

## 예방요령

### 1 금융거래정보 요구는 일절 응대하지 말 것



- ↳ 전화로 개인정보 유출, 범죄사건 연루 등을 이유로 계좌번호, 카드번호, 인터넷뱅킹 정보를 묻거나 인터넷 사이트에 입력을 요구하는 경우 절대 응하지 말아야 하며, 특히 텔레뱅킹의 경우 인터넷뱅킹과 달리 공인인증서 재발급 등의 절차가 필요치 않아 타인이 취득 시 사기피해에 취약

### 2 현금지급기로 유인하면 100% 보이스피싱



- ↳ 현금지급기를 이용하여 세금, 보험료 등을 환급해 준다거나 계좌안전조치를 취해주겠다면서 현금지급기로 유인하는 경우 절대로 응하지 말 것

### 3 자녀납치 보이스피싱에 미리 대비



- ↳ 자녀납치 보이스피싱 대비를 위해 평소 자녀의 친구, 선생님, 인척 등의 연락처를 미리 확보할 것

### 4 개인·금융거래정보를 미리 알고 접근하는 경우에도 내용의 진위를 확인



- ↳ 최근 개인·금융거래정보를 미리 알고 접근하는 경우가 많으므로 전화, 문자메시지, 인터넷메신저 내용의 진위를 반드시 확인할 것

### 5 피해를 당한 경우 신속히 지급정지를 요청



- ↳ 보이스피싱을 당한 경우 경찰청 112콜센터 또는 금융회사 콜센터를 통해 신속히 사기계좌에 대해 지급정지를 요청할 것

### 6 유출된 금융거래정보는 즉시 폐기



- ↳ 유출된 금융거래정보는 즉시 해지하거나 폐기할 것

### 7 예금통장 및 현금(체크)카드 양도 금지



- ↳ 통장이나 현금(체크)카드 양도 시 범죄에 이용되므로 어떠한 경우에도 타인에게 양도하지 말아야 하며, 통장이나 현금(체크)카드 양도는 전자금융거래법 위반으로 형사처벌을 받을 수 있는 범죄임(5년 이하의 징역 또는 3천만원 이하의 벌금)

## 8 발신(전화)번호는 조작이 가능함에 유의



- ↳ 텔레뱅킹 사전지정번호제\*에 가입되었다 하더라도 인터넷 교환기를 통해 발신번호 조작이 가능하므로, 사기범들이 피해자들에게 “사전지정번호제에 가입한 본인 외에는 어느 누구도 텔레뱅킹을 이용하지 못하니 안심하라”고 하는 말에 현혹되지 말 것
- ❗ \* 사전에 등록된 특정 전화번호로만 텔레뱅킹을 할 수 있는 제도

## 9 금융회사 등의 정확한 홈페이지 여부 확인 필요




- ↳ 피싱사이트의 경우 정상적인 주소가 아니므로 문자메시지, 이메일 등으로 수신된 금융회사 및 공공기관의 홈페이지는 반드시 인터넷 검색 등을 통해 정확한 주소인지를 확인할 것


## 10 「전자금융사기 예방서비스」 적극 활용



- ↳ 타인에 의해 무단으로 공인인증서가 재발급되는 것 등을 예방하기위해 '12.9.25일부터 각 은행에서 시범 시행하는 「전자금융사기 예방서비스」 적극 활용할 것

### 정보관리 담당부서 안내

 담당부서 : 금융사기대응단 금융사기대응총괄팀

 전화번호 : 1332