

• SK텔레콤(주)	• 하나생명보험	• 하나펀드서비스
• 하나금융지주	• 하나손해보험	• 하나금융티아이
• 하나은행	• 하나저축은행	• 하나벤처스
• 하나증권	• 하나자산신탁	• 핑크
• 하나카드	• 하나대체투자자산운용	• (사)SW교육혁신센터
• 하나캐피탈	• 하나에프앤아이	



contents

1장 디지털 금융 서비스

3

온라인 금융 서비스와 결제방식 · 5

- 01 온라인 금융이란? · 6
- 02 체크카드와 신용카드 · 13
- 03 간편결제와 온라인쇼핑 · 22
- 04 가짜쇼핑몰과 진짜쇼핑몰 구별하기 · 36

디지털자산 보호 · 45

- 01 디지털 자산이란? · 46
- 02 가상화폐와 블록체인 기술 · 53
- 03 온라인 बैं킹 · 61
- 04 내 자산을 노리는 범죄와 보호방법 · 66

2장 금융범죄와 사이버 보안

73

사이버 공격 알아보기 · 75

- 01 사이버공격이란? · 76
- 02 사이버공격의 유형과 사례 분석 · 81
- 03 사이버공격 예방 방법 · 98
- 04 사이버공격 발생시 대응방법 · 105

금융범죄와 사이버 보안 · 113

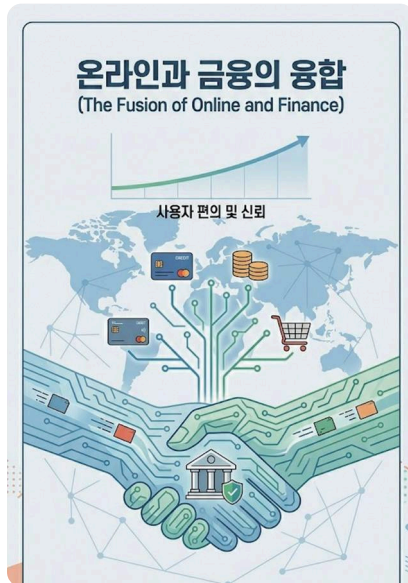
- 01 금융범죄의 이해와 피해현황 및 정부대책 · 114
- 02 금융범죄의 위험성 및 법적 책임 · 124
- 03 금융범죄 발생 시 상황별 대응방법 · 130



디지털 금융 서비스



온라인 금융 서비스와 결제방식



출처 : 제미나이



교육 목표

- 온라인 금융서비스의 특징과 장점에 대해 이해한다.
- 체크카드와 신용카드의 특징과 차이점에 대해 이해한다.
- 간편결제의 장점과 위험성에 대해 이해한다.
- 온라인쇼핑에 대해 이해하고 실제 온라인쇼핑을 이용할 수 있다.
- 가짜 쇼핑몰과 진짜 쇼핑몰을 구분하고 신중히 이용할 수 있다.



이런 활동을 해요

프로젝트 과정	기초	심화
	온라인 금융 서비스와 결제방식	디지털자산 보호
활동 내용	• 온라인 금융이란? • 체크카드와 신용카드 • 간편결제와 온라인쇼핑 • 가짜 쇼핑몰과 진짜 쇼핑몰	• 디지털 자산이란? • 가상화폐와 블록체인 기술 • 온라인 뱅킹 • 내 자산을 노리는 범죄와 보호방법

01

온라인 금융이란?

• 목 표 •

- 1 금융의 개념을 이해한다.
- 2 온라인 금융의 개념을 이해한다.
- 3 실생활에서 찾을 수 있는 온라인 금융의 예를 확인한다.

• 준비물 •

- 1 인터넷이 연결된 PC
- 2 은행 앱이 설치된 스마트폰

• 핵심 사이트 •

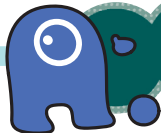
- 1 금융감독원 : fss.or.kr
- 2 하나은행 : kebhana.com
- 3 한국은행 : bok.or.kr
- 4 검색사이트 : naver.com
google.com

• 핵심 활동 •

- 금융의 발전에 대해 학습한다.
- 온라인 금융의 정의에 대해 학습한다.
- 온라인 금융의 주요 특징에 대해 학습한다.
- 생활 속에서 찾을 수 있는 온라인 금융의 유형을 분석한다.

• 핵심 키워드 •

- 금융의 역사, 온라인 금융, 핀테크, 모바일뱅킹, 간편결제, 해외송금, 디지털지갑, 디지털 자산



학습을 위한 사전준비

- ▶ 자본주의 시장경제체제에 대해 미리 알아본다.
- ▶ 핀테크에 해당되는 기술의 범위가 어디인지 확인해본다.
- ▶ 우리나라와 외국의 대표적인 핀테크 기업이 어디인지, 어떻게 시작하였는지 조사한다.

★ 금융이란?

자본주의 경제에서는 '돈'이라는 교환수단이 핵심적인 역할을 한다. 농부가 재배한 쌀을 자동차나 컴퓨터와 직접 바꾸는 것은 현실적으로 어렵다. 물건과 노동의 가치를 객관적으로 비교하고 거래하기 위해서는, 공통적인 가치 기준이 필요하다. 그 기준이 바로 돈이다.

금융은 쉽게 말해 돈의 유통, 돈의 흐름을 말한다. 재화의 수요와 공급에 의해 일어나는 자금의 흐름을 금융이라고 하고, 우리는 매일 금융의 흐름 속에서 삶을 영위하고 있다. 따라서 기술발전에 따라 급변하면서 우리 일상에 녹아들어 있는 금융에 대해 이해하고, 더 나아가 내 자산을 현명하게 지키기 위한 방법에 대해서도 알아볼 필요가 있다.

★ 금융은 어떻게 발전해 왔을까



이미지 출처: 제미나이

하단 잘린 영역 복원

1 물물교환의 시대

금융의 가장 원시적인 모습은 물건과 물건을 직접 바꾸는 물물교환이었다.

2 화폐의 등장

돈이 등장하였다. 처음에는 조개껍데기나 금속 조각처럼 희소한 물건이 사용되었고, 나중에는 금속화폐와 지폐로 발전했다. 물건을 직접 교환하지 않아도 거래를 할 수 있게 되었고, 돈은 '가치의 기준'이자 '교환의 매개체'로서 사회 전반에 자리 잡았다.

3 은행의 출현

돈이 널리 쓰이게 되고 단위가 커지면서 사람들이 안전하게 돈을 보관하고, 필요할 때마다 꺼내 쓸 수 있는 서비스가 등장했다. 바로, 은행이다. 은행은 개인의 돈을 대신 보관하고, 여유 자금을 모아 대출로 운용하면서 수익을 내는 방식으로 수익을 창출하게 되었으며, 금융은 단순히 돈을 주고받는 행위를 넘어 신용과 이자, 투자와 자본 축적이라는 개념으로 확장되었다.

4 근대 금융의 발전

산업혁명 이후 무역이 늘고 기업이 생겨나면서, 금융은 점점 더 복잡해졌다. 국가 운영, 국가와 국가 간 거래 그리고 거대 기업의 성장에도 큰 돈이 필요해졌으며 많은 사람들의 권리관계가 얽힌 복잡한 금융시스템이 개발되었다.

5 디지털 금융의 시작

20세기 후반, 컴퓨터와 인터넷의 발달로 금융의 혁신이 도래했다. 사람들은 카드 한 장으로 결제하고, 전산망을 통해 계좌 간 송금이 가능해졌다. 즉, 금융이 '손에서 화면으로' 이동하면서 돈의 개념 자체가 현찰, 물질에서 숫자나 데이터 등 비물질화되기 시작했으며, 이제 우리는 스마트폰으로 돈을 보내고, 투자하고, 자산을 관리하는 세상에 살고 있다.



온라인 금융의 정의

★ 온라인 금융의 정의

인터넷과 모바일 네트워크를 기반으로 금융 서비스를 제공하는 모든 활동을 온라인 금융(Online Finance)이라고 부른다.

디지털 기술의 발전은 금융의 모습을 완전히 바꾸어 놓았다. 과거에는 돈을 움직이기 위해 은행 창구를 찾아가고, 복잡한 서류를 작성해야 했지만 지금은 스마트폰 하나로 거의 모든 금융 활동을 처리할 수 있다. 기술의 발달로 인해 '사람의 손과 장소'에 묶여 있던 금융이 데이터와 네트워크를 통해 보이지 않게 움직이는 시대로 바뀐지 오래다.

★ 온라인 금융의 주요 특징

1 접근성이 높다.

누구나 스마트폰만 있으면 계좌 개설, 송금, 결제, 투자, 보험 등 다양한 금융 서비스를 이용할 수 있다. 과거처럼 은행에 직접 찾아가 기다릴 필요 없이, 통신이 가능한 스마트폰 안의 서비스로 바뀌었다.

2 시간과 공간의 제약이 없다.

은행 서비스 시간이라면, 밤 늦은 시간에도 송금이 가능하고, 해외에 있는 친구에게도 실시간으로 돈을 보낼 수 있다.

3 개인 맞춤형 서비스가 가능하다.

온라인 금융은 데이터를 기반으로 각 개인의 소비 패턴과 자산 규모를 분석하고 개인 상황에 맞는 금융을 제시할 수 있다. 덕분에 사람마다 다른 대출 조건, 투자 전략, 예금 상품을 추천받을 수 있다.

4 통신 기술과 연관성이 매우 높다.

예전에는 이용자의 요구가 은행 직원에 의해 전산화되고, 전산시스템 속도에 영향을 받았지만, 지금은 이용자가 입력하는 모든 정보가 통신기술에 의해 실시간에 가깝게 반영되고 있다. 거래 속도와 정확성은 금융의 신뢰를 더 강화시킨다.

FinTech에 대한 상식

핀테크(FinTech)는 금융(Financial)과 기술(Technology)의 합성어로, 정보기술(IT)을 활용하여 기존 금융 서비스를 더 편리하고 혁신적으로 제공하는 기술 및 산업을 뜻한다.

간편 결제(삼성페이), 송금(토스), 인터넷 전문은행, 로보어드바이저 등 비대면 금융 서비스가 대표적인 예시이며, 전통적 금융 산업을 대체하는 파괴적 혁신 기술로 평가받고 있다.

① 핀테크의 주요 특징 및 정의

- 금융 + IT 융합 : 인공지능(AI), 빅데이터, 블록체인 등 4차 산업 기술을 금융에 접목.
- 서비스 혁신 : 금융기관 없이 IT 기업이 주도하는 빠르고 편리한 서비스 제공.
- 소비자 혜택 : 수수료 절감, 비대면 거래, 개인 맞춤형 금융 서비스(자산관리 등).

② 주요 핀테크 활용 사례

- 간편 결제 및 송금 : 비밀번호나 생체인증만으로 결제하는 삼성페이, 애플페이, 카카오페이 등.
- 인터넷 전문은행 : 오프라인 지점 없이 앱으로만 운영되는 은행 (카카오뱅크, 토스뱅크).
- 로보어드바이저 : AI가 알고리즘을 통해 자동 자산 관리 및 투자 조언 제공.
- P2P 금융(온라인투자연계금융) : 대출자와 투자자를 온라인 플랫폼에서 직접 연결.
- 클라우드 펀딩: 온라인에서 다수의 사람에게서 자금을 조달.
- 인슈어테크(Insurtech) : 보험(Insurance)과 기술(Technology)을 결합한 서비스.

③ 핀테크의 동의어 및 관련 용어

- 디지털 금융 (Digital Finance)



실생활에서 찾아보는 온라인 금융

장소가 아닌, 네트워크를 통해 돈이 이동하는 세계 즉 눈에 보이지 않는 금융의 세계가 바로 온라인 금융의 세계이다.

우리는 스마트폰과 함께 태어난 알파세대이다. 우리가 너무나 자연스럽게 사용하고 있는 여러 서비스 속에는 이미 온라인 금융 기술이 숨어 있다. 눈에 잘 보이지 않지만, 우리의 소비와 생활을 연결해 주는 중요한 역할을 하고 있다.

★ 우리 생활 속에서 찾을 수 있는 온라인 금융

1 스마트폰 속 은행 - 모바일뱅킹

예전에는 통장에서 돈을 인출하려면 은행에 직접 가야 했다. 오늘날은 휴대폰에 설치된 모바일뱅킹 앱으로 거의 모든 일을 처리할 수 있다.

회사에서 지급한 급여를 확인하고, 친구와 함께 먹은 밥값을 송금하고, 휴대폰 요금이나 세금 등 공과금을 자동이체로 납부하는 것까지 모두 손안에서, 즉 휴대폰 안에서 이루어진다. 돈의 이동이 '장소'가 아니라 '네트워크'를 통해 이뤄지는 대표적인 예로 볼 수 있다.

2 결제의 혁신 - 간편결제 서비스

카카오페이, 네이버페이, 삼성페이 같은 간편결제 플랫폼은 온라인 금융의 가장 익숙한 형태이다. 식당에서 밥을 먹고 결제할 때 또는 카페에서 커피 한 잔을 살 때 굳이 카드나 현금을 꺼낼 필요가 없다. 휴대폰을 한 번 터치하면 결제가 완료된다.

이런 시스템은 '금융행위'를 소비와 직접 연결시켜, 돈이 실제로 눈앞에 없어도 거래를 가능하게 만든 혁신이라 할 수 있다.

3 해외송금과 디지털지갑

예전에는 외국에 있는 가족에게 돈을 보내려면 은행 창구에서 여러 서류를 작성해야 하고, 수수료도 비싸서 불편함이 컸다. 하지만 지금은 디지털 지갑이나 간편 해외송금 앱으로 몇 초 만에 지구 반대편에 있는 사람에게도 돈을 보낼 수 있다. 국경을 넘어 돈이 흐를 수 있게 되었으며, '금융의 글로벌화'가 실현되었다.

4 디지털 자산과 새로운 금융 생태계

최근에는 비트코인 같은 디지털 자산(암호화폐)도 금융의 한 형태로 자리 잡고 있다. 물론 모든 사람이 사용하는 것은 아니지만, 블록체인 기술을 통해 거래가 기록되고 암호화되어 관리된다는 점에서 안전성을 확보한 것으로 보고, 이는 온라인 금융의 확장된 형태로 볼 수 있다.

이런 사례들은 모두 금융이 더 빠르고, 더 투명해지며 개인 맞춤형으로 진화하고 있음을 보여준다. 기술이 금융의 문을 여는 열쇠로 기능하며 이제 금융은 사용자의 니즈에 딱 맞는 형태로 우리의 생활 속에 있게 되었다.



자기 평가하기

★ 온라인 금융에 대해 학습하고 이해한 만큼 아래 평가표에 체크해보자.

평가 내용	매우 우수	우수	보통	부족	매우부족
▶ 금융의 개념과 발전 단계에 대해서 친구에게 설명할 수 있다.					
▶ 온라인 금융의 정의에 대해 이해한다.					
▶ 실생활 가까이 있는 온라인 금융의 유형에 대해 이해한다.					
▶ 핀테크가 금융(Financial)과 기술(Technology)의 합성어로, 정보기술(IT)을 활용한 혁신적인 기술 및 산업을 뜻함을 이해한다.					

★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

02

체크카드와 신용카드

• 목 표 •

- 1 보편화된 카드이용에서의 결제 순서와 시스템을 이해한다.
- 2 카드 이용의 장단점을 확인하고 현명한 소비습관을 위한 카드 이용방법을 배워본다.

• 준비물 •

- 1 인터넷이 연결된 PC
- 2 은행 앱이 설치된 스마트폰

• 핵심 사이트 •

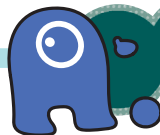
- 1 하나은행 : kebhana.com
- 2 여신금융협회 : crefia.or.kr
- 3 한국은행 : bok.or.kr

• 핵심 활동 •

- 신용카드의 결제시스템을 이해한다.
- 체크카드의 결제시스템을 이해한다.
- 신용카드와 체크카드를 비교한다.
- 현금사용과 카드사용의 장단점을 이해한다.

• 핵심 키워드 •

- 신용카드, 체크카드, 신용, 예금, 계약자, 가맹점



학습을 위한 사전준비

- ▶ 하나은행에 가서 계좌를 개설하고 연결된 체크카드를 만들어본다.
- ▶ 카드사와 이용자가 체결하는 카드이용 계약의 약관을 찾아서 읽어본다.



우리는 평소 생활하면서 카드를 이용해서 많은 것들을 결제하고 있다. 학생들의 경우 부모님이 관리하는 체크카드 또는 위급상황에서 사용하기 위해 제공해 주신 신용카드를 가지고 있을 것이다.

우리가 일반적으로 결제 시 사용하는 카드는 보통 체크카드나 신용카드로 나뉘는데, 두 카드 모두 '현금을 직접 주고받지 않아도 거래를 가능하게 해주는 금융 도구'이다. 하지만 이 둘은 작동 방식과 결제 시스템에 차이가 있어서 사용 시 기본적인 주의가 필요하다.

체크카드 이미지	신용카드 이미지

예를 들어 엄마의 체크카드로 1만 원짜리 연필세트를 사면, 결제가 끝나는 즉시 엄마의 통장에서 1만 원이 빠져나간다. 그러나 신용카드라면 엄마의 통장에 돈이 남아있는지 여부와 상관없이 카드회사가 먼저 가게에 돈을 지급하고, 일정 기간이 지난 후 엄마에게 대신 지불한 카드 사용 금액을 받아가게 된다.

신용카드가 무엇이고 체크카드가 무엇인지 알아보고, 각 카드 이용 시 결제 방식의 차이에 어떤 원리가 숨어 있는지, 그리고 카드 이용을 위해 체결되는 계약 및 결제 방식이 어떻게 다른지 확인해보자.



신용카드와 체크카드

신용카드와 체크카드는 외견상 차이가 없다. 둘 다 비슷한 모양의 플라스틱 재질의 얇은 카드로서 손톱 만한 금속조각이 드러나 있으며, 매장에서 단말기 슬롯에 삽입하거나 태그하여 결제하는 방식도 거의 같다. 그러나 결제 시 금융 측면에서 일어나는 프로세스는 신용카드와 체크카드가 각각 다르기에 그 차이점을 알 필요가 있다.

신용카드 이용자는 카드사와 체결한 계약을 기반으로 계좌 잔고와 무관하게 먼저 소비할 수 있는 반면, 체크카드는 현재 계좌에 있는 돈을 즉시 사용하는 수단이다. 겉으로는 같은 카드처럼 보이지만, 신용카드와 체크카드는 신용을 바탕으로 하고, 체크카드는 예금잔액을 바탕으로 한다. 따라서 두 카드는 결제 방식, 책임의 주체, 자금의 흐름에서 전혀 다른 구조를 가진다.

★ 신용카드란?

신용카드는 개인의 신용도(결제 능력)를 바탕으로 카드사가 물품 대금을 먼저 결제하고, 사용자가 나중에 정해진 지정일에 카드사에 대금을 갚는 후불 결제 금융 수단이다.

결제 순간에는 카드사가 가맹점에 먼저 돈을 지급하는 방식이므로 내 통장에 잔고가 없어도 원하는 물건을 구입하거나 서비스를 이용할 수 있다는 특징이 있어 널리 이용되고 있다.

신용카드의 사용은 다음 순서에 의해 이루어진다.

- 1 사용자가 가맹점에서 신용카드를 제시한다.
- 2 가맹점은 카드 결제 승인을 요청한다.
- 3 카드사는 사용자의 신용한도와 거래 가능 여부를 확인한다.
- 4 승인이 되면 카드사는 가맹점에 대금을 먼저 지급한다.
- 5 사용자는 결제일에 카드사에 카드대금을 갚는다.

이 과정에서 사용자는 소비를 하고, 가맹점은 물건이나 서비스를 제공하며, 카드사는 결제를 보증하고 대금을 우선 지급한다. 사용자는 신용카드 한도 안에서 소비할 수 있고, 카드사는 그 사람의 상환 능력과 신용을 기준으로 거래를 허용한다.

즉, 신용카드를 지금 사고 나중에 갚는 구조이다. 이 구조가 가능한 이유는 카드사가 사용자의 신용을 믿고 먼저 돈을 내주기 때문이다.

★ 신용이란?

신용(信用)이란 “다른 사람(또는 기관)이 나를 믿고 돈이나 서비스를 먼저 제공하는 것”을 뜻한다. 쉽게 말해 ‘빌린 것을 반드시 갚을 것이라는 믿음’이다.

신용은 현대사회에서 금융의 핵심이다. 왜냐하면 신용이 있어야 돈을 빌릴 수 있고, 신용이 높을수록 더 좋은 조건으로 거래할 수 있기 때문이다.

1 신용은 어떻게 생길까?

사람이 돈을 빌리고 갚거나, 카드값을 제때 납부하는 등 금융활동을 하면 그 내역이 금융기관에 기록된다. 이 기록이 쌓여 개인의 신용점수 또는 신용등급을 만들게 된다.

예를 들어 카드값을 항상 제때 갚는 사람은 “이 사람은 믿을 수 있다”는 평가를 받게 되어 신용점수가 높아지지만 반대로 연체나 미납이 많으면 신용이 떨어지게 된다.

2 신용점수가 중요한 이유

대출 한도와 금리에 직접 영향을 준다. 점수가 높으면 더 많은 금액을 빌릴 수 있고, 이자율도 낮아지게 된다. 일자리를 구하거나 임대 계약을 체결할 때에도 영향을 줄 수 있다. 일부 회사나 집주인은 개인의 신용을 간접적으로 참고하기도 한다.

경제적 신뢰의 지표로서 사회적 관계에서도 안정성을 높인다. 즉, 신용점수는 단순한 숫자가 아니라 “내가 금융 시스템 속에서 얼마나 믿음직한가”를 보여주는 척도이다.

3 신용을 관리하는 방법

- 카드대금이나 대출이자를 정해진 날짜에 정확히 갚기
- 불필요한 대출이나 과도한 카드 사용을 줄이기
- 신용정보를 주기적으로 확인해 오류나 연체 기록을 바로잡기

신용은 한번 떨어지면 회복하기 어렵기 때문에, 오랜 시간 꾸준한 관리 습관이 중요하다.

4 핵심 정리

신용은 단지 돈을 빌릴 수 있는 능력이 아니라, 경제 속에서 서로를 믿고 거래하기 위한 보이지 않는 약속의 힘이다. 우리가 신용을 지킨다는 것은 돈을 갚는 행위뿐 아니라, 사회적 신뢰를 쌓는 행동이기도 하다.



함께 해볼까요?

현대사회에서 금융의 도움을 받을 일이 굉장히 많다. 만약 신용관리에 실패하여 신용도가 떨어지게 된다면 디지털 금융생활에서 발생할 수 있는 손해에 대해서 고민해보고 아래 빈 칸을 채워 보자.

구분	답변 작성
대출 승인 여부	신용도가 낮으면 대출이 (거절)되거나 한도가 (줄어들) 수 있다.
대출 금리와 한도	신용도가 낮으면 더 (높은) 대출 금리와 더 (낮은) 한도가 적용될 수 있다.
신용카드 발급과 한도	연체 이력이나 과도한 부채는 카드발급 심사에 (불리)합니다.
할부 및 분할결제 이용	휴대폰 할부, 자동차 금융처럼 장기 분할 상환이 필요한 경우 신용도가 (낮으면) 할부 승인이 (제한)될 수 있다.
전세자금대출	주거 금융에서 전세자금 대출의 (규모), (금리) 등 심사에 신용도가 반영된다.
금융거래 조건 전반	신용도에 따라 (우대금리), (수수료 면제), (추가 한도)같은 조건이 달라진다.

★ 체크카드란?

체크카드는 사용자의 예금계좌와 바로 연결된 카드이다. 따라서 은행을 통해 가입한 은행 계좌가 있어야 하고, 그 은행과 서비스 체결이 된 카드사가 있어야 하며, 그 통장에 잔고가 있어야 사용 가능한 카드이다. 체크카드는 결제와 동시에 내 계좌에서 돈이 빠져나간다. 신용카드처럼 카드사가 대신 지불하고 나중에 이를 갚는 일시적 대출 상태가 아니라, 현재 가진 돈 안에서 바로 결제되는 방식이다.

체크카드 결제는 다음과 같은 순서로 이루어진다.

- 1 사용자가 가맹점에서 체크카드를 제시한다.
- 2 가맹점은 결제 승인을 요청한다.
- 3 카드사와 결제망은 계좌의 잔액을 확인한다.
- 4 결제가 가능하면 연결된 예금계좌에서 금액이 즉시 출금된다.
- 5 가맹점은 정산을 통해 대금을 받는다.

이 과정에서 사용자는 자신의 계좌 잔액 범위 안에서만 소비할 수 있다. 가맹점은 결제 가능한지를 확인한 뒤 물건이나 서비스를 제공한다. 은행은 계좌를 관리하고 실제 출금을 담당한다. 카드사는 결제 승인과 결제망 연결 역할을 수행한다.

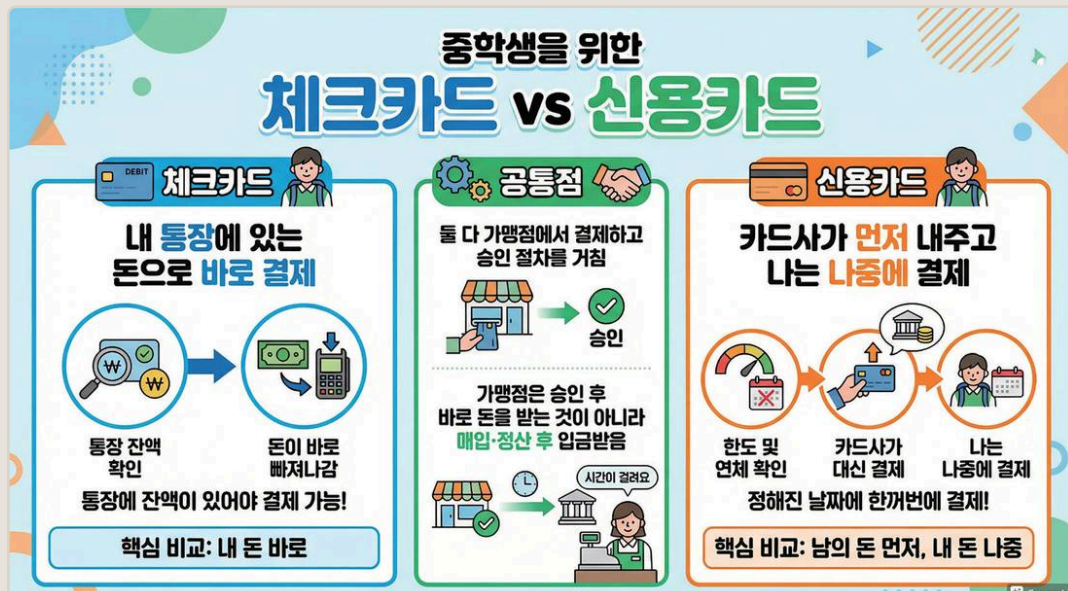
★ 체크카드와 신용카드의 차이점



함께 해볼까요?

아래 표는 체크카드와 신용카드의 차이점을 표로 만들어 놓은 것이다.
빈칸을 채워서 두 카드의 특징을 정확히 표현해보자.

구분	체크카드	신용카드
결제방식	본인 계좌에 돈이 (있을) 때, 결제 가능 돈이 (없으면) 결제 불가	(카드사)가 대신 지불하고, 사용자는 일정 기간 이후 한꺼번에 (카드사)에 상환하는 '외상' 형태
이자발생	없음	연체 시 이자 (발생)
사용한도	본인 계좌 잔액 범위 (내)	개인의 (신용도)에 따라 카드사가 부여
주요 특징	가계부처럼 지출관리에 유리	소비를 미리 할 수 있어 '현금흐름 조절' 에 유리



출처 : 제미나이

태그 결제에 대한 상식

신용카드를 단말기에 삽입하거나 마그네틱 카드를 긁지 않고 가져다 대기만 해도 결제가 된다. 이것을 태그 결제라고 하는데, 여기에는 온라인 금융 기술 뿐만 아니라 전기공학적인 원리가 숨어있다.

비접촉 결제 카드는 얇은 카드 안에 작은 코일형 안테나와 IC칩이 들어 있다.

상시 전자기장을 발생시키는 단말기에 카드를 가까이 가져가면, 카드 내부에 삽입된 구리코일이 유도 전류를 만든다.(페러데이의 전자기 유도법칙) 이 전류는 카드 내부의 IC칩에 전기를 공급하고, 카드의 IC칩이 단말기와 암호화된 통신을 하면서 결제 정보를 전달한다

그래서 태그 결제는 “카드를 대기만 하면 된다”처럼 보이지만, 내부적으로는 전자기 유도 → 전력 공급 → 데이터 통신 → 결제 승인의 순서로 움직인다.

★ 현금 거래와 카드 사용의 차이점

현금 거래는 실물현금이 직접 손에서 손으로 오가는 방식이다. 눈으로 확인할 수 있고, 익숙하지만, 분실 위험이 있고 거래 기록이 남지 않아서 따로 메모해 놓지 않는다면 쉽게 잊어버린다는 단점이 있다.

반면 카드 거래는 디지털 네트워크를 통해 처리되기 때문에 안전하게 기록이 남고, 통계나 소비습관 분석에도 활용할 수 있다. 카드 또한 분실 위험이 있지만, 디지털 사용자가 편리함을 향유하는 대신 카드사는 이를 운영하기 위한 수수료와 관리비용을 받는다.

즉, 현금거래는 단순하고 즉각적이지만 비효율적이고, 카드거래는 보이지 않지만 체계적이며 관리가 용이한 방식이라 할 수 있다.



함께 해볼까요?

아래 내용을 읽고 각자 자신의 생각을 써본 후, 옆사람과 비교해 본다.

- 1 현금을 사용하는 것과 카드를 사용하는 것 중 어떤 방법이 내 재산을 관리하고 지출을 줄이는데 효과적일까? 각각 장점과 단점을 적어보자.

현금을 사용할 때의 장점	카드를 사용할 때의 장점

현금을 사용할 때의 단점	카드를 사용할 때의 단점
결론	

2 카드를 사용한다면, 체크카드와 신용카드 둘 중에 어떤 카드를 사용하는 편이 내 재산을 관리 하는데 효과적일까?

체크카드 사용의 장점	신용카드 사용의 장점
체크카드 사용 시 자산 관리에 미치는 영향	신용카드 사용 시 자산 관리에 미치는 영향

현금유통 감축에 대한 상식

10원짜리 동전을 하나 만드는데 들어가는 비용이 10원 이상이 된다면 현금을 계속해서 만들어 내고 유지할 필요가 있을까? 세계 각 나라에서는 디지털 자산 즉 핀테크의 발달과 기술개발을 기반으로 현금없는 사회를 만드는데 의견을 함께 하고 있다.

- 이스라엘 : 2014년, 현금없는 국가추진위원회 발족
- 프랑스 : 2015.9월이후 1000유로(130만원) 이상 거래 시 현금거래 금지
- 덴마크/스웨덴 : 2030년까지 현금없는 사회로의 전환 추진 중



자기 평가하기

- ★ 체크카드와 신용카드의 작동 프로세스를 배우고 두 카드의 특징과 차이점에 대해 학습한 만큼 아래 평가표에 체크해보자.

평가 내용	매우 우수	우수	보통	부족	매우부족
▶ 체크카드의 결제 방식을 이해하고 설명할 수 있다.					
▶ 신용카드와 체크카드의 차이점을 설명할 수 있다.					
▶ 금융생활에서의 신용의 중요성에 대해 인식하고 설명할 수 있다.					

- ★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

03

간편결제와 온라인쇼핑

• 목표 •

- 1 간편결제의 정의와 유형에 대해 학습한다.
- 2 온라인쇼핑의 발전단계에 대해 학습한다.
- 3 여러 온라인 쇼핑몰의 특징을 알아보고 가장 저렴한 상품을 구매할 수 있다.

• 준비물 •

- 1 인터넷이 연결된 PC
- 2 쇼핑몰에 로그인 할 수 있는 ID
- 3 간편결제 기능이 활성화된 스마트폰

• 핵심 사이트 •

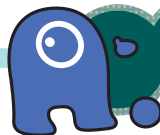
- 1 온라인쇼핑몰 사이트
- 2 유튜브 : youtube.com

• 핵심 활동 •

- 간편결제의 의미와 종류를 알아본다.
- 간편결제의 조건과 위험성을 학습한다.
- 온라인쇼핑에 대해 알아본다.
- 온라인 쇼핑을 통해 가장 저렴한 상품을 구매해본다.

• 핵심 키워드 •

- 간편결제, 온라인쇼핑, 페이스페이



학습을 위한 사전준비

- ▶ 일상 속에서 볼 수 있는 간편결제의 종류에 대해 알아본다.
- ▶ 부모님을 통해 간편결제를 직접 경험해본다.



카드대신 얼굴로 결제하기

지난 주말 정원이는 엄마와 함께 떡볶이를 먹으러 갔다. 순대에 튀김까지 아무지게 먹고 나서 엄마가 결제를 하시려다가 깜짝 놀라 말씀하셨다.

“어머, 내 정신 좀 봐. 카드를 안 가져왔네”

사장님이 빙그레 웃으며 말씀하신다.

“페이스페이도 가능하세요~”

엄마는 카운터에 세워진 단말기에 얼굴을 보여주셨고, 결제가 끝났다.

“엄마, 얼굴로도 결제가 돼요??”

결제에 대한 플러스 상식

우리가 흔히 사용하는 결제와 결재는 전혀 다른 말이다.

결제는 한자어로 決濟라고 쓰고, 거래를 마친다는 의미로 쓰인다. 즉, 거래의 마지막 단계로서 값을 치르는 것을 의미하는 것이며 결재는 한자어로 決裁라고 쓰고 보통 조직에서 부하직원이 올린 내용을 상사가 승인한다는 의미로 쓰인다. 발음은 비슷한데 의미가 전혀 다르기에 일상 생활에서도 꼭 구분해서 사용하여야 한다.



간편결제의 의미와 종류

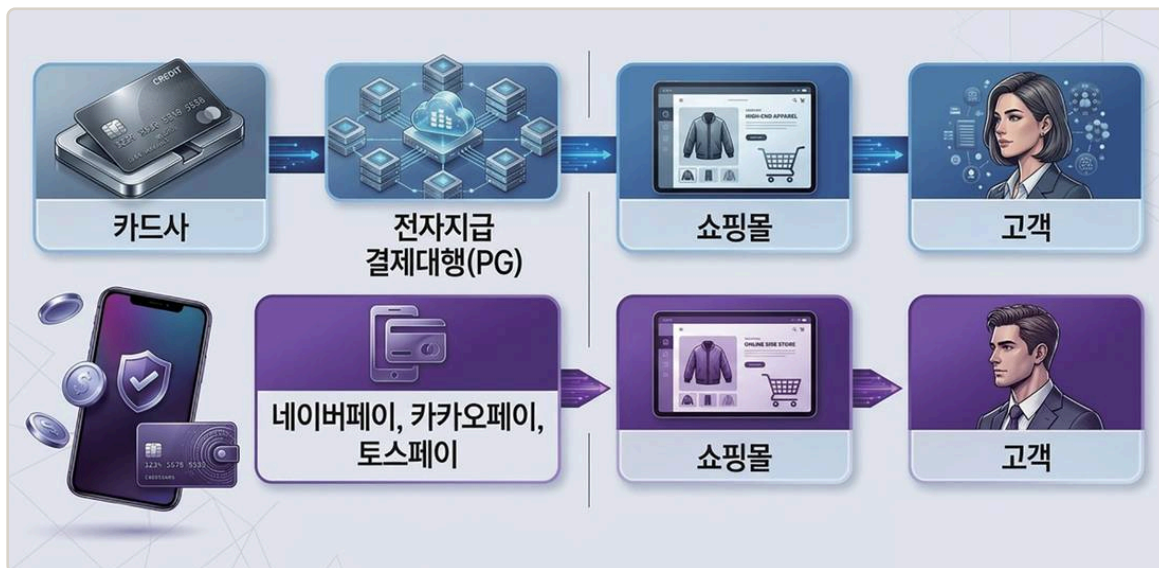
★ 간편결제란?

간편결제란 말 그대로 결제 과정을 간단하게 만든 서비스를 뜻한다.

우리는 이미 일상에서 '결제'라는 말에 익숙해져 있다. 물건을 사거나, 음식을 주문하거나, 교통비를 내는 일까지 모두 결제한다고 표현하며, 현금으로 직접 지불하거나 카드를 사용해 왔다. 하지만 이러한 지불 수단을 조금 더 간편하게 이용하기 위한 기술이 대두되고 있다. 즉 신용카드 또는 체크카드를 사용하는데 있어서 휴대폰 하나로 훨씬 빠르게 결제를 끝내는 경우가 많아졌다. 이것이 간편결제이다.

★ 간편결제의 조건

간편결제는 새로운 결제수단이 아니라, 기존 결제 프로세스를 빠르고 간단하게 해주는 지름길로 이해하면 쉽다. 따라서 간편결제를 이용하기 위해서는 정상적인 결제 시스템에 먼저 가입되어 있어야 한다. 대표적인 것이 앞서 배웠던 신용카드 혹은 체크카드 결제 시스템이다. 지갑에서 카드를 꺼내고 단말기에 삽입하고 본인 확인을 위해 서명하는 일련의 절차를 쉽고 간단하게 변경하는 것이 바로 간편결제 서비스이다.



이미지 출처: 제미나이

★ 간편결제의 종류

간편결제의 종류는 다양하다. 지문인식, 비밀번호 입력, 얼굴인식 등 간단하면서 다양한 방법으로 결제자 본인임을 확인하고 손쉽게 결제를 할 수 있다. 간편결제는 금융을 일상생활 속으로 더 깊이 들어오게 만든 대표적인 Fintech로 손꼽힌다.

다양한 결제 서비스가 간편결제를 지원하고 있는데, 사람들이 자주 이용하는 간편결제 서비스는 대표적으로 카카오페이, 삼성페이, 토스페이를 꼽을 수 있다.



함께 해볼까요?

인터넷 검색을 통해서 카카오페이와 삼성페이, 토스페이의 특징을 아래 빈칸에 정리해 봅시다.
추가적으로 궁금한 간편결제가 있다면 더 조사해서 아래 빈 칸에 적어봅시다.

구분	서비스 시기	편리한 점	불편한 점
카카오페이		카카오톡과 연결, 메신저 이용중에 송금이나 결제	
삼성페이		휴대폰 자체를 결제수단	
토스페이		계좌번호를 몰라도 송금이 가능 얼굴인식만으로 결제가 가능 한 페이스페이 도입	

★ 내 얼굴이 카드가 된다_페이스페이

간편결제 기술은 점점 진화하여 이제는 내 얼굴이 결제방법이 되는 시대가 찾아왔다. 안면인식 기술에 대한 많은 우려가 있었지만, 실제 서비스되고 있는 페이스페이에 대해 알아보자.

