2023 한국인터넷진흥원 본인확인서비스 교육

본인확인수단 및 본인확인입력정보 관리의 중요성

이용자대상

CONTENTS

01 본인확인서비스 수단별 유·노출 사고 사례 및 주의사항

(1) 아이핀 도용으로 쇼핑몰 적립금 탈취 사례

(2) 사칭문자로 인한 인증번호 탈취 사례

(3) 신용카드와 개인정보 유출로 인한 게임아이템 구매 사례

(4) 타인의 PC에 있는 공동인증서로 비대면 대출 사례

본인확인서비스(대체수단)별 유·노출 사고 사례 및 주의사항

아이핀 도용으로 쇼핑몰 적립금 탈취 사례

타인 명의 아이핀 번호를 도용해 쇼핑몰 신규가입 적립금 약 3700만 원을 부정 취득한 30대가 법원에서 징역형의 집행유예를 선고받았다.
A 씨는 2018년 5월부터 2021년 2월까지 한 쇼핑몰 사이트 신규가입 적립금을 노리고 불법 아이핀 판매업자로부터 구매한 타인 명의 아이핀을 이용해 총 1만 930개 아이디를 만들었다.
이렇게 만든 신규 아이디를 통해 A 씨는 약 3700만 원 적립금을 부정 취득한 혐의로 기소됐다.

[일요신문 2021.04.05]

아이핀 도용 의심 시 대처방안

01 아이핀 사이트나 전용 어플리케이션을 통해 인증내역을 조회합니다.

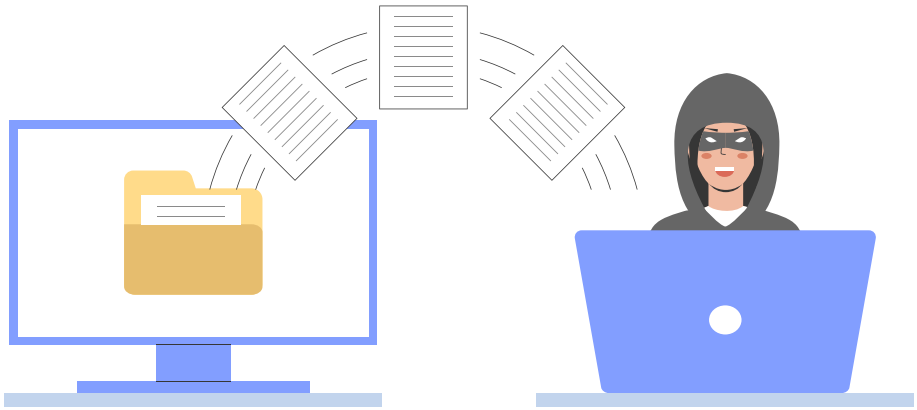
02 아이핀 도용이 확인됐을 경우 즉시 해당 아이핀을 폐기합니다.

03 도용범위를 파악하고 사이트 담당자 혹은 사이버 수사대에 도움을 요청합니다.

사칭 문자로 인한 인증번호 탈취 사례

메신지피싱에 사람들이 속는 이유는 가족이나 지인이 급한 상황이라며 돈을 이체해달라고 부탁하기 때문이다. 예를 들면, 범죄자는 피해자의 아들인 척 속이며 “기존 휴대전화가 망가져서 새로운 SNS 계정을 만들었다. 지금 급한데 90만 원만 이체해줘”라고 말한다.
정부기관과 기업의 공식채널로 가장하며 본인인증을 하거나 특정 앱을 깔아야 한다고 요구하는 경우도 많다. “당신의 계정이 해킹됐다”나 “100만원 결제가 됐다”라는 내용을 전달받을 때 불안함을 느끼게 된 피해자가 이에 응하는 사례가 늘고 있다.

[IT동아, 2023.2.22.]



메신저 피싱

타인의 메신저 아이디를 도용하여 지인에게 금전이나 개인정보를 요구하는 행위

OTP인증번호

무작위로 생성된 1회용 비밀번호로써 일정 시간 동안만 사용 가능하여 추정 불가능한 특징이 있습니다.

