찾기 쉬운 생활법령정보 Q&A

인터넷 이용자



글 | 법제처 법제정보과

법제처에서는 2008년 초부터 국민이 실생활에 필요한 법령을 쉽게 찾아보고 이해할 수 있도록 정부 각 기관의 업무 중심으로 복잡하게 얽힌 법령간의 관계를 국민의 생활 중심으로 재분류하고, 법률전문가의 시각에서 쓰인 어려운 법령의 내용을 국민의 눈높이에서 쉽게 해설하여 제공하는 『찾기 쉬운 생활법령정보시스템(http://oneclick.law.go.kr)』을 구축하여 2014년 3월 현재 약 220여 건의 생활분야에 관한 콘텐츠를 서비스하고 있습니다.

이 코너에서는 서비스 중인 생활분야에 대한 주요 궁금 사항에 대하여 질문과 답변의 형식을 빌려 그 주요내용을 차례로 소개하고자 합니다. 보다 자세한 내용은 『찾기 쉬운 생활법령정보시스템(http://oneclick.law.go.kr)』에 접속하셔서 '백문백답' 등을 통하여 찾아보실 수 있습니다.

Q **최근 인터넷, 휴대폰 등 전기통신 수단을 이용한 전자금융범죄가 빈번하게 발생하고 있는데요. 전자금융범죄의 종류에는 어떤 것들이 있나요?**

A 전자금융범죄의 주요 유형에는 피싱(Phishing), 스미싱(Smishing), 파밍(Pharming), 메모리해킹 등이 있습니다.

* 전자금융범죄의 주요 유형

- 피싱(Phishing)은 개인정보(Private data)와 낚는다(Fishing)의 합성어로 피해자를 기만 또는 협박하여 개인정보 및 금융거래정보를 요구하거나 피해자의 금전을 이체하도록 하는 수법을 말합니다.
- 스미싱(Smishing)은 문자메시지(SMS)와 피싱(Phishing)의 합성어로, 문자메시지를 이용하여 소액결제를 유도하거나, 스마트폰에 악성프로그램을 유포하여 개인정보 및 금융거래정보를 편취하는 수법을 합니다.

- 파밍(Pharming)은 피싱(Phishing)과 조작하다(Farming)의 합성어로 피해자 PC를 악성프로그램에 감염시켜 정상적인 사이트 주소를 입력하더라도 가짜 사이트로 접속되도록 조작한 후 금융거래정보를 빼내 금전을 부당하게 인출하는 수법을 말합니다.
- 메모리해킹은 피해자 PC 메모리에 상주한 악성프로그램으로 인하여 정상 사이트에 접속하더라도 거래오류를 발생시키거나 팝업창을 띄워 금융거래정보를 입력하게 한 후 금전을 부당하게 인출하는 수법을 말합니다.

Q **청첩장·돌잔치 초대를 사칭한 문자를 받거나 은행 등의 홈페이지를 모방해 만든 가짜 홈페이지를 발견하면 어떻게 해야 하나요?**

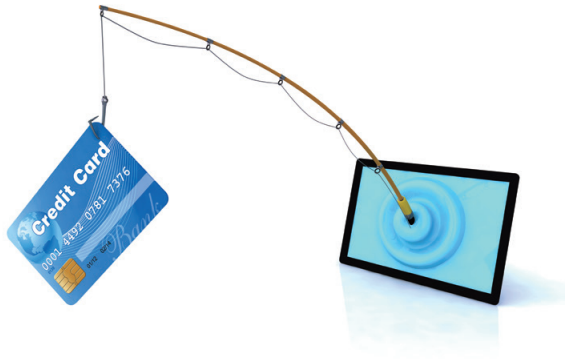
A 스미싱 등으로 의심되는 허위 문자나 가짜 홈페이지 즉, 피싱사이트를 발견하신 경우에는 최대한 빨리 신고를 하여 추가적인 피해를 예방하는 것이 중요합니다.

* 스미싱(Smishing) 대처방법

- 스미싱 등으로 의심되는 허위 문자를 받았다면 경찰청 사이버테러대응센터(☎182)로 신고하고, 해당 이동통신사의 고객센터에 소액결제서비스 차단을 신청하여 본인도 모르는 사이에 소액결제가 되지 않도록 해야 합니다.

* 피싱(Phishing) 대처방법

- 금융거래정보를 빼내기 위해 은행 등의 홈페이지를 모방하여 만든 가짜 홈페이지 즉, 피싱사이트로 의심되거나 확인된 경우에도 역시 경찰청 사이버테러대응센터(☎182)에 해당 사이트를 신고하여 추가적인 피해가 발생하지 않도록 해야 합니다.