충주맨으로 유명한 유튜버 김선태의 영상 속에서 휴대폰 없이, 카드 없이 얼굴만으로 인근 상가에서 손쉽게 결제를 하는 모습을 볼 수 있다. (링크 : <https://www.youtube.com/watch?v=Nyl8AcmgMbl>)



출처 : 김선태 유튜브 썸네일

★ 간편결제의 위험성

1 무절제한 소비의 문제

간편결제는 분명 편리하지만, 편리함에는 늘 그만큼의 책임이 따라온다. 결제가 쉬워진다는 것은 그만큼 돈이 빠져나가는 속도도 빨라진다는 뜻이므로, 소비의 속도가 빨라졌다는 의미이기도 하다. 예전에는 현금을 꺼내면서 “이만큼 쓰는구나” 하고 한 번 더 생각할 수 있었지만, 지금은 화면 몇 번만 누르면 결제가 끝나버린다. 그래서 소비가 너무 쉽게 이루어질 수 있다는 점이 간편결제의 가장 큰 특징이자 동시에 주의할 점이다.

2 간편결제의 보안 문제

간편결제는 휴대폰이나 계정에 결제 정보가 저장되기 때문에 보안 문제도 중요하다. 휴대폰을 잃어버리거나, 비밀번호가 유출되거나, 다른 사람이 내 계정에 접근하게 되면 결제 정보가 악용될 가능성이 생긴다. 휴대폰에서 잠금해제 기술이 도입되었을 때 사진으로 잠금해제가 되는 등 보안의 문제점이 지적된 바 있다. 앞서 언급한 페이스페이에서도 사람의 얼굴을 본인확인에 활용할 수 있을 정도로 정확한 인식이 가능하다는 기술적 보안 문제도 생각해보게 된다.

기술은 우리의 결제를 더 쉽게 만들어 주지만, 동시에 사용자가 자신의 정보와 지출을 더 잘 관리하도록 요구한다. 결국 간편결제는 ‘쉽게 쓰는 것’보다 ‘올바르게 쓰는 것’이 더 중요하다고 말할 수 있다.

★ 간편결제를 안전하게 관리하기 위한 원칙

간편결제를 안전하게 사용하려면 몇 가지 기본 원칙을 지켜야 한다. 가장 먼저 중요한 것은 본인 인증 수단을 철저히 설정하는 것이다. 비밀번호를 단순하게 정하거나 여러 서비스에서 같은 비밀번호를 반복해서 사용하는 것은 매우 위험하다. 지문이나 얼굴인식 같은 생체인증은 빠르고 편리하지만, 오작동 가능성이 있으므로 비밀번호 관리까지 함께 신경 써야 한다.

두 번째로 중요한 것은 결제 내역을 자주 확인하는 습관이다. 간편결제는 너무 쉽게 이루어지기 때문에, 본인이 기억하지 못하는 결제가 생겨도 바로 알아차리지 못할 수 있다. 따라서 정기적으로 결제 내역을 확인하고, 이상한 결제가 보이면 즉시 차단하거나 신고해야 한다.

세 번째는 공공장소에서의 주의이다. 공용 와이파이를 사용할 때나 출처가 불분명한 앱을 설치할 때는 결제 정보가 유출될 위험이 있다. 온라인 금융은 편리하지만, 인터넷과 연결되어 있다는 사실 자체가 곧 보안 관리의 필요성을 의미한다. 결국 사용자는 기술을 믿되, 기술에만 의존해서는 안 된다.

마지막으로, 간편결제는 소비 습관과도 밀접하게 연결되어 있다는 점을 기억해야 한다. 결제가 너무 쉬우면 필요하지 않은 물건까지 자꾸 사게 될 수 있다. 따라서 간편결제를 사용할 때는 “지금 정말 필요한 소비인가?”를 한 번 더 생각하는 태도가 중요하다.

★ 금융기술의 발달과 경각심의 필요성

금융기술은 우리의 생활을 분명 더 편리하게 만들어 주었다. 예전에는 은행에 직접 가야 했던 일들이 이제는 스마트폰 하나로 해결된다. 송금, 결제, 잔액 확인, 자동이체, 투자까지도 손끝에서 이루어진다. 이러한 변화는 시간과 장소의 제약을 줄여 주었고, 사람들은 더 빠르고 쉽게 금융 서비스를 이용할 수 있게 되었다.

하지만 편리함이 커질수록 새로운 문제도 함께 나타나게 된다. 돈이 화면 속에서 너무 쉽게 움직이다 보니, 사용자는 자신이 얼마나 쓰고 있는지 체감하는 것이 어렵다. 또한 금융 서비스가 디지털화될수록 개인정보 유출, 계정 도용, 피싱, 악성 앱, 휴대폰 분실 같은 디지털 안전위험도 커진다. 즉, 금융기술은 편안함을 주는 동시에, 우리가 더 신경써서 깊게 관리해야 할 영역을 넓혀 놓았다.

기술이 편리할수록 사용자는 더 똑똑하게 관리해야 하고, 금융을 배운다는 것은 돈의 흐름을 아는 것 뿐만 아니라 실현될 수 있는 위험요소를 이해하는 것까지 포함되어야 한다.



함께 해볼까요?

지금까지 배운 간편결제에 대해 OX퀴즈를 풀어봅시다.

- 1 간편결제는 무절제한 소비 풍토를 장려하여 가계에 높은 위험도를 가져온다.
(O , X)
- 2 간편결제는 새로운 결제수단의 등장을 의미한다. (O , X)
- 3 간편결제 기술과 서비스가 발달할수록 현금을 사용하는 매장이 줄어든다.
(O , X)
- 4 비밀번호 유출, 휴대폰 분실 등 문제가 생겼을 때 매우 쉽고 빠르게 문제가 해결된다.
(O , X)
- 5 다양한 간편결제 시스템을 이용할 때, 쉽게 결제하기 위해서 비밀번호는 동일하게 설정하는 것이 좋다. (O , X)
- 6 금융기술이 발달할수록 인간의 편의를 위한 안전장치가 많아지기 때문에 위험에 대한 대비를 미리부터 할 필요는 없다. (O , X)



온라인 쇼핑에 대해 알아보자

★ 온라인 쇼핑의 발달

온라인 쇼핑은 통신기술의 발달과 전자상거래의 발전 과정 속에서 서서히 자리 잡은 시스템이다. 1970년대 후반 영국에서 전화선으로 가정용 TV와 기업의 컴퓨터를 연결하는 초기의 온라인 쇼핑 시스템이 시작되었다. 이러한 시도가 오늘날 온라인 쇼핑의 전신으로 평가된다.

1990년대 들어 인터넷과 월드와이드웹이 보급되면서, 본격적인 인터넷 기반 전자상거래가 등장했다. 1994년에는 최초의 온라인 상점(NetMarket)이 만들어졌고, 같은 시기 피자헛은 인터넷으로 피자를 주문하는 서비스를 시작해 “웹에서 물건을 주문한다”는 경험 자체를 세상에 알렸다.

이후 여러 나라에서 온라인 서점, 온라인 경매 사이트, 종합 쇼핑몰이 등장하며 전자상거래는 빠르게 확산되었다.

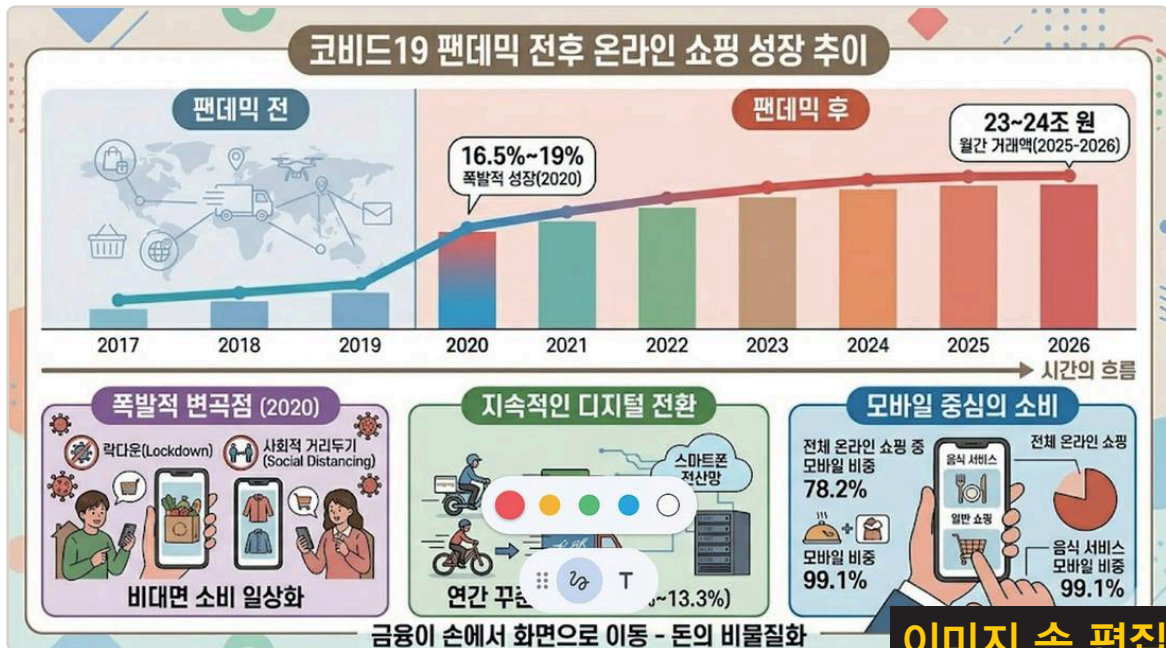
한국에서도 1990년대 후반부터 인터넷 쇼핑몰이 하나둘 생겨났고, 2000년대에 들어서면서 인터파크, G마켓, 11번가 등 대형 오픈마켓이 자리 잡기 시작했다.



이미지 출처: 제미니

이미지 속 편집 툴바
이미지 교체

이어 스마트폰 보급과 함께 모바일 쇼핑이 폭발적으로 성장하면서, 오늘날 온라인 쇼핑은 더 이상 특별한 선택이 아니라 기본적인 소비 방식 중 하나가 되었다. 팬데믹 시기에는 비대면 소비가 일상화되면서 온라인 쇼핑의 비중이 더욱 커졌고, 지금은 필수적인 생활 인프라에 가깝다고 평가된다.



이미지 속 편집 툴바 이미지 교체



함께 해볼까요?

• 온라인 쇼핑물 찾기

현재 한국의 온라인 쇼핑 시장에는 여러 종류의 플랫폼이 공존하고 있다. 유형별로 묶어보면 오픈마켓, 종합몰, 전문몰, 자사몰, 폐쇄몰, SNS 마켓 등 다양한 형태로 나뉘볼 수 있는데 세대별, 연령별 선호 쇼핑물이 각각 다르다. 각 유형별 대표적인 쇼핑물을 몇 가지 직접 찾아보고, 찾은 쇼핑물이 가진 독특한 특징을 설명해보자.

구분	대표 쇼핑물 (최대 3가지)	마켓의 특징	선호연령대	선호 성별
오픈마켓				
종합몰				

전문몰				
자사몰				
폐쇄몰				
SNS 마켓				

이처럼 온라인 쇼핑몰은 각각 다른 강점과 특성을 가지고 있으며, 소비자는 자신의 목적에 따라 플랫폼을 선택하게 된다. 어떤 플랫폼은 배송 속도가 중요하고, 어떤 플랫폼은 가격이나 할인 혜택이 중요하며, 또 어떤 곳은 브랜드 신뢰도나 사후 서비스가 더 중요할 수 있다.

따라서 온라인 쇼핑을 이해한다는 것은 단순히 “어떤 쇼핑몰이 저렴하다”를 아는 것이 아니라, 각 플랫폼의 구조와 특징을 이해하는 것이기도 하다.



함께 해볼까요?

• 가장 저렴한 쇼핑몰 찾기

온라인 쇼핑의 중요한 특징 중 하나는 동일한 상품이라도 판매자와 플랫폼에 따라 가격과 조건이 달라진다는 점이다. 주로 이용하는 안전한 온라인 쇼핑몰 홈페이지 몇 군데에 들어가서 동일한 상품을 검색해보고, 가격이나 판매조건이 어떻게 달라지는지 확인해 볼 필요가 있다.



무엇을 할까요?

- 1 구매하고자 하는 상품을 하나 선택한다.
(예 : 특정 모델의 축구화, 이어폰, 교과서 외 참고서 등.)
- 2 최소 3~4개 온라인 쇼핑몰에서 같은 상품을 검색한다.
(예 : 11번가, G마켓, 네이버쇼핑)
- 3 다음 항목을 비교하여 표로 정리해 본다.

상품명	쇼핑몰구분	표시가격	배송비	예상배송일	반품교환 가능여부	적립금/쿠폰 등 혜택

단순 가격만 볼 때와, 배송비·반품 조건, 적립과 혜택까지 모든 조건을 고려 “가장 합리적인 선택”이 달라지는지 토론해 보자.

합리적인 쇼핑몰	선택한 이유



온라인 쇼핑과 금융데이터

학술적으로 보면 온라인 쇼핑은 전자상거래(Electronic Commerce)의 한 형태이다. 전자상거래란 “상품이나 서비스를 사고파는 과정에서, 계약 체결과 결제, 주문, 청구 등 거래의 전부 또는 일부를 전자문서 형태로 처리하는 상행위”를 의미한다.

그중에서도 기업과 소비자 간에 이루어지는 전자상거래(B2C)가 바로 우리가 익숙하게 사용하는 온라인 쇼핑이다. 인터넷 쇼핑몰, 앱 기반 쇼핑, 모바일 결제 등이 모두 여기에 포함된다.

온라인 쇼핑 이용자는 매장을 직접 방문하는 대신 웹페이지를 방문하고, 현장에서 상품을 만져보거나 확인하는 대신 상인이 상품에 대해 설명한 글과 사진 또는 영상으로 상품을 판단한다. 앞에서 여러 가지 사례로 확인했던 바와 같이 결제와 배송은 비밀번호 몇 개 혹은 지문 인식, 나아가 얼굴 인식으로 더 간단하게 처리된다.

우리가 간과하기 쉬운 사실 중의 하나는, 전자통신기술에 의해 주고받는 데이터 정보들은 기록되기 쉽고, 가공되기 쉬우며 유출되기 쉽다는 점이다.

디지털 금융의 일부로서 온라인 쇼핑은 기업에게 있어 이용자와 관련된 정보를 취득하기 위한 뒤편이나 마찬가지다. 고객의 성별, 연령, 주거지역, 취미, 상품의 종류, 결제방식과 비용, 빈도, 구매 시기와 배송지 등 어마어마하게 다양하고 풍부한 정보가 데이터화 되어 기업에 의해 관리되며, 소비자는 구매 후 후기 작성이나 재구매 여부를 통해 자신의 만족도까지 표현함으로써 기업이 고객유치를 위해 분석할 수 있는 방대한 데이터가 생산되고 활용된다.

우리 이용자가 남기는 금융데이터와 디지털 흔적들은 그대로 뒤도 되는 것일까?

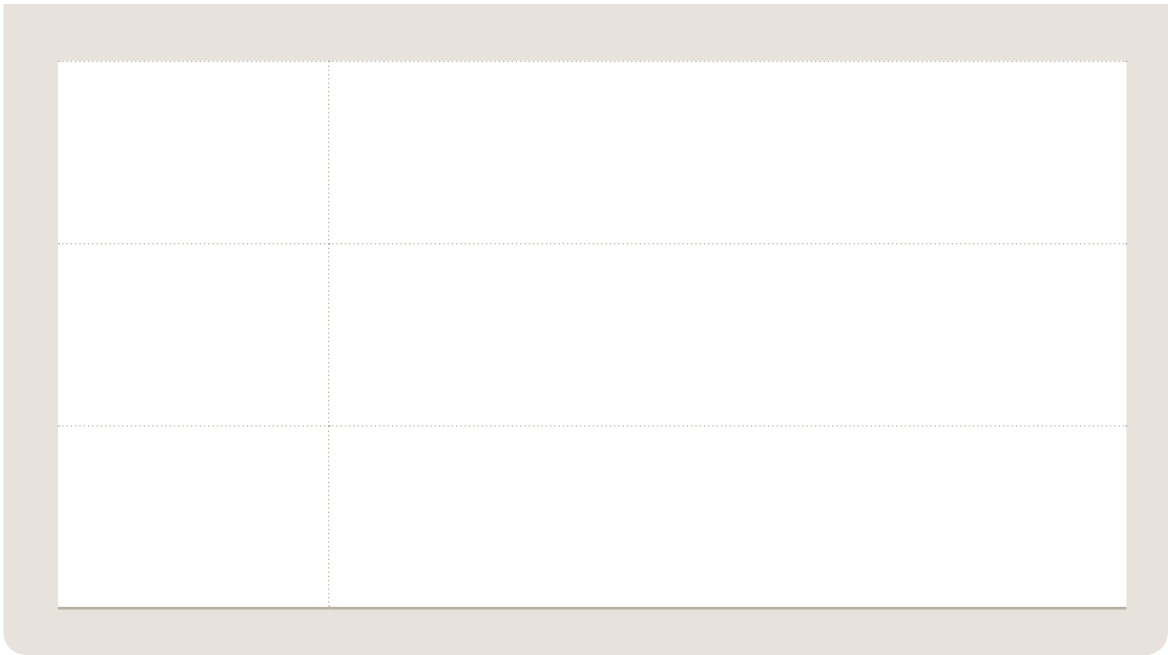


함께 해볼까요?

• 나의 금융데이터의 가치 알아보기

내가 쇼핑을 하면서 누적된 정보에는 어떤 것들이 있을지 작성해보고, 기업이 내 정보 또는 다른 사람의 누적된 정보를 가지고 어떤 일들을 할 수 있는지 아래 빈칸에 작성해보자.

누적되는 나의 정보	기업은 내 정보를 어떻게 활용할까



온라인 쇼핑몰 플랫폼에 가입할 때 동의하는 약관에 대하여

온라인 쇼핑몰에 가입할 때, 함부로 동의 버튼을 누르면 안된다.

온라인 쇼핑몰 회원가입 시 동의하는 약관은 크게 필수 항목과 선택 항목으로 나뉜다. 필수 약관은 서비스 이용의 법적 계약 조건이므로, 꼼꼼히 확인하고 동의해야 피해를 예방할 수 있다.

1 반드시 동의해야 하는 필수 약관 : 동의하지 않으면 가입이 되지 않는다.

- 서비스 이용약관: 쇼핑몰과 회원 간의 기본적인 권리, 의무, 결제, 환불, 그리고 계정 해지 등에 대한 규칙을 명시
- 개인정보 수집 및 이용 동의: 회원 식별, 주문 처리, 배송 및 고객 상담을 위해 필수적인 개인정보(이름, 연락처, 주소 등)를 수집하는 데 동의 (최소 범위)

2 선택해서 동의할 수 있는 약관 (마케팅 동의)

- 개인정보 제3자 제공: 이벤트나 맞춤형 서비스를 위해 제휴사 등에 개인정보를 제공하는 항목
- 마케팅 정보 수신 동의: 이메일, SMS, 앱 푸시 등을 통한 광고, 할인 쿠폰, 이벤트 정보 수신 여부를 결정한다. (선택 약관은 동의하지 않아도 쇼핑몰 회원가입과 기본 서비스 이용에 아무런 불이익이 없다)

주의할 점은, 휴대폰 등으로 가입을 진행할 경우, 쉽게 진행할 수 있도록 [전부 동의] 버튼이 제공 되는데, 이 때문에 선택하지 않아도 되는 개인정보 수집 및 제3자 제공에 동의하게 되는 경우가 많다. 귀찮더라도 약관을 꼼꼼하게 읽어보고 나의 소중한 정보가 누구에게 언제까지, 어디까지 제공되는지 확인할 필요가 있다.



자기 평가하기

- ★ 간편결제 종류와 방식에 대해 배웠으며, 온라인쇼핑의 연혁과 종류에 대해 학습하였다. 또한 구매에 영향을 미치는 요인을 확인하기 위해 온라인 쇼핑몰 검색 실습에 참여한 만큼 아래 평가표에 체크해보자.

평가 내용	매우 우수	우수	보통	부족	매우부족
▶ 간편결제란 기존의 결제방식을 수월하고 빠르게 도와주는 기술적인 지원이라는 사실을 숙지하였다.					
▶ 간편결제의 여러가지 형태에 대하여 설명할 수 있다.					
▶ 온라인 쇼핑몰의 연혁에 대해 숙지하였으며 국내 유명 쇼핑몰에 대해서 분류할 수 있다.					
▶ 합리적인 소비를 위해 고려해야 하는 요소들에 대해서 설명할 수 있다.					

- ★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

04

가짜쇼핑몰과 진짜쇼핑몰 구별하기

• 목 표 •

- 1 가짜 쇼핑몰의 피해사례를 통해 경각심을 고취시킨다.
- 2 가짜 쇼핑몰을 구별할 수 있다.
- 3 피해를 입었을 때, 신속히 조치할 수 있다.

• 준비물 •

- 1 인터넷에 연결된 PC
- 2 SNS 계정이 있는 휴대폰

• 핵심 사이트 •

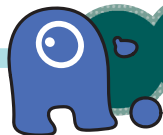
- 1 해외직구 의심 사이트 검색 : consumer.go.kr
- 2 검색 포털 : naver.com
google.com
- 2 SNS : instagram.com
youtube.com
facebook.com

• 핵심 활동 •

- 가짜 쇼핑몰의 다양한 피해사례를 확인한다.
- 가짜 쇼핑몰의 특징을 알아본다.
- 가짜 쇼핑몰에 의해 피해를 입었을 때 행동요령을 학습한다.

• 핵심 키워드 •

- 가짜쇼핑몰, 사이트 주소, 유사이미지, 후기확인, 상품정보



학습을 위한 사전준비

- ▶ 주변에서 가짜 쇼핑몰에 접속한 경험이 있는지 들어가 본 사람이 있는지 조사한다.
- ▶ 문자, 메신저 등으로 가짜 쇼핑몰의 링크가 온 적이 있는지 확인한다.
- ▶ SNS를 통해 광고 사이트에 접속해 본다. (설치 요청이 있으면 거부할 것)



가짜쇼핑몰의 피해사례

★ 가짜 쇼핑몰이란?

가짜 쇼핑몰은 겉으로 보기에는 정상적인 인터넷 쇼핑몰과 거의 구분이 되지 않도록 만들어진 쇼핑몰로서, 소비자들을 현혹하여 재산상 이익을 꾀하는 자들이 만들고 있다. 유명 브랜드의 로고, 디자인, 상품 사진까지 실제 쇼핑몰을 따라 만들기 때문에, 자세히 들여다보지 않으면 "진짜 같다"고 느끼기 쉽다. 이런 사이트들은 보통 시중 가격보다 훨씬 싸게 파는 것처럼 광고하면서, 소비자를 현혹하거나, 비정상 제품을 발송하는 방법으로 소비자에게 피해를 입힌다.

★ 주요 범죄 수법 및 실제 사례

1 유명 브랜드 사칭 및 초저가 유도 (SNS 광고형)

가장 빈번하게 발생하는 수법으로, 인스타그램, 페이스북 등 SNS에 '80~90% 파격 세일', '재고 정리' 등의 광고를 노출하여 가짜 사이트로 유인하는 방식이다. 이들은 공식 홈페이지의 로고, 디자인, UI를 그대로 복제하고 심지어 실제 업체 정보를 하단에 도용하여 신뢰를 얻은 뒤, 결제만 받고 물건을 보내지 않거나 저렴한 가품을 발송한다.

- 사례 (2025년) : '알로(Alo)', '스투시(Stussy)', '우영미(Wooyoungmi)' 등 MZ세대가 선호하는 브랜드의 공식 홈페이지를 사칭한 사이트들이 기승을 부렸다. 피해자들은 SNS 광고를 통해 접속했으며, 결제 후에는 주문 조회조차 되지 않고 사이트가 폐쇄되는 일을 겪었다.

* 출처 : [85% 세일에 속았다... 정교해진 브랜드 사칭 사이트 우후죽순, 연합뉴스TV, 2025.04.17]

2 기업형 짝퉁 유통 및 범죄 수익 은닉

조직적으로 가짜상품 판매 쇼핑몰을 운영하며 대규모로 가품을 유통하는 사례이다. 이들은 자체 쇼핑몰을 구축한 뒤 중국에서 밀수입한 가짜 명품을 판매하였다. 수사기관의 추적을 피하기 위해 가상자산(코인)으로 수익금을 세탁하는 치밀함도 보였다.

- 사례 (2026년) : 인천본부세관은 2022년부터 약 3년간 가짜 명품 7만 7천여 점(정품 시가 1,200억 원 상당)을 유통한 일당을 검거했다. 이들은 수익금을 비트코인 등 가상자산으로 환치기하여 은닉했으며, 수사 중에도 쇼핑몰 이름만 바꿔 영업을 지속하는 대담함을 보였다.

* 출처 : [77,000 Counterfeit Luxury Items Seized in 16.5 Billion Won Smuggling Case, 조선일보(영어판), 2026.01.27]

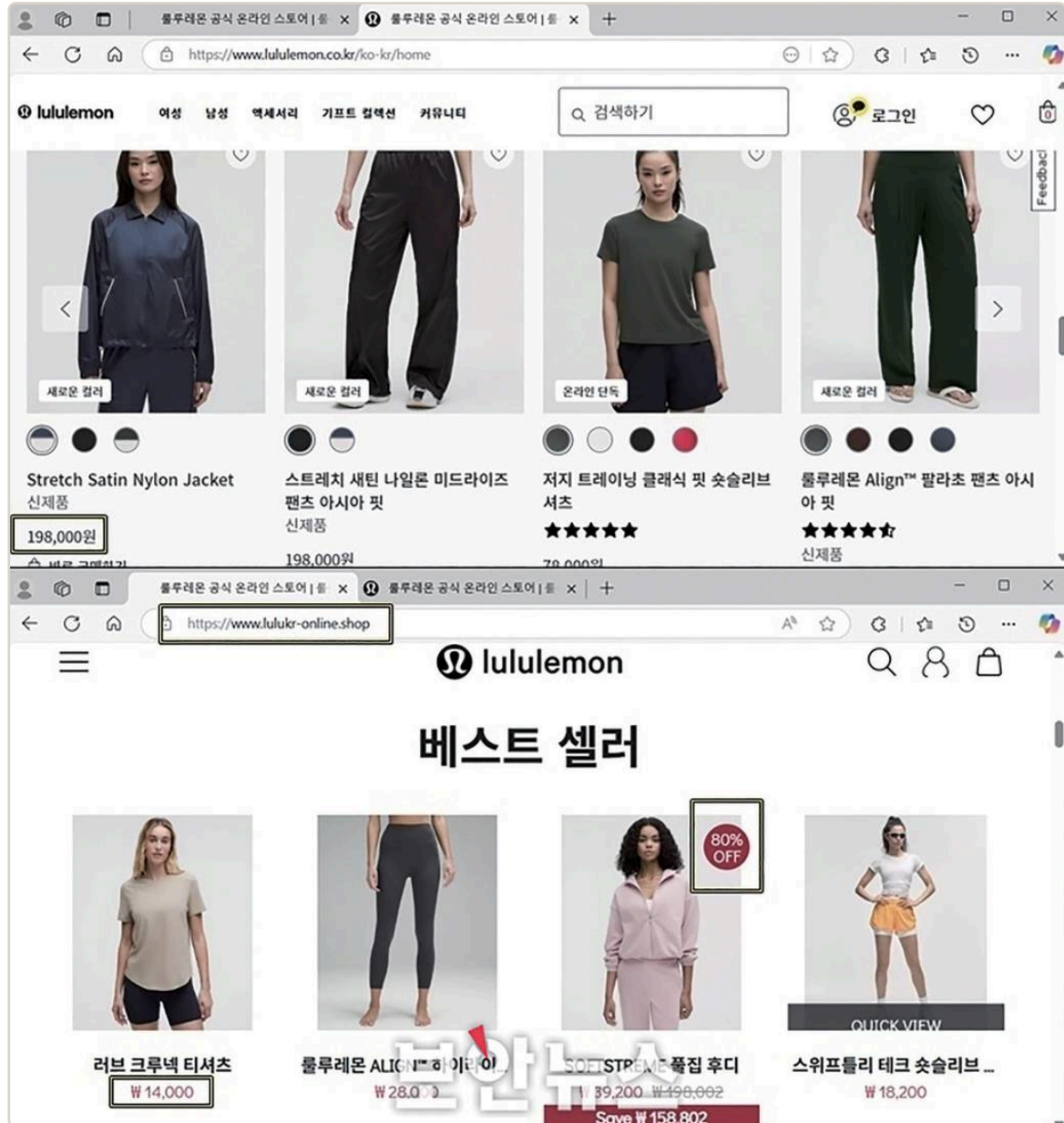
3 고수익 부업 및 미션 수행 사기 (피싱 결합형)

최근 새롭게 떠오르는 유형으로, 단순히 물건을 파는 것이 아니라 '쇼핑몰 일자리'를 미끼로 삼는다. 이들은 "쇼핑몰 주문서를 대신 작성하면 수익을 준다"며 접근한다. 처음에는 소액의 수익금을 입금해 주고 신뢰를 쌓은 뒤, 나중에 '고액 미션'을 수행하려면 본인 돈으로 먼저 물건을 결제해야 한다며 거액을 편취한다.

- 사례 (2026년) : 졸업 후 일자리를 찾던 구직자가 '데이터 입력 및 쇼핑몰 관리' 알바 공고를 보고 지원했으나, 이는 개인정보를 탈취하고 결제를 유도하는 사기였다.

* 출처 : [2025년에 주의해야 할 사기 수법 10가지, ExpressVPN 블로그(트렌드 리포트), 2026.02.25.]

아래 사진은 유명 온라인몰을 사칭하는 가짜 사이트의 예시이다.



룰루레온 사기 사이트 비교 _ 상단 진짜, 하단 가짜



함께 해볼까요?

온라인 검색을 통해 가짜 쇼핑물을 찾아보고 각 가짜 쇼핑물의 특징에 대해 분석해 봅시다.

쇼핑물 명칭	진짜 쇼핑물 URL	가짜 쇼핑물 URL	차이점



가짜쇼핑몰 구별방법

가짜 쇼핑몰 피해 사례는 모두 “싸다”, “할인율이 높다”는 유혹을 이기지 못해 발생하는 경우가 많다. 따라서 우리는 전자상거래를 통해 거래를 하고자 할 때 “싸고 좋은 제품을 찾는 능력”뿐만 아니라 “이 사이트가 안전한지 의심해 보는 능력” 또한 함께 길러야 한다.

가짜 쇼핑몰을 완벽하게 한눈에 구분하는 방법은 없지만, 의심해야 할 신호는 분명히 확인할 수 있다. 실제 보안·소비자 기관과 전문가들이 제시하는 기준을 알아보자.

1 사이트 주소(URL)를 먼저 본다

유명 브랜드 이름을 흉내 낸 이상한 주소(예: nike → n1ke, .com 대신 .shop-kr 등)를 사용하기도 한다. 주소창에 자물쇠 표시와 함께 https://가 있는지, 너무 길고 복잡한 주소는 아닌지 확인한다.

해외 직구 가짜 쇼핑몰 확인방법

정부에서 운영하는 소비자24 홈페이지에는 해외 직구 사기 의심 사이트 검색기능이 있다. 상대적으로 저렴하고 구하기 힘든 상품을 구매하고자 할 때 꼭 사전 확인이 필요하다.

[소비자24] <https://www.consumer.go.kr/user/ftc/consumer/itnld/1073/selectItnldList.do?bbsSe=03>

2 사업자 정보와 약관이 있는지 확인한다

정상 쇼핑몰은 페이지 하단에 사업자등록번호, 주소, 연락처, 통신판매업 신고번호, 이용약관, 개인정보처리방침, 교환·환불 규정을 표시하고 있다. 법적 의무사항이기 때문에 정상적인 쇼핑몰에는 이들 정보가 하단에 표시되어 있는 것이 정상이다. 이런 정보가 없거나, 클릭이 되지 않거나, 주소가 이상하면 의심해야 한다.

온라인 쇼핑몰의 의무사항

전자상거래법에서 요구하는 온라인 쇼핑몰의 의무사항

- 전자상거래법은 사업자에게 소비자가 상품이나 서비스를 선택하는 데 필요한 핵심 정보를 명확하고 정확하게 제공할 의무를 부과한다. 이에 따라 상품명, 가격, 품질, 주요 사양, 배송비, 청약철회 조건, 판매자 연락처 등이 필수적으로 포함되어야 한다.
- 전자상거래법은 소비자의 청약철회권(구매 후 일정 기간 내 계약 취소 권리)을 보장하고 있다. 소비자는 일반적으로 상품 수령 후 7일 이내에 청약철회를 할 수 있으며 사업자는 이에 대해 지체 없이 환불 조치해야 한다.
- 전자상거래에서 사업자는 소비자의 개인정보를 수집·이용·보관하는데 엄격한 규제를 두고 있다.

- 전자상거래법은 거래가 성립되면 소비자에게 계약 내용을 포함한 전자문서를 즉시 제공하도록 규정한다. 제공되는 정보에는 거래 내역, 청약 내용, 대금 결제 조건, 청약철회권 행사 방법 등이 포함된다.

- 전자상거래법은 소비자의 권익을 보호하기 위해 불공정약관 조항을 금지하고 있다. 기업이 이런 약관을 사용할 경우 무효 처리되고 공정위의 시정 권고 및 행정 제재 대상이 된다.

- ▶ 소비자에게 지나치게 불리한 계약 해제 제한 조항
- ▶ 사업자의 일방적 계약 변경 권한 부여
- ▶ 손해배상 책임을 소비자에게 과도하게 부담시키는 내용
- ▶ 청약철회권 행사에 불합리한 조건을 부과하는 조항

3 결제 방식이 '계좌이체만'인지 확인한다.

가짜 쇼핑몰은 카드결제나 간편결제 대신, 계좌이체·가상계좌·현금 결제만 요구하는 경우가 많다. 특히 “현금 결제 시 추가 20% 할인” 같은 과도한 혜택을 제시하면서 서둘러 입금을 요구한다면 위험 신호이다.

4 후기와 외부 평판을 찾아본다.

포털 검색을 이용해서 [쇼핑몰 이름 + “사기”] 또는 [쇼핑몰 이름 + “후기”]를 검색해 다른 사람들의 경험을 확인한다. 검색 결과를 확인했을 때 외부 후기나 리뷰가 거의 없는데 가격만 지나치게 싸다면, 신중하게 다시 생각해야 한다.

5 상품 정보와 글의 품질을 살핀다.

상품 소개 내용에 저화질 사진이 사용되거나 어색한 번역투의 문체, 맞춤법 오류가 자주 보이거나 여러 언어가 뒤섞인 설명 등이 보인다면 다른 곳에서 긁어온 콘텐츠일 가능성이 매우 높다.

페이지 하단의 ‘회사소개’, ‘고객센터’, ‘반품 안내’ 같은 메뉴를 눌렀을 때, 실제로 페이지가 열리는지도 확인해 볼 필요가 있다.

조금이라도 저렴한 상품을 검색하여 현명한 소비를 하는 것은 좋은 습관이지만, 현명한 소비를 위한 노력이 나의 자산, 나의 소비에 대한 위협을 감지하지 못하게 된다면 큰 손해를 가져올 수 있다. 그러므로 싼 가격에 현혹되지 말고 “조금이라도 이상하면 멈추고 다시 확인하는 습관”을 갖추는 현명함 또한 필요하다.



피해를 입었을 때의 조치방법

아무리 조심해도, 때로는 피해가 발생할 수 있다. 이때 중요한 것은 “당했다”는 감정에 머무르는 것이 아니라, 추가적으로 발생할 수 있는 피해를 줄이고, 적절한 대응을 통해 손해를 만회할 수 있는 방안을 강구하는 것이다. 차례대로 우리가 취할 수 있는 방안들을 정리해 보자.

1 즉시 결제를 막거나 취소 요청을 한다

카드로 결제했다면 피해사실을 알았을 때 즉시 카드사 고객센터에 바로 전화해 결제 취소 또는 거래 정지를 요청한다. 계좌이체를 했다면 은행에 연락해 상대 계좌에 대한 지급정지 요청을 할 수 있는지 확인해야 한다. 사기에 의해 상대방 계좌로 이체를 한 경우, 상대방이 해당 계좌에 이체된 금액을 인출할 경우 범죄가 완성되므로 계좌이체를 했을 때에는 지체없이 은행을 통한 조치를 취하는 것이 좋다.

2 증거를 최대한 많이 모은다

많은 사람들이 놓치고 간과할 수 있는 부분이다. 주문 내역, 결제 영수증, 문자·카톡 메시지, 사이트 화면 캡처, 통화 녹음 등 범죄 피해 관련 자료를 모아 두어야 한다. 이런 증거는 나중에 신고나 피해구제 신청을 할 때 매우 중요한 자료가 된다.

3 관련 기관에 신고한다

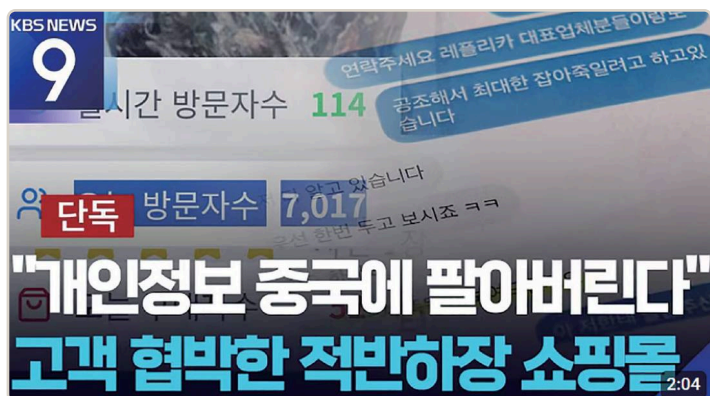
금융범죄가 증가함에 따라 정부에서도 범죄피해 예방과 손해확산 방지를 위해 여러 방안들을 강구하고 있다. 피싱 의심 사이트나 사기 쇼핑물은 경찰(사이버수사대), 공정거래위원회, 한국인터넷진흥원, 한국소비자원 등에 신고할 수 있다.

4 혼자 해결하려 하지 말고, 전문가와 상의한다

학생이 스스로 피해를 방지하거나 문제를 해결할 수 있다는 생각은 금물이다. 피해자가 피해 사실을 숨기고 혼자 해결하려 하면, 오히려 더 큰 피해나 2차 피해로 이어질 수 있다. 전문가에게 피해사실을 밝히고 도움을 요청하는 것이 오히려 용기 있는 행동이라는 사실을 잊지 말아야 한다.