메신저 피싱 피해 예방 방법

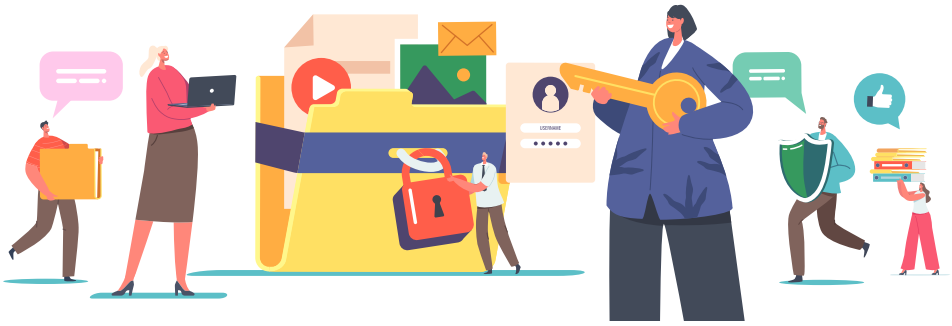
메신저로 가까운 친인척이 금전 및 개인정보 요청 시 반드시 당사자와 직접 전화통화 하여 확인해 보고,

어떠한 경우에도 신분증이나 계좌번호, 비밀번호, 생년월일 등의 개인 정보는 제공해서는 안 됩니다.

신용카드와 개인정보 유출로 인한 게임아이템 구매 사례

A씨의 미성년 자녀는 A씨 허락을 받아 자신의 스마트폰에서 A씨 배우자의 계정을 통해 앱스토어의 인앱(In-App) 결제 시스템으로 모바일게임을 구매하면서 A씨 명의의 신용카드 정보를 입력해 8900원을 결제했다.
A씨 자녀는 이후 자신의 스마트폰에서 A씨 배우자의 계정을 이용해 다른 모바일게임을 다운로드 받고 인앱(In-App) 결제시스템을 통해 25회에 걸쳐 총 261만4000원 상당의 게임 아이템을 구매했다.
그 과정에서 A씨 허락 없이 위 결제시스템에 저장돼 있는 A씨의 신용카드 정보를 그대로 사용해 결제했다.

[컨슈머치 2023.2.10.]



스마트폰 신용카드 본인확인서비스 유출 예방 방법

아이디, 비밀번호는 생일, 기념일 등 개인정보로 유추 가능한 것을 사용하지 않습니다.

사용하지 않는 카드는 즉시 해지합니다.

카드사별 다른 비밀번호 사용합니다.

주기적인 비밀번호 변경이 필요합니다.

모바일이나 PC를 이용한 신용카드 본인확인서비스 이용시 카드정보, 아이디, 비밀번호가 CCTV 또는 주변 사람에게 노출되지 않도록 주의합니다.

타인의 PC에 있는 공동인증서로 비대면 대출 사례

ㄱ씨는 지난해 3월 보이스피싱으로 개인정보를 털려 저축은행과 캐피털업체에 총 4000만원의 빚을 떠안았다. 사기범이 ㄱ씨 명의의 공동인증서를 발급받은 뒤, 비대면 방식으로 신원을 인증해 대출을 받았다. ㄱ씨는 법원에 채무부존재 확인 소송을 냈다. 하지만 법원은 금융사가 “필수적 본인확인 조처를 이행했다”는 이유로 지난달 저축은행 한 곳에 대해 원고(ㄱ씨) 패소로 판결했다.

[한겨레신문 2022.05.09]

공동인증서 관리 방안

01 누구나 접근 할 수 있는PC 또는 핸드폰에는 인증서를 남기지 않습니다.

02 인증서 비밀번호는 개인정보와 관계없는 것으로 사용하는 것을 권장합니다.

03 오랫동안 사용하지 않은 인증서는 폐기합니다.

02 본인확인서비스 안전한 이용방법

본인확인서비스 안전한 이용방법

본인확인서비스 안전한 이용방법

01
본인확인서비스 이용 시
입력하는 개인정보가 유·노출
되지 않도록 주의합니다.

02
본인확인입력정보는 가까운
사이라도 공개하지 않습니다.

03
개인정보로 유추 가능한 패스워드는
피하고, 수단별 패스워드를 달리하며
주기적으로 변경합니다.

04
수시로 본인확인서비스
인증내역을 확인합니다.

본인확인서비스 도용 발생 시 절차

01

본인인증내역 확인 후 도용된
본인확인수단 즉시 폐기합니다.

02

해당 사이트에 방문하여 담당자나
사이버 수사대에 도움을 요청합니다.

03

주로 사용하는 본인확인서비스를
제외한 본인확인수단은 폐기합니다.