

이용자 개인정보보호 교육

2013년 0월 00일



방송통신위원회
KOREA COMMUNICATIONS COMMISSION

KISA

한국인터넷진흥원
Korea Internet & Security Agency

목 차



I. 개인정보보호의 이해

II. 개인정보 침해유형과 대응법

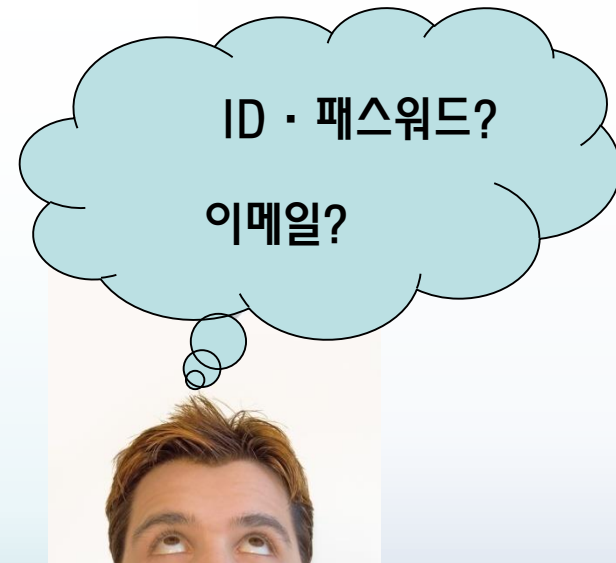
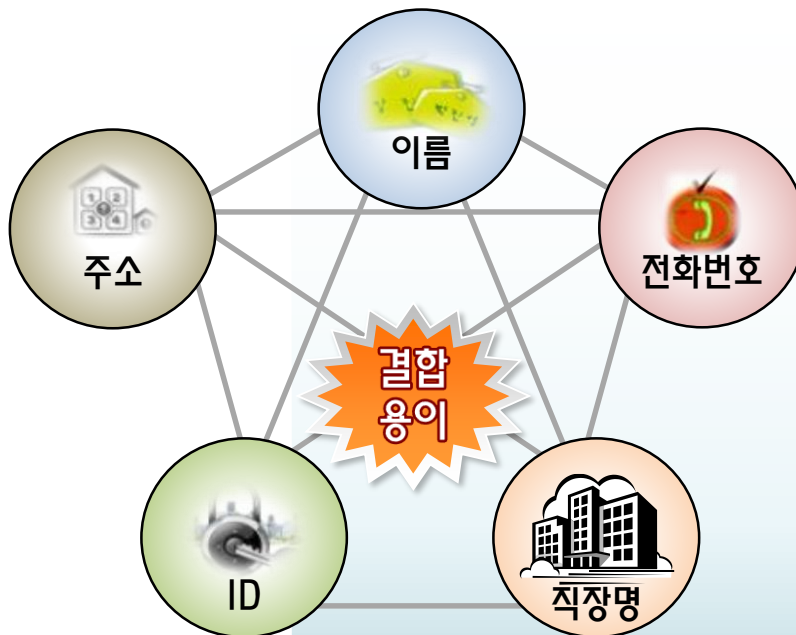
III. 이용자 개인정보보호 수칙

IV. 청소년 셧다운제



I . 개인정보보호의 이해

- ➔ ① 생존하는 개인(自然人)에 관한 정보
- ② 개인에 대한 사실 · 판단 · 평가 등 개인에 관한 모든 정보
- ③ 해당 정보만으로는 특정 개인을 식별할 수 없으나 다른 정보와 용이하게 결합하여 특정 개인을 식별 가능한 경우



개인의 인권

개인의 내외면, 사회관계, 권리를 나타내는
인권적 가치 (개인정보 자기결정권)