★ 가짜 쇼핑몰 피해 관련 영상 시청

가짜 쇼핑몰에서는 쇼핑몰 운영을 위해 수집한 개인정보까지 유출되는 사례가 있다. 이에 대한 피해사례를 취재한 뉴스를 확인해보자.



KBS 뉴스 (2026.3.11.) 유튜브 :

<https://youtu.be/3Hjju7d9cFw?si=h9yAmknBpUzz76KM>



자기 평가하기

- ★ **가짜쇼핑몰과 진짜 쇼핑몰의 특징을 배우고 진위 여부를 판단할 수 있는 여러 방법과 원칙을 확인한 만큼 아래 평가표에 체크해보자.**

평가 내용	매우 우수	우수	보통	부족	매우부족
▶ 가짜 쇼핑몰의 특징에 대해 3가지 이상 설명할 수 있다.					
▶ 가짜 쇼핑몰 범죄를 피하기 위해 숙지하여야 할 기본원칙 5가지 중 3가지 이상 설명할 수 있다.					
▶ 전자상거래에서 사기 등의 피해를 입었을 때 조치 방법에 대해 숙지하고 타인에게 설명할 수 있다.					

- ★ **학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.**

디지털자산 보호



디지털자산 보호에 대해
알아볼까?



출처: 제미나이

교육 목표

- 디지털 자산의 정의와 종류 및 특징을 이해한다.
- 가상화폐가 무엇인지 이해하고 그 기반이 되는 블록체인기술에 대해 이해한다.
- 온라인 banking에 대해 알아보고 안전하게 사용하는 원칙을 숙지한다.
- 디지털 자산을 노리는 범죄와 그 범죄의 예방 방법 및 피해를 입었을 때의 조치 방법에 대해 이해한다.



이런 활동을 해요

프로젝트 과정	기초	심화
	온라인 금융 서비스와 결제방식	디지털자산 보호
활동 내용	• 온라인 금융이란? • 체크카드와 신용카드 • 간편결제와 온라인쇼핑 • 가짜 쇼핑몰과 진짜 쇼핑몰	• 디지털 자산이란? • 가상화폐와 블록체인 기술 • 온라인 banking • 내 자산을 노리는 범죄와 보호방법

01

디지털 자산이란?

• 목 표 •

- 1 디지털 자산의 정의를 이해한다.
- 2 디지털 자산의 종류와 특징을 이해한다.
- 3 디지털 자산에 대한 위협요소를 인식한다.

• 준비물 •

- 1 인터넷에 연결된 PC
- 2 보유 은행계좌에 연결된 온라인 banking ID/PW
- 3 가상화폐의 종류와 가격을 확인할 수 있는 가상화폐 거래소 어플이 설치된 단말기

• 핵심 활동 •

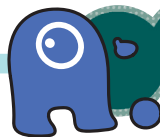
- 디지털자산에 대해 학습한다.
- 디지털자산의 종류에 대해 학습한다.
- 디지털자산의 특징에 대해 학습한다.
- 디지털자산에 대한 위협요소를 학습한다.

• 핵심 사이트 •

- 1 가상화폐 거래소 : bithumb.com
- 2 하나은행 : kebhana.co.kr
- 3 포털 검색 : naver.com
google.com

• 핵심 키워드 •

- 디지털 자산, 보호, 접근권한, 계정탈취, 피싱, 사기



학습을 위한 사전준비

- ▶ 가치가 높은 NFC의 사례를 찾아본다.
- ▶ 암호화폐의 종류와 각 암호화폐별 특징, 가격을 알아본다.
- ▶ 온라인뱅킹 어플리케이션에 로그인해본다.
- ▶ 공용 무료 인터넷을 통한 해킹 사례를 조사해본다.



디지털 자산의 정의

민준이는 MMORPG 게임을 좋아한다. 게임을 하다가 우연히 희귀한 아이템을 얻었지만 민준이의 캐릭터와 맞지 않아 게임 내 거래소를 통해 대량의 게임 내 머니와 교환하였다. 그러던 중 게임 머니를 필요로 하는 다른 사람으로부터 현금을 줄 테니 게임 내 머니를 넘기라는 거래 제안을 받았다. 게임을 통해 얻게 된 게임머니는 자산으로서 가치가 있는 것인가?

★ 디지털 자산의 정의

디지털 자산이란 전자적 기록으로 존재하고, 특정 개인이나 계정이 배타적으로 통제할 수 있으며, 일정한 경제적 가치 또는 교환 가치를 지니는 자산을 말한다. 여기에는 가상자산, 전자지갑 잔액, 포인트, 게임 아이템, NFT, 디지털 콘텐츠 권리, 클라우드에 저장된 자산성 데이터 등이 포함될 수 있다.

중요한 점은 디지털 자산이 “파일” 그 자체가 아니라, 접근권한·소유권·이전가능성이 결합된 가치라는 사실이다. 즉, 같은 이미지 파일이라도 단순한 사진일 수도 있고, NFT처럼 소유권 구조가 붙으면 자산이 될 수도 있다.

달리 말하자면 디지털 자산은 ‘눈에 보이지 않지만, 계정·지갑·플랫폼 안에서 실제 가치를 가지며, 비밀번호와 인증정보가 곧 자산을 지키는 열쇠가 되는 재산’이라고 표현할 수 있다.

눈에 보이지 않지만 실제적으로 가치를 가지고 있는 재화로 게임 아이템, 온라인 포인트, 구독 계정, 디지털 콘텐츠, SNS 계정의 운영 권한 등을 들 수 있다. 실제 이들 중 일부는 직접 현금으로 교환할 수 있거나, 시간과 노력이 축적된 결과물이라는 점에서 법적 보호의 대상이 될 수 있다.

★ 디지털 자산 보호를 위한 인식의 전환

디지털 자산은 물리적 형태가 없기 때문에 분실·도난·복제가 매우 빠르게 일어날 수 있다. 또한 개인키, 비밀번호, 2단계 인증, 복구코드 같은 접근수단이 유출될 경우 자기도 모르는 사이에 자산이 탈취될 수 있다. 그래서 디지털 자산의 보호는 단순한 보안 문제가 아니라 권한 관리, 인증, 저장, 백업, 복구를 포함하는 체계적 문제로 인식해야 한다.

“자산”이라는 개념은 좁은 의미로 현금이나 부동산으로만 국한하여 생각하기 쉽지만, 디지털 환경에서는 계정 정보와 실체 없는 데이터 일지라도 충분히 보호받을 자산이 될 수 있다. 따라서 디지털 자산에 대해 학습할 때, 자산의 실질적 가치 뿐만 아니라 보호필요성이 있는 정보와 권리까지 포함됨을 확인할 필요가 있다.



디지털 자산의 종류와 특징

★ 디지털 자산의 종류

디지털 자산은 한마디로 말하면 전자적인 형태로 존재하면서 재산적 가치가 있는 것이다. 그렇기 때문에 디지털 자산은 생각보다 훨씬 넓은 범위를 가진다. 사람들은 보통 디지털 자산이라고 하면 비트코인 같은 대표적인 가상자산만 떠올리기 쉽지만, 실제로는 여러 종류가 있다.

1 가상자산

가장 많이 알려진 디지털 자산이다. 비트코인, 이더리움 같은 암호화폐가 이 범주에 들어간다. 이런 자산은 인터넷상의 거래소에서 사고팔 수 있고, 가격이 계속 변한다는 특징이 있다. 쉽게 말해, 주식처럼 실물은 없지만, 평가되는 가치가 오르기도 하고 내려가기도 하는 자산이라고 볼 수 있다.

2 전자지갑 잔액

여행지에서 하나머니로 결제해 본 경험이 있는가? 하나머니, 토스머니, 카카오페이머니, 네이버페이 포인트처럼 앱 안에 저장된 포인트 또는 금액도 디지털 자산으로 볼 수 있다. 이것은 눈에 보이는 지폐는 아니지만, 실제 결제에 사용될 수 있기 때문에 분명한 금액적 가치를 가지고 있다.

3 포인트와 마일리지

온라인 쇼핑몰 포인트, 항공사 마일리지, 카드사 적립 포인트도 자산의 성격을 가진다. 예를 들어 쇼핑몰에서 1,000포인트가 있다면 다음 구매 때 내가 지불하는 금액에 더해서 현금처럼 쓸 수 있다. 액수는 작아 보여도, 쌓이면 실제 돈처럼 작동한다는 특징이 있다.

4 게임 아이템과 게임머니

우리가 즐겨 하는 온라인 게임 속에서도 자산이 존재한다. 희귀 아이템, 코스튬, 게임머니, 캐릭터 계정 등이 대표적인 온라인 자산이다. 어떤 아이템은 현금으로 직접 환가할 수 있을 정도로 가치가 크기도 하다. 학생들에게는 가장 익숙한 디지털 자산 사례일 수 있다.

5 디지털 콘텐츠와 계정 권리

전자책, 음악 파일, 유료 강의 계정, 스트리밍 서비스 구독권 같은 것도 넓은 의미에서 디지털 자산이다. 또한 SNS 계정, 구독형 서비스 계정, 클라우드 저장 공간에 대한 접근권도 사실상 가치 있는 자산으로 볼 수 있다. 특히 오래 운영한 계정이나 팔로워가 많은 계정은 실제로 경제적 가치가 생기기도 한다.

6 NFT와 디지털 소유권 자산

NFT는 디지털 파일 자체보다 그 파일의 소유권이나 진본성을 기록하는 방식으로 이해할 수 있다. 예를 들어 같은 그림 파일을 누구나 볼 수 있어도, 특정 NFT가 붙어 있으면 그 “원본 소유자”가 누구인지 기록할 수 있다. 아직 논쟁이 많지만, 디지털 자산의 새로운 형태로 자주 언급된다.



함께 해볼까요?

내가 가지고 있거나 주변에서 찾아볼 수 있는 자산으로 아래 표를 채워본 후 디지털 자산에 해당 하는지 여부를 판단해보자.

자산 명칭	전자적 기록 여부	배타적 소유권	교환가치	디지털 자산여부
	☐	☐	☐	(Y / N)
	☐	☐	☐	(Y / N)
	☐	☐	☐	(Y / N)
	☐	☐	☐	(Y / N)

NFT에 대한 상식

NFT는 블록체인 기술을 활용해 디지털 파일(그림, 영상, 음악 등)에 고유한 인식 값을 부여하여 '원본'임을 증명하는 디지털 인증서이다. Non-Fungible Token의 줄임말로 '대체 불가능한 토큰'이라는 뜻을 가지고 있으며, NFT를 발행한다는 것은 그림, 영상, 음악, 게임 등의 콘텐츠에 블록체인 기반으로 창작자, 소유자, 거래 내역 등의 정보를 실시간으로 기록한다는 의미이다.

NFT를 붙인 디지털 카드는 종이 카드처럼 찢어지지도 않고, 언제든지 스마트폰으로 열어볼 수 있다는 장점도 있지만, 무엇보다 NFT를 통해 구매 이력이 공개되고, 원본 카드가 내 소유임을 증명할 수 있게 된다.

사실 그동안 디지털 재화는 무한대로 복사가 가능해 원본을 소유한다는 것에 자산으로서 큰 가치가 없었으나, NFT의 등장으로 각 재화마다 NFT에 기록된 정보(창작자, 소유자, 거래내역 등)를 확인할 수 있으며 이 정보들을 대조함으로써 디지털 그림의 원본과 복사본을 가릴 수 있게 되었다.

★ 디지털 자산의 특징

디지털 자산은 일반적인 물건과는 다른 성격을 가지고 있다.

책상이나 스마트폰처럼 손에 잡히는 물건이 아니라 디지털의 형태로 존재하기 때문에 여러가지 특징들이 드러난다.

1 눈에 보이지 않는다

디지털 자산은 대부분 화면 속 숫자, 파일, 계정, 코드 형태로 존재한다. 현금처럼 만질 수 없다는 특징이 있기에 사람들이 자산임을 실감하지 못하는 경우가 많지만 재산적 가치를 인정받는다.

2 복사와 전송이 빠르다

디지털 자산은 물리적인 물건보다 훨씬 빠르게 이동한다. 포인트나 코인을 보내는 데는 몇 초면 충분할 수 있다. 대신 이 빠름은 편리함이기도 하지만, 한 번 잘못 넘기면 되돌리기 어려운 위험이기도 하다.

3 접근권한이 핵심이다

디지털 자산은 “그 자체”보다도 누가 접근할 수 있느냐, 접근권한의 부여가 중요하다. 예를 들어 내 계정에 로그인할 수 있는 비밀번호가 있으면 자산을 쓸 수 있지만, 비밀번호를 잃어버리면 자산이 있어도 쓸 수 없게 된다. 즉, 디지털 자산은 소유와 관리가 아주 밀접하다.

4 가치가 빨리 변할 수 있다

디지털 자산 중 가상자산은 가격 변동이 빈번하고 그 폭이 큰 것으로 유명하다. 자산의 가치는 가상자산 뿐만 아니라 각 디지털 자산의 가치는 게임 속 아이템의 인기, 포인트 제도의 변경, 플랫폼 정책 변화 등 다양한 요건에 따라 달라질 수 있다.

5 플랫폼에 의존한다.

디지털 자산은 혼자 존재하지 않는다. 어떤 앱, 어떤 회사, 어떤 거래소, 어떤 서버 위에서 운영되는 경우가 많기 때문에 그 플랫폼이 사라지거나 정책을 바꾸면 자산의 사용 방식도 크게 달라질 수 있다.

6 거래 기록이 남는다.

대부분의 디지털 자산은 전자적 기록이 남는다. 이 기록은 자산현황, 자금출처, 세금 부과 등 다양한 측면에서 투명성을 높일 수 있지만, 반대로 누가 언제 무엇을 했는지도 추적된다는 뜻이기도 하다. 즉, 편리함과 관리성이 동시에 존재한다.

★ 디지털 자산에 대한 위협

디지털 자산을 안전하게 보호하기 위해서는 보안에 신경쓰고 조심해야 한다. 왜냐하면 디지털 자산은 도둑이 직접 훔쳐 가는 것이 아니라, 정보를 빼내서 가져가는 방식으로 탈취되는 경우가 많기 때문이다.

1 가장 큰 위험은 계정 탈취

디지털 자산의 안전에서 가장 중요한 것은 계정의 보안이다. 비밀번호 또는 인증번호의 유출, 다른 사람의 로그인을 통해 내 계정의 권한을 탈취당한다면 소중한 자산이 한순간에 사라질 수 있다. 즉, 디지털 자산은 금고보다 문이 더 중요하다.

2 피싱과 사기

가짜 문자, 가짜 이메일, 가짜 사이트를 통해 로그인 정보를 빼내는 방식이 매우 흔하다.

예를 들어 “포인트가 만료됩니다”, “계정이 정지됩니다” 같은 문구로 사람을 놀라게 한 뒤 링크를 누르게 만드는 경우가 많다. 이런 메시지를 받으면 믿지 말고 바로 누르지 말고, 공식 앱이나 공식 홈페이지로 다시 확인해야 한다.

3 복구가 어려울 수 있다

현금도 잃어버리면 찾기 어렵지만, 디지털 자산은 복구방식이 더 복잡할 수 있다.

비밀번호를 잊거나, 복구코드를 잃어버리거나, 개인키를 분실하여 내 자산에 접근할 수 있는 계정에 접근하지 못한다면 자산의 소유자도 접근하지 못할 수 있다. 이 점이 디지털 자산이 매우 편리하면서도 동시에 매우 위험한 이유이다.

4 플랫폼 사고의 위험

거래소나 서비스 회사가 해킹을 당하거나 서버 문제가 생기면, 내 자산이 직접 도난당하지 않았더라도 사용이 불가능해질 수 있다. 즉, 디지털 자산은 개인 보안만이 아니라 플랫폼의 보안도 중요하다.

5 가격 위험도 있다

안전성은 보안만의 문제가 아니다. 가상자산처럼 가격이 크게 오르내리는 자산은, 내 의사와 다르게 가치가 급격히 줄어둘 수 있다. 그래서 디지털 자산은 “안전하게 지키는 것”과 “가치 변동 가능성”에 대해 함께 배워야 한다.



함께 해볼까요?

아래 보기를 보고 디지털 자산에 대한 위험과 그렇지 않은 것을 분류해 보자. 그리고 그렇게 분류한 이유를 옆 사람에게 설명해보자.

보기

- 가. 로그인 비밀번호를 6개월동안 바꾸지 않았다.
- 나. 통신요금 때문에 카페 와이파이를 자주 이용한다.
- 다. 내가 사용하는 플랫폼이 해킹당했지만 내 정보는 유출되지 않았다.
- 라. 내가 사용하는 사이트마다 비밀번호가 모두 다 다르다.
- 마. 문자나 카톡에 오는 링크는 궁금하므로 다 열어본다.
- 바. 내 암호화폐가 1분만에 30% 수익을 냈다.

위험에 해당

위험이 아님



자기 평가하기

★ 디지털 자산에 대해 익히고 학습한 만큼 아래 평가표에 체크해보자.

평가 내용	매우 우수	우수	보통	부족	매우부족
▶ 디지털 자산의 정의에 대해 정확히 설명할 수 있다.					
▶ 디지털 자산의 종류에 특징에 대해 설명할 수 있다.					
▶ 디지털 자산을 위협하는 요소에 대해 설명할 수 있다.					
▶ 디지털 자산 위협에 대해 대응할 수 있다.					

★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

02

가상화폐와 블록체인 기술

• 목표 •

- 1 가상화폐의 정의와 등장 배경에 대해 학습한다.
- 2 비트코인의 특징과 블록체인 기술의 작동 방식에 대해 이해한다.
- 3 블록체인 기술이 적용될 수 있는 산업분야에 대해 학습한다.

• 준비물 •

- 1 인터넷이 연결된 PC
- 2 bithumb ID/PW

• 핵심 사이트 •

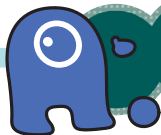
- 1 유튜브 : youtube.com
- 2 가상화폐 플랫폼 : bithumb.com

• 핵심 활동 •

- 가상화폐의 종류를 말해본다.
- 비트코인의 특징을 서로 말해본다.
- 블록체인 기술에 대해 상대방에게 설명한다.
- 스테이블 코인에 대한 동영상을 감상한다.

• 핵심 키워드 •

- 가상화폐, 비트코인, 블록체인 기술, 스테이블 코인



학습을 위한 사전준비

- ▶ 가상화폐의 대표적인 예를 찾아본다.
- ▶ 우리나라에서 가상화폐가 일반 화폐처럼 인식되고 있는지 알아본다.
- ▶ 블록체인 기술이 적용된 최신 기술을 검색해본다.
- ▶ 스테이블코인을 인정한 나라가 있는지 검색해본다.
- ▶ 우리나라에서 스테이블 코인에 대해 어떻게 평가하고 있는지 알아본다.



가상화폐와 블록체인 기술

“비트코인을 사!”

요즘 유행하는 과거 회귀물 소설에서 주인공이 주변 인물들에게 자주 해주는 말이다. 짧은 기간동안 천문학적 수준으로 가치가 향상된 재화이기 때문인데, 일확천금의 대명사인 비트코인은 어떻게 유명해졌고, 대체 어떤 금융수단인지 그 원리에 대해 알아볼 필요가 있다. 왜냐하면 비트코인을 비롯한 암호화폐는 기술적, 가치적으로 디지털 금융의 첨단에서 있고, 가치가 매우 높을 뿐만 아니라 매우 큰 영향력을 끼치고 있으며, 디지털 금융의 특성상 보안이 무너질 경우 자산의 침탈이 매우 쉽게 일어날 수 있기 때문이다.

★ 가상화폐란?

가상화폐는 눈에 보이는 지폐나 동전처럼 물리적인 형태가 있는 돈이 아니라, 인터넷 환경에서 존재하고 거래되는 디지털 형태의 자산이다. 가상화폐는 주로 “분산된 전자기록”과 “암호기술”을 바탕으로 작동한다.

가상화폐를 이해할 때 중요한 점은 이것이 단순한 “게임머니”가 아니라는 사실이다. 물론 실물 현금처럼 만질 수는 없지만, 거래소나 지갑을 통해 보관하고, 다른 사람과 주고받을 수 있으며, 시장에서 가격이 형성된다. 다시 말해, 가상화폐는 디지털 환경에서 가치의 저장과 이전을 가능하게 하는 새로운 형태의 자산이라고 볼 수 있다.

가상화폐의 대표적인 예는 비트코인과 이더리움을 들 수 있다. 비트코인에 대해서는 많이 들어보았을 것이다. 비트코인은 2009년 '사토시 나카모토'라는 가명으로 알려진 인물이 만든 최초의 암호화폐로서, 기존 화폐처럼 은행이나 정부가 발행·관리하지 않고, 인터넷을 통해 P2P(개인 간) 방식으로 자유롭게 거래할 수 있다. 총 발행량은 2,100만 개로 제한되어 있어 '디지털 금'으로 불리며, 블록체인 기술로 모든 거래 기록을 투명하게 저장한다.

채굴이란?

비트코인은 2100만개로 발행 숫자가 제한되어 있기 때문에 한정자원으로 간주된다. 특히 비트코인은 디지털 금이라 불리우며 비트코인을 발급받는 행위를 채굴이라고 표현하고 있다.

쉽게 설명하자면 비트코인 채굴은 금광에서 금을 캐는 것에 비견된다. 채굴자들은 땅(블록체인 네트워크)에서 금(새 비트코인)을 찾기 위해 삽과 곡괭이(고성능 컴퓨터)를 들고 경쟁한다. 가장 먼저 금맥(올바른 해시값)을 발견한 사람이 보상으로 새로 발급된 비트코인을 가져가게 되지만 시간이 지날수록 깊게 땅을 파야 하고(난이도 상승) 경쟁자가 많아지면 더 강력한 장비(ASIC)가 필요해지게 되는 단점이 있다.

★ 블록체인 기술

가상화폐를 이해하려면 블록체인 기술을 먼저 알아야 한다. 블록체인 기술은 위변조 및 복사가 쉬운 디지털 데이터에 대한 신뢰를 높일 수 있는 방안으로서 개발되었다. 블록체인은 디지털 거래 기록을 여러 곳에 나누어 저장하고, 그 기록을 서로 실시간 연결함으로써 원본과 상이한 부분에 대해 판단할 수 있게 하는 위조를 어렵게 만드는 기술이다.

쉽게 비유하면, 블록체인은 “한 사람만 갖고 있는 장부”가 아니라 “여러 사람이 동시에 같은 장부를 가지고 서로 확인하는 방식”이다. 예를 들어 누군가 블록체인을 통해 돈을 보냈다면 그 기록이 블록에 저장되고, 저장된 블록은 독립적으로 존재하는 것이 아니라 이전 블록의 기록과 연속되는 내용을 포함하고 있다. 이렇게 여러 블록이 차례대로 이어지면서 하나의 긴 사슬이 만들어지는데, 이것이 바로 블록체인이다.

이 기술의 핵심은 분산성과 무결성이다.

분산성은 한 곳에만 기록을 두지 않고 여러 컴퓨터가 나누어 보관한다는 뜻이고, 무결성은 기록이 쉽게 바뀌지 않는다는 뜻이다. 만약 누군가 과거 거래 기록을 몰래 바꾸려 한다면, 다른 사람들의 기록과 맞지 않게 되어 바로 드러나게 된다. 그래서 블록체인은 “믿을 만한 중앙기관이 없더라도 기록을 신뢰할 수 있게 해 주는 기술”로 설명할 수 있다. 이 때문에 블록체인은 가상화폐뿐만 아니라, 계약 관리, 물류 추적, 인증 시스템 등 다양한 분야에서도 활용될 수 있다.

즉, 블록체인은 가상화폐의 기술적 기반이면서 동시에 더 넓은 디지털 생활에 신뢰를 부여하는 시스템적 핵심 기술이라고 볼 수 있다.

★ 블록체인 기술의 특징

- 탈중앙화 (Decentralization): 중앙 집중 또는 중앙에서 관리하는 데이터베이스 없이 모든 참여자가 동일한 데이터를 보유하고 관리한다.
- 불변성 (Immutability): 한 번 기록된 데이터는 변경하거나 삭제할 수 없기 때문에 데이터의 신뢰성을 보장할 수 있다.
- 투명성 (Transparency): 모든 거래 내역이 모든 참여자에게 공개되어 투명하게 확인할 수 있다.
- 보안성 (Security): 암호화 기술과 분산 저장을 통해 데이터의 해킹이나 위변조를 방지한다.



경제길잡이 유튜브(2026.5.21.) 썸네일 :

<https://youtu.be/EIDh8HHT7xc?si=0ZF58SwAm2gCoBA7>

★ 블록체인의 구조

블록체인은 거래 정보를 블록 단위로 연결하여 여러 참여자가 공동으로 검증·저장하는 분산원장기술이며, 해시, 합의 알고리즘, 분산 저장을 통해 데이터의 무결성과 투명성을 확보하는 것이 특징이다. 다시 말해, 블록체인은 중앙집중형 신뢰 구조를 분산형 신뢰 구조로 전환하는 기술적 기반이라 할 수 있다.

1 기본 개념

블록체인은 거래 정보를 일정한 단위의 블록에 저장하고, 이 블록들을 시간 순서대로 연결한 체계이다. 각 블록에는 이전 블록과의 연결 정보를 포함한 해시값이 들어 있어, 하나의 기록이 임의로 변경되면 전체 연결 구조의 정합성이 깨지게 되며, 이 구조 때문에 기록의 위변조가 어렵고, 데이터의 추적 가능성이 높아진다.

블록(Block)은 데이터를 담고 있는 상자로 생각할 수 있으며 각 블록에는 다음과 같은 정보가 포함된다. 체인으로 연결될 때 이전 블록의 해시값을 포함함으로써 블록 간의 연결을 보장하고, 중간 블록의 데이터를 변경하면 이후 모든 블록의 해시값이 변경되어 무단 변경을 감지할 수 있게 된다.

- 데이터 (Data) : 거래 내역, 계약 정보 등 저장하고 싶은 정보
- 해시값 (Hash) : 이전 블록의 정보를 암호화한 값으로, 블록들을 연결하는 역할을 맡는다.
- 타임스탬프 (Timestamp) : 블록이 생성된 시간 정보
- 체인 (Chain) : 블록들이 해시값을 통해 연결된 형태를 의미한다.



이미지 출처: 제미나이

2 핵심 특징

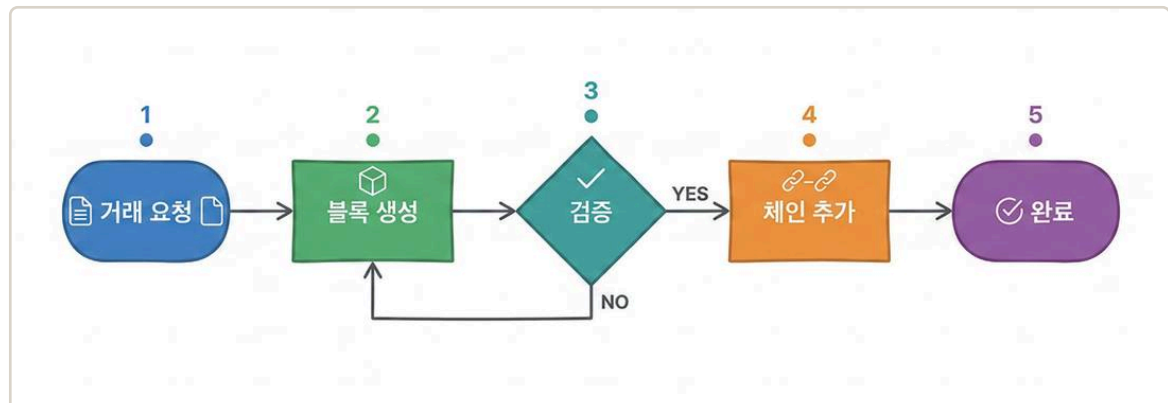
- 분산성 : 하나의 중앙 서버가 아니라 다수의 노드에 동일한 장부가 복제·저장된다.
- 투명성 : 허용된 참여자는 거래 내역을 검증할 수 있어 기록의 가시성이 높다.
- 무결성 : 해시와 합의 절차를 통해 데이터 변조를 어렵게 만든다.
- 비가역성 : 일단 기록된 거래는 임의로 수정하기 어렵기 때문에 이력 관리에 유리하다.
- 신뢰의 자동화 : 기술적 규칙과 합의 메커니즘으로 중개기관이 보장하던 신뢰를 대체한다.

3 작동 원리

블록체인에서는 참여자들이 새 거래의 유효성을 검증하고, 합의된 규칙에 따라 블록을 추가한다. 이 과정에서 합의 알고리즘이 중요한 역할을 하며, 네트워크 참여자들 사이의 신뢰를 절차적으로 확보하게 된다. 따라서 블록체인은 단순한 데이터 저장 방식이 아니라, 검증·기록·보존을 통합한 분산 시스템이라고 볼 수 있다.

- 거래 요청 : 누군가 새로운 데이터를 블록체인에 추가하고 싶다면 거래 요청을 생성한다.
- 블록 생성 : 네트워크 참여자들은 거래 요청을 확인하고, 유효한 거래를 모아 새로운 블록을 생성한다.
- 블록 검증 : 생성된 블록은 네트워크의 다른 참여자들에게 전송되어 검증을 받는다.
- 블록 추가 : 검증이 완료된 블록은 기존 블록체인에 추가된다.
- 데이터 공유 : 추가된 블록의 데이터는 모든 참여자에게 공유된다.

블록체인의 작동 원리



이미지 출처 : 제미나이

4 활용 분야

블록체인은 가상자산뿐 아니라 금융, 물류, 공공기록, 전자계약, 인증, 공급망 관리 등 다양한 분야에 적용될 수 있다. 특히 다자간 거래 이력 관리가 필요하거나, 기록의 위변조 방지가 중요한 분야에서 유용하다. 이러한 점에서 블록체인은 디지털 금융과 전자적 신뢰 인프라의 핵심 기술로 자주 논의된다.

★ 가상화폐가 가진 특징

1 빠른 전송과 낮은 경계 비용

국경을 넘어 돈처럼 이동할 수 있고, 전통적인 금융기관을 거치지 않고도 거래가 가능하다는 점에서 통용 화폐에 비해 편리하다. 또한 블록체인 구조를 통해 거래 기록이 투명하게 관리되며 신뢰성이 높다. 일부 사람들은 이를 “금융의 민주화”라고 부르기도 한다.

2 기술 혁신의 가능성

가상화폐는 새로운 결제 방식과 새로운 계약 구조를 실험하는 장이 되었다. 디지털 자산, 스마트 계약, 탈중앙화 금융 같은 새로운 기술 경제적인 개념들이 이 흐름에서 나왔다.

3 지나친 가격 변동성

24시간 지역에 구애받지 않고 동시간대 거래가 가능하므로 국제 정세에 영향을 많이 받기도 하고 유명인사들의 동향만으로도 몇 분, 몇 초만에 가치가 크게 오르기도 하고 크게 떨어지기도 한다.

4 사기와 해킹 위험

가상화폐는 계정과 지갑 보안이 매우 중요하기 때문에, 잘못 관리하면 디지털 자산을 한 순간에 침탈당하기 쉽다. 위조, 변조의 위험이 없는 대신 관리 계정에 대한 보안관리가 소홀한 경우 높은 가치의 자산이 침탈당할 수 있다.

가상화폐에 대해 공부하는 이유는 가상화폐를 거래하여 경제적 이익을 얻기 위함이 아니다. 이 기술의 도입은 어떤 문제를 해결하기 위해서인지 이해하고, 편리함 이면에 숨어 있는 위험성에 대해서 잘 알아야 디지털 시대의 신뢰를 어떻게 만들 것인지에 대한 해답을 구할 수 있기 때문이다.

★ 스테이블 코인에 대하여

스테이블코인(Stablecoin)은 미국 달러나 금 등 실제 자산의 가치에 가격을 고정(Pegging)하여 가격 변동성을 최소화한 암호화폐를 말한다. 비트코인처럼 가치가 급등락하지 않고 1코인이 1달러와 같은 안정적인 가치를 유지하도록 설계되어 '디지털 달러'로도 불린다.

암호화폐 거래소에서 다른 코인을 구매하거나 거래할 때 기축통화처럼 사

용될 수 있으며 은행망을 거치지 않는 블록체인 P2P(개인 간) 전송 방식을 활용해 저렴하고 빠르게 세계



<스테이블 코인이란? [시사기획 창 | KBS 251021 방송]>

<https://youtu.be/hT1I-ONq6J0?si=9zV8FLvzzOj6IRBH>

출처 : 유튜브 썸네일 캡처

어디든 자금을 이동시킬 수 있다는 장점이 있다. 경제 상황이 불안정하거나 자국 통화 가치가 급락하는 국가에서 가치 보존 수단으로 쓰일 수도 있다.

스테이블 코인에 대하여

스테이블 코인(Stablecoin)은 이름 그대로 가치가 안정되도록 설계된 가상화폐이다. 일반적인 가상화폐는 가격 변동이 매우 크지만, 스테이블 코인은 미국 달러나 원화 같은 법정화폐, 또는 금과 같은 자산의 가치에 연동되도록 만들어진다. 이를 보통 페깅(Pegging)이라고 부른다.

쉽게 말하면, 스테이블 코인은 “코인데 가격에 크게 흔들리지 않도록 만든 코인”이다. 예를 들어 어떤 스테이블 코인이 “1코인 = 1달러”처럼 유지되도록 설계되었다면, 사용자는 가격 변동 걱정을 줄이면서 디지털 환경에서 결제하거나 송금할 수 있다.

스테이블 코인이 주목받는 이유는 가상화폐의 장점과 화폐의 안정성을 동시에 기대할 수 있기 때문이다. 일반 가상화폐는 가격이 급등락해서 안정적인 결제수단으로서의 신뢰도가 낮은 반면, 스테이블 코인은 그 문제를 감소시킬 수 있다.

예를 들어 해외 송금을 할 때 스테이블 코인을 이용하면, 전통적인 은행망보다 빠르게 자금을 이동시킬 수 있다는 기대가 있다. 또한 블록체인의 위에서 작동하므로 거래 기록이 굉장히 투명하게 남는다는 점도 장점으로 거론된다.

스테이블 코인은 편리해 보이지만, 각국 정부가 공식 화폐처럼 허용할지에 대해서는 큰 논쟁이 있다. 스테이블 코인의 인정이 단순한 기술 문제가 아니라, 통화정책 · 지급결제 · 금융안정과 직접 연결되기 때문인데 아래와 같은 문제점이 예상된다.

첫째, 스테이블 코인이 널리 쓰이면 사람들은 은행 예금 대신 스테이블 코인을 더 선호할 수 있다. 이렇게 되면 은행에 들어가야 할 돈이 줄어들어, 은행의 자금조달 구조가 약해질 수 있다.

둘째, 스테이블 코인이 사실상 ‘민간이 만드는 돈’처럼 작동할 수 있다는 점도 논란이다. 스테이블 코인은 법정화폐처럼 보이지만, 실제로는 민간 기업이 발행하고 운영하는 경우가 많기 때문에 “정부가 아닌 민간이 보장할 수 있는가?”라는 위험이 상존한다.

셋째, 준비자산이 충분하지 않거나 관리가 부실하면 스테이블 코인의 가치를 믿기 어려워진다. 과거 일부 알고리즘형 스테이블 코인의 붕괴 사례는 이런 우려를 크게 키웠다.

스테이블 코인의 인정여부에 대해 각 나라별 태도가 상이한 이유가 여기에 있다. 원화 스테이블 코인 논의도 이런 맥락에서 충분한 검토가 필요한 것으로 이해할 수 있다



자기 평가하기

★ 암호화폐와 블록체인에 대해 이해한 만큼 아래 평가표에 체크해보자.

평가 내용	매우 우수	우수	보통	부족	매우부족
▶ 암호화폐가 어떤 방식으로 발행되는지 설명할 수 있다					
▶ 비트코인이 위 변조를 막을 수 있는지 설명할 수 있다.					
▶ 블록체인 기술이 어느 분야에 적용될 수 있는 지 설명할 수 있다.					
▶ 가상화폐의 장점과 위험성에 대해 3가지 이상 설명할 수 있다.					

★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

03

온라인 뱅킹

• 목 표 •

- 1 온라인뱅킹의 정의와 중요성에 대해 학습한다.
- 2 온라인뱅킹의 사용법을 숙지하고 계좌를 개설해 본다.

• 준비물 •

- 1 인터넷에 연결된 PC
- 2 은행의 최신 app 이 설치된 스마트폰
- 3 주거래 은행의 로그인 ID와 PW
- 4 신분증(학생증, 여권, 청소년증)

• 핵심 사이트 •

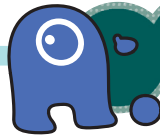
- 1 계좌정보통합관리사이트 : payinfo.or.kr
- 2 하나은행 : kebhana.com
- 3 국민은행 : kbstar.com
- 4 신한은행 : shinhan.com
- 5 우리은행 : wooribank.com

• 핵심 활동 •

- 온라인 뱅킹의 정의를 학습한다.
- 온라인 뱅킹의 위험성에 대해 알아본다.
- 안전한 온라인 뱅킹 사용법을 알아본다.
- 미성년자 하나은행 계좌를 개설해 본다.

• 핵심 키워드 •

- 모바일, 뱅킹, 비대면, 상시처리, 자동화, 효율성, 보안



학습을 위한 사전준비

- ▶ 온라인으로 돈을 송금할 수 있는 다양한 방법을 찾아본다.
- ▶ 어떤 산업에서 온라인뱅킹을 주로 사용할 것인지 생각해본다.
- ▶ 미성년자가 은행 계좌를 만들 수 있는 방법을 알아본다.
- ▶ 온라인뱅킹에서 계정을 보호하기 위한 은행의 대응 방안을 조사해본다.
- ▶ 계정을 탈취당했을 때 입을 수 있는 피해에 대해서 조사한다.



★ 온라인 뱅킹이란?

온라인 뱅킹은 인터넷이나 모바일 네트워크를 이용해 은행 업무를 처리하는 서비스를 말한다. 은행 창구에 직접 가지 않아도 계좌 조회, 송금, 이체, 자동이체 신청, 예금 관리 같은 업무를 할 수 있도록 만든 디지털 금융 서비스이다.

이 서비스의 핵심은 돈 그 자체를 화면 속에 보여 주는 것이 아니라, 계좌에 기록된 자금의 이동을 전자적으로 처리하는 것에 있다. 즉, 온라인 뱅킹은 현금을 들고 다니는 방식이 아니라, 계좌와 계좌 사이의 숫자 이동을 기술로 처리하는 방식이다. 그래서 온라인 뱅킹은 디지털 자산이라기보다 디지털 자산과 금융 거래를 다루는 통로라고 보는 것이 더 정확하다.

