



금융감독원

보도참고



금융보안원
FINANCIAL SECURITY INSTITUTE

보도	2026.7.6.(월) 조간	배포	2026.7.3.(금)		
담당부서	금융감독원 중소금융검사3국	책임자	국 장	김익남	(02-3145-8810)
		담당자	팀 장	이진우	(02-3145-8805)
	금융보안원 침해대응부	책임자	부 장	김기철	(02-3495-9400)
		담당자	팀 장	장운영	(02-3495-9420)

카드 부정 사용 피해를 줄이기 위한 「소비자경보」 발령 - 온라인 쇼핑몰 결제창, 진짜인지 한 번 더 확인하세요! -

■ 소비자경보 2026 - 21 호

등급	주의	경고	위험
대상	금융소비자 일반		

소비자경보 내용

◆ 최근 온라인 쇼핑몰 내 피싱·해킹에 의한 카드정보 탈취 정황이 확인되어, 카드 부정 결제 우려가 높아지고 있습니다.

→ 소비자는 카드정보 입력·결제시 다음을 반드시 유념하여 행동하세요!

※ 소비자 유의사항 및 행동요령

- 1 **결제 시 주민등록번호 전체 숫자, 비밀번호 전체 숫자 등의 과도한 개인정보 입력을 요구한다면 의심하고 이를 거절하세요!**
 - 일부 온라인 쇼핑몰에서 해커가 교묘하게 피싱 페이지를 구성하여 카드 정보를 탈취한 정황이 확인되어 주의가 필요합니다.
- 2 **온라인 쇼핑 후 카드정보 피싱 등이 의심되는 경우 즉시 카드사에 카드 정지·재발급 및 비밀번호 변경을 신청하세요!**
 - 카드사의 부정 사용 의심거래 알림(전화·문자 등)을 잘 확인하여 부정 결제 추가 피해를 막을 수 있습니다.
 - 카드정보 유출 의심이 있는 경우 불편하더라도 반드시 카드 사용 정지·재발급 및 비밀번호(PIN번호 포함)를 변경하는 것이 안전합니다.
- 3 **정보 유출 추가 피해가 의심되는 경우 경찰에 즉시 신고하세요!**
 - 비대면 금융사고 피해가 발생할 경우, 즉시 통합신고센터(☎112)에 신고하고, 사건사고사실원 등을 준비하여 카드사에 배상 신청하여야 합니다.

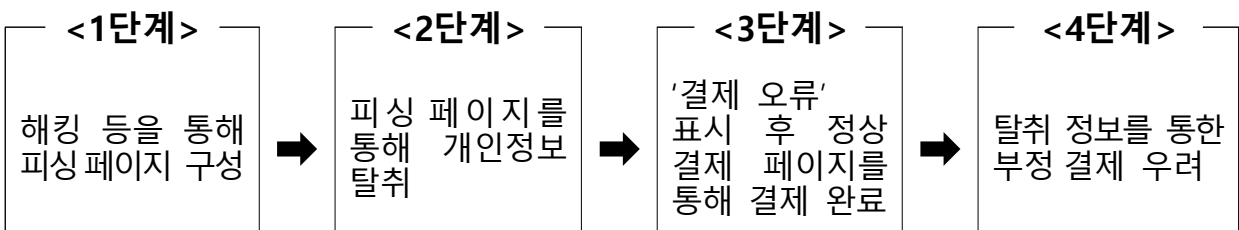
I. 소비자경보 발령 배경

- 최근 금융보안원은 국내 일부 온라인 쇼핑몰에 대한 해킹·피싱 공격으로 신용카드 정보를 탈취한 정황을 확인*하여, 금융감독원에 관련 내용을 통보
 - * 카드정보를 탈취하는 전문적인 공격조직에 의해 총 5,707건이 탈취('26.6.29. 현재)
- 이에, 금융감독원은 금융보안원·카드사와 긴밀한 공조 체계를 구축하여 즉각 대응 중
 - 금융보안원은 탈취된 카드 정보 등을 카드사에 전달하여, 부정 결제 시도를 차단토록 지원
 - 각 카드사는 정보 탈취 고객에 대한 개별 안내, 카드 재발급, 부정 결제 차단 등 소비자 보호 조치를 즉시 수행
- 한편, 탈취 정보가 부정 사용에 악용될 가능성이 매우 높고, 정보 탈취가 현재도 계속 진행될 수 있는 만큼 소비자 유의사항을 안내

II. 카드 정보 등 유출 경위

- ☑ 신원 미상의 공격 조직은 일부 보안이 취약한 온라인 쇼핑몰에 피싱 페이지를 구성하여 카드 정보 등을 탈취

<피싱 페이지를 통한 카드 정보 등 유출>



※ 카드 결제시, 실제 피싱 페이지 예시는 붙임 참조

- ① 일부 국내 온라인 쇼핑몰 내 카드 결제 과정에서 실제 결제 화면과 유사하게 꾸며진 피싱 페이지를 해킹 등을 통해 구성
- ② 피싱 페이지는 결제를 위해 카드 정보 등 개인정보를 모두 입력해야 하는 것처럼 착각하도록 설계되어, 정상 결제 과정에는 필요하지 않은 개인정보를 과도하게 수집·탈취

* 카드번호, 유효기간, CVC, 신용카드 비밀번호(전체), 주민등록번호 등

③ 카드 정보 탈취 이후 '결제 오류' 등 경고창 표시하고 정상 결제 페이지를 재호출하여, 결제 정보 재입력시 정상 결제 완료

※ 결제가 정상적으로 완료되어 소비자는 피싱 페이지를 인지하기 어려움 !!