기업의 영업자산

고객의 정보를 수집 · 활용하여 영업
활동 및 수익창출



사회의 핵심요소

공공 · 민간 서비스, 기업경영 등 대부분의
사회 활동이 개인정보를 기반으로 이루어짐



I - 3. 최근 5년간 주요 개인정보 유출 사례

이용자 개인정보보호 교육



I - 4. 개인정보 유출 경로





II. 개인정보 침해유형과 대응법



“개인정보를 낚아 올린다”는 뜻으로 음성(voice)+개인정보(Private Data)+낚시(Fishing)를 합성한 신조어

➡ 기망행위로 타인의 재산을 편취하는 사기범죄의 하나로 전기통신수단을 이용한 비대면거래를 통해 금융 분야에서 발생하는 일종의 특수사기범죄



II - 2. 보이스피싱 - 보이스피싱은 어떻게 이루어지나

이용자 개인정보보호 교육



사기이용계좌 확보

예금통장 매입, 대출 등 미끼로 편취

전화 · 문자메시지 시도

해외(중국 등)콜센터에서 국내로 전화

기망 · 공갈

개인정보 유출, 범죄사건 연루 등으로 기망

계좌이체

송금 · 이체유도 또는 사기범이 직접 이체

인출 · 송금

현금인출책 · 송금책을 통해 해외송금

1. 자녀 납치 및 사고 빙자 편취

2. 메신저 상에서 지인을 사칭하여 송금을 요구

3. 인터넷 뱅킹을 이용해 카드론 대금 및 예금 등 편취

4. 금융사, 금감원 명의 허위 긴급공지 문자메시지로 피싱사이트 유도

5. 전화통화를 통해 텔레뱅킹 이용정보를 알아내어 금전 편취

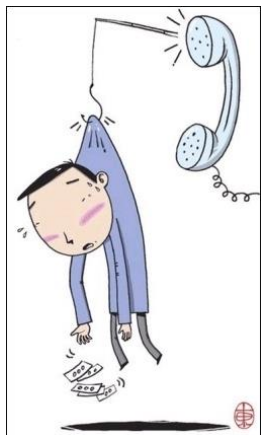
6. 피해자를 기망하여 자동화기기로 유인 편취

7. 피해자를 기망하여 피해자에게 자금을 이체토록 하여 편취

8. 신용카드정보 취득 후 ARS를 이용한 카드론 대금 편취

9. 상황극 연출에 의한 피해자 기망 편취

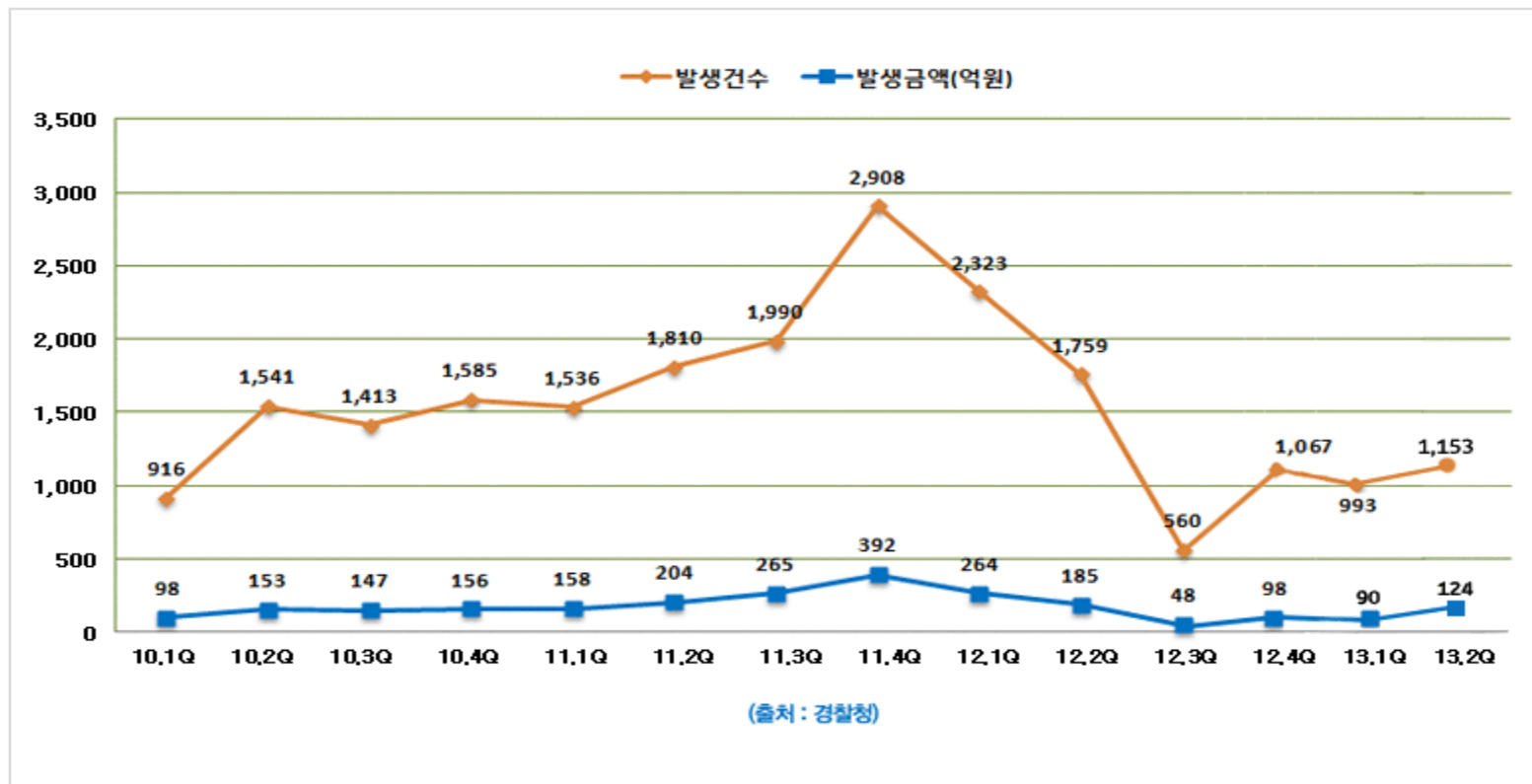
10. 물품대금 오류송금 빙자로 피해자를 기망하여 편취



❖ 피해 현황 (2006년 6월~2013년 3월)

○ 피해 건수 : 42,197건

○ 피해 금액 : 4,420억



II - 4. 보이스피싱 - 예방 요령 (2)

1

전화로 개인정보 유출, 범죄사건 연루 등을 이유로 계좌번호, 카드번호, 인터넷뱅킹 정보를 묻거나 인터넷 사이트에 입력을 요구하는 경우 절대 응하지 말아야 할 것

2

세금, 보험료 등을 환급해 준다거나 계좌안전조치를 취해주겠다면서 현금지급기로 유인하는 경우는 100% 보이스피싱

3

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

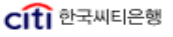
4

개인·금융거래정보를 미리 알고 접근하는 경우에도 내용의 진위를 확인

5

보이스피싱을 당한 경우 경찰청 112콜센터 또는 금융회사 콜센터를 통해 신속히 사기계좌에 대해 **지급정지**를 요청할 것

▶ 은행 및 관련기관 콜센터 번호

금융회사명	전화번호	금융회사명	전화번호
 우리은행	1588-5000 , 1599-5000	 제주은행	1588-0079
 Standard Chartered	1588-1599	 전북은행	1588-4477
 하나은행	1588-1111 , 1599-1111	 경남은행	1588-8585
 KEB 외환은행	1588-3555	 KDB산업은행	1588-1500
 신한은행	1544-8000	 IBK기업은행	1588-2588
 citi 한국씨티은행	1588-7000	 NH농협은행	1588-2100 , 1544-2100
 KB 국민은행	1588-9999 , 1599-9999	 수협중앙회	1588-1515
 DGB대구은행	1588-5050	 신협	1566-6000
 BS부산은행	1588-6200	 우정사업본부	1588-1900
 광주은행	1588-3388 , 1600-4000	 새마을금고	1599-9000