★ 온라인 뱅킹의 특징

온라인 뱅킹은 정보통신기술을 기반으로 은행의 전통적 기능을 원격으로 구현한 전자금융 서비스이며, 시간과 장소의 제약을 최소화하고 금융 거래의 효율성과 접근성을 극대화하는 특징을 지닌다.

1 비대면 금융 서비스

이용자는 은행 창구를 방문하지 않고도 금융 거래를 처리할 수 있다. 이는 거래 시간과 이동 비용을 절감하며, 금융 서비스의 공간적 제약을 완화한다.

2 24시간 상시 접근성

온라인 뱅킹은 영업시간에 제한되지 않고, 언제 어디서나 접속할 수 있다. 따라서 시간 제약이 큰 현대 사회에서 금융 서비스의 이용 편의성을 현저히 높일 수 있다.

3 실시간 정보 처리

계좌 잔액, 입출금 내역, 거래 상태 등을 즉시 확인할 수 있는 실시간성을 특징으로 하므로 자금 관리의 신속성과 정확성을 향상시킬 수 있다.

4 거래 자동화와 효율성

송금, 자동이체, 예약 이체, 공과금 납부 등 반복적 업무를 시스템을 통해 자동으로 처리할 수 있다. 그 결과 업무 처리 속도와 운영 효율성이 향상된다.

5 다양한 채널 연계성

온라인 뱅킹은 온라인에 접속할 수 있는 PC, 스마트폰, 태블릿 등 다양한 디지털 기기와 연동된다. 이러한 호환성 덕분에 사용자는 동일한 금융 계정을 여러 환경에서 일관되게 활용할 수 있게 된다.

6 보안 통제의 중요성

온라인 환경에서 거래가 이루어지므로 인증, 암호화, 접근 통제, 이상거래 탐지와 같은 보안 장치가 필수적이다. 동시에 피싱, 해킹, 개인정보 유출 등의 위험에도 주의해야 하는 것은 당연하다.

★ 온라인 뱅킹에 대한 위협

온라인 뱅킹은 편리하지만, 편리한 만큼 위험성도 존재한다. 현금을 직접 들고 다니는 대신 통신과 화면으로 관리하기 때문에, 보안이 약하면 계정 탈취, 피싱, 악성 앱, 인증정보 유출 같은 문제가 발생할 수 있다.



출처 : 제미니아이

하지만 위험이 있다고 해서 온라인 뱅킹을 쓰지 말아야 한다는 뜻은 아니다. 오히려 온라인 뱅킹은 현대 금융에서 매우 중요한 역할을 하기 때문에, 위험을 이해하고 안전하게 사용하는 능력이 필요하다. 금융 교육의 핵심도 바로 여기에 있다.

★ 온라인 뱅킹을 안전하게 하는 방법

온라인 뱅킹을 안전하게 사용하려면 몇 가지 기본 원칙을 지켜야 한다.

1 비밀번호와 인증수단을 강하게 설정해야 한다.

생일이나 전화번호처럼 쉽게 추측할 수 있는 비밀번호는 피해야 하고, 가능하면 2단계 인증을 사용하는 것이 좋다. 2단계 인증은 아이디/비밀번호 입력 후에도 본인임을 인증하는 다른 정보를 입력하는 것이다. 그것은 이메일 주소를 통해 발송된 링크를 클릭하는 것일 수도 있고, 본인 전화번호로 걸려온 전화에 정해진 코드번호를 입력하는 방식일 수도 있다.

2 출처가 불분명한 링크는 누르지 않아야 한다.

은행은 보통 문자로 비밀번호 입력을 요구하지 않는다. 의심스러운 메시지는 반드시 공식 앱이나 공식 홈페이지를 통해 다시 확인해야 한다.

3 공용 기기나 공용 와이파이에서는 조심해야 한다.

PC방이나 공공장소의 컴퓨터에서 서비스에 로그인한 뒤 로그아웃을 깜빡하면 큰 문제가 생길 수 있다. PC는 빠른 속도를 위해서 캐시값이라는 임시 저장 기능을 가지고 있어서 로그인 후 브라우저를 켜다만 했더라도 브라우저를 다시 켜면 그대로 로그인 상태가 유지되는 경우가 있다. 내 서비스 권한을 몽땅 타인에게 넘겨줄 수도 있다.

4 이체 내역을 자주 확인해야 한다.

온라인 뱅킹은 모든 흔적이 남는다. 작은 금액이라도 모르는 이체내역이 있다면 바로 확인하고 은행에 문의해야 한다.

5 휴대폰과 앱을 항상 최신 상태로 유지해야 한다.

PC, 스마트폰은 끊임없는 업데이트를 통해 보안의 문제점을 보완하고 있다. 보안 업데이트를 무시하면 알려진 취약점이 그대로 남을 수 있으므로 공식 업데이트는 꼭 받아서 최신의 보안 기능을 사용해야 한다.



함께 해볼까요?

• 미성년자 하나은행 계좌 만들기

1 미성년자 본인 내점시

- 학생증, 여권, 청소년증(청소년증 발급신청 확인서 포함)
- 주민등록번호 뒷자리가 없는 학생증의 경우(택1)
 - ① 학생증 + 주민등록초본
 - ② 학생증 + 본인기준 가족관계증명서(일반 또는 상세)

※ 만 14세 미만 미성년자 단독거래 불가

2 부 또는 모(친권자중 1인) 내점시

- 내점 부 또는 모의 실명확인증표
- 가족관계확인서류 : 주민등록등본 또는 가족관계증명서(가족관계 기재된 경우 限)
- 미성년자 기준 기본증명서(특정 또는 상세)
- 통장 신고 인감(서명불가)

3 기타

- 서류 유효기간 : 발급일로부터 3개월 이내(주민등록번호 전부 표시)



자기 평가하기

★ 온라인뱅킹에 대해 학습한 만큼 아래 평가표에 체크해보자.

평가 내용	매우 우수	우수	보통	부족	매우부족
▶ 온라인뱅킹은 은행 창구에 직접 가지 않아도 계좌 조회, 송금, 이체, 자동이체 신청, 예금 관리 같은 업무를 할 수 있도록 만든 디지털 금융 서비스라는 사실을 설명할 수 있다.					
▶ 온라인뱅킹을 안전하게 사용하기 위해 유의해야 할 보안규정을 숙지하고 있다.					
▶ 하나은행에 방문하여 내 계좌를 개설할 수 있다.					

★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

04

내 자산을 노리는 범죄와 보호방법

• 목 표 •

- 1 디지털 자산을 노리는 범죄의 유형을 학습한다.
- 2 디지털 자산의 피해를 입었을 때 조치방법을 학습한다.
- 3 내 자산을 지키기 위한 원칙을 숙지한다.

• 준비물 •

- 1 인터넷이 연결된 PC

• 핵심 활동 •

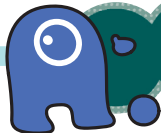
- 범죄유형을 숙지한다.
- 역할극을 통해 디지털 자산의 피해를 입었을 때 신고하는 방법을 숙지한다.
- 내 디지털 자산을 보호하기 위한 기본원칙을 완성해본다.
- 시나리오를 통한 상황별 대응방법을 익혀본다.

• 핵심 사이트 •

- 1 경찰청 사이버범죄 신고 : ecrm.police.go.kr
- 2 금융감독원 : fss.or.kr
- 3 한국인터넷진흥원 : boho.or.kr
- 4 검색 포털 : naver.com
google.com

• 핵심 키워드 •

- 디지털 자산, 피싱, 스미싱, 파밍, 계정탈취, 신고



학습을 위한 사전준비

- ▶ 주변 사람에게 스미싱, 피싱 문자 등을 받은 적이 있는지 물어본다.
- ▶ 내가 사용하는 인터넷 사이트의 아이디와 비밀번호를 동일하고 사용중인지 확인한다.
- ▶ 동일한 비밀번호로 오랫동안 사용하였다면 비밀번호를 변경해본다.



내 자산을 노리는 범죄와 보호방법

★ 디지털 자산 범죄의 종류

디지털 자산을 노리는 범죄는 여러 방식으로 이루어진다. 가장 흔한 수법은 다음과 같다.

1 피싱(Phishing)

가짜 문자, 가짜 이메일, 가짜 사이트를 이용해 비밀번호나 인증번호를 빼내는 방식이다. 해커들이 f를 ph로 변경해서 표시하던 문자가 낚시를 뜻하는 fishing에 반영되어 Phishing으로 굳어졌다.

“계정이 정지되었습니다”, “보안 점검이 필요합니다” 같은 문구로 급하게 행동하게 만들고, 사용자가 스스로 정보를 입력하게 유도한다.

2 스미싱(Smishing)

문자메세지 SMS와 fishing이 합쳐져 생성된 표현이다. 문자메시지에 악성 링크를 넣어 피해자가 누르게 만드는 방식이며 링크를 누르는 순간 가짜 로그인 화면으로 연결되거나, 악성 앱이 설치되어 연락처 또는 비밀번호나 사진자료 등 개인정보가 유출될 수 있다.

3 파밍(Pharming)

정상적인 사이트 주소를 입력해도 가짜 사이트로 연결되게 만드는 방식이다. 겉보기에는 진짜 사이트와 거의 같아서, 피해자는 정상적인 아이디와 비밀번호를 입력함으로써 계정정보를 통째로 제공하는 등 사용자가 속기 쉽다.

4 계정 탈취

비밀번호 재사용, 단순한 비밀번호, 보안 설정 미흡 등을 노려 계정을 빼앗는 방식이다. 한 번 계정을 빼앗기면 그 안에 있는 포인트, 가상자산, 결제 정보, 개인 자료까지 모두 위험해질 수 있다.

5 투자 사기

가상자산이나 디지털 자산을 이용해 “원금 보장”, “확정 수익”을 약속하는 방식이다. 실제로는 신규 투자자를 계속 끌어들이며 기존 피해자에게 수익을 지급하는 구조이거나, 아예 처음부터 자산을 빼앗는 사기일 수 있다.

이런 범죄의 핵심은 기술 자체보다도 신뢰를 가장한 속임수에 있다. 따라서 디지털 자산을 보호하려면 기술 보안뿐 아니라, 진위를 의심하고 확인하는 태도가 중요하다.



함께 해볼까요?

만약 디지털 자산 관련 피해를 입었다면, 혼자 고민하지 말고 즉시 도움을 요청해야 한다. 우리나라에는 디지털 자산 관련 피해를 입었을 때 신고할 수 있는 여러가지 루트가 존재하고 있다. 피해는 시간이 지날수록 복구가 어려워지기 때문에 빠른 대응이 중요하다. 피해사실을 기관에 신고하는 상황을 염두에 두고, 신고하는 사람과 신고받는 사람으로 역할을 나누어 옆 사람과 신고 연습을 해보자.

신고자	기관
여보세요 계정탈취 신고를 하고 싶어요	본인 확인 후에 도와드리겠습니다. 피해를 입으신 정확한 시점과 해당 플랫폼, 그리고 피해 금액이 발생했는지 말씀해 주시겠습니까?
오늘 오전 10시경 포털 사이트 계정이 탈취되었고, 연결된 카드로 게임 사이트에서 30만 원이 결제되었습니다.	계정 비밀번호를 본인이 누군가에게 알려주거나, 피싱 사이트에 입력하신 적이 있습니까? 아니면 악성 프로그램 설치가 의심되는 링크를 클릭하셨나요?
모르는 번호로 온 택배 주소지 확인 문자의 링크를 누른 적이 있는데, 그 이후에 로그인 안 되고 결제 문자가 왔습니다.	전형적인 스미싱(Smishing) 수법에 의한 계정 탈취로 보입니다. 현재 카드 승인 취소나 계정 정지 등의 긴급 조치는 취하하셨습니까?
네 카드 정지는 시켜냈습니다.	수사를 진행하기 위해 신고자께서 준비해 주셔야 할 필수 증거 자료가 있습니다. - 접속 로그 : 해당 포털 사이트 고객센터에 요청하여 '로그인 기록(IP 주소 포함)'을 캡처하거나 출력하십시오. - 결제 내역서 : 카드사나 결제 대행사에서 발행한 '결제 상세 내역서'가 필요합니다. - 유입 경로 : 클릭하셨던 문자 메시지 원본과 링크 주소가 보이도록 화면을 캡처해 두십시오. (휴대폰은 공장 초기화를 하지 말고 보관하십시오.)
자료를 준비하면 바로 범인을 잡을 수 있나요?	확보하신 자료를 지참하여 가까운 경찰서에 방문하거나 '사이버범죄 신고시스템(ECRM)'을 통해 온라인 접수를 하셔야 정식 수사가 개시됩니다. 상대방의 IP 주소를 추적하여 가해자를 특정하는 과정을 거치게 됩니다.
네, 자료 준비해서 방문하겠습니다. 추가로 주의할 점이 있을까요?	동일한 비밀번호를 사용하는 다른 사이트들도 위험하오니 모두 변경하시고, 휴대폰 내의 공인인증서나 보안카드를 폐기 후 재발급받으시길 권고드립니다.

★ 피해사실 인지 시 즉시 조치할 일



이미지 출처 : 제미나이

다양한 신고루트

- 경찰청 : 112 통합신고 / 182 민원상담**
사기, 해킹, 계정 탈취, 스미싱 등 범죄 의심 사례는 경찰청 사이버 관련 상담과 신고 창구를 통해 도움을 받을 수 있다. 특히 범죄가 명확하거나 금전 피해가 발생했다면 신속하게 신고해야 한다.
- 금융감독원 : 1332 콜센터 상담**
금융 사기, 계좌 관련 피해, 부당한 금융 거래 문제는 금융감독원 상담창구를 통해 안내를 받을 수 있다. 은행 계좌, 카드, 전자금융 관련 문제가 있으면 여기서 도움을 요청할 수 있다.
- 한국인터넷진흥원 보호나라 : 118**
한국인터넷진흥원은 해킹으로 인한 랜섬웨어, 디도스 공격, 그 밖의 해킹 대한 상담과 대응 안내를 제공한다. 의심스러운 문자나 사이트를 발견했을 때도 도움을 받을 수 있다.
<https://www.boho.or.kr/>
- 경찰청 사이버범죄 신고시스템 (ECRM)**
인터넷 사기, 사이버 명예훼손, 계정 탈취 등 일반 사이버 범죄를 신고할 수 있다.
<https://ecrm.police.go.kr/minwon/main>



함께 해볼까요?

• 내 자산을 지키기 위한 원칙

보안 프로그램, 암호화 기술, 방화벽 등 기본적인 첨단 보안 기술도 중요하지만, 디지털 자산을 지키는 가장 좋은 방법은 이용자가 기본 원칙을 꾸준히 지키는 것이다. 아래 표에서 왼쪽 주제에 대해 고민해 보고 이용자의 기본원칙을 작성해 본다.

비밀번호는?	▶ 난이도를 높게 설정하고 주기적으로 변경한다. 생일, 전화번호, 이름 조합처럼 쉽게 추측할 수 있는 비밀번호는 피해야 한다. 대문자, 소문자, 숫자, 특수문자를 섞어 사용하는 것이 좋으며, 정기적으로 변경해 주는 것이 좋다.
인증코드는?	▶ 절대 함부로 공유하지 않는다. 인증번호, 복구코드, 개인키는 자산의 열쇠와 같다. 가족이나 친구라도 쉽게 알려주면 안 된다.
첨부된 링크는?	▶ 바로 누르지 않는다. 문자나 메신저로 온 링크는 먼저 의심해야 한다. 반드시 공식 앱이나 공식 홈페이지로 다시 확인하는 습관이 필요하다.
2단계 인증은?	▶ 조금 번거롭더라도 2단계 인증과 보안 설정을 사용한다. 보안성이 강한 비밀번호만으로는 부족하다. 추가 인증을 설정하면 계정이 훨씬 안전해진다.
공공장소에서는?	▶ 공용 와이파이, 공용 컴퓨터, 출처가 불분명한 앱은 위험할 수 있으니 사용을 자제한다. 공용 와이파이, 공용 컴퓨터는 누구나 접근해서 사용할 수 있는 반면 보안에 취약하고, 공용 컴퓨터는 이용은 편하지만 나의 계정정보를 누군가 모니터링하거나 남은 흔적을 이용할 가능성이 높다. 출처가 불분명한 앱은 내가 허락하지 않은 권한을 탈취하는 기능이 포함되어 있을 수 있으므로 함부로 설치해서는 안 된다.



함께 해볼까요?

• 상황별 대응방법 선택하기

“택배가 발송되었습니다”라는 문자를 받았는데, 택배 위치를 확인하고 싶으면 클릭하라는 링크가 첨부되어 있습니다. URL을 봤더니 택배를 주문한 사이트로 보인다.

- ① 링크를 눌러 바로 확인한다.
- ② 공식 앱으로 접속해 다시 확인한다.

친한 친구가 “이 코인은 원금 보장이 되며 곧 10배 오른다”고 하며 특정 주식에 대한 투자 설명자료를 보냈다.

- ① 친구의 원금보장을 믿고 바로 입금한다
- ② 부모님과 상의한다
- ③ 해당 기업에 대한 배경지식을 조사하고 직접 판단하여 투자를 결정한다.

새벽 3시경 내 계정에서 내가 하지 않은 결제가 발견되었다.

- ① 내가 하지 않은 것이 확실하므로 그냥 둔다
- ② 비밀번호를 바꾸고 고객센터에 연락한다
- ③ 착오가 있었을지도 모르니 다음 날까지 기다린다



자기 평가하기

★ 내 자산을 노리는 범죄와 예방방법에 대해 이해한 만큼 아래 평가표에 체크해보자.

평가 내용	매우 우수	우수	보통	부족	매우부족
▶ 디지털 자산을 노리는 여러가지 범죄 방법에 대해 숙지하고 친구에게 설명할 수 있다.					
▶ 디지털 자산 관련 범죄 피해를 입었을 때, 당황하지 않고 피해를 최소화할 수 있도록 조치하는 방법을 숙지하고 있다.					
▶ 범죄 피해를 입었을 때, 피해사실에 대해 관련 기관에 신고할 수 있다.					
▶ 나의 디지털 자산을 지키기 위한 원칙을 숙지하고 있다.					

★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

금융범죄와 사이버 보안



사이버 공격 알아보기

금융범죄와 사이버 공격: 내 정보를 지키는 안전 가이드

사이버 공격은 인터넷과 디지털 기기를 이용해 개인정보나 금전을 탈취하는 악의적인 행위입니다. 범죄자들은 기술적 해킹뿐만 아니라 사람의 긴박함, 공포, 호기심과 같은 심리적 취약점을 교묘히 이용하므로 주요 유형을 파악하고 예방 수칙을 지키는 것이 중요합니다.

사이버 공격의 목적과 심리



주요 공격 유형 및 예방 수칙



교육 목표

- 사이버공격의 개념을 이해한다.
- 주요 사이버공격 유형을 구분할 수 있다.
- 실생활 속 사이버공격 사례를 분석할 수 있다.
- 사이버공격 예방 방법을 실천할 수 있다.
- 사이버공격 발생 시 대응 방법을 익힌다.

이런 활동을 해요

프로젝트 과정	기초	심화
	사이버공격 알아보기	금융범죄와 사이버 보안
활동 내용	• 사이버 공격이란? • 사이버공격의 유형과 사례 분석 • 사이버공격 예방방법 • 사이버공격 발생 시 대응방법	• 금융범죄란 무엇일까? • 금융범죄의 피해 현황 및 정부대책 • 금융범죄의 위험성 및 법적 책임 • 금융범죄 발생 시 상황별 대응방법

01

사이버공격이란?

• 목표 •

- 1 사이버공격의 개념을 이해할 수 있다.
- 2 사이버공격의 다양한 목적을 설명할 수 있다.
- 3 사람들이 왜 쉽게 속는지 이유를 파악할 수 있다.

• 준비물 •

- 1 PPT 또는 학습자료
- 2 실제 피싱/스미싱 사례 이미지
- 3 학생 활동지 및 필기구
- 4 스마트폰 또는 태블릿(선택)
- 5 퀴즈 자료

• 핵심 활동 •

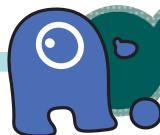
- 사람들을 왜 속이는지 이유 토론하기
- 실제 사례 보고 어떤 공격인지 맞추기
- 내가 받은 의심 문자 공유하기
- 공격자의 입장에서 목적 생각해보기
- “속지 않는 방법” 발표하기

• 핵심 사이트 •

- 1 사이버공격은 디지털 기기를 이용한 범죄
- 2 개인정보, 돈, 기기 통제 등을 노림
- 3 공격자는 사람의 심리를 이용
- 4 긴급함, 두려움, 신뢰를 이용해 속임
- 5 누구나 피해자가 될 수 있음

• 핵심 키워드 •

- 사이버공격
- 개인정보
- 피싱 / 스미싱
- 악성코드
- 랜섬웨어
- 해킹
- 심리조작



학습을 위한 사전준비

- ▶ 스마트폰 사용 경험 떠올리기
- ▶ 의심스러운 문자 받아본 경험 생각하기
- ▶ 개인정보의 종류 미리 알고 오기
- ▶ “속았던 경험” 또는 “속을 뻔한 경험” 공유 준비



사이버공격 이해하기

★ 사이버공격이란?

우리가 매일 사용하는 스마트폰, 컴퓨터, 태블릿이 범죄자들의 공격 대상이 될 수 있다는 사실을 알고 있나요? 사이버공격이란 인터넷과 디지털 기기를 이용해 개인정보를 훔치거나, 돈을 빼앗거나, 기기를 망가뜨리는 모든 악의적인 행위를 말합니다.

★ 왜 사람들을 속일까요?

- 1 돈을 빼앗기 위해
 - ① 가장 큰 이유는 금전적 이익임
 - ② 공격자는 사람을 속여서 계좌번호, 카드번호, 비밀번호, 인증번호를 알아낸 뒤 돈을 갈취
- 2 개인정보를 훔치기 위해
 - ① 개인정보는 그 자체로 큰 가치가 있어 다른 범죄에 다시 사용됨
 - ② 예를 들면 : 이름, 생년월일, 전화번호, 주소 주민번호 계정 비밀번호
- 3 컴퓨터나 휴대폰을 장악하기 위해
 - ① 악성코드를 설치해서 내 기기를 마음대로 조종하려는 목적
 - ② 예시 : 카메라 몰래 켜기, 파일 삭제, 연락처 복사, 사진 유출, 저장된 계정 탈취
 - ③ 이후 랜섬웨어로 연결되어 돈을 요구
- 4 사이트나 시스템을 마비시키기 위해
 - ① 기업, 학교, 공공기관을 공격해서 서비스를 멈춤
 - ② 예시 : 학교 홈페이지 마비, 쇼핑몰 서버 다운 게임 서버 접속 불가
 - ③ 금전 요구, 경쟁 방해, 혼란 조성 목적일 가능성
- 5 재미나 과시, 보복 목적
 - ① 일부는 돈보다 과시욕이나 보복심리로 공격
 - ② 예시 :
 - 특정인 SNS 해킹
 - 학교 친구 계정 도용
 - 악성 댓글 및 허위 게시글 작성
 - 학생들에게는 이 부분이 특히 현실적으로 와닿습니다.
 - 학생용 예시 문장
 - 친구 계정을 몰래 사용해 장난치는 것도 사이버 범죄

**아이템화 한 항목들의
통일성 향상(2의 경우
예시를 나열하였으나
5의 경우 아이템화하였음)**

내용확인바랍니다.

★ 사람들이 쉽게 속는 이유

피싱은 기술보다 사람의 심리를 이용

1 급한 상황을 만들기 때문

- ① “지금 바로 하지 않으면 계정 정지”
- ② 오늘 안에 입금해야 함” 처럼 긴급함을 유도
- ③ “믿을 만한 사람처럼 보이기 때문
- ④ 가족, 친구, 은행, 경찰처럼 익숙한 이름을 사용하면 쉽게 믿게 됨

2 불안과 두려움을 이용하기 때문

- ① 사람은 무서울 때 빨리 행동하려는 경향을 이용
- ② 예 :
 - 벌금 부과
 - 계정 정지
 - 수사 대상

3 호기심과 욕심을 자극하기 때문

- ① “당첨되었습니다”
- ② “무료 쿠폰 지급”

★ 왜 금융을 노릴까 - 공격자의 목적 이해하기

1 인터넷의 익명성 : 범죄자가 신분을 숨기기 쉬운 환경

- ① 물리적인 신원 증명 없이도 활동이 가능한 공간
- ② 이러한 특성을 악용하여, 현실의 자신과 디지털상의 행위를 분리
- ③ 겹겹의 암호화 네트워크(예 : Tor 브라우저, 다크웹 등)를 사용하여 자신의 실제 IP 주소와 위치를 숨긴 채 범죄를 모의하고 실행

2 해외 서버 사용 (수사 지연 및 단절)

- ① 수사 관할권의 한계 악용
 - 사이버 공간에는 국경이 없지만, 수사 기관에는 국경과 관할권이 존재
 - 공격자가 A국가에 거주하면서 B국가의 서버를 해킹해 경유지로 삼고, C국가의 금융망을 타격
- ② 국제 공조의 벽
 - IP를 추적해, 해외 서버라면 해당 국가의 법적 협조 요청에 많은 시간 소요됨
 - 사법 공조가 어려운 국가의 서버를 의도적으로 선택해 추적의 끈을 완전히 끊어버림

3 가짜 번호 사용 (신뢰 악용 및 신분 세탁)

- ① 명의 도용(대포폰/유령법인) :

- 훔친 개인정보나 노숙자 등의 명의로 개통된 기기 사용
- 통화나 문자를 추적하더라도 범죄의 말단에 있는 명의 대여자만 잡힐 뿐, 진짜 설계자는 숨을 수 있음

② 발신번호 조작(스푸핑, Spoofing)

- 기술적인 조작을 통해 피해자의 스마트폰 화면에 실제 은행 대표번호나 경찰, 금융감독원 번호가 뜨게 만듦.
- 피해자를 쉽게 속임과 동시에 통신 기록의 발신지 교란

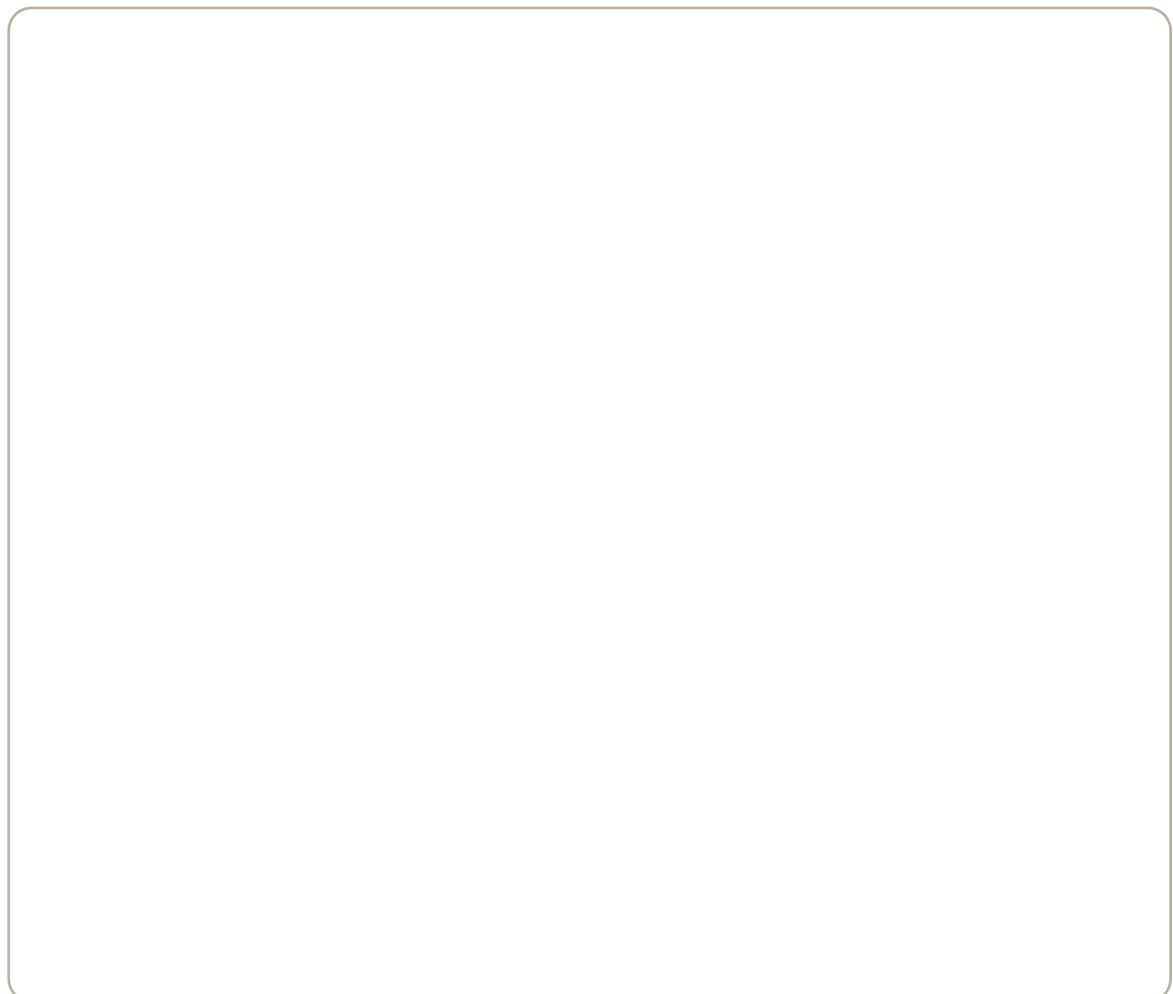
4. 가짜 사이트(피싱 사이트) 제작 (정보의 자발적 헌납 유도)

① 완벽한 위장과 기만

- 실제 금융기관의 홈페이지와 시각적으로 100% 동일한 가짜 사이트 만듦.
- 악성코드를 억지로 설치하지 않아도, 속은 피해자가 스스로 자신의 로그인 정보, 보안카드 번호 등을 입력 유도

② 치고 빠지기(Hit and Run) :

- 이 가짜 사이트들은 대체로 짧은 시간(며칠, 혹은 몇 시간) 동안만 운영됨.
- 피해자의 정보와 자금을 빼내고 나면 사이트를 즉각 폐쇄하고 서버 데이터를 삭제
- 수사 기관이 인지하고 차단 조치를 내릴 즈음엔 이미 디지털 흔적을 지우고 사라짐.





자기 평가하기

평가 내용	정답
▶ 다음 중 사이버공격의 목적이 아닌 것은 무엇일까요? ① 개인정보 탈취 ② 돈 갈취 ③ 컴퓨터 장악 ④ 친구와 우정 쌓기	④
▶ 다음 문자 메시지를 보고 어떤 심리를 이용한 것인지 골라보세요. “[긴급] 오늘 안에 인증하지 않으면 계정이 정지됩니다.” ① 호기심과 욕심 이용 ② 급한 상황과 불안감 이용 ③ 건강 정보 제공 ④ 단순 안내 메시지	②
▶ 다음 행동 중 안전한 행동은 무엇일까요? ① 은행 문자가 와서 링크를 바로 누른다. ② 친구 계정으로 장난 글을 올린다. ③ 출처가 불분명한 앱을 설치한다. ④ 의심스러운 링크는 누르지 않고 확인한다.	④

★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

02

사이버공격의 유형과 사례 분석

• 목 표 •

- 1 사이버공격의 주요 유형을 구분할 수 있다.
- 2 피싱, 스미싱, 파밍의 차이를 설명할 수 있다.
- 3 랜섬웨어와 DDos 공격의 특징을 이해할 수 있다.

• 준비물 •

- 1 필기구 (노트, 펜)
- 2 스마트폰 (문자 사례 확인 및 활동용)
- 3 활동지 (수업 중 배부)
- 4 교과서 또는 프린트 학습자료
- 5 개인 이어폰 (영상 시청 시 필요)

• 핵심 활동 •

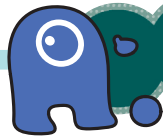
- 사람들을 왜 속이는지 다시 정리하기
- 피싱·스미싱·파밍 사례 구분하기
- 실제 문자 보고 위험 요소 찾기
- 랜섬웨어 상황 대응 방법 토론하기
- “이건 어떤 공격일까?” 퀴즈 진행

• 핵심 사이트 •

- 1 피싱은 가짜 사이트로 유도해 정보를 입력하게 함
- 2 스미싱은 문자 링크 클릭을 통해 악성코드를 설치
- 3 파밍은 사용자를 몰래 가짜 사이트로 연결
- 4 랜섬웨어는 파일을 잠그고 돈을 요구
- 5 DDos는 서버를 마비시키는 공격

• 핵심 키워드 •

- 피싱 (Phishing)
- 스미싱 (Smishing)
- 파밍 (Pharming)
- 랜섬웨어 (Ransomware)
- DDos 공격
- 악성코드
- 개인정보 탈취



학습을 위한 사전준비

- ▶ 의심스러운 문자 경험 떠올리기
- ▶ 인터넷 쇼핑 또는 로그인 경험 생각하기
- ▶ 파일 다운로드 경험 돌아보기
- ▶ “링크 클릭 전 확인해야 할 것” 생각해오기



사이버공격의 유형과 사례 분석

★ 사이버공격의 유형

피싱/스미싱/파밍, 랜섬웨어, DDos

★ 피싱

‘개인정보(Pprivate data)와 낚는다(Fishing)’의 합성어로, 전화·문자·메신저·가짜사이트 등 전기통신수단을 이용하여 피해자를 기망·공갈함으로써 이용자의 개인정보나 금융정보를 빼낸 후 금품을 갈취하는 사기 수법

1 방식 :

범죄자가 공식 기관(은행, 정부, 포털사이트)인척 위장 ▶ 이메일, 전화 등을 통해 가짜 사이트나 이메일로 유도 ▶ 아이디, 비밀번호, 개인정보를 직접 정보를 입력하게 만들어 금융정보 탈취 ▶ 범인 계좌로 이체

2 예방법 :

① OTP(일회성 비밀번호생성기),보안토큰(비밀정보 복사방지) 사용

② ‘출처불명’또는 금융기관 주소와 다른 주소’로 발송된 이메일 즉시 삭제

※ 이메일 첨부파일에 확장자가‘exe,bat, scr 등 압축파일’이면 열람 금지

3 행안부 보이스피싱 예방 영상

https://www.youtube.com/watch?v=jFdG0_b-BHc

4 종류

구분	내용
보이스피싱	유선전화 발신번호를 수사기관 등으로 조작하여 해당기관을 사칭하면서 금품을 편취하거나 자녀납치, 사고빙자 등 이용자 환경의 약점을 노려 금품을 편취하는 수법
스미싱	문자메시지(SMS)와 피싱(Phishing)의 합성어로, ① ‘무료 쿠폰 제공’, ‘돌잔치 초대장’, ‘모바일 청첩장’ 등의 내용으로 하는 문자메시지(SMS) 내 인터넷 주소(링크) 클릭하게 하여 → ② 악성코드가 스마트폰에 설치 → ③ 피해자가 모르는 사이에 소액결제 피해 발생 또는 개인·금융 정보를 탈취당하는 범죄
파밍	사용자의 PC에 악성코드를 감염시켜 위장한 가짜 사이트로 연결되도록 하여 주민등록번호, 계좌번호, 신용카드 등의 정보를 입력하도록 유도하여 탈취하는 범죄
메신저피싱	SNS, 모바일(또는 PC) 기반 메신저 등 신규인터넷 서비스의 친구추가 기능을 악용하여 친구나 지인의 계정으로 접속한 후 금전 차용 등을 요구하는 수법

식 통일
화 사용 여부)

피싱사이트	불특정 다수에게 문자, 이메일 등을 보내 정상 홈페이지와 유사한 가짜 홈페이지로 접속을 유도하여 개인정보 및 금융정보를 편취하는 수법
몸캠피싱	스카이프 등 스마트폰 채팅 어플을 통해 음란 화상 채팅(몸캠피싱)을 하자고 접근하여 상대방의 음란한 행위를 녹화한 후 피해자의 스마트폰에 악성코드를 심어 피해자 지인의 연락처를 탈취한 다음 지인들에게 녹화해둔 영상(사진)을 유포하겠다고 협박하여 금전을 갈취하는 범죄 수법
스피어 피싱	고위 공직자, 유명인 등 특정 개인 및 회사를 대상으로 개인정보를 캐내거나 특정 정보 탈취 목적으로 하는 피싱 공격하는 수법
큐싱	출처가 불분명한 'QR코드'를 스마트폰으로 찍을 경우, 악성 앱을 내려 받도록 유도하거나 악성프로그램을 설치하게 하는 금융사기 수법 - QR코드 + phishing의 합성어로, 스미싱에서 한 단계 더 진화된 신종 금융사기 수법
로맨스스캠	SNS 및 이메일 등 온라인상으로 접근하여 호감을 표시한 뒤 재력, 외모 등으로 신뢰를 형성한 후 각종 이유로 금전을 요구하는 방법의 사기

출처 : 경찰청 사이버수사국, 전기통신금융사기 통합대응단



함께 해볼까요?

내용수정
목과 형식이 통일되지
며, 정의가 마지막에
명도한 예시가 혼용되
명확하지 않음

1. 마시지업소 보이스피싱편

피싱범

피해 보실 만한 일이 좀 생겨서 연락을 드렸어요.

피해자

피해를 봤다고요?

피싱범

네, 좀 간단하게 좀 말씀드릴게요. ㅇㅇ 씨.

피해자

네.

피싱범

그때당시에 저희가 장사가 너무만들어서 일에는 실장들 시켜서 밤마다 카메라를 설치해 놓고 영상을 좀 촬영했고요. 그 영상을 정리하던 중에 김OO 씨 영상이 나와서 지금 연락한 통드리게 된 거고, 저희가 흥산소를 같이 운영하다 보니까 김OO 씨 뭐 OO년 O월 O일인 것부터 해서 본인 가족, 지인들 연락처를 한 40개 정도 확보한 상태에서 연락 한 통 드렸고요.

피해자

네.

피싱범

김OO 씨 지금 사채 파악이 전혀 안 되시는 것 같은데 내가 지금부터 사채 파악이 되게끔 단톡방 하나 만들어서 가족, 지인들 한 스무 명 초대해 놓고 본인 영상 돌려서 지지분하게 얘기할까요? 아니면 나랑 함께 한 번 얘기해 보실래요?

피해자

뭐 일단 확인부터 좀 해볼게요.

피해자

장난 같아요?

피싱범

장난 아니죠.

지금 단톡방 하나 만들 테니까 거기서 확인하시고...

2. 대출병자 보이스피싱편

피싱범

고객님, 지금 휴대폰에 은행 어플 이용하시는 거 있으시죠?

피해자

네.

피싱범

네, 그 은행 어플 안에 고객님의 금융인증서나 공동인증서 있으시잖아요.

