타인에게 쉽게 노출될 수 있는 매체에 기록하지 않고 타인에게(금융회사 직원을 포함) 알려 주지 않기

전자금융 거래에 필요한 정보가 타인에게 알려지는 일이 없도록 분실가능성이 있는 수첩, 지갑 등에는 관련 정보를 기록하지 말아야 합니다. 또한, 타인에게 절대 전자금융거래 관련 정보를 알려주지 말며, 특히 은행 직원을 사칭하여 정보를 취득하는 경우가 있으므로, 은행창구가 아닌 곳에서는 은행직원이라고 말 하더라도 금융정보를 알려주지 말아야 합니다. 금융기관에서는 전화나 메일 상으로 개인의 금융정보를 요구하지 않습니다.

3. 금융 계좌, 공인인증서 등의 각종 비밀번호는 서로 다르게 설정하고 주기적으로 변경하기

비밀번호는 본인확인을 위한 수단이므로 생일, 전화번호 등과 같이 타인이 알기 쉬운 번호를 사용해서는 안 됩니다. 또한, 가능한 범위내에서 비밀번호 자릿수를 최대한 늘리고, 영문자도 혼합. 사용하며, 각각 다른 번호를 사용하고, 주기적으로 변경하여 타인이 비밀번호를 예상하지 못하도록 해야 합니다.

4. 금융거래 사이트는 주소창에서 직접 입력하거나 즐겨찾기로 사용하기

스팸메일 본문이나 게시판, 대출사이트 등에 링크되어 있는 URL을 그대로 클릭할 경우 개인정보나 금융정보를 빼내 가려는 해당 기관의 사칭사이트로 연결될 수 있기 때문에 금융거래 사이트는 주소창에 올바른 주소를 직접 입력하거나 즐겨찾기에 추가하여 사용해야 합니다.

5. 전자금융거래 이용내역을 본인에게 즉시 알려주는 휴대폰 서비스 등을 적극 이용하기

금융회사에서는 신용카드 사용내역, 계좌 이체내역 등 전자금융거래 이용내역을 실시간으로 휴대폰 SMS나 메일을 통해 알려주는 서비스를 제공하고 있으니, 이를 적극적으로 활용하시어 타인이 무단으로 전자금융거래를 이용하였을 경우 곧바로 이를 신고하여 피해를 예방할 수 있도록 해야 합니다.

6. 공인인증서는 USB, 스마트카드 등 이동식 저장장치에 보관하기

공인인증서는 신원확인 및 거래사실 증명 등을 위해 사용되는 중요한 거래 수단이므로, 해킹위험을 예방하고 공인인증서를 보다 안전하게 이용하시기 위해서는 하드디스크에 저장하여 사용하는 것보다는 이동식 저장장치를 활용하시는 것이 좋습니다. 또한, 이동식 저장매체를 이용하면 어느

PC에서든 공인인증서를 편리하게 이용하실 수 있습니다. 단, 이동식 저장장치를 분실하지 않도록 유의해야 합니다.

7. PC방 등 공용 장소에서는 인터넷 금융거래를 자제하기

여러 사람이 사용하는 공용 PC는 바이러스나 트로이목마 등 악성코드가 설치되기 쉬어 해킹 당하기 쉽습니다. 또한 공용 PC에서 공인인증서를 다운받아 전자거래를 이용할 경우 개인정보나 비밀번호 등 금융거래 정보의 노출 위험이 있습니다. 따라서, 공용장소에서는 가급적 전자금융 거래 이용을 하지 않는 것이 좋습니다.

8. 바이러스백신, 스파이웨어 제거프로그램을 이용하고 최신 윈도우보안패치를 적용하기

백신프로그램과 스파이웨어 제거프로그램은 PC의 보안을 위해 꼭 설치하며, 컴퓨터가 시작되면 자동 실행 및 자동 업데이트 되도록 설정합니다. 또한 윈도우즈 취약점을 이용한 해킹이나 웜바이러스를 막기 위해 윈도우 보안패치를 설치하고, 최신 업데이트를 유지하기 위해 자동 업데이트 기능을 이용하도록 합니다.

※자세한 설정방법은 정보보호실천수칙1(http://www.boho.or.kr) 참조하시기 바랍니다.

9. 의심되는 이메일이나 게시판의 글은 열어보지 말고, 첨부파일은 열람 또는 저장하기 전에 백신으로 검사하기

출처가 불분명하고 본문 내용이 본인과 직접적인 관련이 없는 경우 메일이나 게시물은 삭제하거나 무시하고, 꼭 필요한 경우에는 실행하거나 저장하기 전에 반드시 백신으로 점검하여 바이러스나 악성코드에 감염되지 않았는지 여부를 확인하여야 합니다.

10. 선수금 입금 요구, 상식수준 이상의 대출 조건을 제시하는 경우 해당 금융회사에 동 대출 취급여부를 직접 확인하기

최근 인터넷 포털 사이트 등에 신용에 관계없이 즉시대출을 해준다는 등 상식수준 이상의 대출 조건을 제시하는 광고를 게재한 후 이를 통해 급전이 필요한 사람에게 접근하여 은행직원을 사칭, 거래실적이 필요하다면서 돈을 입금토록 하는 등 선수금 입금을 요구하는 사기 금융사고가 발생하고 있으므로 이에 유의해야 합니다.