▶ 경찰청(국번없이 112) : 보이스피싱 피해신고 및 지급정지 요청

KISA

▶ 한국인터넷진흥원(국번없이 118) : 금융기관 등을 사칭한 스팸메시지 신고 및 피싱사이트 차단*

* [피싱 사고신고 바로가기](#) > 피싱사이트 발견 즉시 인터넷을 통해 홈페이지 차단 신고가 가능



▶ 대한법률구조공단(국번없이 132) : 보이스피싱 피해금 반환을 위한 민사소송절차 안내

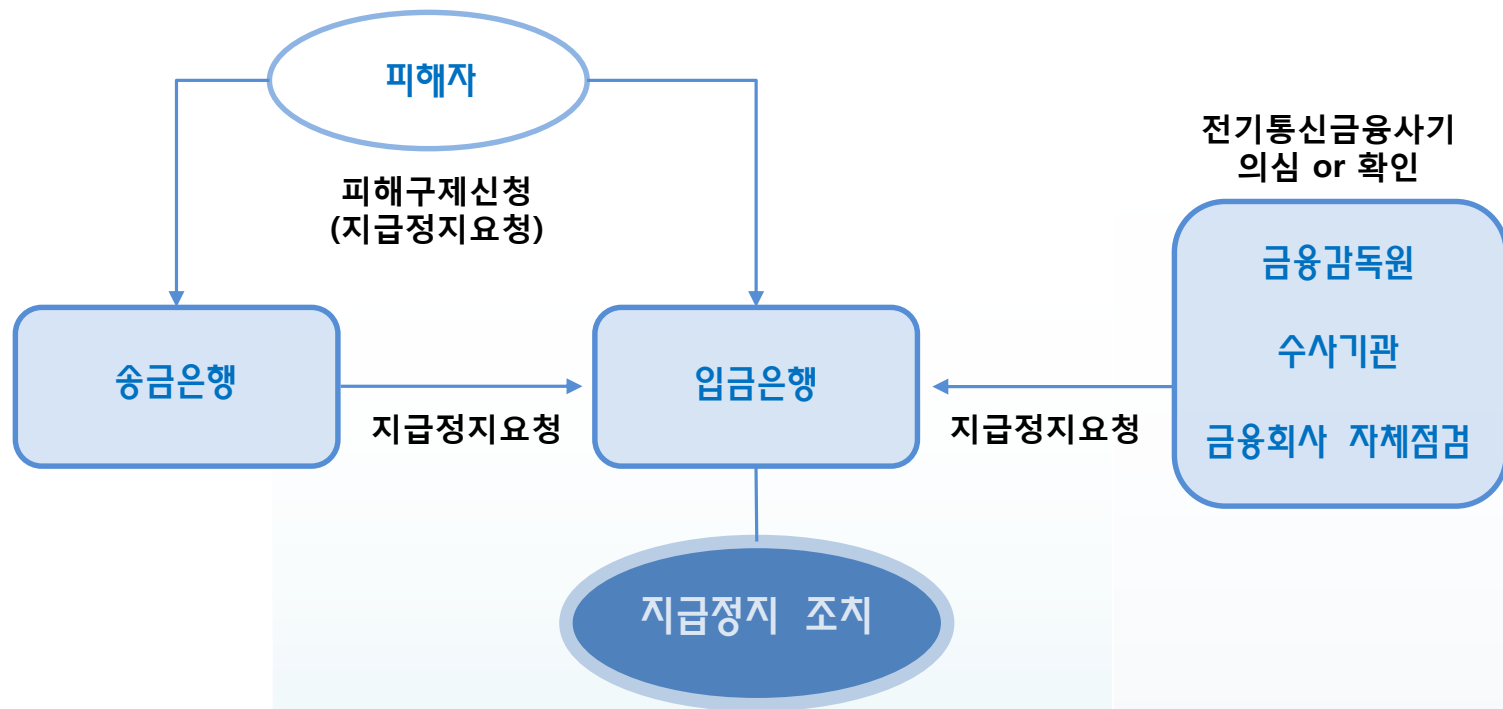
금융회사는 「전기통신금융사기 피해금 환급에 관한 특별법」 제4조에 의거 거래내역 등의 확인을 통하여 전기통신금융사기의 사기이용계좌로 의심할 만한 사정이 있다고 인정되면 해당 사기이용계좌의 전부에 대하여 지급정지 조치를 하여야 함



주요 내용의 통지 : 금융회사는 지급정지 조치 후 이와 관련한 주요내용을 피해자 및 명의인에게 서면통지 등의 방법으로 통지하여야 함

- 통지사항지급정지의 일시, 사유 및 금액 등에 관한 사항
- 사기이용계좌에 관한 사항 (지급정지와 관련된 점포, 예금종별 및 계좌번호 등)
- 지급정지를 요청한 금융회사에 관한 사항

< 지급정지 요청 흐름 >



II - 4. 보이스피싱 - 예방 요령 (2)