피해자

네.

피싱범

요즘 워낙에 인증서 해킹을 통한 스미싱, 보이스피싱 범죄가 빈번하게 일어나서 지금 현재 저희 쪽 보안프로그램 작동하게 되면서 고객님의 인증서 보호를 위해 은행 어플 같은 게 잠시 차단 처리가 되실 거예요.

피해자

네.

피싱범

차단이 되셨다고 해서 고객님의께서 다시 설치하셔서 이용하시는 게 아니시고요. 전자서명 하시면 자동으로 전산 복구처리 되시기 때문에 불편하시더라도 서명하시기 전까지만 은행권 어플 이용은 안 되시고요. 서명하시고 나서는 은행권 어플 전산 풀어드릴 거고, 고객님의 대출금 들어온 거 확인해보셔야 되시잖아요. 그 다음에 은행권 어플 이용은 가능하세요. 그러시고 지금 신청서 작성해주신 거 결제부로 이관처리 도움 드릴 거고, 한 시간 안쪽으로 저희 대표번호로 연락 들어가실 거예요. 최종 승인전와 들어가시는 건데, 고객님의께서 대출 신청한 게 맞는지, 뭐 결제일은 며칠로 지정을 할 건지 등등 몇 가지 여쭙보실 건데, 그때 말씀만 잘 해주시면 되시고요.

3. 검찰 수사관 보이스피싱편

피싱범: 000 씨 맞습니까?

피해자: 아, 네, 맞아요.

피싱범: 네, 수고하십니다. 서울중앙지검 장다해 수사관입니다. 잠시 통화 괜찮으십니까?

피해자: 네.

피싱범: 개인정보 유출 사건 관련해서 몇 가지 확인 연락을 드린 거고요. 부산 출신인 김수영 씨라고 아시는 지인분은 맞습니까? 저희 측에서 얼마 전에 김수영 씨 중심으로 한 금융범죄사기단을 감가한 현장에서 지금 000 씨 명의로 되어있는 농협은행과 우리은행 통장이 발견이 되었고요. 본인 명의의 통장이 발견이 되었다고 해서 본인을 무조건 가짜자로 보는 건 아닙니다. 다만 아직까지 피해자라고 입증 가능한 증거가 없기 때문에 현재 지금 피해자 입증 조사를 해주셔야 되시는 부분이고요. 이 부분은 3차 목소리, 잡음 소리 들려면 증거불충분 법원 측에서 채택 자체가 불가능하신데, 혹시 메모지랑 불변 증거시키고요. 잠시만 조용한 공간으로 이동 좀 가능하시겠습니까?

피해자: 아... 지금 당장은...

피싱범: 조사자분 측에서 통화가 어렵다라고 했을 경우 저희 측에서 소환장 보내드릴 테니깐요. 본장을 방문해서 소환조사를 받으시면 되십니다.

피해자: 혹시 언제 방문해야 하나요?

피싱범: 빠른사건 급요임 안쪽으로도 무조건 방문을 해야 되는 부분입니다. 날짜는 서류상에 기재가 되어 있으시고요. 검찰청에서 조사받는 것 때문에 잠깐 통화를 해야 된다면 이렇게 얘기하면 아무래도 직장 내 사신이라는 게 좋지 않은 압을 겁니다. 잠만 뒤 친구하고 통화를 하고 온다는 건지 이 부분은 유도로 있기 대처하시고요. 이거 신속하게 진술만 해주셔야 하는 부분입니다.

4. 납치범자 보이스피싱편

피싱범: ㅇㅇ이 엄마죠?

피해자: 네? 네, 네.

피싱범: 받아봐, (아이 목소리) 엄마...

피해자: 왜?

피싱범: (아이 목소리) 빨리와...

피해자: 뭐?

피싱범: (아이 목소리) 이 사람이 때렸어.

피해자: 어? 누가?

피싱범: (아이 목소리) 술 취한 사람이.

피해자: 어디? 어디에 너?

피싱범: (아이 목소리) 골목에...

피해자: 너 어디, 어디 골목인데?

피싱범: OO아, 뭐봐, 울지 말라고, 아.

피해자: 누구세요? 아, 아니 저희 딸... 저희 딸한테 왜 그러세요!

피싱범: 아, 내가 말하는 거 듣고, 너는 말을 하지 마.

피해자: 네.

피해자: 네, 뭐 해주면 되는데요?

피싱범: 네 계좌에 100만 원, 100만 원, 200만 원만 넣어줘, 농협 불러줄게요. 지금 바로 입력하세요, 농협...

피해자: 아니, 저희 딸을 어디 데리고...

피싱범: 아, 네 딸을 위한 네 마지막 살릴 기회인데!

피해자: 계좌번호 알려주세요.

피싱범: 그러면 100만 원 지금 이체하세요. 20초 내로 안 보내면 전화 끊겠다. 이제 완료했나?

피해자: 네.

피싱범: 지금 잔액 얼마 남았나?

피해자: 제가 월급날 다시 드릴게요. 저희 딸만 보내주세요.

피싱범: 실려준다 했잖아. 그래서 너는 엄청 고마운 거야. 그래서 조금 전에 돈 보낸 것 사진 달라고. 지금 잔액이 70만 원인데 왜 거짓말했을까? 사람은 거짓말을 하면 안 돼. 내가 계좌번호 다른 거 불러줄 테니까 여기에 70 넣으세요.

피해자: 다시 통째로 다 보낼게요. 저희 딸 어디 있는대요?

피싱범: 그거 송금하고 나서 아 진짜 골짜기? 아송아. 지금 남편한테 전화해서 '이래서 돈을 보내는데 신고하지 말자.' 하고 남편 보고 내 번호로 전화하라 해. 지금 바로.

5. 카드배송원 보이스피싱편

피싱범
여보세요? 아 예, 카드배송 기사인데요. 000 씨 맞으세요?

피해자
네.

피싱범
아이거 00카드 배송하려고 하는데 지금 자택에 계시나요?

피해자
아 지금 2-3분이면 도착해요.

피싱범
아, 다섯 시 전에 들어갈 거예요. 지금은 아니고요.

피해자
아니 00에서 무슨 카드요?

피싱범
000 씨 아니세요?

피해자
아, 맞아요. 제가 뭘 신청했나?

피싱범
근데 설명 안 하셨어요?

피해자
네.

피싱범
신청을 안 하셨는데 카드가 나올 일이 없는데 잠시만요. 카드 우편물을 보면 받는 분 000 씨. 58년생 0월 0일 전화번호로, 정보가 다 맞다고요?

피해자
네, 맞아요.

피싱범
그럼 제가 지금 배송자점 들어가기 전에 확인 전화 드린 건데 주소, 자택 주소가 서울 마포구 도화동...

피해자
아니 서울이 아니고 여기 청주예요.

피싱범
청주시라고요?

피해자
네.

피싱범
어 이거 그럼 신청하신 것도 아니고, 본사랑 통화할 도 안 하셨잖아요. 주소도 틀리고 하니까 00카드사에 전화하셔서 취소 접수를 한 번 해주시겠어요? 제가 반송 처리하게.

피해자
에, 알겠습니다.

피싱범
아 이왕이면 사고예방팀이라고 있거든요. 거기로 찾아서 전화를 한 번 해보세요.

피해자
사고예방팀

피싱범
주소도 틀리고 그래니까...

피해자
주소가 왜 서울로 돼 있어요?

피싱범
그거는 제가, 전 배송기사라... 잠시만요. 이 우편물에 보면 00카드 사고예방팀 전화번호 있는데 불러드릴게요.

피해자
에, 불러주세요.

피싱범
예, 1800-0000이요. 이게 제발급인지 아예 뭣지 주소도 틀리다고 한 번 얘기를 해보시고. 그럼 저는 전화가 오면 반송 처리하든가 아니면 이거 주소 변경하면 그거 해드릴게요.

피해자
네, 알겠습니다.

6. 검사 사칭 보이스피싱편

피싱범
네, 저는 아석규 사무관이에요. 제가 피해자 입증 절차를 위해서 담당 검사님께 연결 해드릴 거예요 지금. 검사님 연결되시면 본인 사건 번호랑 성함 말씀하시면 됩니다.

피해자
네.

피싱범
네, 전화 연결됐습니다. 저는 이번 7404 보안 건 3팀 팀장을 맡고 있는 김진아 검사라고 합니다. 네, 일단 000 씨가 조사 받으시면서 유의하셔야 될 점들이 두 가지가 있기 때문에 말씀을 좀 드릴 겁니다. 첫 번째로는 수사 중에 전화가 5분 이상 끊어질 경우 가해자 혐의를 은닉하는 시간으로 판단하고 자동 영장 집행되실 겁니다. 두 번째로는 본 사건은 증거되지 않은 공범들이 있기 때문에 비공개 수사 중입니다. 본 사건에 대해서 제3자에게 발설 시에는 000 씨 혐의와는 무관하게 비밀누설죄와 위계에 의한 공무집행방해죄로 가설 수 있고요.

피해자
네, 네.

피싱범
현재 공문을 심물로 받아본 게 아니라고 전달을 받았는데요. 어떻게 받아보신 건가요?

피해자
그, 앞전에 통화하던 분이 그 인터넷에 검색하라고 한 숫자 검색하고 제 이름이랑 주민번호를 치니까 이제 사건 조회에 나와 가지고 통화하고 있어요.

피싱범
조사방법부터 설명을 드리고 진행을 도와드릴 건데요. 일단 구속 수사와 압식 수사 두 가지가 있습니다. 구속 수사는 본인이 할 일이 없어요. 14일에서 최대 20일 동안 서울 구치소에서 수감되셔서 조사 받으시면 됩니다. 이어서 압식 조사 설명을 드릴게요. 지금처럼 유선상으로 비대면으로 수사를 진행하는 건데, 단면하게 생각하시면 안 됩니다.

피해자
네.

피싱범
협조가 잘 이루어지지 않고, 제3자 유료가 우려될 시에는 저희 판단 하에 언제든지 압식 조사 철회하고 구속 수사 전환시킬 겁니다.

피해자
네.

피싱범
어떤 수사로 진행하실 건지 지금 말씀하시면 돼요.

피해자
그러면 구조상 직장을 다녀야 해서 압식으로 해야 될 것 같아요.

피싱범
예, 답변 받았고요. 저희 검찰은 피해자 입증 절차를 대비해서 조사만 할 뿐이고, 000 씨 피해사 입증은 실질적으로 금융감독원에서 이루어질 겁니다. 따라서 금융감독원으로 직접 방문을 하실 건데, 지금 연락처 반차 사용하러 가셔서 나오시면 제가 마저 공문서 설명드리고 그 다음에 이동을 할 거예요.

피해자
아, 지금 일정 나와야 되나요?

피싱범
네, 맞습니다. 본인이 공함을 열람하신 후부터 사건에 대해서 인지 다 하셨잖아요.

피해자
네.

피싱범
본인 앞으로 집행명령 시간이 발부가 되어 있기 때문에 그 시간 안에 방문이 안 되시면 본인 체포영장 떨어요.

☆ 스미싱

SMS+Fising의 합성어로 문자를 이용한 금융사기입니다.

1 방식

- ① '무료쿠폰 제공', '돌잔치 초대장', '모바일 청첩장' 등을 내용으로 하는 문자메시지 내 인터넷주소 클릭
- ② 악성코드가 스마트폰에 설치되어
- ③ 피해자가 모르는 사이에 소액결제 피해 발생 또는 개인·금융정보 탈취

2 예방법

- ① 출처가 확인되지 않은 문자메시지의 인터넷주소를 클릭 금지
- ② 미확인 앱이 함부로 설치되지 않도록 스마트폰의 보안설정 강화
- ③ 직접 통화하여 확인하거나 통화가 안된다면 당사자에게 질문하기

3 참고사이트

- ① <https://www.fss.or.kr/edu/fec/contMng/view.do?menuNo=300017&contentsSln=9&check=1> (금융감독원 e-금융교육센터)
- ② <https://www.boho.or.kr/kr/bbs/view.do?searchCnd=&bbsId=B0000030&searchWrd=&menuNo=205027&pageIndex=1&categoryCode=&nttId=71280>

4 사례

① 지인사칭

범죄자가 가족, 친구, 자녀, 직장 동료인 척 연락하는 방식입니다.

- “엄마, 휴대폰이 고장 나서 번호 바꿨어. 급하게 돈 좀 보내줘.”
- 메신저에서 친구 프로필 사진을 도용해 “급하게 결제 좀 대신해줘”
- “인증번호 좀 알려줘”
- 건강보험공단 사칭 '[건강보험공단]건강검진 통보내역 정상발송. 내용보기 <http://xx.xxx.xx>'

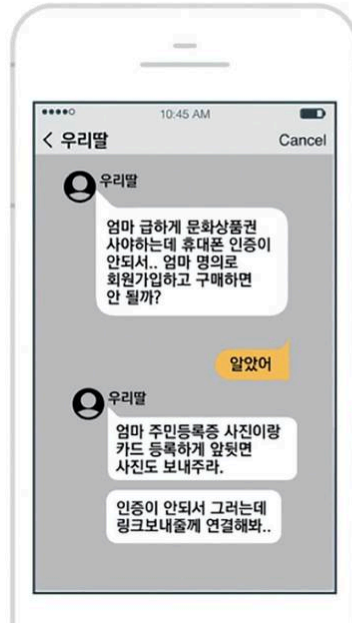
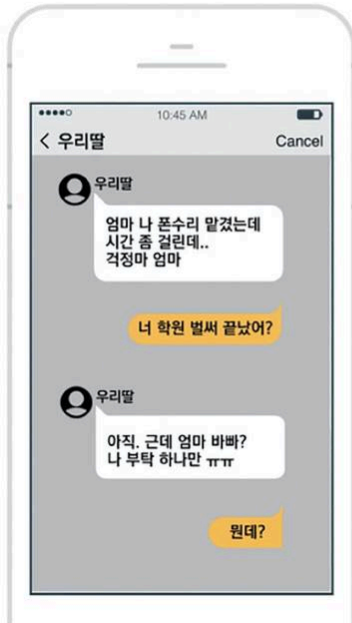
② 기관사칭

은행, 경찰, 검찰, 카드사, 택배회사 등을 사칭하여, 기관 로고와 이름을 똑같이 사용해서 진짜처럼 보이게 함

- “고유가 피해지원금 신청 안내”
- “국세청 환급금 신청”
- “은행 보안 점검”
- “교통법규 위반 과태로 미납안내”
- '[oo택배]물품배송불가(도로명불일치) 배송 주소를 수정해주세요. <http://xx...>'
- 지인 부고 사칭 '아버지께서 오늘 별세하셨기에 삼가 알려 드립니다. 장례식장 주소 <http://xx...>'

1

휴대폰 고장 핑계 유형

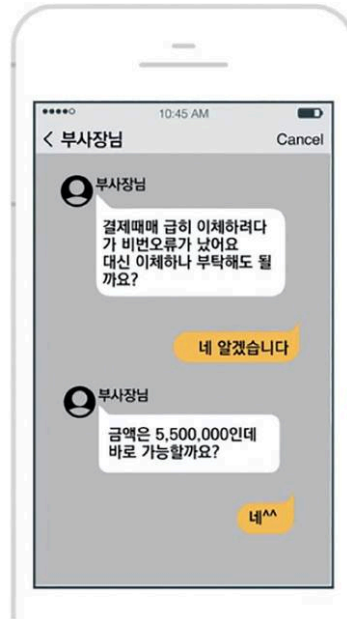


2

호칭이 쉬운 상대에게 접근 유형



3 인증오류 핑계로 송금요구 유형



인증오류 이유로
송금요청에
주의하세요!!

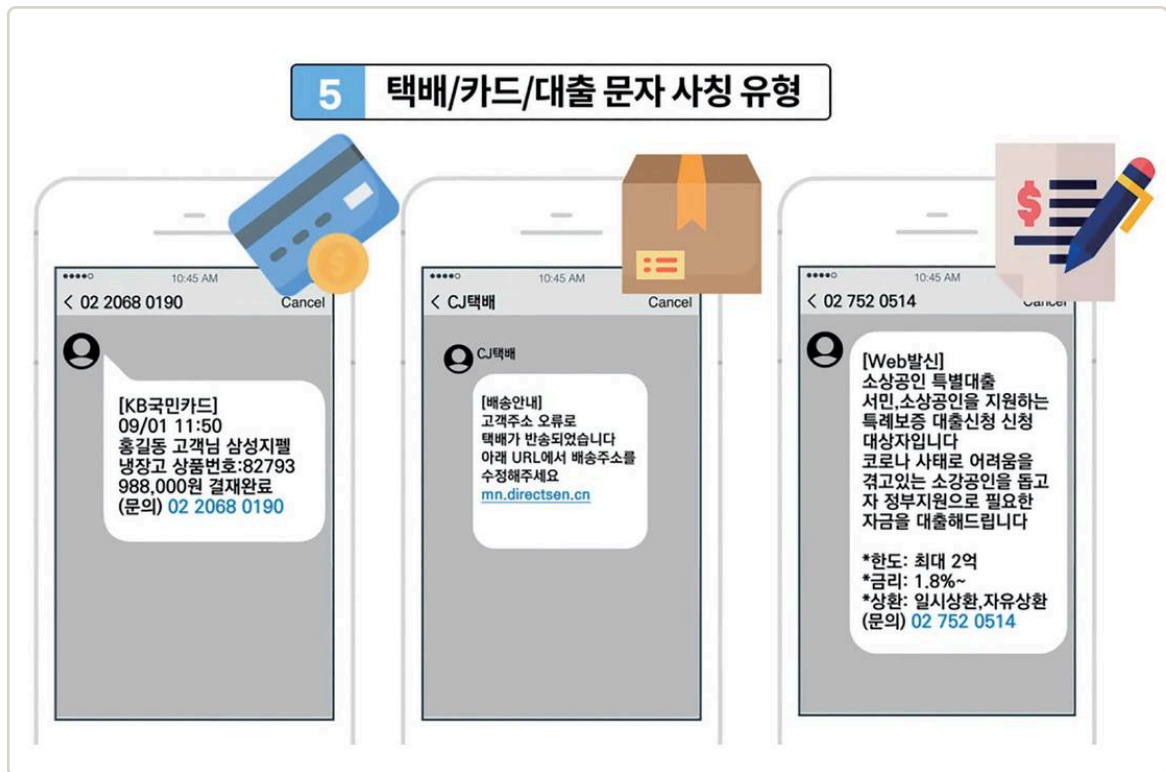


4 대리로 상품권 구매유도 유형



갑자기 상품권을
대신 사달라는
문자나 메세지 주의!!





★ 파밍

가짜 사이트로 몰래 유도해서 개인정보를 빼내는 사이버 범죄로 진짜 사이트와 거의 똑같이 구분이 아주 어려움

1 방식

- ① 사용자PC가 악성코드에 감염됨
- ② 정상 홈페이지에 접속하여도 피싱(가짜)사이트로 유도
- ③ 금융정보 탈취
- ④ 범행계좌로 이체 등 정상 홈페이지로 가장하여 금융정보(보안카드번호 전부) 입력을 요구, 신종금융사기의 주요 범행수단

2 예방법

- ① 컴퓨터·이메일 등에 공인인증서, 보안카드 사진, 비밀번호 저장 금지
- ② OTP(일회성 비밀번호생성기),보안토큰(비밀정보 복사방지) 사용
- ③ 불분명한 경로로 전송된 이메일 열지 않기

3 사례

- ① 인터넷에서 옷을 구매하여 결제방식을 계좌이체를 선택하였으나 가짜 은행사이트로 이동됨
- ② 참고사이트 : https://www.easylaw.go.kr/CSP/CnpClsMain.laf?popMenu=ov&csmSeq=1592&ccfNo=2&cciNo=3&cnpClsNo=1&search_put=

실제 피해 사례

금융감독원 e-민원센터 사칭 피싱 사기 피해 과정

피해금액
4,578만 원

STEP 1

스미싱 문자 수신 및 전화 유도

불안감 조성으로 피해자의 신뢰 획득

수신 문자

"카메라 구입 398,000원
지불"이라는 문자 수신



업체 전화

C씨가 업체에 전화하여
구매 사실 없음을 항의



통화 종료

"결제 취소해 드리겠
다"며 전화를 끊음

* 사기범이 먼저 피해자의 신뢰를 얻고 불안감을 심어주는 단계입니다.

STEP 2

사이버경찰청 사칭 및 금융정보 탈취

위조 사이트로 유도 후 개인정보 입력 요구

사기 전화 내용 (사이버경찰청 팀장 사칭)

"C씨가 금융사기 피해를 당한 사실이 확인되었으니, 통장 안전조치를 위해 금융감독원 e-민원센터 홈페이지에 접속하여 아래 정보를 입력하세요."

요구한 정보 (위조 피싱 사이트에 입력 유도)

주민등록번호

카드번호

통장번호

비밀번호

공인인증번호

* 실제 금융감독원 사이트를 그대로 위조한 피싱 사이트입니다. 공공기관은 절대 이런 정보를 요구하지 않습니다.

STEP 3

탈취한 정보로 계좌이체 실행

피해자 모르게 즉시 이체, 회수 불가

피해자
C씨 계좌
잔액 감소

4,578만 원

→
무단 이체

사기범
사기범 계좌
즉시 인출

* 사기범은 탈취한 인증정보로 본인인증 절차를 우회하여 피해자가 인지하기 전에 이체를 완료했습니다.

예방 핵심

경찰청·금융감독원 등 공공기관은 전화나 문자로 금융정보를 절대 요구하지 않습니다.

의심스러운 연락을 받으면 즉시 끊고, 해당 기관의 공식 번호(금융감독원 1332)로 직접 확인하세요.

출처 : 금융감독원 보이스피싱 피해 사례

★ 랜섬웨어

몸값(Ransom)과 소프트웨어(Software)의 합성어로, 피해자의 컴퓨터나 휴대폰의 사진, 문서, 파일을 잠가서 열지 못하게 만든 뒤 돈을 요구하는 악성 프로그램.

1 방식

수상한 문자의 링크나 이메일 첨부파일을 클릭, 불법프로그램 다운로드, 가짜 업데이트 설치 등을 하면 잠김

2 조심할 파일형태

exe, apk, zip, 알수 없는 pdf/문서파일

3 예방법

중요파일 정기적 백업, 백신프로그램 항상 최신 유지, OS·소프트웨어 업데이트

4 랜섬웨어인 경우



STEP 1 · 즉시 실행

네트워크 연결 완전 차단

Wi-Fi를 즉시 끄고, 랜 케이블을 물리적으로 분리하세요. 추가 확산을 막는 가장 중요한 첫 번째 조치입니다. 유선·무선 모두 차단해야 합니다.

추가 확산 방지 최우선



STEP 2 · 즉시 실행

외장 저장장치 즉시 분리

USB 드라이브, 외장하드, SD 카드 등 연결된 모든 외부 저장매체를 즉시 분리하세요. 랜섬웨어는 연결된 드라이브에도 암호화를 시도합니다.

USB · 외장하드 · SD카드 전부



STEP 3 · 절대 금지

감염 PC 재부팅 금지

재부팅 시 랜섬웨어가 부팅 과정을 가로채 추가 암호화를 진행할 수 있습니다. 전원을 끄거나 재시작하지 말고 현재 상태를 유지하세요.

절전·종료·재시작 모두 금지



STEP 4 · 분석

랜섬웨어 종류 파악

화면에 표시된 확장자(.locked, .encrypted 등)나 랜섬 메시지를 사진으로 찍어두세요. 다른 기기에서 ID Ransomware 사이트(idransomware.malwarehunterteam.com)에 접속해 종류를 확인하세요.

다른 기기로 조회



STEP 5 · 복호화 시도

No More Ransom 무료 복호화 도구 활용

nomoreransom.org에서 랜섬웨어 종류에 맞는 무료 복호화 툴을 검색하세요. 유로폴·인터폴·보안 기업이 협력해 운영하는 공식 프로젝트입니다. 몸값 지불보다 먼저 시도해야 합니다.

nomoreransom.org 무료 제공



STEP 6 · 최후 수단

포맷 후 백업에서 복원

복호화 툴이 없거나 효과가 없을 때, 감염된 드라이브를 완전 포맷한 뒤 사전에 만들어둔 백업에서 데이터를 복원합니다. 복원 전 반드시 악성코드가 완전히 제거되었는지 확인하세요.

오프라인 백업이 생명줄

5 백업전략

3-2-1 백업 규칙 + 실천 수칙

백업이 있으면 랜섬웨어는 협박 수단을 잃습니다.

3

원본 포함 총 3개 사본

원본 데이터 1개 + 백업 사본 2개를 항상 유지합니다.

2

2가지 서로 다른 매체

외장하드, NAS, USB 등 서로 다른 종류의 저장매체에 보관합니다.

1

1개는 반드시 오프사이트

클라우드나 원격지에 1개를 별도 보관해 물리적 재해에 대비합니다.



수칙 1 · 물리적 격리

외장하드는 평소에 분리 보관

백업 완료 후 외장하드를 PC에서 분리해 보관하세요. 상시 연결 시 랜섬웨어가 외장하드까지 암호화합니다. 백업할 때만 연결하고 즉시 분리하는 습관이 중요합니다.

백업 후 즉시 분리



수칙 2 · 클라우드 버전 히스토리

클라우드 이전 버전 복원 기능 활성화

구글 드라이브, OneDrive, 네이버 MYBOX 등에서 버전 기록 기능을 켜주세요. 랜섬웨어가 파일을 암호화해도 감염 이전 버전으로 되돌릴 수 있습니다.

[구글 드라이브](#)

[OneDrive](#)

[네이버 MYBOX](#)



수칙 3 · 복원 테스트

백업 복원 테스트 분기별 1회 실시

백업이 있어도 실제로 복원이 되는지 확인하지 않으면 의미가 없습니다. 3개월마다 한 번, 백업 파일을 실제로 복원해 보는 테스트로 백업의 신뢰성을 검증하세요.

3개월마다 · 실제 복원 확인

6 사례

- ① 가족사진
- ② 학교 과제파일
- ③ 회사문서
- ④ 엑셀 거래명세서 등을 암호화해서 열리지 않게 만들고 '피해복구 비용 청구'로 협박



랜섬노트 내용 (화면 전체에 표시)

"귀사의 모든 파일이 암호화되었습니다. 72시간 내에 비트코인 3 BTC를 아래 지갑 주소로 송금하지 않으면 복호화 키를 영구 삭제하고 탈취한 데이터를 외부에 공개합니다."

72시간

지불 기한

3 BTC

요구 금액

2중

협박

데이터 공개 위협

전면

마비

업무 중단

* 몸값을 지불해도 복호화 키를 제공하지 않는 경우가 많습니다. 전문기관에 즉시 신고하는 것이 우선입니다.

예방 및 대응 핵심

- ✓ 출처 불명 이메일의 첨부파일·링크는 절대 클릭하지 않습니다.
- ✓ 중요 데이터는 인터넷과 분리된 오프라인 백업을 주기적으로 수행합니다.
- ✓ OS·보안 소프트웨어를 항상 최신 버전으로 유지합니다.
- ✓ 감염 즉시 네트워크를 차단하고 한국인터넷진흥원(KISA 118)에 신고합니다.
- ✓ 몸값 지불은 복구를 보장하지 않으며 추가 공격 대상이 될 수 있습니다.

출처 : 한국인터넷진흥원(KISA) 랜섬웨어 피해 사례 / KISA 침해사고 신고 118

★ DDoS

해커가 악성코드로 여러 컴퓨터(зом비 PC)를 감염시켜 특정 사이트(예: 쇼핑몰, 은행)에 공격 명령을 내리면 수천~수만 대가 동시에 접속하여 서버가 버티지 못하고 느려지거나 다운됨

실제 피해 사례

зом비 PC를 이용한 대규모 DDoS 공격

및 온라인 서비스 마비 피해

서비스 중단

수십 시간

매출 손실 발생

STEP 1 **зом비 PC 확보 및 공격 인프라 구성**

악성코드 배포로 대규모 봇넷 구성

악성코드 유포

불법 SW·토렌트 파일에 악성코드를 숨겨 PC에 몰래 설치

→

봇넷 형성

감염된 수만 대의 PC가 해커 명령서버(C2)에 연결, 원격 제어 가능한 зом비 PC로 전환

→

공격 준비

해커가 명령서버를 통해 공격 대상·시각·트래픽 규모를 일괄 설정 완료

* зом비 PC 소유자는 본인 PC가 공격에 악용되고 있다는 사실을 인지하지 못합니다.

STEP 2**대규모 트래픽 폭주 및 서비스 마비**

정상 처리 용량을 초과하는 트래픽으로 서버 다운

공격 상황 (쇼핑몰 F사 사례)

수만 대의 좀비 PC가 동시에 F사 웹서버에 접속 요청을 쏟아냄. 평소 대비 수백 배에 달하는 트래픽이 몰리며 서버 응답 불가 상태 진입. 정상 이용자의 접속이 완전히 차단됨.

주요 공격 유형

- UDP 플러드 — 대역폭 고갈
- HTTP 플러드 — 웹 요청 폭주
- SYN 플러드 — 서버 자원 소진
- DNS 중독 — 대량 응답 유발

피해 현상

- 웹사이트 및 앱 접속 전면 불가
- 서버 CPU·메모리 100% 점유
- 내부 직원 업무 시스템도 마비
- 고객 불만 폭주 및 신뢰도 하락

평소 대비 수백 배 트래픽

다수 국가 IP 혼용

IP 차단 무력화

* 공격 트래픽이 전 세계 수만 개 IP에서 분산 발생하여 단순 IP 차단으로는 방어가 불가능합니다.

STEP 3**협박 및 금전 요구, 피해 지속**

공격 중단 조건으로 암호화폐 갈취

해커 협박 메시지

"지금 당장 공격을 멈출 수 있습니다. 24시간 내에 비트코인 2 BTC를 송금하면 공격을 중단하겠습니다. 미지불 시 공격 강도를 높이고 기간을 연장합니다."

수입 시간

서비스 중단 시간

수익 원

매출·복구 비용 손실

브랜드 신뢰도

고객 이탈 및 하락

법적 책임

개인정보 유출 시
과태료

* 몸값을 지불해도 공격이 재개되는 경우가 많습니다. 전문 보안업체 및 KISA에 즉시 신고하고 대응하는 것이 우선입니다.

예방 및 대응 핵심

- ✓ DDoS 대응 전문 서비스(CDN, 클라우드 스크러빙)를 평시에 미리 도입합니다.
- ✓ 공격 탐지 시 즉시 ISP(인터넷 서비스 제공업체)에 트래픽 차단을 요청합니다.
- ✓ 서버 용량·대역폭을 여유 있게 유지하고 임계치 초과 알림을 설정합니다.
- ✓ 불법 소프트웨어 사용을 금지하여 좀비 PC가 되지 않도록 예방합니다.
- ✓ 공격 발생 즉시 한국인터넷진흥원(KISA 118)에 신고하고 대응 지원을 받습니다.

출처 : 한국인터넷진흥원(KISA) DDoS 피해 사례 / KISA 침해사고 신고 118



함께 해볼까요?

번호	문제	정답
1	“무료 쿠폰을 준다는 문자 링크를 눌렀다가 악성 앱이 설치되었다면 스미싱이다.” (O , X)	0
2	다음 중 파밍에 해당하는 것은? ① 친구가 돈을 빌려달라고 메신저로 요청 ② 가짜 은행 사이트로 접속하게 만들어 정보 입력 ③ 전화로 경찰을 사칭하여 돈 요구 ④ SNS에서 연애 감정으로 접근 후 돈 요구	2
3	“QR코드를 찍었더니 앱 설치가 유도되었다면 큐싱일 가능성이 있다.” (O , X)	0
4	다음 중 메신저피싱의 특징은? ① 이메일로만 이루어진다 ② QR코드를 이용한다 ③ 지인 계정을 도용해 돈을 요구한다 ④ 컴퓨터를 잠그고 돈을 요구한다	3
5	다음 중 랜섬웨어 특징은? ① 전화로 협박한다 ② 개인정보를 몰래 수집한다 ③ 파일을 잠그고 돈을 요구한다 ④ 친구를 사칭한다	3



자기 평가하기

★ 아래 문장을 읽고 나의 수준 체크 (O / X)

평가 내용	O	X
▶ 나는 의심스러운 문자 링크를 클릭하지 않는다.	☐	☐
▶ 나는 친구나 가족이 돈을 요구하면 반드시 직접 확인한다.	☐	☐
▶ 나는 모르는 앱이나 파일(.apk, .exe 등)을 설치하지 않는다.	☐	☐
▶ 나는 가짜 사이트와 진짜 사이트를 구분하려고 노력한다.	☐	☐
▶ 나는 사이버 범죄 상황이 발생하면 신고 방법을 알고 있다.	☐	☐

★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

03

사이버공격 예방 방법

• 목 표 •

- 1 사이버공격 발생 시 올바른 대응 방법을 설명할 수 있다.
- 2 피해 상황에 따라 적절한 조치를 선택할 수 있다.
- 3 신고 및 예방 서비스를 활용할 수 있다.