Q **피싱·스미싱 등의 전자금융범죄로 인해 금전적인 피해가 발생한 경우 어떻게 해야 하나요?**

A 피해금을 송금·이체한 계좌를 관리하는 금융회사 또는 사기이용계좌를 관리하는 금융회사 등에 피해구제 신청을 하여 피해금을 환급받을 수 있도록 요청하면 됩니다.

* 지급정지 및 피해금 환급 신청

- 피싱 또는 파밍사기 등으로 인해 금전적인 피해가 발생한 피해자는 ① 신속히 경찰서나 금융회사 콜센터를 통해 지급정지 요청을 한 후 ② 해당 은행에 경찰이 발급한 '사건사고 사실확인원'을 제출하여 피해금에 대한 환급 신청을 하면 됩니다.

* 결제취소·환불 등의 요구

- 휴대폰 소액결제로 인해 피해를 입은 이용자는 해당 결제대행사의 고객센터, 미래창조과학부 CS센터(☎1355) 또는 휴대전화/ARS결제 중재센터(☎1644-2367) 등에 결제취소·환불 등을 적극적으로 요구할 필요가 있습니다.

Q **전자금융범죄를 당해 경찰에 신고하고 범죄 이용계좌를 지급 정지시킨 다음 확인해 본 결과 사기계좌에 피해금이 남아 있다면 다시 환급받을 수 있나요?**

A 전자금융범죄를 당한 경우에는 피해구제 신청을 하여 채권소멸절차를 거치면 범죄 이용계좌에 남아 있는 잔액의 범위 내에서 피해금을 환급 받을 수 있습니다.

* 전자금융범죄의 범위

- 「전기통신금융사기 피해금 환급에 관한 특별법」상 피해금 환급은 전기통신 금융사기의 피해자에 한정되고 "재화의 공급 또는 용역의 제공 등을 가장한 행위는 제외"된다는 점에 주의하셔야 합니다.
- "재화의 공급 또는 용역의 제공 등을 가장한 행위"는 중고사이트에서 물건을 사고 받지 못하는 사기를 당하는 경우가 이에 해당합니다. 이런 중고거래는 전기통신금융사기에 해당되지 않아 계좌를 지급정지 시키거나 환급을 받으실 수 없는 거래에 해당합니다.

* 피해구제 신청 방법

- 피해구제 신청은 피해금을 송금·이체한 계좌를 관리하는 금융회사 또는 사기이용계좌를 관리하는

금융회사에 하면 됩니다.

- 이 경우 금융회사에 피해구제신청서와 피해자의 신분증 사본을 첨부해 제출해야 합니다. 다만, 긴급하거나 부득이한 사유가 있는 경우에는 전화 또는 구술로도 신청할 수 있습니다.

* 피해금 환급 절차

- 피해구제 신청을 받은 금융회사는 다른 금융회사의 사기이용계좌로 피해금이 송금 · 이체가 되었다면 해당 금융회사에 지급정지를 요청하게 되고, 요청받은 금융회사는 입금내역 등을 확인한 후 계좌 전체에 지급정지 조치를 하게 됩니다.
- 금융회사는 지급정지 후 금융감독원에 채권이 소멸되는 절차를 개시하기 위한 공고를 요청해야 하며, 금융감독원의 개시 공고 후 이의제기 없이 2개월이 경과하면 해당 계좌의 채권이 소멸됩니다(「전기통신금융사기 피해금 환급에 관한 특별법」 제5조제1항 및 제9조제1항).
- 금융감독원은 채권소멸일로부터 14일 이내에 환급금액을 결정해 금융회사에 통지하고, 통지를 받은 금융회사는 지체 없이 피해환급금을 피해자에게 지급하는 것으로 절차가 마무리됩니다.

Q **보이스피싱과 같이 타인을 속여서 획득한 개인정보 및 금융거래정보를 이용하여 재산상 이익을 취득한 사람은 어떠한 죄로 처벌을 받게 되나요?**

A 전자금융범죄 행위는 「형법」상 사기죄, 사기방조죄 및 공갈죄 등으로 처벌됩니다.

* 사기죄에 따른 처벌

- 타인을 속여서 획득한 개인정보 및 금융거래정보를 이용하여 재산상 이익을 취득하는 범죄행위는 「형법」상 사기죄에 따라 처벌받을 수 있습니다.

* 컴퓨터등 사용사기죄에 따른 처벌

- 명의를 도용하여 공인인증서를 발급받거나 타인의 보안카드번호를 편취하여 예금을 이체하는 행위 또는 악성프로그램을 유포하는 등 권한없는 자에 의한 정보처리 업무를 통해 재산상 이익을 취득하는 범죄행위는 「형법」상 컴퓨터등 사용사기죄로 처벌받을 수 있습니다.