6

유출된 금융거래정보는 즉시 해지하거나 폐기

7

통장이나 현금(체크)카드 양도 시 범죄에 이용되므로 어떠한 경우에도 타인에게 양도 금지

8

발신 (전화)번호는 조작이 가능함에 유의

9

문자메시지, 이메일 등으로 수신된 금융회사 및 공공기관의 홈페이지는 반드시 인터넷 검색 등을 통해 정확한 주소인지 확인

10

2012.9.25일부터 각 은행에서 시범 시행하는 「전자금융사기 예방서비스」 적극 활용

II - 3. 파밍 - 파밍(Pharming)이란

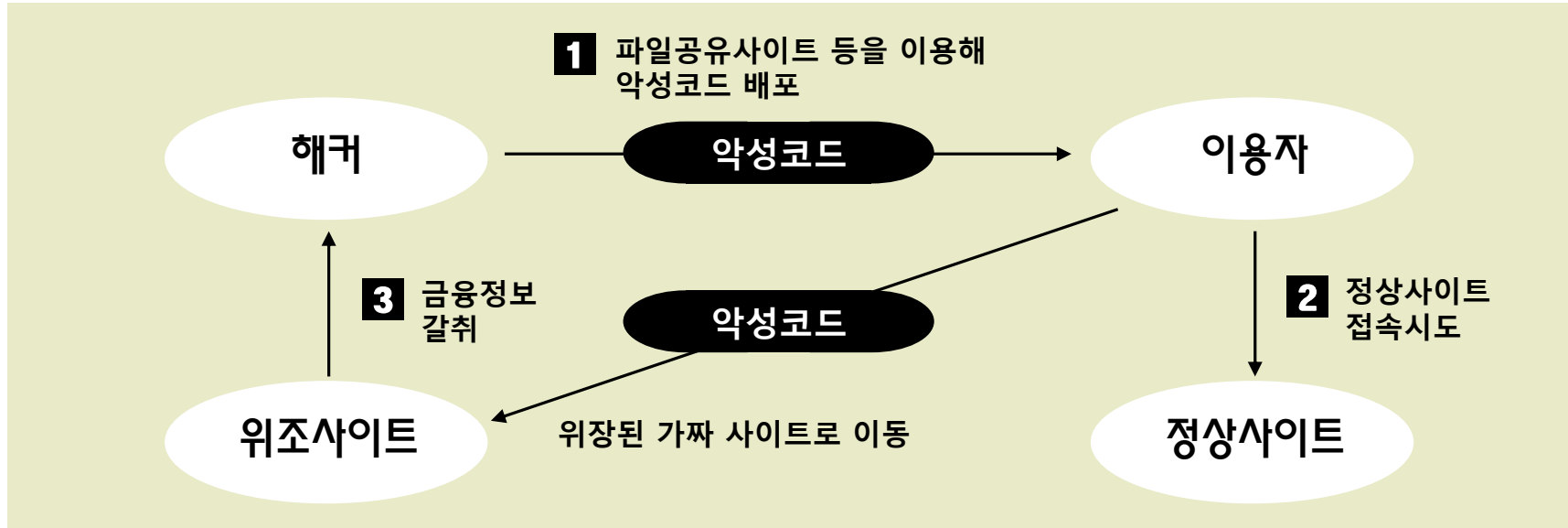
사용자의 PC를 악성코드로 감염시킨 다음 정상적인 은행 주소를 넣어도 사기꾼들이 만든 사기 사이트로 연결되어 금융정보를 빼내는 수법



<진짜 웹사이트>



<가짜 웹사이트>



※ 피싱(Phishing) 4대 유형

- 보호형 : 금융정보 유출 등을 막아주겠다며 유인
- 협박형 : 가족을 납치했다는 식으로 공갈협박
- 사칭형 : 지인으로 행세하며 접근, 급전이나 교통사고 합의금 요구
- 보상제공형 : 세금을 환급해준다고거나 경품에 당첨됐다고 유인

1 출처가 불분명한 동영상 · 이메일은 악성코드 감염 우려가 있으므로 다운로드 자제

2 보안카드 코드표 전부 입력을 요구하는 경우, 가짜 은행사이트로 판단되므로 반드시 확인 후 사용

3 백신 프로그램을 설치하고 ‘파밍캡’ 프로그램으로 검사



① “1”과 같이 “비정상”으로 뜨는 항목이 있다면 “3”의 “제거” 버튼을 누른 후 사용하고 있던 웹브라우저 창을 모두 닫고 다시 실행할 것

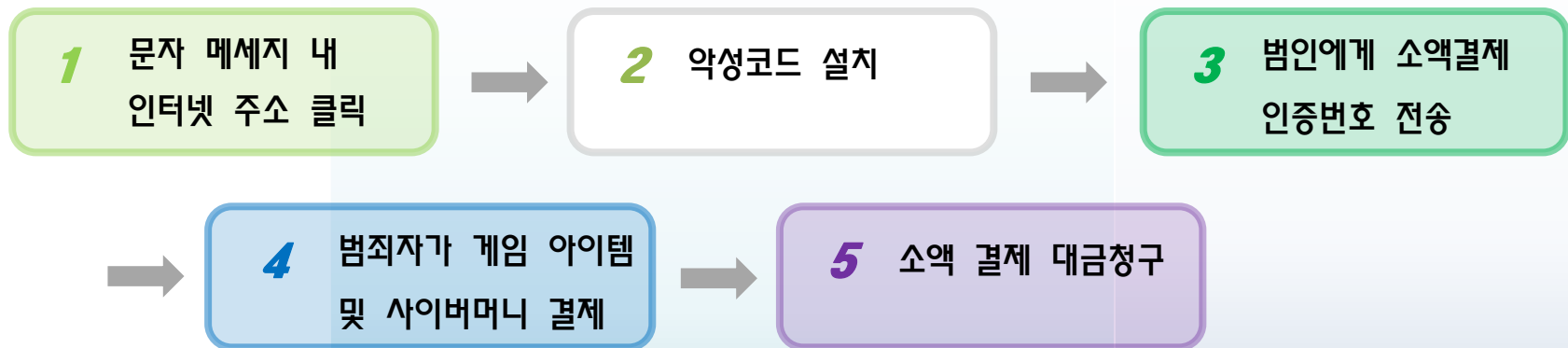
② “2”에서 보이는 것과 같이 모든 금융 사이트가 “정상”이라면 정상적인 금융거래가 가능하며 “닫기” 버튼을 누르면 됨

II - 4. 스미싱 - 스미싱(Smishing)이란

SMS와 Phishing의 결합어로 문자메시지를 이용하여 피싱하는 방법을 말함. 웹사이트 링크가 포함된 문자 메시지를 보내 휴대폰 사용자가 링크를 클릭하면 트로이목마를 주입해 범죄자가 휴대폰을 통제할 수 있게 함