• 준비물 •

- 1 스마트폰 (설정 및 신고 방법 확인용)
- 2 필기구 및 활동지
- 3 수업자료 (프린트 또는 PPT)
- 4 이어폰 (영상 시청 시)
- 5 개인 계정 보안 점검 체크리스트

• 핵심 활동 •

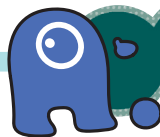
- 피싱 문자 발견 시 신고 연습하기
- “이 상황에서 어떻게 할까?” 역할극
- 스마트폰 보안 설정 점검하기
- 악성앱 탐지 과정 체험하기
- 개인정보 유출 상황별 대응 방법 정리하기

• 핵심 사이트 •

- 1 의심 전화·문자는 즉시 신고
- 2 악성앱이 의심되면 기기 사용을 중단
- 3 개인정보 유출 여부에 따라 대응이 다름
- 4 112, 1394 등 신고 기관을 활용
- 5 예방 서비스(명의도용방지, 결제차단)를 미리 설정

• 핵심 키워드 •

- 신고 (112 / 1394)
- 악성앱
- 개인정보 유출
- 비행기모드
- 보안설정
- 명의도용방지



학습을 위한 사전준비

- ▶ 스마트폰 문자/통화 사용 경험 떠올리기
- ▶ 스팸 문자 받아본 경험 생각하기
- ▶ 앱 설치 경험 돌아보기
- ▶ “이상한 상황에서 내가 했던 행동” 생각해오기



사이버공격 예방 방법

★ 서비스 이용하기

1 명의도용 방지서비스 이용

- ① 신규 또는 명의변경으로 이동통신에 가입시 계약이 체결된 사실을 문자 또는 등기우편물로 안내해주는 서비스로 엠세이퍼, PASS앱, 카카오톡 앱에서 신청가능



② 엠세이퍼 홈페이지 신청

홈페이지 접속(<https://www.msafar.or.kr>) ▶ 명의도용방지서비스 메뉴 ▶ 가입제한서비스

③ PASS앱 이용시

PASS앱 전체메뉴 ▶ 보안 ▶ 명의도용방지 ▶ 가입제한설정

④ 카카오톡앱 이용시

카카오톡앱 전체메뉴 ▶ 보안 ▶ 명의도용방지 서비스 ▶ 조회하기

2 통신사조치

① 이용 중인 통신사 고객센터(114) 또는 통신사 앱을 통해 신청

② 번호도용차단서비스

- 인터넷을 이용한 문자 발송시 신청고객의 번호를 발신번호로 발송할 수 없도록 차단하는 서비스
- 신청자 본인도 인터넷 문자발송에 제한됨

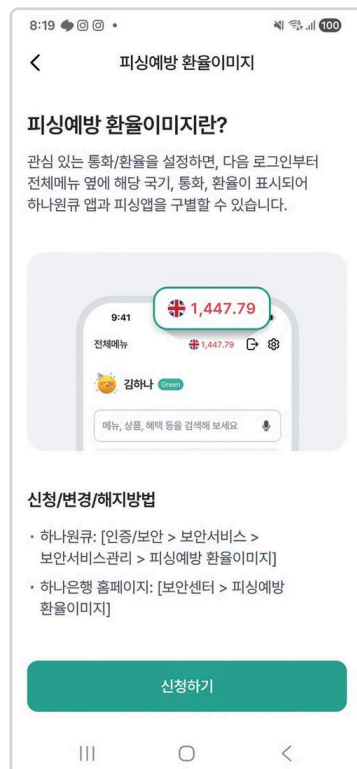
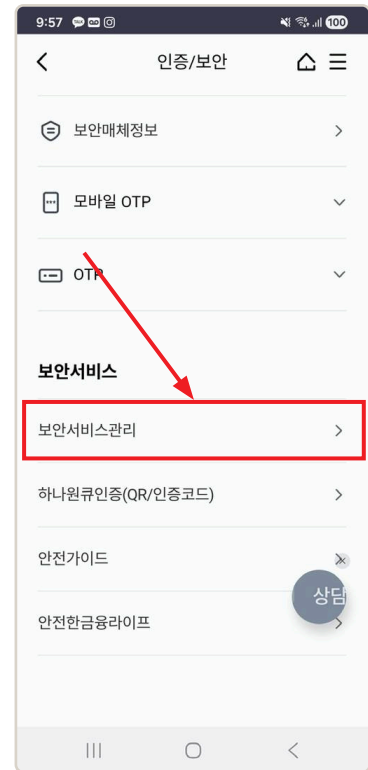
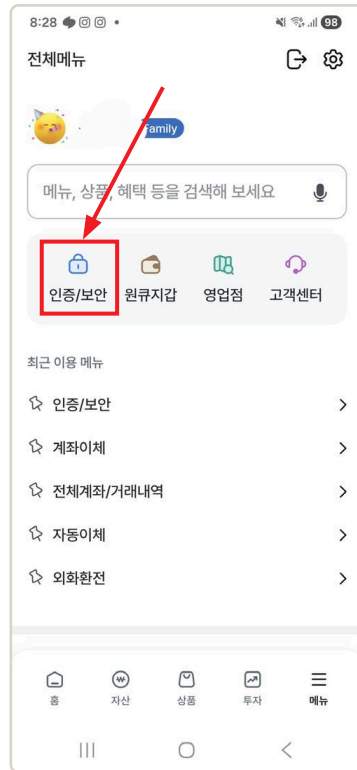
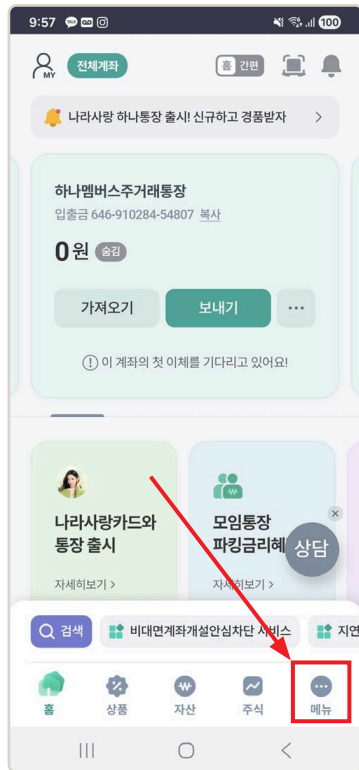
③ 소액결제 차단서비스

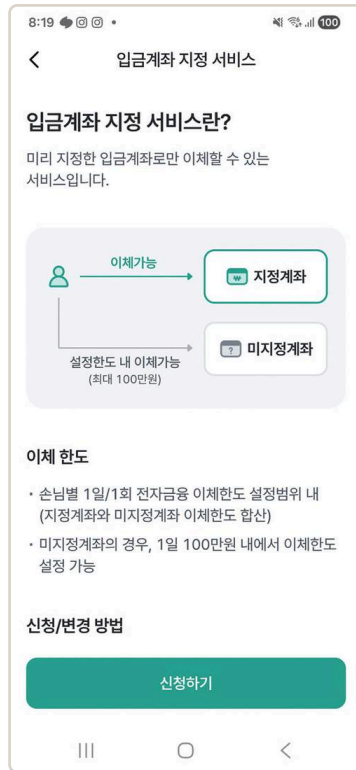
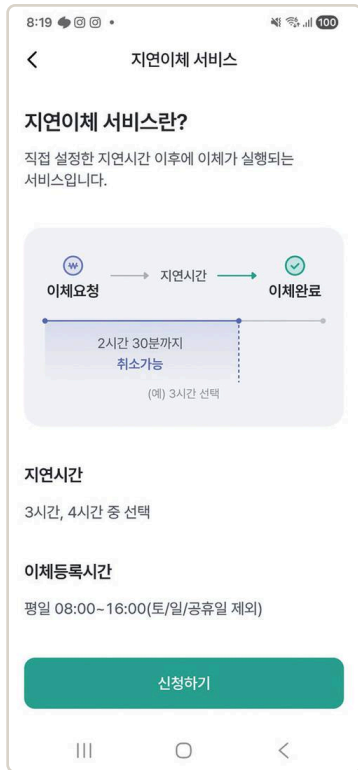
④ 콘텐츠 이용 결제 차단

3 금융권조치

① 피싱예방 환율이미지, 해외IP차단 서비스, 지연이체 서비스, 입금계좌 지정서비스, 오픈뱅킹 안심 차단서비스, 비대면 계좌개설 안심차단 서비스, 단말기지정 서비스(PC), 인증서 안심거래 서비스(PC)

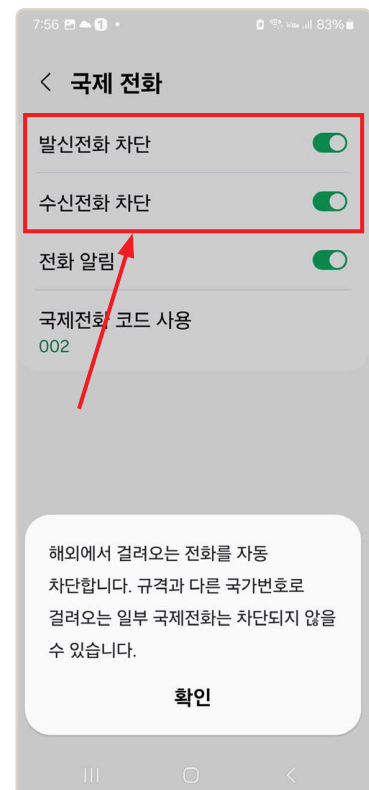
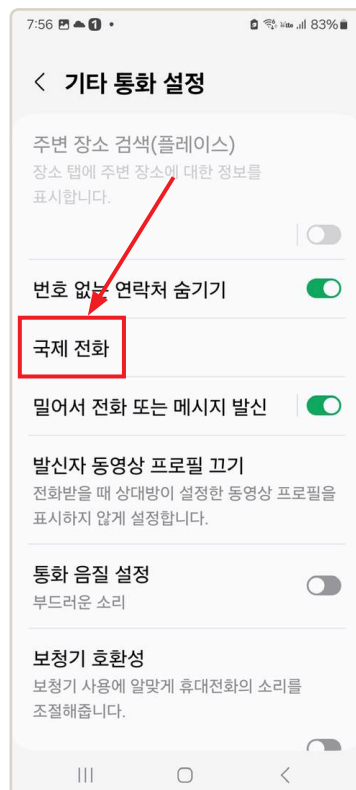
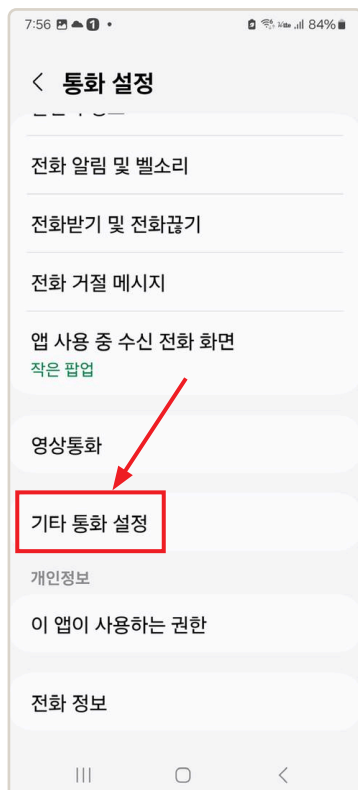
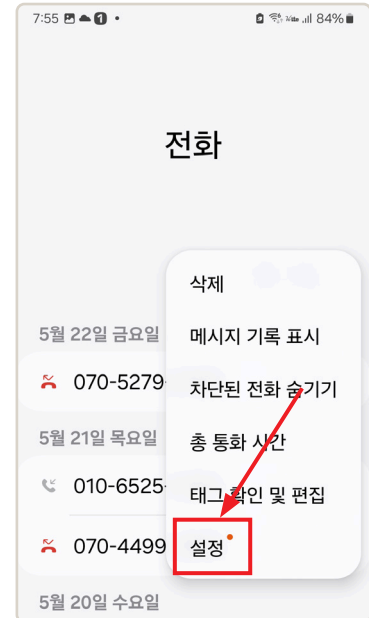
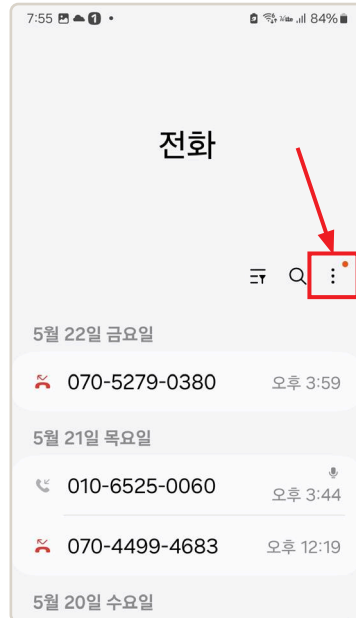
- 메뉴 ▶ 인증/보안 ▶ 보안서비스관리 ▶ 목록중 원하는 서비스를 클릭하여 신청
- 차단신청은 앱에서, 해제신청은 은행방문





4 휴대폰설정

- ① 출처를 알수 없는 앱 설치 제한 : 휴대폰에 기본으로 설정됨
- ② 국제전화 발신제한 : 전화앱 ▶ 오른쪽 상단 점세개 ▶ 설정 ▶ 기타 통화 설정 ▶ 국제전화 ▶ 발신전화 차단, 수신전화 차단을 활성화



- ③ 금융사기 예방앱(시티즌코난, 피싱아이즈) 설치



함께 해볼까요?

- 보이스피싱범은 누구일까요?

보이스피싱 체험하고 피싱범 잡기 (<https://www.fss.or.kr/fss/pk/voice.html>)

다음 중 어떤 것이 진짜 보이스피싱범의 음성일까요?

다섯명의 목소리 중 보이스피싱범으로 의심되는 목소리를 골라보세요.



하단 버튼을 클릭하여 보이스피싱범을 선택해 주세요~



**진짜 보이스피싱범
결과 확인하기**



자기 평가하기

평가 내용	정답
▶ 명의도용 방지서비스를 신청할 수 있는 앱이 아닌 것은 무엇일까요? ① PASS 앱 ② 카카오톡 앱 ③ 엠세이퍼(Msafer) ④ 게임 앱	④
▶ 다음 중 통신사에서 신청 가능한 서비스는 무엇일까요? ① 번호도용 차단 서비스 ② 화면 밝기 조절 서비스 ③ 배경화면 변경 서비스 ④ 게임 점수 저장 서비스	①
▶ 다음 중 금융사기 예방에 도움이 되는 행동은 무엇일까요? ① 출처를 모르는 앱 설치하기 ② 해외 IP 차단 서비스 이용하기 ③ 비밀번호를 친구와 공유하기 ④ 의심 링크를 바로 클릭하기	②
▶ 다음 중 휴대폰에서 설정하면 도움이 되는 보안 기능은 무엇일까요? ① 국제전화 발신·수신 차단 ② 화면 자동화전 해제 ③ 알람 볼륨 증가 ④ 배터리 절약 모드	①
▶ 어느 날 휴대폰에 “무료 쿠폰 지급! 앱 설치 시 즉시 지급”이라는 문자가 왔습니다. 가장 안전한 행동은 무엇일까요? ① 링크를 바로 누른다. ② 친구에게 대신 눌러보라고 한다. ③ 출처를 확인하고 의심되면 삭제한다. ④ 개인정보를 먼저 입력한다.	③

★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

04

사이버공격 발생시 대응방법

• 목 표 •

- 1 피싱 의심 상황에서 올바르게 신고할 수 있다.
- 2 개인정보 유출 여부에 따라 대응 방법을 구분할 수 있다.
- 3 실제 상황에서 스스로 대처하는 방법을 익힌다.

• 준비물 •

- 1 스마트폰
- 2 필기구 및 활동지
- 3 보안 앱 설치 가능 환경
- 4 수업자료 (프린트/PPT)
- 5 이어폰 (영상 시청 시)

• 핵심 사이트 •

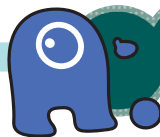
- 1 의심 전화·문자는 바로 신고
- 2 링크를 눌렀다면 즉시 기기 사용을 중단
- 3 악성앱은 검사 후 바로 삭제
- 4 개인정보 유출 여부에 따라 대응이 다름
- 5 1394, 112 등 신고 기관을 적극 활용

• 핵심 활동 •

- 피싱 문자 신고 직접 따라하기
- 상황별 대응 방법 카드 맞추기 활동
- “유출 O/X” 상황 판단 게임
- 악성앱 탐지 과정 체험하기
- 대응 순서 말하기 (멈춤→확인→신고)

• 핵심 키워드 •

- 피싱신고
- 비행기모드
- 악성앱
- 1394 신고
- 개인정보 유출
- 보안앱



학습을 위한 사전준비

- ▶ 스팸 문자 받은 경험 떠올리기
- ▶ 앱 설치 경험 생각하기
- ▶ 링크 클릭 경험 돌아보기
- ▶ “이상한 상황에서 내가 한 행동” 정리해오기

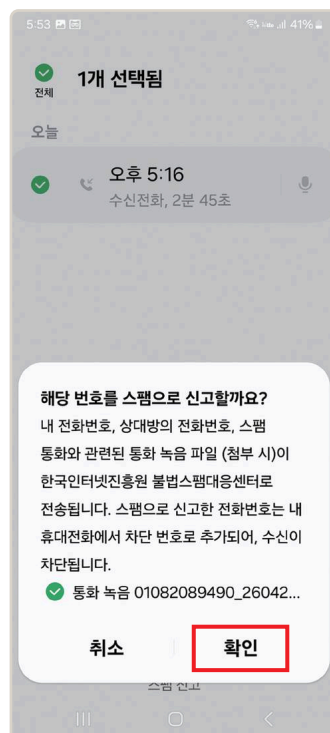
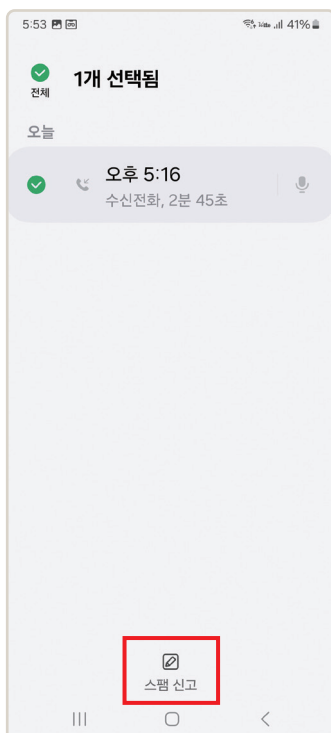
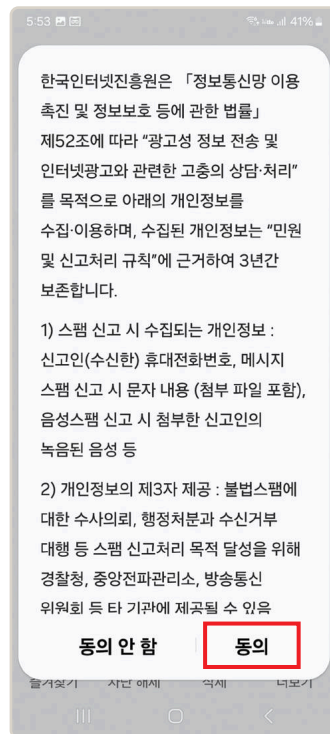
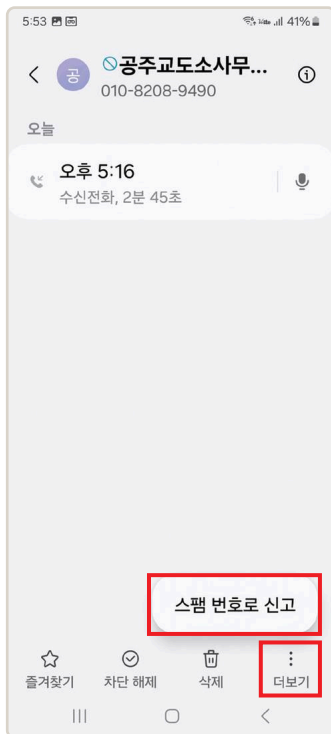


사이버공격 예방 방법

★ 피싱의심 전화번호 신고

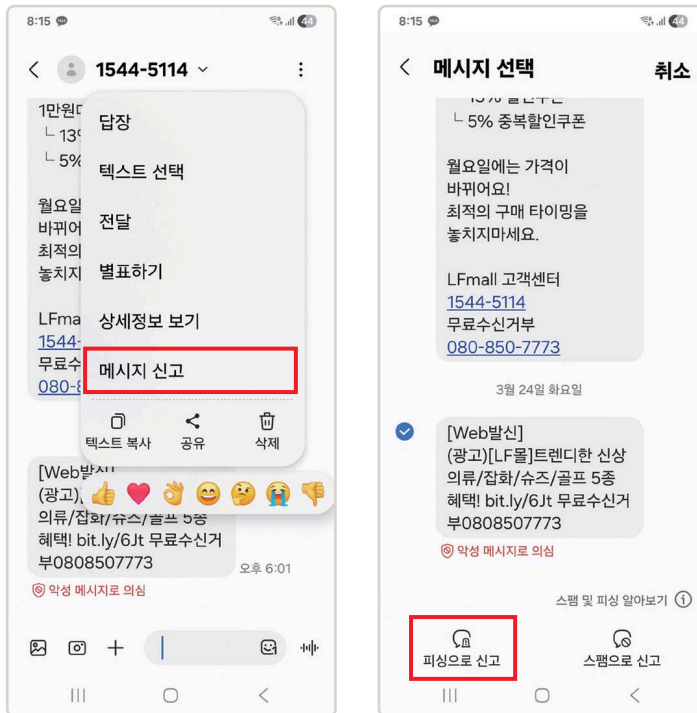
1 피싱전화번호 확인하고 제보하기

더보기 ▶ 스팸번호 신고 ▶ 동의 ▶ 스팸신고 ▶ 확인



2 휴대폰 문자에서 바로 신고

메시지를 길게 누르기 ▶ 메시지 신고 ▶ 피싱으로 신고



★ 1394로 신고하기

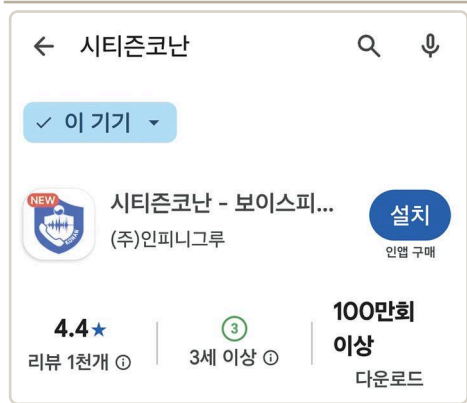
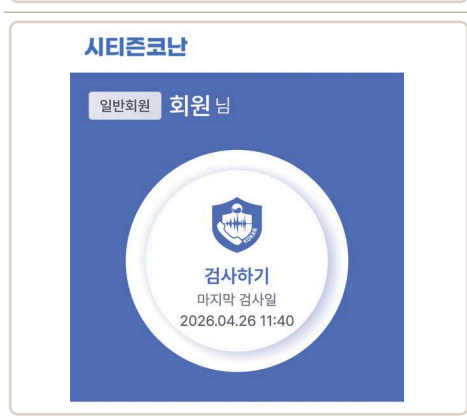
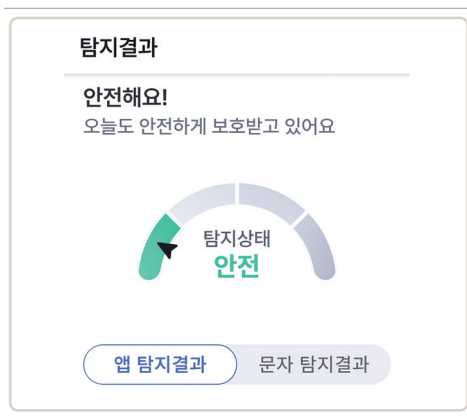


★ 개인정보 유출이 안된 경우

초기화 전까지 휴대전화 전원을 끄거나 비행기모드 전환

1 경찰청 앱으로 악성앱 설치 확인하기

시티즌코난은 경찰청과 보안 전문 기업 인피니구루가 협력하여 만든 공식 보안 앱으로, 스마트폰에 숨겨진 악성 앱이나 원격 제어 스파이앱을 실시간으로 탐지하여 범죄 피해를 사전에 예방하는 역할

	< 첫번째 > - 구글 플레이스토어에 접속하여 '시티즌코난' 검색 (개발사: (주)인피니구루 확인) - 필수 권한 허용: 전화, 저장공간, 알림 접근 권한을 반드시 '허용'으로 설정 - 접근성 활성화: '모든 파일에 대한 접근' 설정에서 시티즌코난 항목을 찾아 ON 상태로 변경
	< 두번째 > - 검사 실행: 앱 메인 화면의 [검사하기] 버튼을 클릭 - 결과 확인: '위험', '주의', '정상' 단계 중 결과를 확인
	< 세번째 > 즉시 삭제: 만약 '위험' 항목이 발견된다면 우측 휴지통 아이콘을 눌러 즉시 제거

★ 개인정보 유출이 된 경우

01 피해신고 및 지급정지 요청



경찰(112), 금융원(1332), 금융회사에 피해신고 및 지급정지 요청

02 개인정보 노출등록



개인정보 노출자 사고예방시스템 (<http://pd.fss.or.kr>) 사고등록

03 계좌 일괄 지급정지 신청



계좌정보통합서비스(www.payinfo.or.kr) 및 금융회사 영업점에서 일괄지급정지

04 명의도용 신고



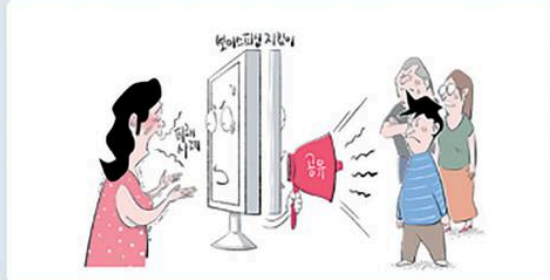
명의도용방지서비스(www.msafar.or.kr) 및 금융회사 영업점에서 일괄지급정지

05 악성앱 삭제 및 휴대전화 초기화



악성코드 감염시 바로 삭제 및 휴대전화 초기화

06 피해사례 공유



보이스피싱지킴이 사이트에 접속하여 피해사례 공유

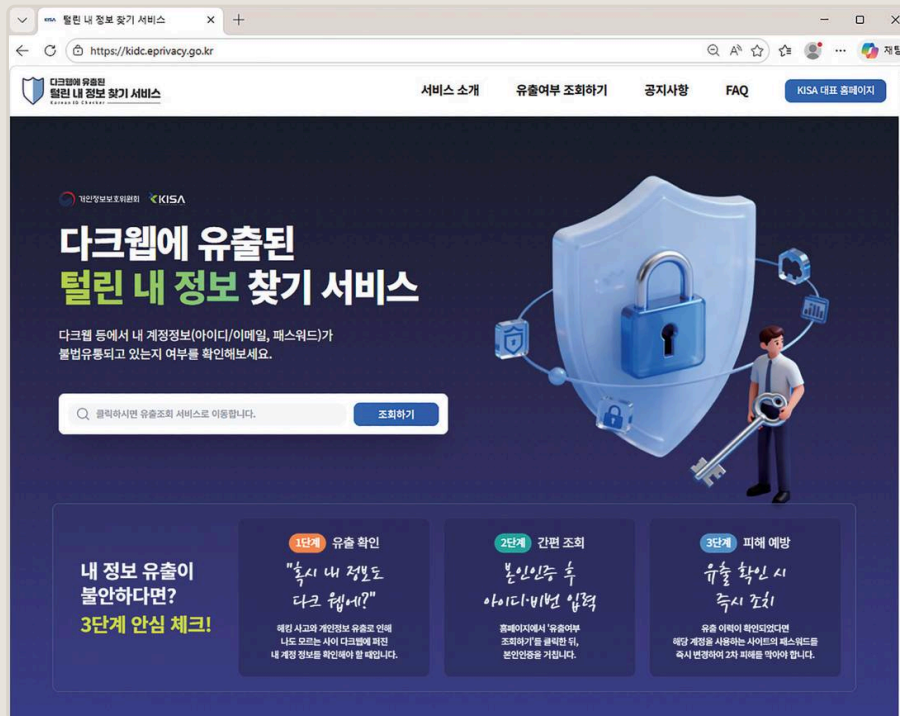
출처 : 금융감독원 <https://www.fss.or.kr/fss/main/contents.do?menuNo=200365>



함께 해볼까요?

• 털린 내 정보 찾기 서비스

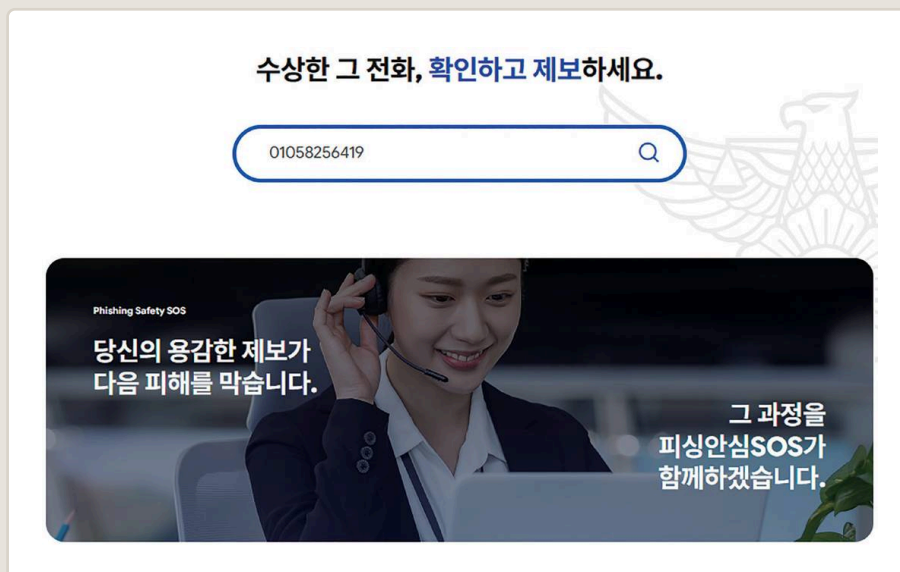
네이버에 한국인터넷진흥원(<https://kidc.eprivacy.go.kr/>)을 검색하여 클릭



• 피싱번호 검색하기

- 네이버에 피싱안심SOS(<https://www.counterscam112.go.kr/main.do>)을 검색하여 클릭

- 공무원사칭 전화번호 "010-5825-6419, 010-8208-9490"를 입력하고 확인





자기 평가하기

평가 내용	정답	
▶ 피싱 의심 문자를 받으면 링크를 눌러 내용을 먼저 확인해야 한다.	O	X
▶ 개인정보가 유출되지 않았다면 휴대폰 전원을 끄거나 비행기 모드로 전환하는 것이 도움이 된다.	O	X
▶ 피싱 의심 전화를 받았을 때 가장 먼저 해야 할 행동은 무엇일까요? ① 개인정보를 알려준다 ② 상대방 말에 따라 앱을 설치한다 ③ 전화를 끊고 확인 및 신고한다 ④ 문자 링크를 눌러본다	③	
▶ 다음 중 악성앱이 의심될 때 사용할 수 있는 앱은 무엇일까요? ① 계산기 앱 ② 시티즌코난 앱 ③ 카메라 앱 ④ 음악 앱	②	
▶ 개인정보가 이미 유출된 상황에서 가장 적절한 대응은 무엇일까요? ① 아무 조치도 하지 않는다 ② 비밀번호를 그대로 사용한다 ③ 신고기관과 금융기관에 즉시 알린다 ④ 휴대폰을 계속 사용한다	③	

★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

금융범죄와 사이버 보안

금융범죄, 아는 만큼 지킵니다: 현황부터 대응까지 한눈에 보기

[현황] 기관사칭형 보이스피싱 피해 현황

기관사칭형 피해액
6,753억 원

보이스피싱 전체 피해액의 76.2%를 차지하며 심각한 수치를 기록했습니다



2030 청년층 피해 비중 52%
기관사칭형 범죄 피해자 절반 이상이 사회 초년생인 청년층에 집중되었습니다

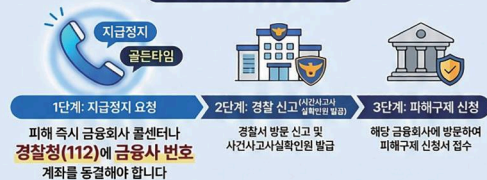
건당 피해액
76.3% 급증

건당 피해액이 약 7,438만 원으로 건당 대비 크게 증가했습니다

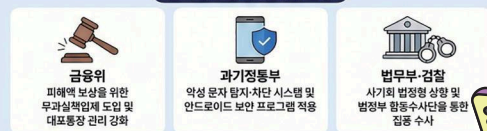


[대책/대응] 정부의 통합 대책 및 피해 대응 요령

피해 발생 시 3단계 대응 절차



범부처 통합 대응 체계 가동



교육 목표

- 금융범죄의 개념을 이해한다.
- 금융범죄의 피해 현황과 정부대책을 알 수 있다.
- 금융범죄의 위험성과 법적 책임을 알 수 있다.
- 금융범죄 발생 시 상황별 대응방법을 알 수 있다.



이런 활동을 해요

프로젝트 과정	기초	심화
	사이버공격 알아보기	금융범죄와 사이버 보안
활동 내용	• 사이버 공격이란? • 사이버공격의 유형과 사례 분석 • 사이버공격 예방방법 • 사이버공격 발생 시 대응방법	• 금융범죄란 무엇일까? • 금융범죄의 피해 현황 및 정부대책 • 금융범죄의 위험성 및 법적 책임 • 금융범죄 발생 시 상황별 대응방법

01

금융범죄의 이해와 피해현황 및 정부대책

• 목 표 •

- 1 금융범죄의 개념을 이해할 수 있다.
- 2 금융범죄와 일반 사기의 차이를 구분할 수 있다.
- 3 금융범죄의 위험성과 심각성을 인식할 수 있다.

• 준비물 •

- 1 필기구 및 활동지
- 2 스마트폰 (사례 확인용)
- 3 수업자료 (프린트/PPT)
- 4 이어폰 (영상 시청 시)
- 5 개인 경험 정리 메모

• 핵심 활동 •

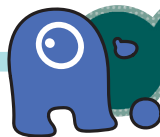
- 금융범죄 vs 일반사기 구분하기
- 실제 사례 보고 어떤 범죄인지 맞추기
- “이건 금융범죄일까?” 카드 분류 활동
- 친구에게 설명해보기 (1분 설명 활동)
- 금융범죄 피해 사례 토론

• 핵심 사이트 •

- 1 금융범죄는 전기통신을 이용해 돈이나 정보를 빼앗는 범죄
- 2 피싱·보이스피싱 등이 대표적인 금융범죄
- 3 단순 물건 사기(중고거래 등)는 금융범죄에서 제외
- 4 해킹은 금융범죄가 아니라 ‘전자적 침해행위’
- 5 결국 사람을 속여 돈을 빼앗는 것이 핵심

• 핵심 키워드 •

- 금융범죄
- 보이스피싱
- 전기통신
- 개인정보
- 사기
- 전자적 침해행위



학습을 위한 사전준비

- ▶ 중고거래 경험 떠올리기
- ▶ 사기 당할 뻔한 경험 생각하기
- ▶ 문자·전화 받은 경험 정리
- ▶ “돈과 관련된 위험 상황” 생각해오기



금융범죄란 무엇일까?

전기통신금융사기란

전기통신을 이용하여 타인을 기망·공갈함으로써 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는다음 각 목의 행위를 말한다. 다만, 재화의 공급 또는 용역의 제공 등을 가장한 행위는 제외하되, 대출의 제공·알선·중개를 가장한 행위는 포함한다.



☐ '전기통신금융사기'란

- 가. 자금을 송금·이체하도록 하는 행위
- 나. 개인정보를 알아내어 자금을 송금·이체하는 행위
- 다. 자금을 교부받거나 교부하도록 하는 행위
- 라. 자금을 출금하거나 출금하도록 하는 행위

출처 : 보이스피싱지킴이 <https://www.fss.or.kr/fss/main/contents.do?menuNo=200354>

제외되는 행위

1 재화의 공급 등을 가장한 행위

- ① 재화의 공급과 같은 상거래(전자상거래 포함)로서 본인의 의지로 계약 또는 신청하여 발생한 사기
- ② 예시 : 물품 대금(전자상거래 포함) 사기, 물품 하자 및 계약 불이행 관련 사기, 중고물품 중개사기, 인터넷 쇼핑물 사기, 인터넷 무역사기 등

2 용역의 제공 등을 가장한 행위

- ① 통상의 서비스 용역 거래에 있어서 본인의 의지로 신청 또는 계약을 하여 발생한 사기는 전기통신금융 사기에서 제외
- ② 예시 : 알선 및 중개행위 수수료 빙자 관련 사기(자동차 중개, 부동산 중개, 골동품 중개 등), 인터넷 게임 아이템 사기, 사이버 경매 사기, 사이버 주식 사기, 인터넷 취업사기 등

3 비정상적인 재화의 공급 또는 용역의 제공 등의 행위

- ① 불법한 거래와 관련한 재화의 공급 또는 용역의 제공 등은 전기통신금융 사기에서 제외(민법 제746조의 불법원인급여에 해당)
 - ※ 피해금이 불법적 재화 또는 용역의 대가가 아니라 공갈 행위로 인한 것인 경우에는 전기통신금융 사기에 해당

- ② 예시 : 물품 대금(전자상거래 포함) 사기, 물품 하자 및 계약 불이행 관련 사기, 중고물품 중개사기, 인터넷 쇼핑몰 사기, 인터넷 무역사기 등

4 해킹

- ① 해킹은 전자적 침해행위* 중 하나로, 전기통신을 이용하여 타인을 기망(欺罔)·공갈(恐喝)한 행위는 아니므로 제외
- ② 전자적 침해행위 : 해킹, 컴퓨터 바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 전자금융 기반 시설을 공격하는 행위



금융범죄의 피해 현황 및 정부대책

★ 금융범죄의 피해 현황

- 2025년 1월부터 8월까지 기관사칭형 보이스피싱 범죄의 피해액은 6,753억 원으로, 전체 보이스피싱 피해액(8,856억 원)의 76.2%를 차지
- 특히 기관사칭형 보이스피싱 1건당 피해액은 7,438만 원으로 전년 같은 기간 1건당 피해액인 4,218만 원에 비해 76.3% 증가
- 기관사칭형 보이스피싱의 연령대별 피해 현황을 살펴보면 20~30대 청년층의 피해 비율이 전체의 52%로 절반을 넘김

<보이스피싱 유형별 피해 현황>

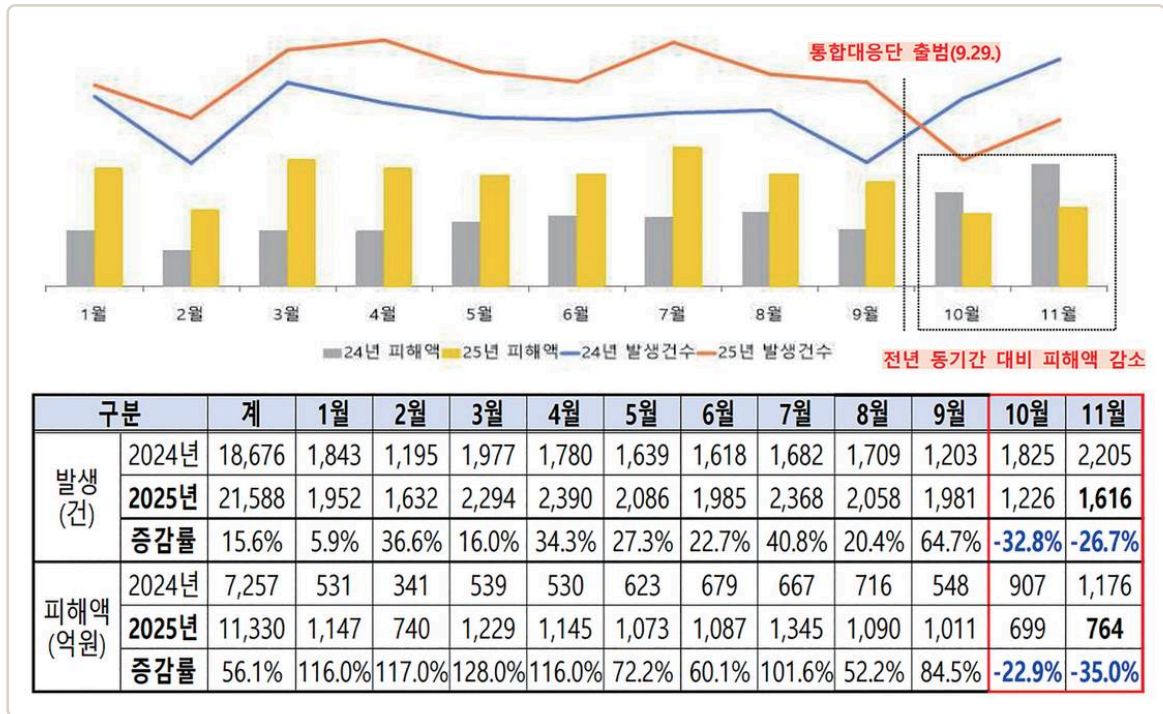
구분	합 계			기관사칭형			대출사기형		
	발생 건수	피해액 (억 원)	건당 피해액 (만 원)	발생 건수	피해액 (억 원)	건당 피해액 (만 원)	발생 건수	피해액 (억 원)	건당 피해액 (만 원)
24년(~8월)	13,443	4,625	3,440	5,993	2,528	4,218	7,450	2,097	2,814
25년(~8월)	16,765	8,856	5,282	9,079	6,753	7,438	7,686	2,103	2,736
증감	24.7% ↑	91.5% ↑	53.5% ↑	51.5% ↑	167.1% ↑	76.3% ↑	3.2% ↑	0.3% ↑	2.8% ↓

<기관사칭형 보이스피싱 피해자 연령대별 현황 / 단위: 명>

구분	합계(비율)	20대 이하	30대	40대	50대	60대 이상
24년(~8월)	5,993(100.0)	3,242(54.1)	524(8.7)	319(5.3)	535(8.9)	1,373(22.9)
25년(~8월)	9,079(100.0)	3,748(41.3)	1,013(11.2)	433(4.8)	821(9.0)	3,064(33.7)
증감	51.5% ↑	15.6% ↑	93.3% ↑	35.7% ↑	53.5% ↑	123.2% ↑

출처 : 경찰청 및 뉴스기사(<https://medicalworldnews.co.kr/news/view.php?idx=1510970196>)

- 보이스피싱 피해 추이를 비교 분석한 결과 2025년 11월까지 보이스피싱 총 발생건수는 15.6%(18,676건 → 21,588건), 피해액은 56.1%(7,257억 → 1조1,330억) 각각 증가하였지만
- 8.28 정부대책이 실효성 있게 이행되면서 연초부터 줄곧 매월 전년도 통계를 상회하던 보이스피싱 피해지표(건수, 피해액)가 10월~11월에는 감소
- 10월은 추석연휴가 포함되어 시기적으로 피해지표가 감소하는 특성이 있지만, 연휴 효과와 문관한 11월에도 전년대비 상당부분 감소



출처 : 국무조정실/국무총리비서실 보도자료 2025.12.30.

