행정안전부

개인 인증서 유출 사고·사례 기반 예방교육 자료

[1] 사고 사례 및 원인 분석

사례 1

메일로 전송한 인증서 해킹

사고내용

직원 A는 인증서를 집에서 쓰기 위해 본인 이메일로 보냄
며칠 뒤 이메일 계정이 피싱으로 탈취되어 인증서 파일이 외부 유출
해커가 인증서를 가져가 정부 사이트 해킹시도

원인

인증서를 메일로 전송 → 정책 위반
이메일 계정 보안 미흡

예방 방법

✓인증서 이메일·메신저 전송 금지
✓ 이메일, 클라우드 저장소에 인증서 보관 금지
✓ 보안USB 등에 암호 설정 후 보관

사례 2

PC방 사용 후 인증서 미삭제

사고내용

B씨가 급하게 인증서가 필요해 PC방에서 본인 인증 진행 사용 후 인증서를 삭제하지 않고 종료
이후 다른 사람이 인증서를 가져가 정부 사이트 해킹시도

원인

외부 PC에서 인증서 사용
삭제 및 휴지통 비우기 미실시

예방 방법

✓ 공용 PC(PC방·도서관·민원실 등)에서 인증서 사용 금지
✓ 부득이하게 사용 시 인증서 삭제 → 휴지통까지 완전 삭제

사례 3

해킹메일 열람으로 인한 인증서 및 비밀번호 탈취

사고내용

C씨는 안내 메일를 받고 링크 클릭
실제와 매우 비슷한 '정부기관 로그인 페이지'에서 인증서를 선택해 비밀번호 입력
입력 직후 인증서 파일과 비밀번호가 공격자 서버로 전송됨
해커가 인증서를 가져가 정부 사이트 해킹 시도

원인

정부 기관을 사칭한 해킹메일에 포함된 URL 확인 없이 클릭
가짜 정부 사이트에서 인증서 비밀번호 입력

예방 방법

✓ 출처가 불분명하거나 이상한 메일 열람 금지
✓ 메일내 포함된 URL 링크 직접 클릭 금지
✓ URL 접속이 필요한 경우 주소창에 직접 공식주소 입력

사례 4

USB 분실로 인증서 노출

사고내용

D씨는 인증서를 USB에 넣어 가지고 다님
USB가 암호화되어 있지 않아 분실 시 인증서가 그대로 노출
공격자가 USB를 열어 인증서·개인키·비밀번호 힌트 정보 확보

원인

일반 USB 무암호 저장
인증서 파일 암호화 미적용

예방 방법

✓ 인증서를 USB 저장시 반드시 암호 설정(zip 압축시 암호설정 가능)
✓ USB 분실 대비 비밀번호는 절대 파일로 보관하지 않기

사례 5

메모장에 저장된 인증서 비밀번호 유출

사고내용

E씨는 인증서 비밀번호를 헷갈려서 바탕화면 메모장에 저장
악성코드 감염으로 PC 탐색기능이 실행되어 메모장 내용 전부 유출
인증서 파일이 같은 PC에 있어 합쳐서 탈취됨

원인

비밀번호를 텍스트로 저장
PC 악성코드 감염

예방 방법

✓ 비밀번호 텍스트·사진·메모앱 저장 금지
✓ 백신 실시간 감시·정기 업데이트 필수
✓ 인증서 저장 PC 2차 인증 적용

행정안전부

[2] 사고 예방을 위한 핵심 수칙 (요약)

1. **PC 보안 강화** : 백신 및 운영체제·브라우저 최신 업데이트 적용
2. **외부 PC 사용 금지** : 부득이한 경우 삭제 + 휴지통 비우기 필수
3. **이메일·메신저 전송 절대 금지** : 인증서·비밀번호 전송 금지
4. **인증서 공유 금지** : 동료에게도 절대 공유하지 않기
5. **비밀번호 파일 저장 금지** : 텍스트나 메모장 저장 금지
6. **해킹 메일 주의** : 출처가 불분명하거나 알수 없는 메일 열람 금지
7. **USB 암호화 필수** : 인증서를 USB에 저장시 암호설정(zip 압축시 암호설정 가능)
8. **강력한 비밀번호 사용** : 영문자+숫자+특수문자 조합

[3] 결론

인증서 유출사고의 대부분이 사용자의 부주의로 발생하며
사고 한 번만으로도 개인정보 침해·계정 탈취 등 큰 손실이 발생합니다.

**“인증서는 전자 신분증이다.
절대 외부에 노출시키지 않는다.”**

이 원칙만 지켜도 대부분의 사고는 예방할 수 있습니다.