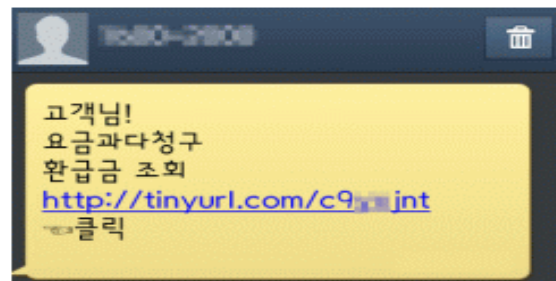
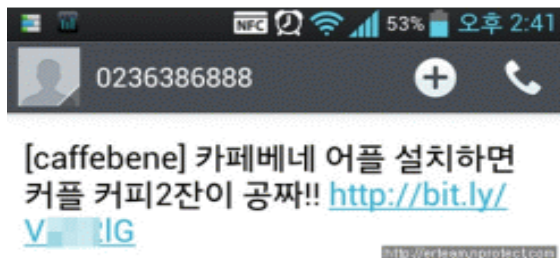
➡ 이러한 압축파일을 열면 컴퓨터는 개인정보를 빼가는 악성코드에 감염 → 모니터화면은 물론 키보드 입력내용까지 실시간으로 유출

❖ 사기 과정



2012년 말부터 집중적으로 발생한 스미싱 사건은 ‘무료쿠폰 제공, 모바일 상품권 도착, 스마트명세서 발송’ 등을 비롯하여 최근에는 정부기관을 사칭하거나 안드로이드 업데이트’ 등의 내용으로 진화

❖ 스미싱 범주에 이용된 문자메시지





각 통신사 고객센터에 전화하거나 통신사 인터넷 홈페이지를 이용하여 소액결제를 원천적으로 차단하거나 결제금액을 제한

※ 소액결제 차단 방법

	통신사	고객센터를 통한 소액결제 차단방법
1	SKT	1) 자신의 스마트폰으로 114로 통화버튼을 눌러 SKT고객센터로 연결 2) '3'번을 눌러 상담원과 연결 3) 소액결제 모두 차단
2	KT	1) 100을 눌러 '5'번, 그리고 '1'번을 순차적으로 눌러 KT 모바일 고객센터로 연결 2) 상담원과 통화하여 오프라인결제·무선결제·청구대행·본인인증차단 등을 선택적으로 신청하여 소액결제 차단 ※ 자신의 스마트폰으로 114를 눌러 상담원과 연결해도 소액결제 차단 가능
3	LGU+	1) 자신의 스마트폰으로 114를 눌러 전화를 하면 LGU+고객센터로 연결 2) '0'번을 눌러 상담원과 연결 3) 자동결제·인증결제 모두 차단

2

스마트폰용 백신프로그램을 설치하고 주기적으로 업데이트하여 악성코드 설치 차단

※ 환경설정 → 보안 → 알 수 없는 출처에 체크를 “해제”

3

확인되지 않은 앱(App)이 함부로 설치되지 않도록 스마트폰의 보안설정을 강화

※ **스마트폰 보안설정 강화방법** : 환경설정 > 보안 > 디바이스 관리 > ‘알 수 없는 출처’에 V체크가 되어 있다면 해제

4

쿠폰, 상품권, 무료, 조회, 공짜 등으로 스팸 문구를 미리 등록하여 내 스마트폰에 스미싱 문자가 전송되는 것을 사전에 차단

※ **스마트폰내 스미싱 문자발송 차단방법** : 문자메시지로 들어가서 ‘설정 > 스팸 메시지 설정 > 스팸 문구로 등록’ 클릭

5

T스토어 · 올레마켓 · U+앱마켓 등 공인된 오픈마켓을 통해 앱(App)을 설치

6

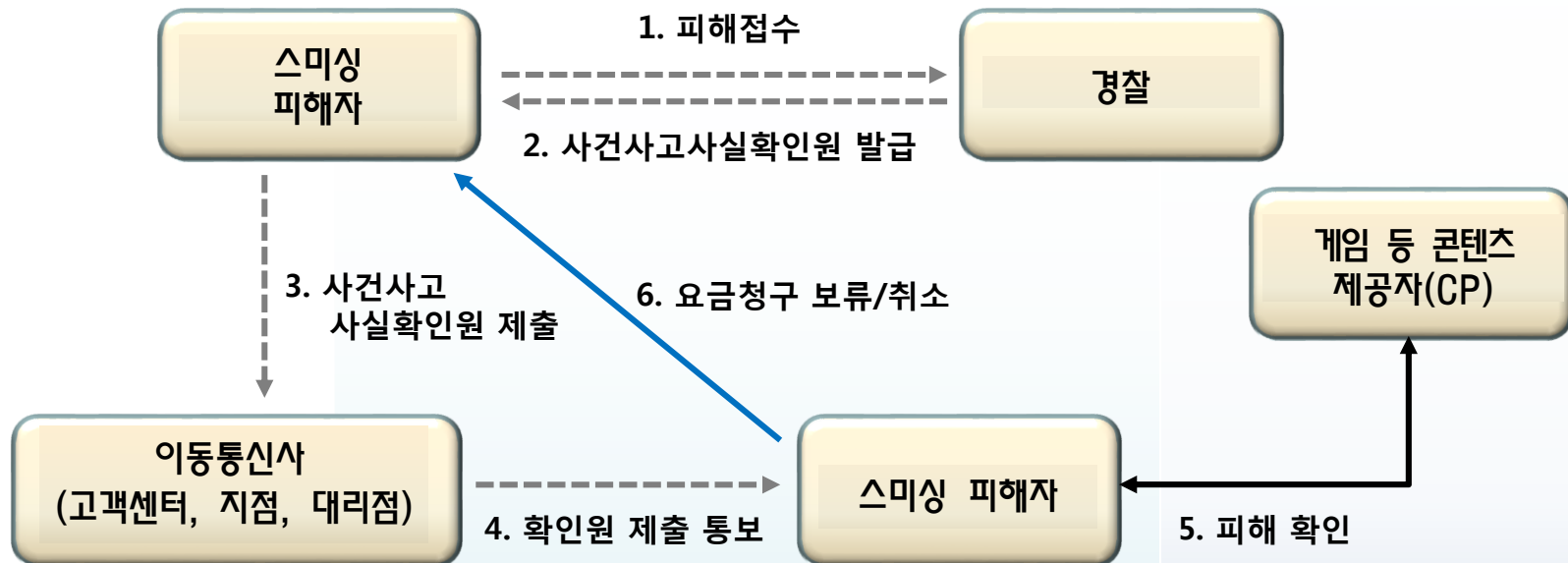
출처가 확인되지 않은 링크를 클릭하지 않도록 하고, 인터넷상에서 apk파일을 다운받아 스마트폰에 저장하지 말 것