★ 정부대책

1 정부의 정책 과제별 주요 성과로는

- ① 보이스피싱 범정부 통합대응단 구축 · 운영(9.29~)
- ② 범죄 이용 전화번호 10분 이내 긴급차단 도입(11.24~)
- ③ 휴대폰에 AI 기반 보이스피싱 자동탐지 · 경고 기술(opt-out 방식) 적용

2 금융위·금감원

- ① 선제적으로 의심거래를 탐지·대응할 수 있는 '보이스피싱 AI 플랫폼(ASAP) 가동(10.29~)
- ② 피해금액의 일정 한도 범위에서 금융회사가 피해액 보상하는 무과실책임제 도입
- ③ 대포통장의 개설·유통방지를 위한 법인계좌, 외국인계좌등에 대한 관리 강화방안 마련 예정

3 과기정통부

- ① 의심문자 발송방지를 위한 '악성 문자 탐지·차단 시스템' 도입
- ② 과기정통부-구글 MOU(9.8)를 통해 악성 앱 자동설치방지하는 보안프로그램 안드로이드 3,500만대에 모두 적용(11.18)
- ③ 대포폰 방지를 위한 여권으로 1회선만 개통(9.30~)하며, '안면인증제도 도입(12.23~)'
- ④ 휴대폰 불법 개통에 대해 이동통신사의 관리책임 강화예정
- ⑤ 발신번호 변작 중계기의 국내 제조 · 유통 등 금지하여 거짓 표시된 전화번호도 원천차단 예정
- ⑥ 휴대전화 제조사와 이통3사가 자체 개발한 전화 앱의 보이스피싱 탐지·알림 기능을 기본으로 활성화를 제공

4 법무부

- ❶ 형법상 사기죄의 법정형을 상향
- ❷ 범죄수익을 필요적으로 몰수·추징 : 범죄기간 중 취득 재산을 범죄수익으로 추정하여 피해자에게 환부할 수 있도록 부패재산몰수법을 개정완료
- ❸ 「해외 보이스피싱 사범 대응 범정부 TF」를 발족·운영함으로써 우선송환대상 범죄인 선정 및 해외 범죄단지 단속을 통한 총책급 범죄인 검거, 범죄조직 감금 피해자 구출을 적극 추진

5 검찰청

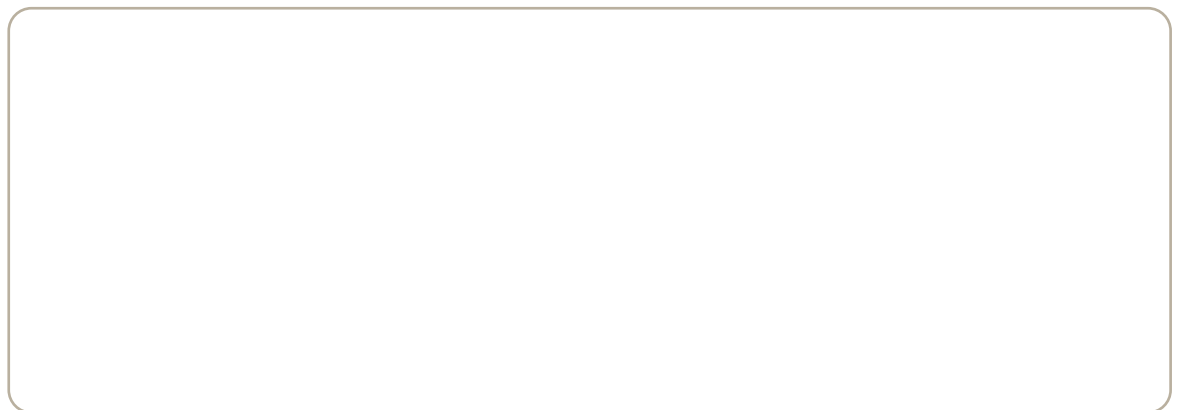
- ❶ 검찰, 경찰, 금감원, 국세청, 관세청, 법무부 출입국·외국인정책본부 등이 참여하는 '보이스피싱 범죄 정부합동수사단'을 중심으로 범죄조직에 대한 집중 수사 실시
- ❷ 필리핀 국가수사청(NBI) 파견수사관을 통해 현지 공조수사를 실시하여 25년총책 등 주요 조직원 19명 검거 성과를 거두었고, 중국·캄보디아 등과의 협력관계 구축 등 공조강화도 계속 추진할 예정
- ❸ 내부조직원이 범죄조직이나 상위 조직원을 제보할 경우 그 형을감경하거나 면제하는 '사법협조자 형벌감면제도' 도입도 적극 추진

6 개인정보위원회

- ❶ 민간·연구기관의 AI 기반 피싱 예방기술 개발에 필요한 개인정보의 안전한 공유 및 활용여건 조성
- ❷ 보이스피싱 예방과 같은 사회적·공익적 목적으로 꼭 필요한 AI 기술 개발에 개인정보 원본을 활용할 수 있도록 개인정보 보호법 상의 특례 조항을 신설하는 입법 논의를 적극 지원할 예정
- ❸ 불법 유통된 개인정보가 보이스피싱 범죄 등에 악용될 우려를 차단하기 위해 개인정보 불법유통에 대한 처벌근거를 신설하고 관련 유통 정보를 수집·분석하는 법적 근거를 도입하는 등 대응책을 마련할 예정

7 방송미디어통신위원회

- ❶ 불법스팸어 이동전화 신규가입 제한, 블랙리스트 차단, 이통3사 삼성전자 협업을 통한 AI 기반 불법스팸 걸러내기 강화 등을 추진
- ❷ 불법스팸 관련자에 대한 과징금 부과, 범죄수익 몰수 추징을 규정한 「정보통신망법*」 개정을 통해 국민불편과 피해를 방지하여 안전한 디지털서비스 이용환경을 조성해 나갈 예정



참고

종합대책 관련 입법과제 추진현황

부처	법안명	주요내용
금융위 (정무위)	▶ 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법	① 보이스피싱 의심정보 공유 ② 가상자산 지급정지 및 환급 조치 ③ 무과실배상책임 법제화 ④ 금융회사 인력 및 시설 확충
현황	▶ ① 법사위 의결(12.3) / ② 정무위 전체회의 의결(12.17) ③ · ④ 조인철 · 강준현 의원 발의(12.23)	
과기부 (과방위)	▶ 전기통신사업법 (① 한민수 의원, ② 한정애 의원) (③ 한정애 / 조인철 / 박정훈 / 조은희 의원)	① 불법개통 대리점 계약해지, 이통사 영업정지 · 등록취소 ② 휴대폰 개통 시 대포폰 불법성 고지 ③ 사설증계기 수입 · 유통 금지
현황	▶ ① · ② 법사위 의결(12.3) / ③ 과방위 법안소위 상정 예정(병합심사 예정)	
방미통위 (과방위)	▶ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 (최민희 / 황정아 / 이현승 의원)	불법스팸 발송 관련자에 대한 과징금 부과 및 범죄수익 몰수 · 추징
현황	▶ 법사위 의결(12.3)	
개보위 (정무위)	▶ 개인정보보호법 (민병덕 / 고동진 의원)	공익 목적의 AI개발 시 개인정보 처리 근거 마련
현황	▶ 정무위 법안소위 상정 추진	
법무부 (법사위)	▶ 형법(이종배 / 김기표 의원)	사기죄 법정형 상향
현황	▶ 법률 공포 및 시행(12.23.)	
법무부 (법사위)	▶ 부패재산물수법(박균택 의원)	보이스피싱 범죄수익 환수 강화
현황	▶ 법률 공포되어 '26. 6. 17. 시행 예정	
법무부 (법사위)	▶ 범죄수익은닉규제법 (박균택 / 한정애 의원 등)	보이스피싱 범죄에 대한 독립몰수제 도입
현황	▶ 법사위 논의 중(법안1소위 논의 중)	
검찰청 (정무위)	▶ 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법 (조인철 / 한정애 의원)	사범협조자 형벌 감면제 도입
현황	▶ 조인철 의원 발의(11.28) / 한정애 의원 발의(12.8)	
경찰청 (미확정)	▶ 전기통신 이용 다중피해사기 방지법(제정안) (채현일 의원)	전기통신 이용 다중피해사기 정의, 범행이용수단 차단, 전담부서 운영 등
현황	▶ 채현일 의원 발의(12.29.)	

출처 : 국무조정실/국무총리비서실 보도자료 2025.12.30.

III. 정책목표와 추진과제

정책목표

예방중심의 유관기관 통합대응으로
보이스피싱 근절

3대 전략

① 대응 거버넌스 개편

② 예방중심·선제대응

③ 배상책임·처벌강화

6대 정책과제

1. 유관기관 통합대응체계 구축

2. 범죄수단 원천 차단,
접근경로 봉쇄
[접근단계]

3. 첨단기술을 활용한
범행탐지 강화
[기망단계]

4. 금융권 등 피해방지·
배상책임 강화
[편취단계]

5. 수사 및 처벌 강화
[수사단계]

6. 전방위 홍보·교육

15개 실천과제

① 24시간·365일 가동되는 보이스피싱 통합대응단 구축

② 불법스팸·악성앱 3중 차단체계 구축

③ 피싱 전화번호 긴급차단 제도 도입

④ 통신사의 범죄예방 의무 및 제재 강화

⑤ 대포폰 유통 및 전화번호 거짓표시 차단체계 구축

⑥ 구인광고를 빙자한 범죄조직원 모집 모니터링 강화

⑦ AI 기반 보이스피싱 탐지·차단체계 구축

⑧ 범행차단 기술 고도화를 위한 정보공유 환경 조성

⑨ 금융회사 등의 범죄피해 배상책임 법제화

⑩ 금융회사 자체 대응역량 강화

⑪ 가상자산거래소 등 범죄 사각지대 해소

⑫ 보이스피싱 전담수사체계 구축, 국가수사역량 집중

⑬ 보이스피싱 등 사기죄 처벌 법정형 강화

⑭ 해외거점 조직검거를 위한 국제공조 강화

⑮ 범죄예방 콘텐츠 제작 및 교육프로그램 강화

범
행
단
계
별
대
응

<이전과 달라지는 주요 내용>

현행

- ◆ 보이스피싱 신고대응센터
 - ▶ 단순 상담·안내 위주 대응
 - ▶ 평일 주간(09~22) 운영, 응답률 60%
 - ▶ 번호 차단까지 평균 2~3일 소요
(알뜰폰은 긴급 차단 불가)

- ◆ 불법스팸·악성앱 사전차단 체계 부재
- ◆ 휴대폰 불법개통에 대한 통신사 등 제재 無
- ◆ 외국인 여권 휴대전화 개통시 1인 2회선 허용
* 외국인 명의 대포폰(22년 7,295건→24년 71,416건)

- ◆ 사전 예방보다 사후 수습에 치중,
신종 수법에 수동적 대응

- ◆ 실효성 없는 금융사 책임분담 제도 등
'고객 보호 의무' 조치 미흡*
* 자율배상제 시행('24.1월) 이후
배상액은 1.6억에 불과
- ◆ 가상자산거래소 범죄계좌 조치 불가능

- ◆ 분산된 수사조직으로 수사력 집중 한계
- ◆ 범죄의 중대성에 비해 낮은 형량

개선

- ◆ 보이스피싱 통합대응단 구축·운영
 - ▶ 통신·금융·수사 등 통합 대응
 - ▶ 24시간·365일 운영, 응답률 100%
 - ▶ 10분 이내 긴급 차단(알뜰폰도 번호 긴급차단)

- ◆ 불법스팸·악성앱 3중 차단 체계 구축
* ①문자사업자(IR-raj 도메인) ②통신사(악성 URL, 위변조 번호차단)
③휴대전화 단말기(악성앱 자동 차단)
- ◆ 불법개통시 통신사·대리점 등에 대해 제재 부과
(one strike-out)
- ◆ 외국인 여권 휴대전화 개통 1회선으로 제한

- ◆ AI 보이스피싱 탐지 앱으로 피해 예방
- ◆ AI 플랫폼 구축·활용 등을 통해 사전 범죄 예방

- ◆ 금융회사 등 실질적인 배상책임 법제화
- ◆ 금융회사 자체 대응역량 강화
* 금융회사별 범죄대응 인력·시설 확충
* 금감원의 금융사에 대한 관리·감독 강화
- ◆ 가상자산거래소 범죄계좌 규제 신설
* 지급정지 및 환급조치가 가능하도록 환급법 개정

- ◆ 「보이스피싱 대응TF」 신설(400여명 전담 수사)
- ◆ 보이스피싱 등 사기죄 처벌 강화
* 법정형 상향 및 가중처벌, 범죄수익 환수 강화



자기 평가하기

평가 내용	정답
▶ 다음 중 금융범죄에 해당하는 것은 무엇일까요? ① 중고거래 후 물건을 보내주지 않는 경우 ② 쇼핑물 배송 지연 ③ 은행 직원을 사칭하여 계좌번호와 인증번호를 요구하는 경우 ④ 게임 아이템 거래 사기	③
▶ 다음 중 금융범죄에서 제외되는 행위는 무엇일까요? ① 보이스피싱 ② 피싱 문자 ③ 해킹 ④ 기관사칭 금융사기	③
▶ 금융범죄의 핵심 특징으로 가장 알맞은 것은 무엇일까요? ① 사람을 속여 돈이나 개인정보를 빼앗는다 ② 컴퓨터 성능을 높여준다 ③ 인터넷 속도를 빠르게 한다 ④ 스마트폰 배터리를 절약한다	①
▶ 다음 중 정부가 시행 중인 대책으로 알맞은 것은 무엇일까요? ① 의심 전화번호 긴급 차단 ② 게임 이용시간 확대 ③ 무료 데이터 무제한 제공 ④ 스마트폰 가격 인하	①
▶ 2025년 기관사칭형 보이스피싱 피해가 많이 발생한 연령층은 어디일까요? ① 10대 ② 20~30대 ③ 40대 ④ 70대 이상	②

★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

02

금융범죄의 위험성 및 법적 책임

• 목 표 •

- 1 사이버 금융범죄의 위험성을 설명할 수 있다.
- 2 금융범죄가 개인·사회에 미치는 영향을 이해할 수 있다.
- 3 금융범죄 가담 시 법적 책임을 알 수 있다.

• 준비물 •

- 1 필기구 및 활동지
- 2 사례 자료 (프린트/PPT)
- 3 스마트폰 (사례 확인용)
- 4 토론 준비 메모
- 5 이어폰 (영상 시청 시)

• 핵심 사이트 •

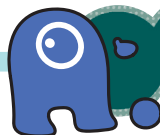
- 1 금융범죄는 개인·기업·국가 모두에 큰 피해
- 2 단순 피해를 넘어 심리적 후유증까지 발생
- 3 청소년도 범죄에 가담하면 처벌
- 4 “몰랐다”는 이유로 처벌을 피할 수 없음
- 5 계좌 제공, 전달책도 모두 공범이 될 수 있음

• 핵심 활동 •

- 금융범죄 피해 사례 읽고 감정 공유하기
- “피해자 vs 가담자” 입장 토론
- 판결 사례 보고 형량 예측하기
- 역할별(총책/수거책) 처벌 비교 활동
- “이건 범죄일까?” 상황 판단 퀴즈

• 핵심 키워드 •

- 금융범죄 피해
- 심리적 후유증
- 공범
- 법적 책임
- 사기죄
- 전자금융거래법



학습을 위한 사전준비

- ▶ 뉴스에서 본 사기 사례 떠올리기
- ▶ 아르바이트 경험 또는 관심 생각하기
- ▶ “쉽게 돈 버는 방법”에 대한 생각 정리
- ▶ 범죄와 처벌에 대한 기본 인식 정리



금융범죄의 위험성 및 법적 책임

★ 사이버 금융범죄의 유형

- 1 피싱이나 스팸메일을 통해 개인정보를 불법적으로 획득하여 금융범죄에 이용하는 경우
- 2 인터넷 쇼핑몰에서 결제를 위장해 타인의 돈을 가로채는 경우
- 3 악성프로그램 배포로 사용자의 컴퓨터를 감염시키고 이를 통해 정보를 빼내거나 시스템마비 시켜 금전을 요구하는 경우

★ 사이버 금융범죄가 미치는 영향

개인뿐만 아니라 기업과 국가에도 큰 영향을 미침

- 1 개인의 경우, 신용카드 정보나 계좌 정보가 유출될 경우 경제적으로 큰 타격을 받을 수 있으며, 심한 경우 그로 인해 개인의 신용이 손상되기도 함
- 2 기업 또한 고객데이터를 보호하지 못할 경우 막대한 법적 책임을 지게 되며, 이는 손실로 이어질 수 있음.
- 3 국가적으로는 정보 인프라가 공격받음으로써 국가 안보에 위협이 될 수 있어, 사이버 범죄의 심각성은 날로 증가하고 있음.

★ 금융범죄 피해자의 심리적 후유증

피해자는 "내가 어리석어서 당했다"는 자책감 때문에 신고를 꺼려하고, 범죄자들은 계속 활개치는 형태를 가짐

피해자 생각	실제 현실
"내가 멍청하게 당했다"	치밀하게 설계된 조직적 범죄
"가족한테 말하면 혼난다"	신고 지연 → 피해구제 기회 상실
"경찰에 가면 창피하다"	신고 안하면 범죄자만 이득
"얼마 안되는 돈인데..."	미신고가 반복 피해 유발

- 1 심리적외상(트라우마)-PTSD은 날로 증가하고 있음.
 - ① 재경험 → 피해 장면이 반복적으로 떠오름, 악몽
 - ② 과각성 → 잠 못 잠, 작은 자극에도 예민하게 반응
 - ③ 회피 → 은행, 스마트폰, 전화 자체를 피하게 됨
 - ④ 신체화 → 두통, 소화불량, 혈압 이상 등
 - ⑤ 자책 → "내 탓이야" → 우울증, 극단적 선택 위험

2 사례

- ❶ 보이스피싱으로 7억원을 피해 본 A씨 가족은 5일 만에 집을 급매로 내놓고 빚을 갚아야 하는 상황에 몰렸다. A씨는 "큰아이가 수험생이라 공부에 몰두해야 하는데 학원은커녕 문제집도 못 사줄 상황이다. 둘째가 김과 김치만 놓인 식탁을 보고 왜 '텅 비었어?'라고 말하자 눈물이 났다"며 막막함을 호소했다. 이들은 현재 월 800만원이 넘는 이자를 내고 있다.
- ❷ 굿네이버스 관계자는 "보이스피싱 피해를 입은 취약계층의 경우 회복하기 힘든 재산상 피해와 심리적인 어려움으로 극단적 선택까지 하는 사례가 발생하고 있다"며 긴급 생활비 및 심리 상담, 법률 상담 지원이 절실함
- ❸ 청소년이 직접 가담자(수거책 등)가 된 경우 → 전과 기록 → 학교 징계 → 학업 중단으로 이어지는 경우가 더 직접적 충격이 큼

3 지원기관 안내

기관	연락처	지원 내용
금융감독원	1332	피해금 환급, 심리 상담 연계
경찰청	112	즉시 신고 및 수사
굿네이버스 보이스피싱제로	홈페이지 신청	생활비·심리상담·법률상담지원
신용회복위원회	1600-5500	긴급자금 대출지원

★ 사이버 금융범죄 사례 및 판결

1 사례

- ❶ 열아홉 고등학생 둘, 친구딸 범죄 조직에
 - "네 계좌 주면 180만 원 벌 수 있어." 친구의 솔깃한 제안에 A는 선뜻 자신의 토스뱅크 계좌 정보를 넘겼다. 친구 B가 소개한 고수익 아르바이트의 정체는 자금세탁, 보이스피싱이었다. A 명의의 계좌는 보이스피싱 피해자들에게서 탈취한 돈이 송금되는 자금 통로로 쓰였다. 10대 계좌는 성인이 되는 순간 한도가 폭발적으로 늘어나는 '성장형 대표통장'으로 이용됩니다.
 - 판결 : 서울동부지법 형사합의12부는 전자금융거래법 위반과 통신사기피해환급법 방조 혐의로 기소된 A의 범죄수익금을 전액 추징하고 징역 10개월 형을 선고했다.
- ❷ 캔들포장 알바 공고 보고 보고 지원한 18세
 - 만 18세였던 A씨는 '캔들포장 알바 채용공고'를 보고 이력서를 제출 → 당장채용이 어려우니 다른 회사 사무보조 아르바이트 소개 → 의뢰인에게 돈을 전달받는 업무리며 세금문제로 100만원 씩 무통장 입금을 지시받음 → 보이스피싱 수거책으로 참여한 혐의로 기소됨
 - 판결 : 1심은 징역 1년 8개월, 집행유예 3년을 선고받았으나 항소심·대법원에서 '몰랐을 가능성'을 인정해 최종 무죄를 선고. 단, 수사·재판 과정 자체가 청소년에게 엄청난 심리적 충격임

③ SNS 대리입금 사기

- SNS를 통해 청소년을 대상으로 게임 아이템 구입비, 연예인 굿즈나 콘서트 티켓 구입비 등 주로 10만원 내외를 대신 납부해주고 '수고비'·'지각비'를 부과하는 불법 대부 행위로, 일부 피해자는 상환 압박과 개인정보 유출 피해까지 겪고 있다.
- 돈도 뺏기고, 개인정보도 빼앗겨 추가 협박·금융사기에 노출됨
- 피해금액이 500만원 이상일 경우 실형 선고 사례가 존재하며, 조직적 범행이나 피싱사이트 활용 시 정보통신망법 위반까지 병합 적용됨

④ 기타

유형	실제 사례	법적 결과	출처
기관사칭	검사 사칭 2400만원	국제 판결 + 환수 사기죄	한겨레신문
대출사기	9000만원 명의도용 피해자가 개인정보 및 인증정보 제공	피해자도 채무 부담 범죄자는 사기죄	뉴스토마토
가담자	현금수거 알바	벌금형	대법원
기업사기	착신전환 2억 피해	가중처벌 실형	파이낸셜뉴스
해외조직	필리핀 도피한 보이스피싱 조직 경찰이 전세기 투입해 49명 강제송환	실형	뉴스토마토

★ 사이버 금융범죄 법적 책임

1 보이스피싱 관련 처벌 수위

사기죄	10년이하 징역 또는 2천만원 이하 벌금
전자금융거래법	3년이하 징역 또는 2천만원 이하 벌금
통신기기 명의대여	1년이하 징역 또는 1천만원 이하 벌금
개인정보보호법	5년이하 징역 또는 5천만원 이하 벌금
특정경제범죄 가중처벌법 (피해액 5천만원~5억원이상)	3년이상 또는 무기징역 가능
범죄단체조직·가입	1년이상 10년이하 징역
통신기기이용 사기죄(2020년 개정)	반복적 통신수단 사기 가중처벌(최대 15년까지가능)

2 가담 유형별 형량 차이

- ① 총책/조직 운영자 → 실형 가능성 매우 높음
- ② 관리책/ 중간책 → 징역형 가능성 높음
- ③ 수거책/ 전달책 → 집행유예 ~실형까지 다양
- ④ 단순가담이라 하더라도 반복 참여나 금액이 클 경우 실형 가능성 높아질 수 있음

3 형량을 결정하는 주요 요소

- ① 피해 금액 규모, 범행 횟수 및 기간
- ② 조직내 역할, 범죄 인식 여부(고의성)
- ③ 피해 회복 여부(합의 여부)
- ④ 피해금액과 합의 여부는 가장 중요한 요소로 작용

4 감형 및 선처 가능성 요소

- ① 피해자와 합의 및 피해금 반환
- ② 초범 여부
- ③ 단순가담 여부
- ④ 반성문 및 재범 방지 노력
- ⑤ 수사 협조 여부
- ⑥ 피해회복이 이루어진 경우 형량에 큰 영향을 미침

5 주의해야 할 부분

- ① “몰랐다”는 주장만으로는 부족
- ② 단순 아르바이트라도 공범 인정 가능
- ③ 계좌 제공도 처벌대상
- ④ 조직 범죄로 가중처벌 가능성



자기 평가하기

평가 내용	정답
▶ 다음 중 사이버 금융범죄가 개인에게 미칠 수 있는 영향으로 가장 알맞은 것은 무엇일까요? ① 신용 상승 ② 경제적 손실과 신용 손상 ③ 휴대폰 성능 향상 ④ 인터넷 속도 증가	2
▶ 다음 중 금융범죄 피해자가 겪을 수 있는 심리적 후유증이 아닌 것은 무엇일까요? ① 불안과 악몽 ② 은행이나 전화 사용 회피 ③ 두통이나 수면장애 ④ 집중력과 자신감 증가	4
▶ 친구가 “계좌만 빌려주면 쉽게 돈 벌 수 있어”라고 제안했습니다. 가장 적절한 행동은 무엇일까요? ① 잠깐 빌려준다 ② 친구라서 믿고 제공한다 ③ 돈만 받으면 괜찮다고 생각한다 ④ 거절하고 위험성을 확인한다	4
▶ 다음 중 금융범죄 가담 시 법적 책임에 대한 설명으로 맞는 것은 무엇일까요? ① 청소년은 처벌받지 않는다 ② “몰랐다”라고 말하면 처벌되지 않는다 ③ 단순 전달책도 공범이 될 수 있다 ④ 계좌 제공은 범죄가 아니다	3
▶ 형량을 결정하는 요소로 가장 관련이 큰 것은 무엇일까요? ① 좋아하는 음식 ② 피해 금액과 합의 여부 ③ 휴대폰 기종 ④ 학교 성적	2

★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

03

금융범죄 발생 시 상황별 대응방법

• 목표 •

- 1 금융범죄 상황별 대응 방법을 구분할 수 있다.
- 2 금전 피해 발생 시 즉시 조치할 수 있다.
- 3 개인정보 유출 시 추가 피해를 예방할 수 있다.

• 준비물 •

- 1 스마트폰
- 2 필기구 및 활동지
- 3 수업자료 (프린트/PPT)
- 4 상황 카드 (활동용)
- 5 이어폰 (영상 시청 시)

• 핵심 사이트 •

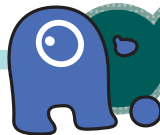
- 1 피해 인식 즉시 "지급정지"가 가장 중요
- 2 개인정보 유출 시 추가 피해 차단이 핵심
- 3 신고는 빠를수록 피해 회복 가능성이 높음
- 4 악성앱은 반드시 검사 후 삭제
- 5 상황에 따른 대응 방법

• 핵심 활동 •

- 상황별 대응 순서 맞추기 게임
- "이 상황에서 무엇을 먼저 할까?" 토론
- 신고 절차 역할극
- 피해 유형별 대응 카드 분류
- 나만의 대응 매뉴얼 만들기

• 핵심 키워드 •

- 지급정지
- 112 / 1394 신고
- 개인정보 유출
- 악성앱
- 명의도용
- 피해구제



학습을 위한 사전준비

- ▶ 금융사기 사례 떠올리기
- ▶ 문자·전화 경험 정리
- ▶ "돈 관련 위험 상황" 생각하기
- ▶ 앱 설치 경험 돌아보기



금융범죄 발생 시 상황별 대응방법

★ 금전피해 발생시

1 계좌 송금의 경우

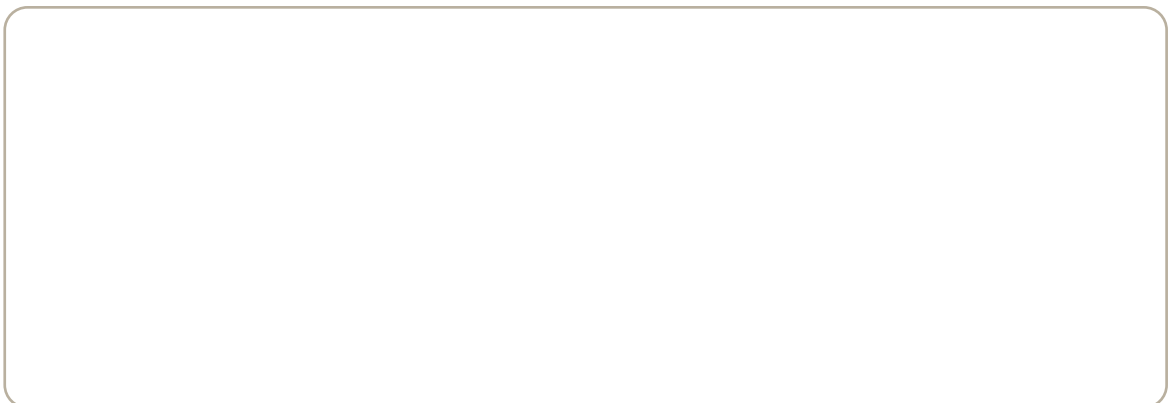
- ① 피해 인식 즉시 송금 또는 입금 금융회사 지급정지 콜센터로 계좌 지급정지를 요청
- ② 2차 피해 발생 예방을 위해 개인정보유출에 따른 명의도용 피해 예방법 조치 및 휴대전화 악성앱 검사 등 실시
- ③ 신분증과 피해를 입증할 수 있는 증거자료(송금내역서, 대화내역서 등)를 지참하여 신고자 주거지를 관할하는 경찰서에 사건 접수 후 '사건사고사실확인원' 발급
- ④ 지급정지를 신청한 금융회사를 방문하여 피해구제 신청서류 접수

2 대면편취의 경우

- ① 현장성이 있을 경우 :
- ② 즉시 112로 전화하여 경찰관 출동 요청
- ③ 현장성이 없을 경우 :
- ④ 2차 피해 발생 예방을 위해 개인정보유출에 따른 명의도용 피해 예방법 조치 및 휴대전화 악성앱 검사 등 실시 후 신분증과 피해를 입증할 수 있는 증거자료(통화기록화면, 대화내역서 등)를 지참하여 신고자의 주거지 관할 경찰서에 방문 신고

3 소액결제 피해의 경우

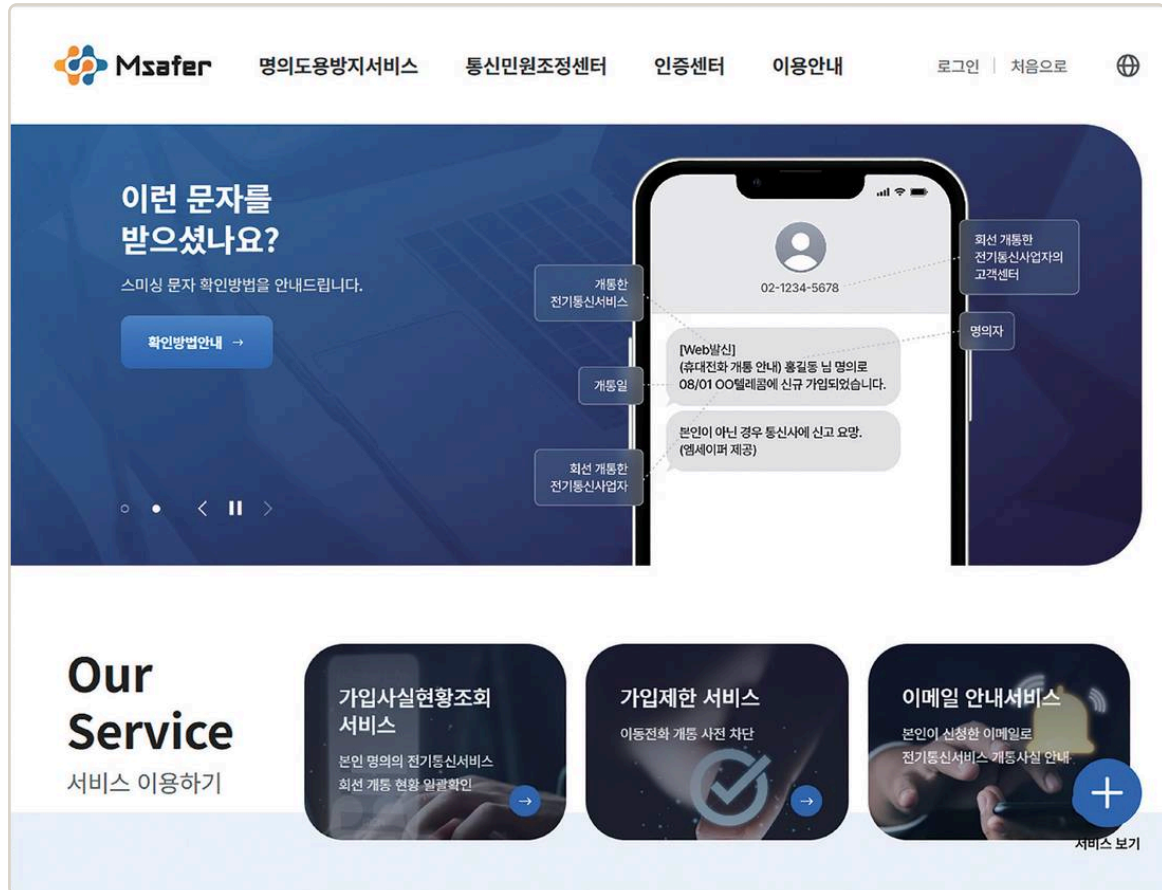
- ① 통신사로 소액결제 내역 확인 및 결제처 연락처 확인하여 유선으로 우선 환불 요청
- ② 2차 피해 발생 예방을 위해 개인정보유출에 따른 명의도용 피해 예방법 조치 및 휴대전화 악성앱 검사 등 실시
- ③ 신분증과 피해를 입증할 수 있는 증거자료(송금내역서, 대화내역서 등)를 지참하여 신고자 주거지를 관할하는 경찰서에 사건 접수 후 '사건사고사실확인원' 발급 받은 후 통신사·게임사·결제대행사 등에 환불 요청 접수



★ 개인정보 유출시

1 명의도용방지서비스(Msafer) 신청 및 조회

- ① 한국정보통신진흥협회 명의도용방지서비스(www.msafer.or.kr) 접속하여 공동인증서 인증으로 로그인(모바일 이용가능, 인증서 필요)



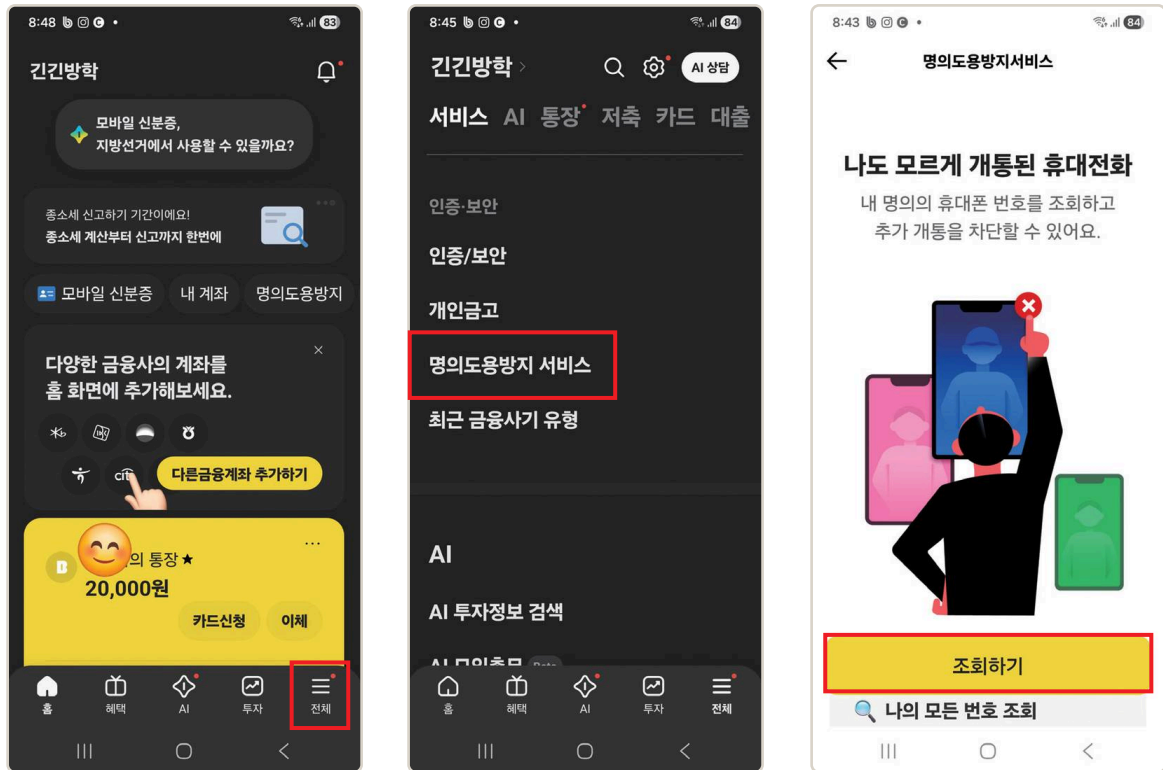
- '가입제한 서비스' 메뉴로 본인 명의의 휴대전화 신규 개설 차단
- '가입사실현황조회 서비스' 메뉴로, 본인 명의로 개설된 휴대전화 개설 여부를 확인
- 통신사의 지점 또는 직영점에 방문하여 신청 가능(신분증 지참 必)
- 이동통신사 지점은 1곳만 방문하여도 '일괄 이동전화 가입제한' 신청 가능
- 통신사 방문을 통한 가입사실현황조회는 각 통신사별로 확인(타사 정보에 대해 전산조회 불가, 3사 동일)

② PASS 앱 통해 신청/조회 가능

- PASS 앱 실행 ▶ 전체 ▶ 명의도용방지서비스 메뉴에서 신청/조회 가능
- 카카오톡 앱 통해 신청/조회 가능

③ 카카오톡 계좌 有 앱 실행 ▶ 로그인 ▶ 인증/보안 ▶ 명의도용방지서비스 메뉴 ▶ 조회하기

- 명의도용 휴대전화가 개통된 경우, 즉시 해당 이동통신사 등에 회선해지 신청 및 명의도용 신고
- 본인 명의의 통신서비스 가입현황 확인 및 통신서비스 가입 시 자동 안내



2 '번호도용차단', '소액결제(자동)차단 또는 한도 감액', '콘텐츠자동결제차단' 신청

- ① 이용 중인 통신사 고객센터(114) 또는 통신사 앱을 통해 신청
- ② 소액결제 원천차단의 경우 각 통신사별로 상이하므로 통신사로 문의
- ③ 번호도용 차단 서비스 신청 시 내 번호로 웹사이트를 통한 문자발송 차단 등 일부 제한되는 부분 있으므로 통신사 상담 후 신청

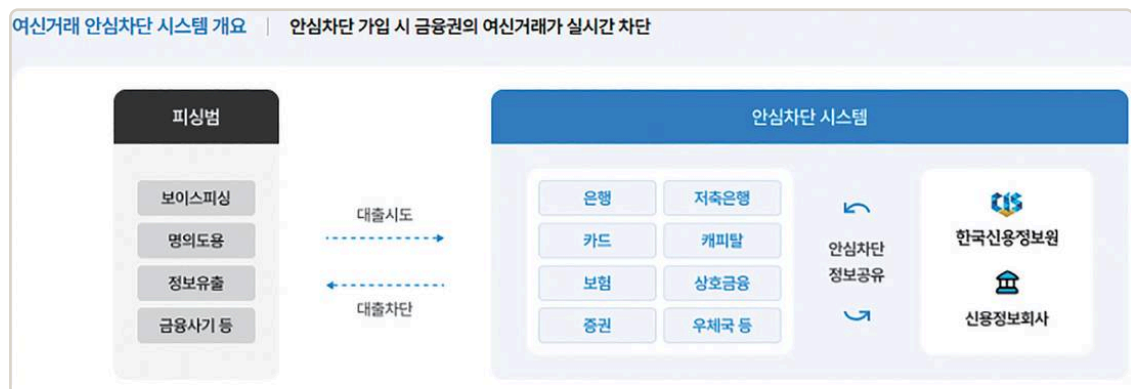
3 개인정보노출자 사고예방시스템 신청서비스 바로가기

- ① 금융감독원 개인정보노출자 사고예방시스템(<https://pd.fss.or.kr/>)에 접속하여 이용약관, 개인정보 제공 등 본인 인증 확인 후 '노출사실등록'을 신청

- ② 은행 지점에 직접 방문(신분증 지참 必)도 가능하고, 개인정보 노출자가 아니어도 신청이 가능하며 범죄에 취약한 부모님, 자녀들을 대신하여 등록 가능
- ③ 금융거래 시 엄격한 본인확인 절차를 거쳐 개인정보 유출로 인한 피해 예방 가능
- ④ '노출사실등록'된 개인정보는 금융회사에 공유되어 노출자 명의의 거래가 시도될 경우 일부 금융 거래가 제한될 수 있음
- ⑤ 신규계좌 개설, 신용카드 발급, 휴대전화 단말기 할부구입시 보증보험 가입등 노출사실 해제사유가 발생하거나 제한된 금융거래를 재개하고자 하는 경우 은행 방문 또는 홈페이지를 통해 등록 해제를 신청

4 여신거래 안심차단 신청

- ① 신용대출, 카드로, 신용카드발급, 예.적금 담보대출 등 모든 신규 여신거래차단
- ② 거래중인 은행 영업점 방문 또는 비대면(모바일/인터넷 뱅킹)으로 신청가능(단, 해제는 은행 방문만 가능)
- ③ 인터넷전문은행(카카오뱅크 등)은 해당 은행앱으로 신청 가능(단, 해제는 은행 방문, 거래실적 무관)



5 비대면 계좌개설 안심차단

- ① 수시입출식 계좌가 비대면으로 신규 개설되지 않도록 신청하는 서비스
- ② 거래 중인 금융회사를 직접 방문하거나, 모바일·인터넷뱅킹 또는 금융결제원(어카운트인포)를 통해 신청 가능



- ③ 해제는 가까운 금융회사 영업점을 방문하여 가능(기존 거래여부 무관, 신분증 必)
- ④ 본인신용정보열람서비스(<https://www.credit4u.or.kr:2443/>)에서 신청 내역 확인 가능
- ⑤ 신청 내역에 대해 반기 1회 문자 또는 이메일 등으로 주기적으로 통지

6 오픈뱅킹 안심차단서비스 신청

- ① 금융회사를 선택하여 오픈뱅킹 서비스를 사전에 차단하는 서비스
- ② 금융회사 영업점 또는 금융결제원 어카운트인포 앱 등을 통해 신청
- ③ 거래 중인 은행 영업점을 방문하거나 모바일·인터넷뱅킹 또는 금융결제원(어카운트인포 앱)을 통해 신청
- ④ 해제는 은행 영업점을 방문하여 가능
- ⑤ 신청 내역에 대해서는 주기적으로 통지(연1회 가입사실을 문자, 이메일 등으로 통지)

※ 'OO은행'을 차단 신청하면 'OO은행'계좌를 통한 간편송금/간편결제 서비스 이용불가, '경기지역화폐', '서울페이' 등 지역화폐 구매불가 등 주요 핀테크 오픈뱅킹 금융서비스에 제한이 발생할 수 있습니다. 자세한 사항은 금융결제원(1577-5500) 또는 거래중인 은행 영업점 또는 고객센터로 문의하시기 바랍니다.



