전자금융거래 이용자 10계명

1 전자금융거래 비밀번호와 계좌비밀번호를 반드시 다르게 사용할 것

- 실명확인번호, 생년월일, 전화번호, 차량번호, 연속숫자 등 타인이 알기 쉬운 번호를 사용하지 말아야 합니다.

2 비밀번호를 정기적으로 변경하고, 특히 비밀번호가 노출되었다고 의심되는 경우 빠른 시간 내에 금융회사 앞 통보 및 변경 조치할 것

- 각각 다른 번호를 정기적으로 변경하여 타인이 비밀번호를 예상하지 못하도록 해야 합니다.

3 공동인증서는 USB, IC카드 등 이동식 저장장치에 보관할 것

- 공동인증서는 신원확인 및 거래사실 증명 등을 위해 사용되는 중요한 수단이므로 해킹위험을 예방하고 보다 안전하게 이용하기 위해서는 하드디스크보다 USB등 이동식 저장장치에 저장하는 것이 좋습니다.

4 출처가 불분명한 이메일이나 의심되는 게시판의 글은 열어보지 말 것

- 출처가 불분명하고 본인과 직접적인 관련이 없는 메일이나 게시물은 삭제하거나 무시하고, 첨부된 파일을 열람 또는 설치하기 전에 반드시 백신 프로그램 등으로 바이러스나 악성코드 감염여부를 먼저 검사하는 것이 바람직합니다.

5 전자금융거래에 필요한 정보를 수첩, 지갑 등에 기록하지 말 것

- 전자금융거래에 필요한 정보가 타인에게 알려지는 일이 없도록 분실 가능성이 있는 수첩, 지갑 등에 관련 정보를 기록하지 말아야 합니다.

6 휴대폰 문자통보서비스(SMS), 일회용비밀번호(OTP) 이용하기

- 현금인출 또는 자금이체를 친구 및 동료에게 부탁하지 말아야 하며, 금융회사 직원 등 누구에게도 비밀번호를 알려주지 말아야 합니다.
- 아울러 금융기관에서는 전화나 메일상으로 개인의 금융정보를 요구하지 않습니다.

7 전자금융거래 이용내역을 본인에게 즉시 알려주는 서비스를 적극 이용할 것

- 전자금융거래 내역을 본인의 핸드폰 등으로 실시간 확인할 수 있는 문자서비스(SMS) 등을 이용하여 타인이 무단으로 전자금융거래를 이용하였을 경우 인지 즉시 금융회사에 신고하여 피해를 예방할 수 있도록 해야 합니다.

8 PC방 등 개방된 컴퓨터는 가급적 사용을 자제하고, 사용한 경우에는 관련 정보를 삭제할 것

- 여러 사람이 사용하는 공용PC는 바이러스나 악성코드에 의해 해킹 당하기 쉽습니다.
- 공용PC에서 공동인증서를 다운받아 전자거래를 이용할 경우 개인정보나 비밀번호 등 금융거래 정보의 노출 위험이 있는 공공장소에는 가급적 전자금융거래 이용을 하지 않는 것이 좋습니다.

9 전자금융거래의 1회 이체한도 및 1일 이체한도를 적절히 설정할 것

10 인터넷 금융거래 이용하는 PC에 백신 프로그램 설치 및 최신윈도우 보안패치를 적용하여 해킹 등으로부터 PC를 보호할 것

- 백신 프로그램과 스파이웨어 제거 프로그램은 PC의 보안을 위해 꼭 설치해야 하며, 최신 해킹 공격을 예방하기 위해서는 윈도우 자동 업데이트 기능을 설정하는 것이 바람직합니다.