II - 4. 스미싱 - 피해구제

경찰서(☎112)에 신고
하여 스미싱 피해 확인서
(사건사고 사실 확인원)
발급 요청



발급받은 '사건사고 사실확인원'을 이동통신사,
게임사, 결제대행사 등 관련 사업자에 제출하면
결제 청구를 보류, 취소하거나 이미 결제된
피해액을 돌려받을 수 있음

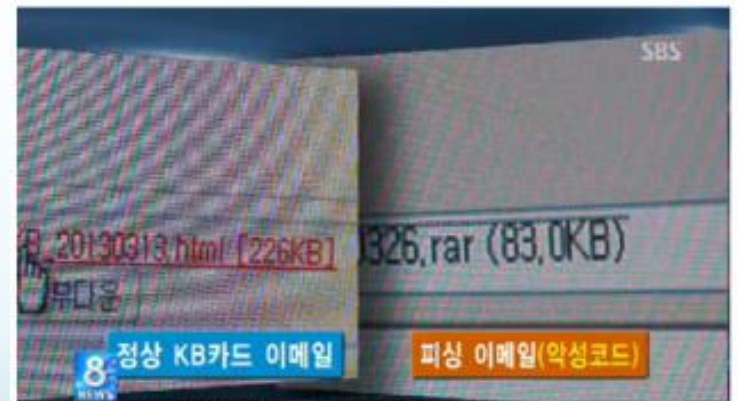


이메일 첨부파일 종류가 일반 웹페이지와 같은 html파일이 아닌 압축파일(악성코드) 형태로 첨부



이러한 압축파일을 열면 컴퓨터는 개인정보를 빼가는 악성코드에 감염 → 모니터화면은 물론 키보드 입력내용까지 실시간으로 유출

- 정상 KB카드 이메일 : KB_20130313.html (226KB)
- 피싱 이메일(악성코드) : **KB_20130313.rar (83.0KB)**



1

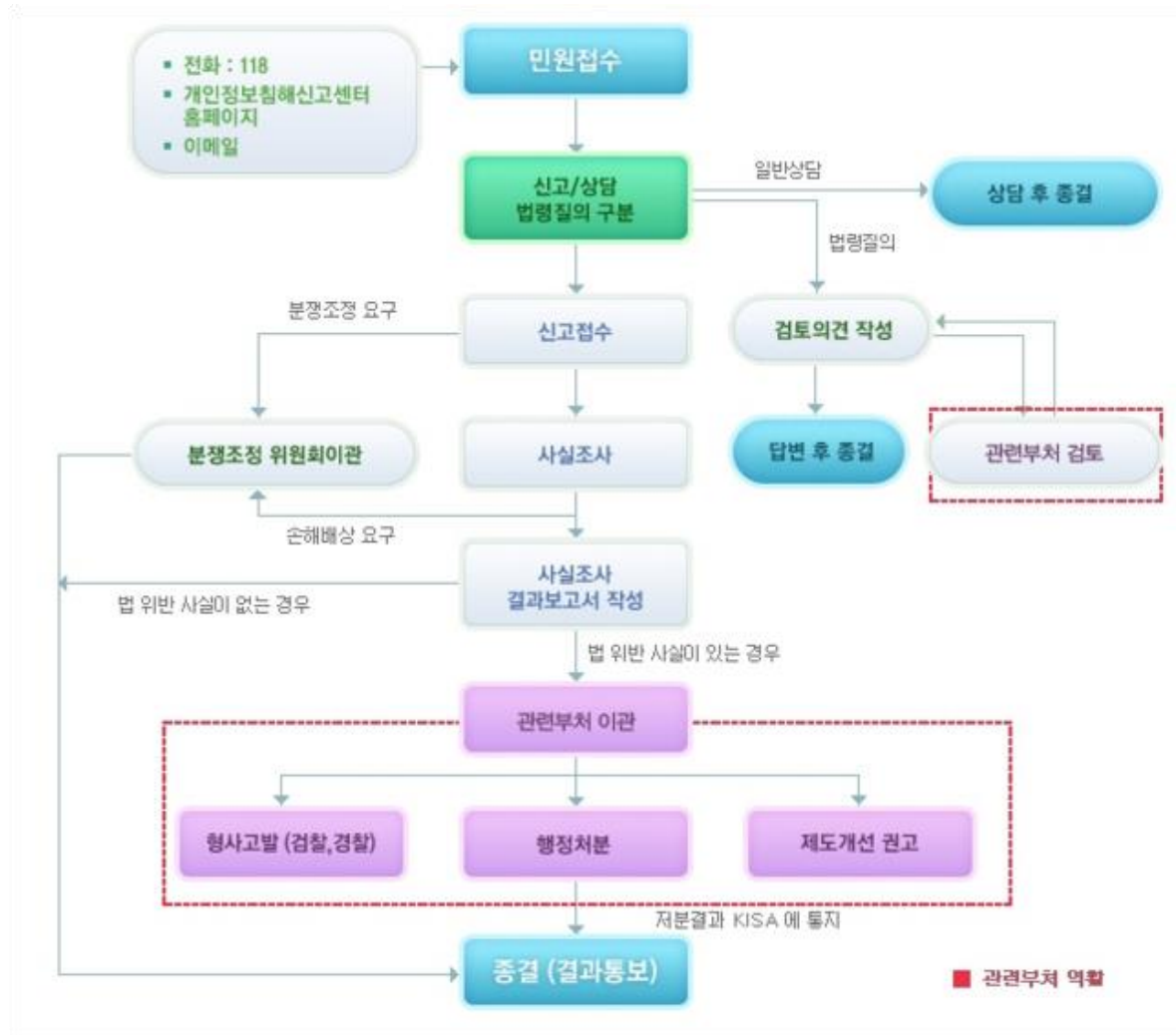
압축파일 zip, rar 첨부 등 평소와 다른 제목 개인정보 보안카드 번호 등 요구하는 메일은 무시하고 삭제