7 신분증 재발급 신청

신분증이 유출되거나, 원격제어(www.teamviewer.com, www.helpu.kr 등) 및 악성 앱 설치로 인해 해킹 가능성이 있는 경우 조치

① 주민등록증 재발급

- <https://plus.gov.kr> 에서 재발급신청
- 주소지와 상관없이 가까운 동, 면, 읍 행정복지센터에 방문하여 신청 가능(사진 필요)
- 재발급 신청이 즉시 불가능할 경우에는 분실신고 우선진행

For Foreigners

어린이

시니어

지원

회원하기

정부24 AI

통합검색

로그인

회원가입

민원서비스

혜택알리미

생활

정책정보

고객센터

Home > 민원서비스

주인등록증 재발급 신청

이 페이지의 구성

서비스 개요

주인등록증 재발급 신청

서비스 개요

기본정보

신청 방법 및 절차

제출 서류

부가정보

정보 변경내역

신청하기

신청방법

인터넷, 방문

신청자격

법령상의 자격이 있는 자(제3자)

처리기간

총 14일

처리기간 계산 방법

신청서

주인등록증 재발급 신청서 (주인등록법 시행령 : 별지서식 32호)

신청작성예시

구비서류

있음 (하단 참조)

수수료

IC칩 미포함: 5,000원 // IC칩 포함: 10,000원

2 여권 재발급

- <https://plus.gov.kr> 에서 재발급신청
- 기존 여권발급 이력이 있는 18세 이상 우리 국민만 온라인 재발급 가능
- 위의 조건에 해당하지 않는 경우 가까운 여권사무대행기관에 직접 방문하여 신청
- 재외국민은 재외동포365(<https://www.g4k.go.kr>)에서 신청

For Foreigners

어린이

시니어

지원

회원하기

정부24 AI

통합검색

MyGOV

로그아웃

민원서비스

혜택알리미

생활

정책정보

고객센터

Home > 민원서비스 > 여권 재발급 온라인 신청

여권 재발급 온라인 신청

이 페이지의 구성

유효기간 만료 등 사유로 여권을 다시 발급받기 위해 신청하는 서비스

신청하기

어떤 내용인지 궁금하시죠?

지원대상

해당없음

지원내용

18세 이상 성인이 온라인을 통해 여권 재발급 신청을 하고 본인이 지정한 여권 사무대행기관에서 교부받는 서비스(수령기관 변경 불가)

이런 분들께 해당합니다.

지원대상

■ 기존에 전자여권을 한 번이라도 발급 받은 이력이 있는 18세 이상의 우리 국민

■ 아래 사유에 해당하는 경우 [정부24]에서는 신청이 불가하나, 가까운 여권사무대행기관에 직접 방문하여 신청하여 주시기 바랍니다.

- 만 18세 미만 미성년자
- 생애 최초 전자여권 신청자
- 외교관 · 관공 · 간접 여권 신청자
- 로마자성명 변경이 필요한자(혼인관계 변동으로 배우자 성명 변동이 발생한자 포함)
- 개당 및 주민등록상보 장성지(개량 및 주민등록상보 장성 후 여권발급이력 존재 시 신청 가능)
- 영상 재발급, 상습 분실자
- 여권 신청일 기준 유효기간이 남은 여권을 소지하고 있는 자로 5년 이내 1회 이상 분실이력이 있는 자

분야별 서비스 Best 5

1 여권 재발급 온라인 신청

2 여권 발급 이력 조회

3 여권정보증명서(국문) 발급

4 여권 발급 상태 조회

5 여권 분실 신고

기관별 서비스 Best 5

1 해외안전여행 대박생 서포터스 ...

2 외교부 소식지 제공 서비스

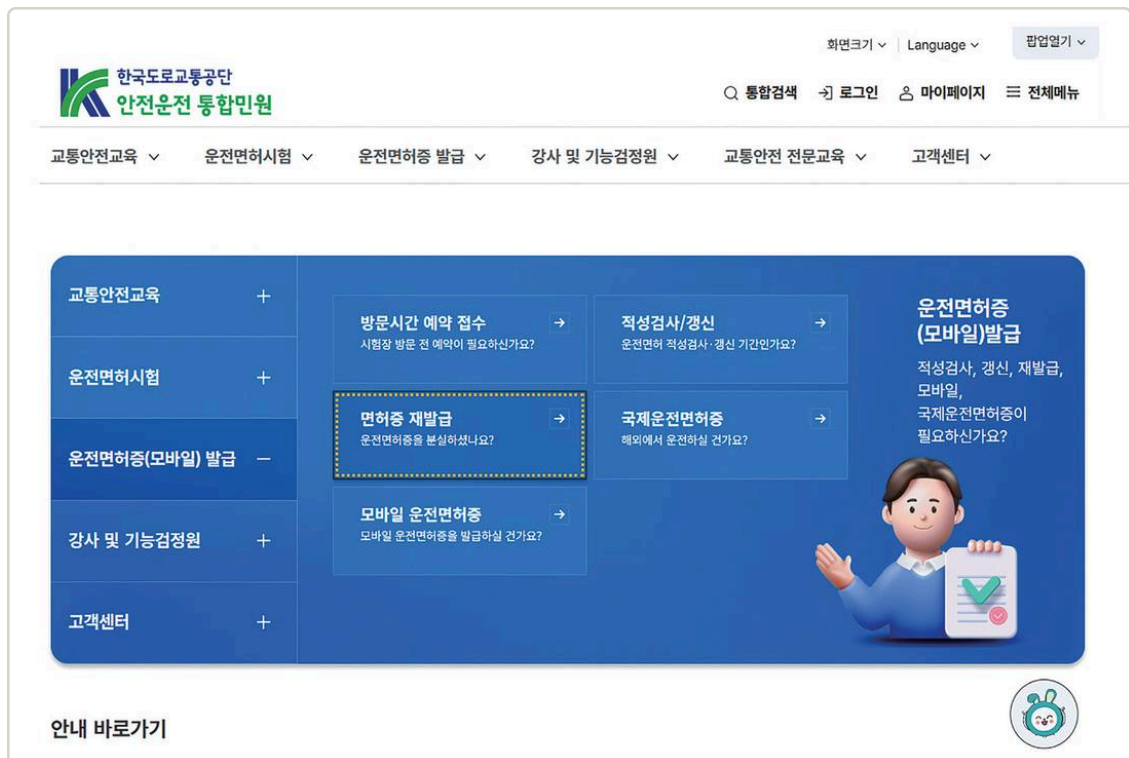
3 여권 유효기간 만료일 사전알림 ...

4 여권정보증명서(국문) 발급

5 해외여행 등록제 증명

136 • 행복시코딩스쿨 _ 디지털 금융과 보안

3 운전면허증



- <https://www.safedriving.or.kr> 에서 재발급 신청
- 기존 면허증 분실 여부에 “예”를 반드시 선택해야 기존 면허증 정보가 폐기됨
- 운전면허시험장 및 경찰서 민원실에 방문하여 신청 가능(강남경찰서 제외)
- 재발급 신청이 즉시 불가능할 경우에는 경찰민원콜센터로 분실신고 가능
- 모바일 운전면허증의 경우 도로교통공단에 등록된 면허정보와 연동되므로 단순 분실신고 시 모바일 운전면허증 화면에서 ‘유효하지 않은 면허증’문구가 확인되어 사용불가

여권

정부24(www.gov.kr)에 접속하여 민원서비스에서 여권 재발급 온라인 신청 메뉴 클릭하여 민원신청 가능

* 잔여 여권기간에 따른 재발급 비용과 기본 구비서류가 신청인에 따라 상이할 수 있으므로 영사콜센터(02-3210-0404)로 문의해야 함

운전면허증

도로교통공단 안전운전 통합민원(www.safedriving.or.kr)에 접속하여 면허증 발급 > 면허증 재발급 메뉴 클릭하여 실명인증 후 신청

* 간편인증·공동인증·휴대폰인증·디지털원패스 중 택1 가능

- 기존면허증 분실 여부에 “예”를 반드시 선택해야 기존 면허증 정보가 폐기됨
- 운전면허시험장(근무시간내 3시간) 및 경찰서(총15일) 민원실에 방문하여 신청 가능(강남경찰서 제외)
- 재발급 신청이 즉시 불가능할 경우에는 경찰민원콜센터로 분실신고 가능
- 모바일 운전면허증의 경우 도로교통공단에 등록된 면허정보와 연동되므로 단순 분실신고 시 모바일 운전면허증 화면에서 ‘유효하지 않은 면허증’ 문구가 확인되어 사용 불가

8 기존 공동인증서 폐기·재발급

- 1 원격제어(www.teamviewer.com, www.helpu.kr 등) 및 악성 앱 설치로 인해 해킹 가능성이 있는 경우 조치

- ② 기존 사용중인 공동인증서는 인증서를 발급 받은 은행을 통해 즉시 폐기하고, 재발급을 받아 사용
▶ 해당 은행의 인터넷뱅킹 접속하여 인증센터 ▶ 인증서폐기 메뉴

9 본인이 개설하지 않은 명의도용된 계좌·카드·대출 개설 여부 조회

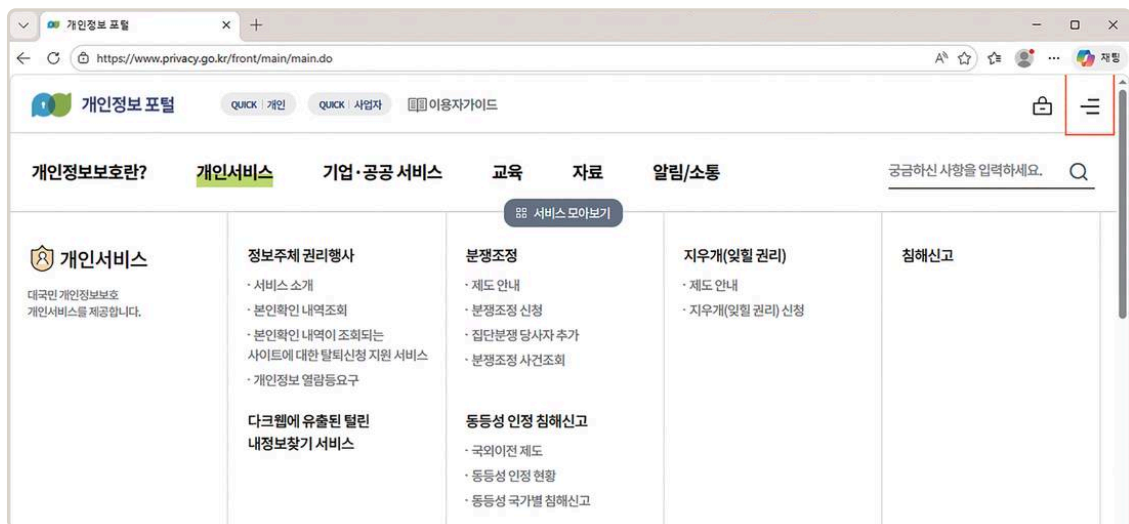
- ① 금융결제원 계좌정보통합관리서비스(www.payinfo.or.kr) 접속하여 주민번호 입력, 인증서 로그인 후 휴대전화 인증으로 본인 확인



- ② '내계좌한눈에' '내카드한눈에' '금융정보조회' 메뉴 클릭하여, 본인명의로 개설된 예금·카드·대출 계좌 상세내역 확인
- ③ 명의도용 계좌 개설 및 비대면 대출이 실행된 경우, 즉시 해당 금융회사에 피해사실 신고 및 지급 정지 신청
- ④ 어카운트인포 계좌정보통합관리 앱을 통해서도 조회 가능

10 본인 내역 확인 및 가입된 웹사이트 조회

- ① 개인정보 포털(<https://www.privacy.go.kr>) 접속하여 '개인서비스 ▶ 정보주체 권리행사' ▶ 본인 확인내역이 조회되는 웹사이트에 대한 탈퇴 지원 서비스

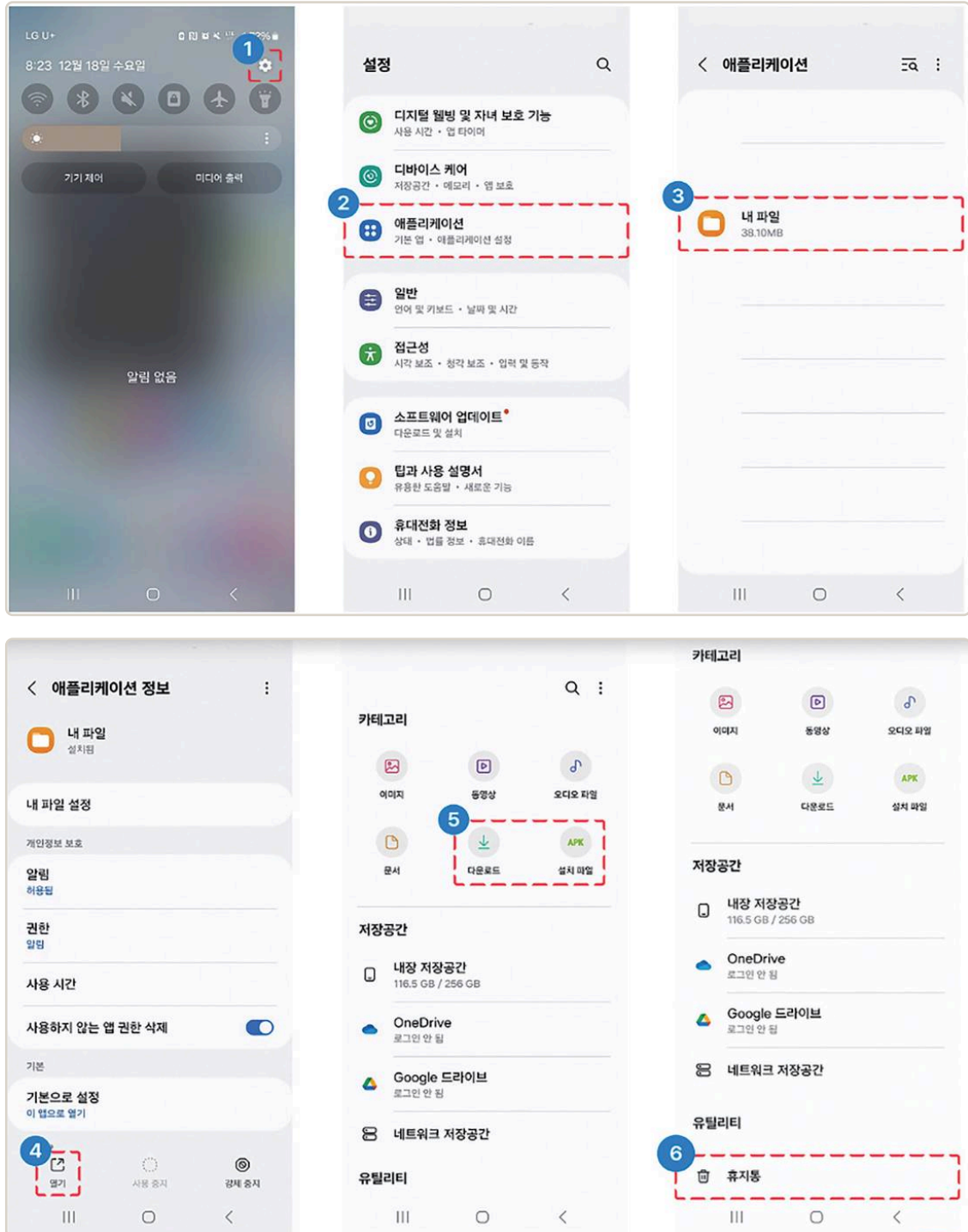


- ② '본인확인 내역 통합 조회' 서비스 이용을 위한 개인정보 수집·이용에 동의가 필요
- ③ 본인확인 절차 후 실명인증을 진행해야 이용 가능
- ④ 본인 명의의 ①간편인증 ②공동인증서 ③아이핀 ④휴대폰 ⑤신용카드 중 택1
- ⑤ 가입된 웹사이트 조회 결과는 탈퇴 신청 가능과 불가능으로 구분되며, 불가능의 경우 해당 사이트로 직접 회원 탈퇴 신청을 해야 함

★ 악성링크 접속 및 악성앱 설치 시

1 악성 애플리케이션 설치파일 유무 확인 후 삭제

- ① 구글 안드로이드 : 파일관리자 또는 내파일의 '다운로드' 'APK설치파일' 카테고리에서 확인 및 삭제 후 휴지통 비우기 실행



② 애플 iOS : 파일 앱의 다운로드에서 확인 및 삭제

- 부고장.apk m부고장.apk efine.apk govkorea.apk kca.apk 000 live.apk 등

2 검증된 모바일 백신으로 악성코드 검사 및 삭제

- 구글 안드로이드 : Play스토어에서 다운로드 가능(알약, V3등)
- 애플 iOS : iOS용 바이러스 백신

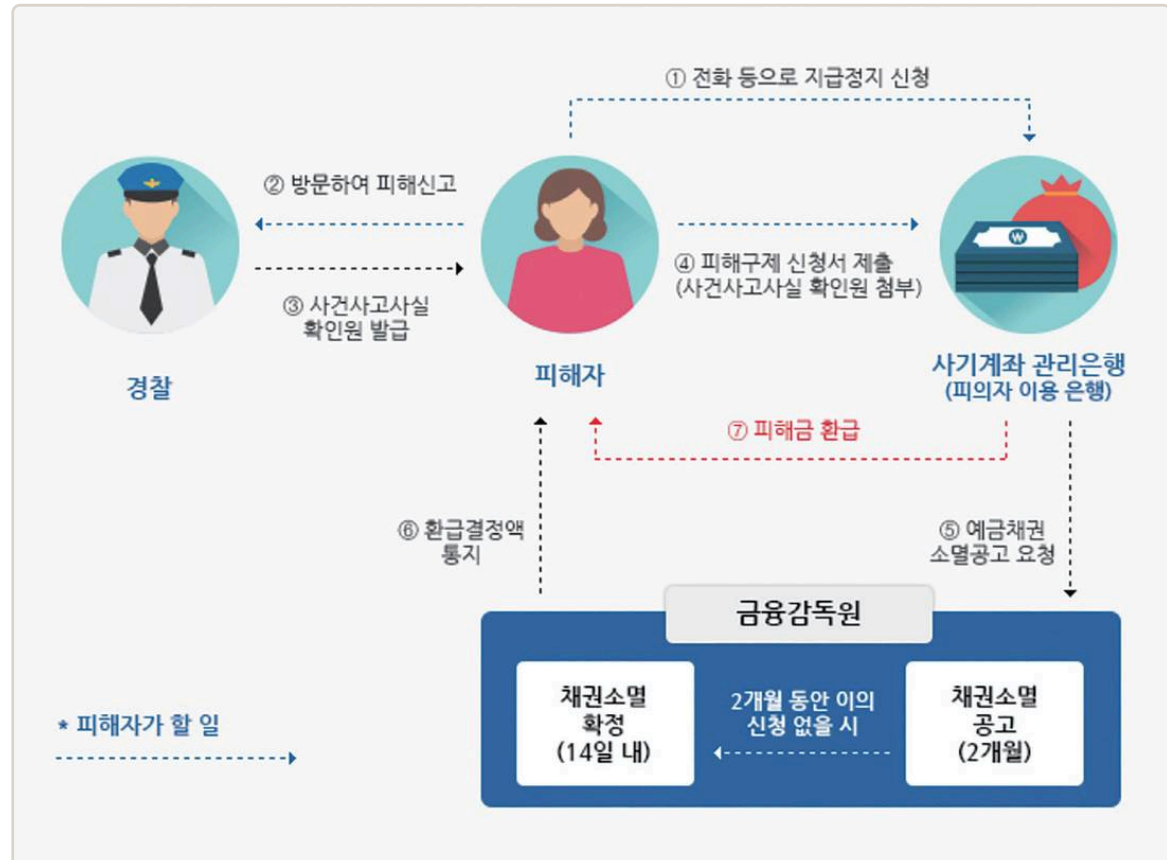
3 2차 피해를 예방하기 위해 개인정보유출에 따른 명의도용 피해 예방조치 실시

- ① 악성 설치 파일(.apk) 또는 악성앱이 확인된 경우에는 개인정보유출에 따른 명의도용 피해 예방조치를 실시하여 2차 피해를 예방해야 합니다.
- ② 피싱범과의 통화기록, 문자 내용, 카카오톡 대화 내용 등을 캡처하여 보관 후 제조사 서비스센터를 방문하여 초기화를 진행한 후 사용하는 것이 안전합니다.

★ 유형별 피해구제 절차

1 보이스피싱

- ① 피해자는 범죄에 이용된 계좌를 관리하는 금융회사에 전화로 지급정지를 신청. 전화로 하는 경우 3일 이내에 지급정지에 필요한 서류(사건사고사실확인원, 피해구제신청서)를 제출
- ② 피해자는 거주지 관할경찰서(사이버수사팀)에 방문하여 피해사실을 신고하고
- ③ 신고를 접수한 경찰관에게 요청하여 '사건사고사실확인원'을 발급
- ④ 피해자는 지급정지를 신청한 금융회사를 방문하여 '피해구제신청서'를 작성해서 '사건사고사실확



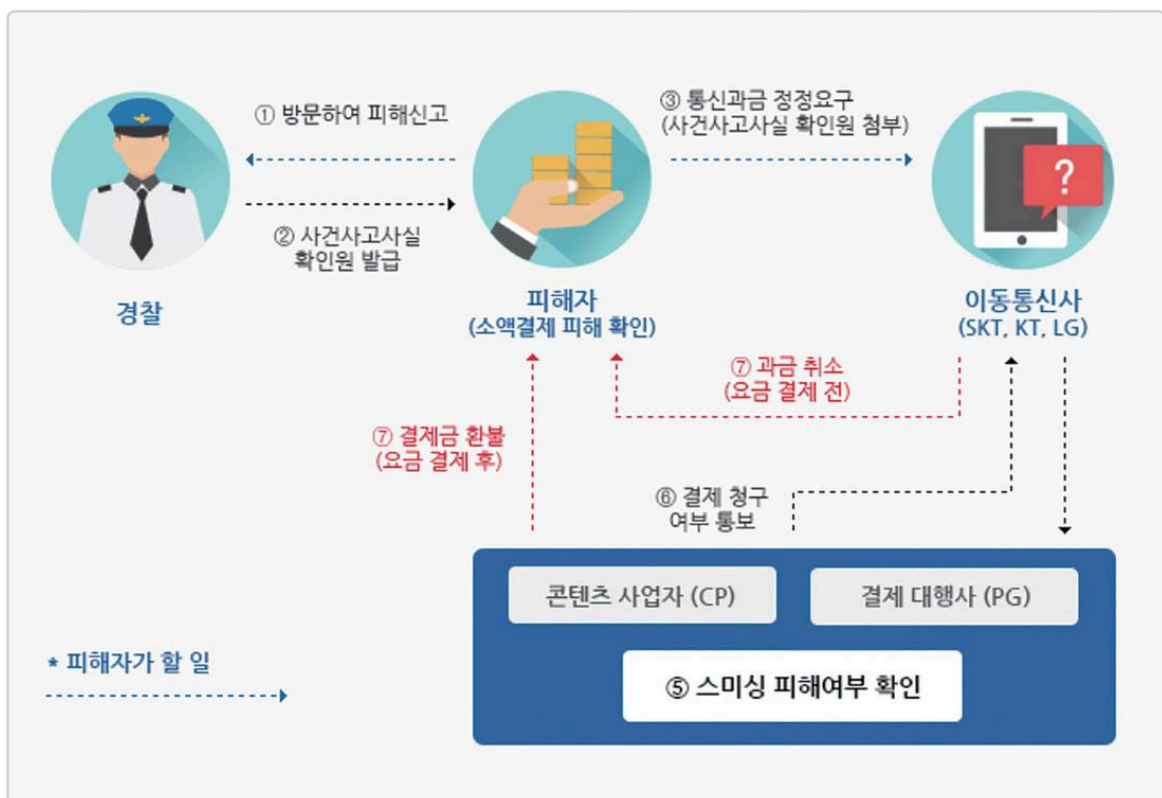
출처 : 사이버범죄 신고시스템 피해자 구제 제도

인원'과 함께 제출

- ⑤ 금융회사는 신청된 계좌에 대하여 지급정지 조치를 취하고 금융감독원에 예금채권 소멸공고를 요청
- ⑥ 금융감독원은 2개월간 채권소멸공고를 하고 이 기간 내에 이의신청이 없으면 채권소멸을 확정하고 환급결정액을 금융회사에 통지
- ⑦ 위 환급결정액이 금융회사에 통지되면 금융회사에서는 피해자에게 해당 금액을 환급(통상 2~3일 소요)
- ⑧ 유의할점
 - 피해구제절차를 통한 환급은 범죄에 이용된 계좌에 잔액이 남아 있을 경우에 가능
 - 잔액이 남아 있지 않고 전부 인출된 경우에는 피의자를 대상으로 별도의 민사소송 진행
 - 또한 범죄에 이용된 계좌에 남아 있는 잔액과 비교하여 피해자가 많고 각 피해자의 피해금액의 합계가 잔액보다 큰 경우에는 피해자별로 피해금액 전부를 환급받지 못할 수 있음

2 스미싱

- ① 통신요금 청구서 등을 통해 본인이 직접 결제하지 않은 소액결제 건을 확인하면 소액결제 내역을 지참하여 가까운 경찰서 사이버수사팀을 방문하여 피해사실을 신고합니다.
- ② 신고를 접수한 경찰에게 요청하여 '사건사고사실확인원'을 발급받습니다.
- ③ 피해자는 본인이 가입한 이동통신사 고객센터를 방문하여 통신요금 정정요구를 하면서 '사건사고사실확인원'과 함께 제출합니다.
- ④ 이동통신사는 결제대행사와 콘텐츠사업자에게 해당 결제청구에 대한 보류 또는 취소를 요청하고,



출처 : 사이버범죄 신고시스템 피해자 구제 제도

- ⑤ 결제대행사와 콘텐츠사업자는 상호 협의하여 청구된 내용에 대해 스미싱 사기 여부를 확인하게 되고
- ⑥ 스미싱에 의한 피해로 판명되면 콘텐츠사업자는 이동통신사에 소액결제 청구를 취소한다고 통보합니다.

- ⑦ 피해자가 통신요금을 아직 납부하지 않은 경우라면 이동통신사에서 피해자에게 소액결제를 제의시킨 통신요금 청구서를 다시 발급하게 되고, 피해자가 이미 통신요금을 납부한 경우라면 콘텐츠사업자가 피해자에게 결제된 소액결제 대금을 환불해 주게 됩니다.

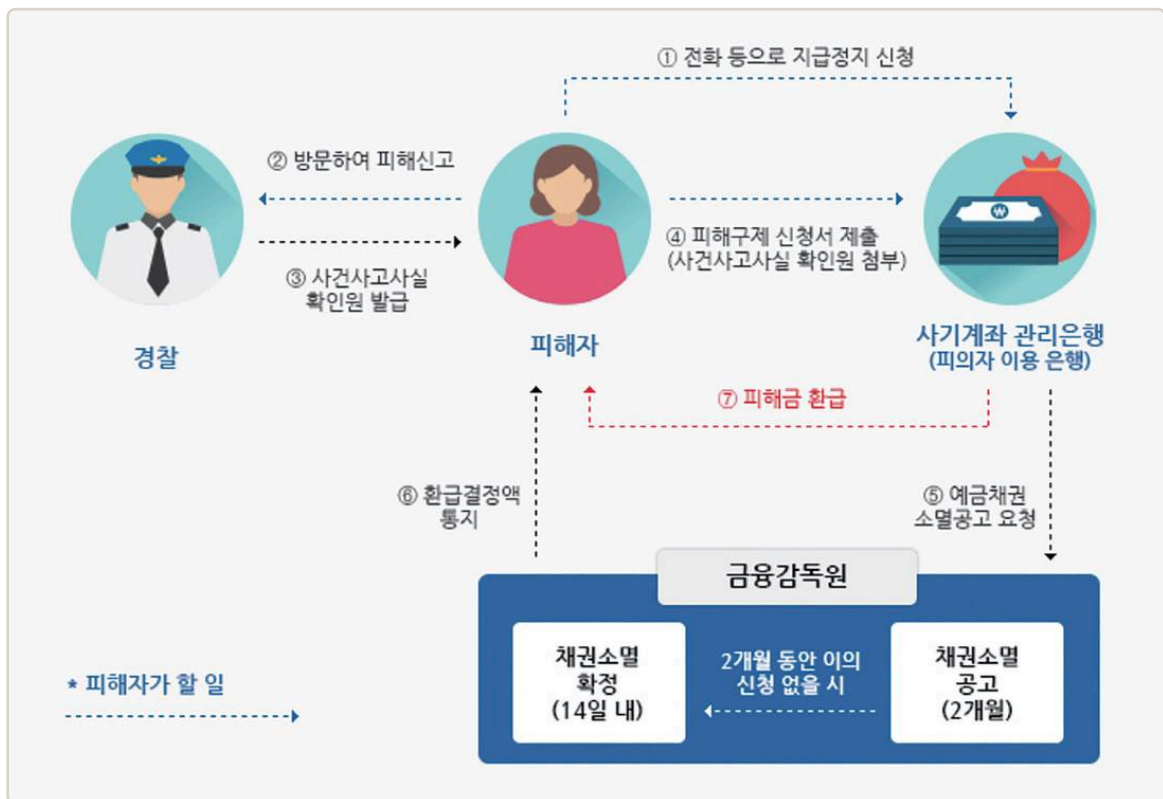
※ 피해자가 이동통신사에 통신요금 정정요구를 한 시점부터 소액결제 환불결정이 완료되기까지 통상 14일 정도 소요됩니다.

※ 유의할점

- 스미싱에 의한 소액결제에 의한 피해구제는 통신요금으로 과금된 소액결제금에 대하여 이의를 제기하였을 때 통신사가 아닌 결제대행사와 콘텐츠 제공사가 협의하여 “결제금청구 취소 여부”를 결정하는 것으로
- 스미싱에 의한 범죄피해가 아닌 “콘텐츠 구매 후 번심으로 인한 소액결제 환불 요청”이나 “스미싱에 의한 범죄피해가 아닌 경우”에는 구제되지 않음

3 파밍

- ① 피해자는 범죄에 이용된 계좌를 관리하는 금융회사에 전화로 지급정지를 신청합니다. 전화로 하는 경우 3일 이내에 지급정지에 필요한 서류(사건사고사실확인원, 피해구제신청서)를 제출해야 합니다.



출처 : 사이버범죄 신고시스템 피해자 구제 제도

- ② 피해자는 거주지 관할경찰서(사이버수사팀)에 방문하여 피해사실을 신고하고
- ③ 신고를 접수한 경찰관에게 요청하여 '사건사고사실확인원'을 발급받습니다.
- ④ 피해자는 지급정지를 신청한 금융회사를 방문하여 '피해구제신청서'를 작성해서 '사건사고사실확인원'과 함께 제출합니다.
- ⑤ 금융회사는 신청된 계좌에 대하여 지급정지 조치를 취하고 금융감독원에 예금채권 소멸공고를 요청합니다.
- ⑥ 금융감독원은 2개월간 채권소멸공고를 하고 이 기간 내에 이의신청이 없으면 채권소멸을 확정하고 환급결정액을 금융회사에 통지합니다.
- ⑦ 위 환급결정액이 금융회사에 통지되면 금융회사에서는 피해자에게 해당 금액을 환급하여 주게 됩니다. (통상 2~3일 소요)

※ 유의할 점

- 피해구제절차를 통한 환급은 범죄에 이용된 계좌에 잔액이 남아 있을 경우에 가능.
- 잔액이 남아 있지 않고 전부 인출된 경우에는 피의자를 대상으로 별도의 민사소송 진행
- 또한 범죄에 이용된 계좌에 남아 있는 잔액과 비교하여 피해자가 많고 각 피해자의 피해금액의 합계가 잔액보다 큰 경우에는 피해자별로 피해금액 전부를 환급받지 못할 수 있음.



자기 평가하기

평가 내용	정답
▶ 금전 피해를 인식했을 때 가장 먼저 해야 할 행동은 무엇일까요? ① 휴대폰 배경화면 변경 ② 지급정지 신청 ③ 앱 삭제 ④ 친구에게 알리기	2
▶ 피싱 링크를 눌렀고 개인정보 유출이 의심되는 상황입니다. 가장 적절한 행동은 무엇일까요? ① 아무 일 없었던 것처럼 계속 사용한다 ② 휴대폰을 친구에게 맡긴다 ③ 전원을 끄거나 비행기 모드로 전환한다 ④ 문자만 삭제한다	3
▶ 다음 중 개인정보 유출 시 추가 피해 예방 방법으로 알맞지 않은 것은 무엇일까요? ① 명의도용방지 서비스 신청 ② 여신거래 안심차단 신청 ③ 공동인증서 재발급 ④ 비밀번호를 친구와 공유하기	4
▶ 악성앱 설치가 의심될 때 해야 할 행동은 무엇일까요? ① 그대로 사용한다 ② 앱 검사를 실시하고 삭제한다 ③ 휴대폰을 숨긴다 ④ 배터리를 충전한다	3
▶ 다음 금융범죄 대응 절차를 올바른 순서로 나열하세요. (가) 지급정지 신청 (나) 피해구제 신청 (다) 비행기모드 전환 (라) 피해금 환급	다 - 가 - 나 - 라

★ 학습활동을 통해 느낀 점이나 새롭게 궁금해진 내용들을 적어보자.

저 자 조 한 진 (극동대학교 소프트웨어학과 교수)

이 세 종 (영남대학교 컴퓨터학부 조교수)

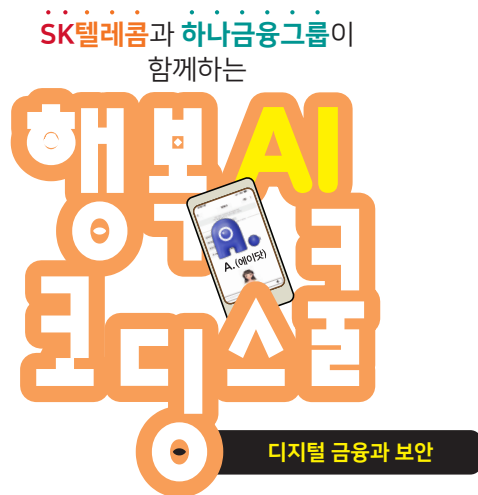
SK텔레콤 지속가능경영실 SV추진팀

하나금융그룹

감 수 이 윤 준 (KAIST 전산학과 명예교수)

• 행복SI코딩스쿨 참여 그룹 •

- | | | |
|------------|--------------|---------------|
| • SK텔레콤(주) | • 하나생명보험 | • 하나펀드서비스 |
| • 하나금융지주 | • 하나손해보험 | • 하나금융티아이 |
| • 하나은행 | • 하나저축은행 | • 하나벤처스 |
| • 하나증권 | • 하나자산신탁 | • 핑크 |
| • 하나카드 | • 하나대체투자자산운용 | • (사)SW교육혁신센터 |
| • 하나캐피탈 | • 하나에프앤아이 | |



발 행 처 SK텔레콤, 하나금융그룹, (사)소프트웨어교육혁신센터(SWKOREA)

인 쇄 일 2026년 08월 15일

발 행 일 2026년 08월 31일

디자인 · 인쇄 제이케이디자인(010-2269-1428)

ISBN 979-11-90695-27-5 43500

※ 이 교재는 저작권법에 의해 보호를 받는 저작물이므로 SK텔레콤(주), 하나금융그룹, (사)SW교육혁신센터의 동의 없이는 무단 전재와 복제를 포함한 어떠한 형태나 수단으로도 이 책의 내용을 이용할 수 없습니다.