* 공갈죄에 따른 처벌

- 피해자에게 “아들을 납치했다” 또는 “개인정보가 유출됐다” 등의 말로 공포를 느끼게 하여

피해자의 재산을 편취하는 범죄행위는 「형법」상 공갈죄로 처벌받을 수 있습니다.

* 위반 시 제재

■ 위의 범죄행위를 한 경우에는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처해집니다.

※ 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」에 따른 처벌

그동안 전자금융범죄에 대한 처벌은 「형법」상의 사기죄 등을 통해 처벌해 왔으나, 「전기통신금융사기 피해금 환급에 관한 특별법」이 개정되어 전기통신금융사기죄가 신설됨으로써 2014년 7월부터는 변종 보이스피싱 행위를 포함한 대부분의 전자금융범죄는 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」에 따라 처벌되며, 처벌 수위도 한층 강화되었습니다.

Q **전자금융범죄의 숙주로 활용되고 있는 대포통장이 꾸준히 증가하고 있다고 하는데요. 피싱과 스미싱 등의 전자금융범죄에 이용된 대포통장의 명의인도 처벌 받게 되나요?**

A 단순히 명의대여자라 하더라도 통장 및 현금카드 등이 사기범행에 사용될 것을 알고 이를 양도한 사람은 「전자금융거래법」 위반죄와는 별도로 「형법」상 사기방조죄로 처벌 받을 수 있습니다.

* 「전자금융거래법」에 따른 처벌

■ 전자금융거래가 가능한 통장 및 현금카드 등을 타인에게 양도 또는 대여한 경우에는 「전자금융거래법」 위반죄로 처벌을 받을 수 있습니다.

■ 이를 위반한 경우에는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처해집니다.

* 「형법」에 따른 처벌

■ 직접 사기 범행에 가담하지 않았더라도 통장 및 현금카드 등이 사기범행에 사용될 것을 알고 이를 양도한 사람은 「전자금융거래법」 위반죄와는 별도로 「형법」상 사기방조죄에 따른 처벌을 받을 수 있습니다.

■ 위의 범죄행위를 한 경우에는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처해집니다.

Q **전자금융범죄의 수법이 날로 진화하고 변화하고 있지만 예방만이 최선의 길일 뿐 뚜렷한 대응책이 없다는 게 현실입니다. 전자금융범죄 피해를 예방하는 방법에는 어떠한 것들이 있나요?**

A 전자금융범죄 예방 기본 요령을 숙지하여 본인의 개인정보가 유출되지 않도록 항상 주의를 기울이고, "전자금융사기 예방서비스"에 가입하면 전자금융범죄에 따른 피해를 예방할 수 있습니다.

* 전자금융사기 예방서비스

- "전자금융사기 예방서비스"란 ① 공인인증서를 재발급 받거나(유효기간 내 갱신은 제외함) 타행(기관) 발급 공인인증서를 등록하는 경우, ② 인터넷뱅킹을 통해 300만원 이상(1일 누적기준) 이체 하는 경우에 본인확인 절차를 강화함으로써 전자금융범죄에 따른 피해를 예방하는 제도를 말하며, 개인 고객이 거래은행 인터넷뱅킹 홈페이지에서 신청할 수 있습니다.

* 소액결제 피해 예방

- 평상시 휴대폰 소액결제를 사용하지 않을 경우에는 통신사 콜센터를 통해 소액결제를 차단하거나 소액결제의 한도를 낮춰 두는 것도 전자금융범죄에 따른 피해를 예방할 수 있는 좋은 방법입니다.

* 전자금융범죄 예방 기본 요령

- 개인정보를 절대 알려주지 않습니다.
- 금융회사의 보안강화 서비스에 반드시 가입합니다.
- 금융회사는 온라인을 통해 보안승급 등을 요구하지 않는 점을 명심합니다.
- 인터넷뱅킹 거래 중 보안카드번호 등의 입력을 요구하는 팝업화면이 뜨는 경우 해당 정보를 입력하지 말고 거래 금융회사에 문의합니다.
- 금융회사의 인터넷뱅킹 사이트 이용 시 백신프로그램 등을 이용하여 악성프로그램을 탐지 · 제거합니다.
- 무료 다운로드 사이트 이용 자제 및 출처가 불분명한 파일은 다운로드를 받지 않습니다.
- OTP(일회용 비밀번호 생성기)·보안토큰(비밀정보 장치외부 복사방지) 등 안전성이 높은 보안매체를 사용합니다.