2

이것도 저것도 불안하다면 해당 카드사의 홈페이지에 직접 접속해 거래명세를 확인하거나 우편으로 명세서를 받아보는 것이 안전



[참고] 개인정보 침해 신고 절차





III. 이용자 개인정보보호 수칙

III - 1. 개인정보 오남용 피해예방 10계명 (1)



01 회원가입을 하거나 개인정보를 제공할 때에는 개인정보취급방침 및 약관을 꼼꼼히 살핍니다

02 회원가입시 비밀번호를 타인이 유추하기 어렵도록 영문/숫자 등을 조합하여 8자리 이상으로 설정합니다

03 가급적 안전성이 높은 주민번호 대체수단(아이핀:i-PIN)으로 회원가입을 하고, 꼭 필요하지 않은 개인정보는 입력하지 않습니다

04 자신이 가입한 사이트에 타인이 자신인 것처럼 로그인하기 어렵도록 비밀번호를 주기적으로 변경합니다

05 타인이 자신의 명의로 신규 회원가입 시 즉각 차단하고, 이를 통지받을 수 있도록 명의도용 확인서비스를 이용합니다

III - 1. 개인정보 오남용 피해예방 10계명 (2)



06 자신의 아이디와 비밀번호, 주민번호 등 개인정보가 공개되지 않도록 주의하여 관리하며 친구나 다른 사람에게 알려주지 않습니다

07 인터넷에 올리는 데이터에 개인정보가 포함되지 않도록 하며, P2P로 제공하는 자신의 공유폴더에 개인정보 파일이 저장되지 않도록 합니다

08 금융거래 시 신용카드번호와 같은 금융정보 등을 저장할 경우 암호화 하여 저장하고, 되도록 PC방 등 개방 환경을 이용하지 않습니다

09 인터넷에서 아무 자료나 함부로 다운로드 하지 않습니다

10 개인정보가 유출된 경우 해당 사이트 관리자에게 삭제를 요청하고, 처리되지 않는 경우 즉시 개인정보침해신고센터(118, www.118.or.kr)에 신고합니다



1. 의심스러운 애플리케이션 다운로드하지 않기
2. 신뢰할 수 없는 사이트 방문하지 않기
3. 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기
4. 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기
5. 블루투스 기능 등 무선 인터페이스는 사용 시에만 켜놓기
6. 이상증상이 지속될 경우 악성코드 감염 여부 확인하기
7. 다운로드한 파일은 바이러스 유무를 검사한 후 사용하기
8. PC에도 백신프로그램을 설치하고 정기적으로 바이러스 검사하기
9. 스마트폰 플랫폼의 구조를 임의로 변경하지 않기
10. 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트 하기



1. SNS에 올린 개인정보, 사진, 영상등의 정보는 누구나 볼 수 있고 악용될 수 있으니 신중히 선택하여 공개하세요

2. 가족, 친구 등 타인의 개인정보도 나의 개인정보 못지 않게 중요하므로 함부로 게시 공개하거나 확산시켜서는 안돼요

3. SNS는 기본적으로 많은 개인정보를 공개하도록 요구하는 경향이 있으므로 반드시 공개설정 범위를 직접 확인하고 재설정하세요

4. SNS에서 타인과의 네트워킹은 자신의 정보를 광범위하게 공개하는 것으로 주의해야 하며, 신뢰할 수 있는 사람만 친구로 추가하세요

5. SNS에 업로드한 개인정보나 게시글은 퍼나르거나 검색엔진 등을 통해 빠르게 확산되어 삭제가 쉽지 않다는 위험이 있다는 것을 잊지 마세요

6. SNS 이용시 나의 행동 정보가 원치 않는 맞춤형 광고나 마케팅에 이용될 수 있으므로 개인정보활용에 동의하실 때에 신중하세요

7. SNS를 통해 나의 위치정보와 이동경로가 노출되어 악용될 수 있으니 활용하지 않을 때는 반드시 서비스를 꺼두세요

8. 아동·청소년이 SNS를 이용하면서 자신과 타인정보를 무분별하게 공개하거나 부적절한 내용의 글 등을 게시하는 것을 방지하기 위해 부모님과 선생님들께서 관심을 가지고 지도해 주세요

9. 누구나 자신의 개인정보를 보호받을 권리를 가지고 있다는 점을 잊지 말고 SNS상에서 내 개인정보를 지키기 위한 권리를 적극적으로 행사하세요

10. SNS 이용시 내 개인정보가 유출 또는 오남용된 사실을 알게 된 때에는 118에 도움을 요청하세요





1. 회사기밀이 누설될 수 있는 사무실이나 타인과 공용되어 사용하는 PC, 또는 개인 정보가 포함된 파일이 많은 PC에는 가급적 P2P 프로그램을 설치하지 마십시오

2. P2P 서비스를 제공하고 있는 사이트의 개인정보보호방침, 이용약관, 개인정보와 관련한 각종 공지사항들을 확인하십시오

3. P2P 프로그램 설치 시 설치마법사 등 자동 설치보다는 수동 설치를 이용하고, "C:", "D:"등 루트 디렉터리 전체를 공유하거나 "내문서(My document)" 폴더를 공유 폴더로 지정하지 않도록 주의하십시오

4. P2P 프로그램을 사용하지 않을 때는 프로그램을 완전히 종료하십시오

5. 부모는 자녀의 파일공유를 중요한 개인정보가 유출되고 있는지 항상 주의해야 하며 자녀에게 그 위험성에 대해 가르치십시오

➡ 개인정보가 누설된 사정을 알면서 부정한 목적으로 개인정보를 제공받는 경우

정보통신망법 제28조의2(개인정보의 누설 금지) ② 누구든지 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받아서는 아니 된다.