④ 탈취 정보를 이용한 부정 결제가 발생할 개연성이 매우 높고, 카드 회원 개인정보와 비밀번호의 불법 유통 및 추가적인 피해* 발생 우려

* 개인정보 및 비밀번호(PIN번호 포함)가 노출되어 여러 사이트에서 동일 비밀번호를 중복 사용하는 경우, 크리덴셜 스테핑 등 추가 공격에 노출될 수 있음

※ [참고] 크리덴셜 스테핑(Credential Stuffing)

불법으로 습득한 아이디와 비밀번호(PIN번호) 등을 이용해 웹사이트 등에 무작위로 대입하여 로그인을 시도하여, 무단 결제(예: 상품권, 전자기기 등 현금성 높은 상품을 구매)하거나 추가적인 정보 유출을 야기하는 공격 기법

Ⅲ. 소비자 유의사항

① 결제 시 과도한 개인정보 입력을 요구하는 경우 일단 의심하세요 !

- 온라인 쇼핑몰 등에서 카드 결제 시 주민등록번호, 카드 비밀번호 전체 숫자 등 과도한 정보를 입력하도록 요구한다면 의심하고 이를 거절

→ 정상적인 결제 과정에서 주민등록번호 전체 숫자, 카드 비밀번호 네자리 등을 모두 입력하도록 요구하는 경우는 없습니다.

② 온라인 쇼핑 후 카드정보 피싱 등이 의심되는 경우, 카드사에 즉시 카드 정지, 재발급 및 비밀번호(PIN번호 포함) 변경을 신청하세요 !

- 카드사의 부정 사용 의심거래 알림(전화·문자 등)을 잘 확인하여 부정 결제 추가 피해를 미연에 방지
- 카드정보 유출 의심이 있는 경우라면 불편하더라도 반드시 카드 사용정지·재발급 받아 부정사용 가능성을 근절

→ 유출된 비밀번호(PIN번호 포함)를 다른 사이트에서 중복 사용하는 경우 반드시 변경하여 추가 피해를 예방하여야 합니다.

③ 정보 유출 추가 피해가 의심되는 경우 경찰에 즉시 신고하세요 !

- 비대면 금융사고 피해가 발생할 경우, 즉시 통합신고센터(☎112)에 신고(지급정지 요청)하고, 사건사고사실원 등을 준비하여 카드사에 배상 신청

※ 해킹 등 부정한 방법으로 탈취된 정보를 이용한 카드 부정 사용에 대해서는 소비자에게 고의·중과실이 없는 경우, 카드사에서 보상받을 수 있습니다.

☞ 본 자료를 인용하여 보도할 경우에는 출처를 표기하여 주시기 바랍니다.(<http://www.fss.or.kr>)

※ 이미지 제공 : 금융보안원

① 상품 구매페이지

회원가입 0 점

무분류수 무분류최

할인: 0 점

무분류용 적립: 0 점

* 정상적으로 결제가 완료되지 않은 주문에 사용한 쿠폰은 [마이페이지] > [주문내역] > [상세보기] 페이지에서 무분 사용 취소 후 다시 사용할 수 있습니다.

0 원 (보유적립금 : 3,000원)

적립금 10원부터 9,100원까지 사용이 가능합니다.
주문금액 최소 30,000원 이상 주문시 적립금 사용 가능.
보유적립금이 1,000원 이상 일 경우 사용하실 수 있습니다.

결제금액 12,100 원

• 결제수단

일반결제

무통장입금 신용카드 가상계좌

• 구매내용확인

구매내용확인 구매하실 상품의 상품정보 및 가격을 확인하였으며, 이해동의합니다. (전자상거래법 제8조 제2항)

결제하기 취소

CUSTOMER CENTER BANKING ACCOUNT

② 피싱 페이지 구성

상품명

상품금액 12,100 원

제공기간 자동결제

카드번호

CVC: 카드 뒷면 숫자 세자리

유효기간 MM 월 YYYY 년

생년월일 (4자리) YYMMDD 공용법인카드

비밀번호 앞 4자리

전채동의

전자금융거래 이용약관 보기 >

개인정보 수집 및 이용동의 보기 >

개인(신용)정보 제3차 제공 및 위탁동의 보기 >

자동결제 서비스 이용에 동의합니다.

③ 탈취 및 재결제 유도

checkout shop 내용:

카드사 오류로 인하여 결제 실패되었습니다. 앱을 통하여 다시 결제해주세요.

확인

④ 정상 결제 페이지

PAY KOR X

12,100 원

별도 제공기간 없음

포인트 무이자

롯데 5만원 이상 무이자 2-5개월

삼성 모니모페이로 결제하세요 !!

KB Pay(국민)	신한(SOL페이)	현대
하나Pay	비씨(페이북)	농협(NH페이)
우리	카카오뱅크	토스뱅크
케이뱅크	진빅	* 더보기