(위반 시) 5년 이하의 징역 또는 5천만원 이하의 벌금

➡ 인터넷상 명예훼손

정보통신망법 제70조(벌칙) ① 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 3년 이하의 징역이나 금고 또는 2천만원 이하의 벌금에 처한다.
② 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.

➡ 타인의 주민등록번호 도용

주민등록법 제37조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

8. 다른 사람의 주민등록증을 부정하게 사용한 자

10. 다른 사람의 주민등록번호를 부정하게 사용한 자



IV. 청소년 섯다운제

 청소년의 인터넷게임 중독을 예방하기 위해 2011년 5월 청소년보호법 개정을 통해 청소년 섯다운제 도입

- 인터넷게임서비스 제공자는 오전 0시 이전에 접속한 만 16세 미만의 청소년에 대해서는 오전 0시가 되면 인터넷게임 이용을 중단시키고, 오전 0시부터 오전 6시까지는 만 16세 미만 청소년의 신규접속을 차단

< 청소년보호법 >

제26조(심야시간대의 인터넷게임 제공시간 제한) ① 인터넷게임의 제공자는 16세 미만의 청소년에게 오전 0시부터 오전 6시까지 인터넷게임을 제공하여서는 아니 된다.

② 여성가족부장관은 문화체육관광부장관과 협의하여 제1항에 따른 심야시간대 인터넷게임의 제공시간 제한대상 게임물의 범위가 적절한지를 대통령령으로 정하는 바에 따라 2년마다 평가하여 개선 등의 조치를 하여야 한다.

 인터넷게임서비스 제공자는 청소년보호법, 게임산업진흥에 관한 법률 등 이행을 위해 실명·연령확인 및 본인을 인증하도록 하여 만 16세 미만의 청소년 구분

- 2012년 8월 18일부터 정보통신망법 개정 시행에 따라 인터넷게임서비스 제공자 또한 주민번호 수집·이용이 전면 제한
- 청소년 섯다운제 등 법규 준수를 위해서는 주민번호를 사용한 실명·연령확인 및 본인 확인 대신 대체수단 사용

※ **본인확인수단** (게임산업진흥에 관한 법률 시행령 제8조의3)

- ① 공인인증기관, 그 밖에 본인확인서비스를 제공하는 제3자 또는 행정기관에 의뢰
- ② 대면확인

< 게임산업진흥에 관한 법률 >

제12조의3(게임과몰입·중독 예방조치 등) ① 게임물 관련사업자[「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 정보통신망(이하 "정보통신망"이라 한다)을 통하여 공중이 게임물을 이용할 수 있도록 서비스하는 자에 한한다. 이하 이 조에서 같다]는 게임물 이용자의 게임과몰입과 중독을 예방하기 위하여 다음 각 호의 내용을 포함하여 과도한 게임물 이용 방지 조치(이하 "예방조치"라 한다)를 하여야 한다.

1. 게임물 이용자의 회원가입 시 실명·연령 확인 및 본인 인증

< 게임산업진흥에 관한 법률 시행령>

제8조의3(게임과몰입·중독 예방조치 등) ③ 게임물 관련사업자(법 제12조의3제1항에 따른 게임물 관련 사업자로 한정한다. 이하 이 조에서 같다)는 법 제12조의3제1항제1호에 따라 게임물 이용자의 회원가입 시 「전자서명법」 제2조제10호에 따른 공인인증기관, 그 밖에 본인확인서비스를 제공하는 제3자 또는 행정기관에 의뢰하거나 대면확인 등을 통하여 게임물 이용자가 본인임을 확인할 수 있는 수단을 마련하여야 한다.

< 심야시간대 인터넷게임의 제공시간 제한 대상 게임물 범위 (적용기간 : 2013년 5월 20일~2015년 5월 19일) >

1. 적용대상 게임물

○ 「게임산업진흥에 관한 법률」 상 게임물로서 영리를 목적으로 정보통신망을 통해 실시간으로 제공되는 인터넷게임물

< 적용례 >

- 기기별 : PC(노트북 포함)
- 게임물별 : 온라인PC게임, 웹게임, PC패키지게임 등

2. 적용제외 게임물

○ 「전기통신사업법」 제5조제3항제1호에 따른 기간통신사업자가 제공하는 이동통신 서비스를 이용하는 이동통신 단말기기를 이용한 게임물

○ 「전기통신사업법」 제5조제3항제1호에 따른 기간통신사업자가 무선으로 제공하는 기간통신역무를 이용할 수 있는 휴대용 정보 단말기기를 이용한 게임물

○ 「게임산업진흥에 관한 법률」 제25조제1항제4호에 따른 게임기기 자체만으로는 오락을 할 수 없는 기기를 이용한 게임물. 다만, 정보통신망법 제2조제1항 제1호에 따른 정보통신망을 통하여 게임물을 유료로 제공받는 경우는 제외

- 비영리를 목적으로 제공되고 개인정보를 수집 또는 이용하지 않는 게임물

※ 비영리 목적, 개인정보 수집 및 이용 관련 심야시간대 인터넷게임의 제공시간 제한제도 적용 여부 판단기준

구분		개인정보 수집 또는 이용 여부	
		수집 또는 이용하지 않음	수집 또는 이용함
게임 이용료	무료	제도 적용 제외	제도 적용
	유료	제도 적용	제도 적용

- 「게임산업진흥에 관한 법률」 제21조제1항제3호에 따라 등급분류를 받지 않는 게임물 중 시험용게임물
- 「게임산업진흥에 관한 법률」 제21조제1항제1호 및 제2호에 따라 등급분류를 받지 않는 게임물 중 게임대회·전시회용 게임물, 교육·공익홍보용 게임물

< 적용례 >

- 기기별 : 스마트폰, 태블릿PC, 콘솔기기

※ 다만, 콘솔기기는 유료(게임물의 이용을 위해 어떤 방식으로든 추가적인 비용이 요구되는 경우)로 제공되는 경우는 심야시간대 인터넷게임의 제공시간 제한 대상에 포함

- 게임물별 : 플래시게임 중 일부, PC패키지게임물 중 일부



감사합니다.