



디지털성범죄 '몸캠피싱' 예방 안내

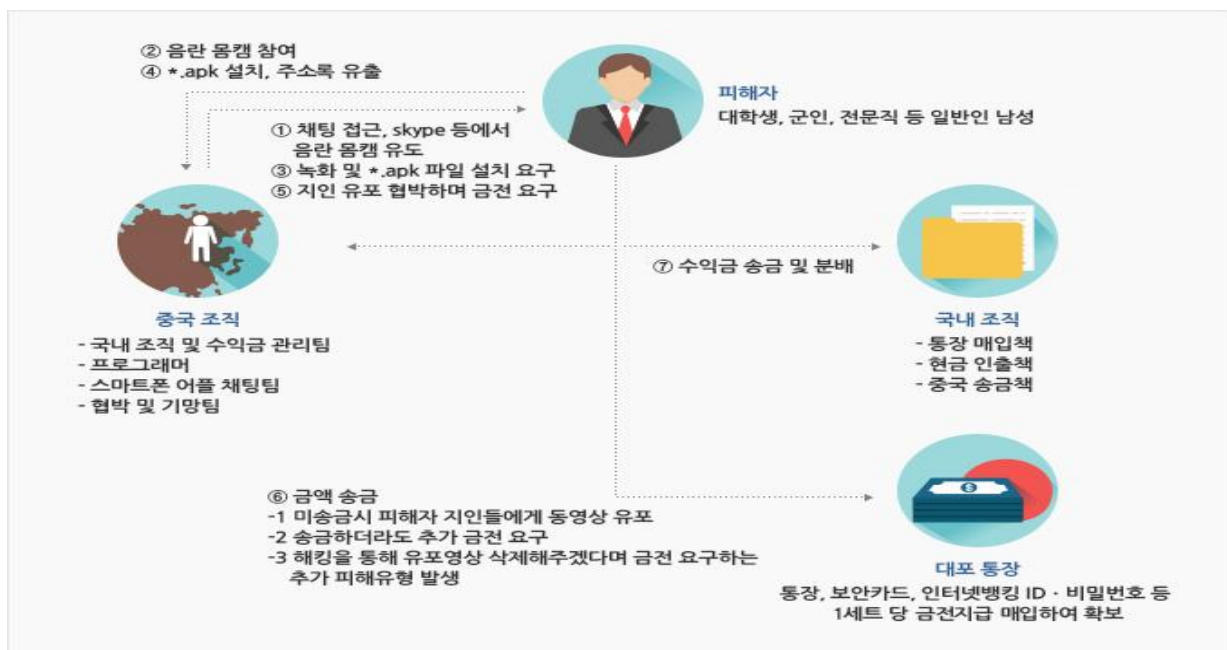
1

개념

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

가. 특징

- 스카이프 등 스마트폰 채팅 어플을 통한 「몸캠피싱」은 ▲여성을 고용할 필요가 없고 ▲범죄 행위가 비교적 단기간에 종료되며 ▲주소록을 이용한 ‘음란한 사진 · 동영상 유출 협박 행위’의 실효성이 높아 범인들은 더 조직화되고 있음
- 「랜덤 채팅」 어플은 대부분 익명성 보장을 이유로 개인정보와 채팅 내용을 서버 등에 저장하지 않고 있으며, 대표적인 화상채팅 어플인「스카이프」는 미국에 본사가 있어 범죄 수사에 어려움이 있음



가. 채팅 접근

- 타인 사진을 도용하여 여성으로 가장한 범죄자가 「랜덤 채팅」 어플 또는 「모바일 메신저」 등을 통해 남성 피해자에게 접근
- 또는 채팅방을 만들어 남성이 접근하기를 기다림

나. 「스카이프(skype)」 등으로 이동하여 화상채팅 제의

- 협박에 필요한 피해자의 음란 동영상 확보하기 위해, “오빠, 야하게 놀래“ 등으로 유혹하며, 「skype」 등으로 이동하여 화상채팅 할 것을 피해자에게 제의
- ※ skype : 대표적인 인터넷전화 브랜드로서, iOS-안드로이드 사이 뿐만 아니라, 스마트폰-PC 사이에도 음성·화상통화(채팅)가 가능해 몸캠피싱에 가장 많이 이용됨

다. 얼굴이 나오게 하여 음란행위 유도

- 미리 준비해 둔 여성 동영상을 보여주며, 상대방도 함께 음란행위를 하도록 유도
- 협박할 때 유용하게 사용하기 위해 피해자에게 얼굴과 중요 부위가 함께 화면에 나타나도록 요구

라. 주소록을 유출하는 *.apk 설치 요구

- 화상채팅에 필요한 어플이라거나, 화상채팅 중 상대방의 목소리가 들리지 않아 '음성지원용'으로 필요하다며 특정한 파일을 스마트폰에 설치해 달라고 피해자에게 요구함
- 대부분 다양한 명칭의 *.apk 파일로서 음란 동영상 녹화에 들어가기 전이나 녹화한 이후에 피해자에게 설치할 것을 요구함
- ※ '음성지원', 'skype 1.02', 'con6' 등 명칭으로 직접 전달하거나 특정 url에서 다운 유도
- 악성코드 설치 시 피해자의 주소록이 범죄자에게 유출됨

마. 지인 연락처 명단을 보이며 피해자에게 금전 요구

- 피해자에게 피해자 지인들의 명단과 연락처를 보여주면서 동영상을 유포하겠다는 협박과 함께 돈을 요구
- 연락처가 유출되지 않았더라도 “각종 게시판에 올리겠다“며 협박하는 경우도 있음

바. 대부분 동영상 유포, 송금하더라도 오히려 추가로 돈을 요구

- 피해자가 돈을 송금하지 않은 사례에서 협박범은 대부분 피해자 지인들로 채팅 그룹을 만든 후 피해자의 동영상을 유포하고 있음
☞ ‘돈을 보내지 않으면 동영상을 유포해 버리더라’ 는 소문을 냄으로써 다른 피해자 사례에서 돈을 보내게 하려는 의도적인 행위로 판단됨
- 그러나, 피해자가 돈을 송금하더라도 협박범은 협박을 멈추지 않고 오히려 추가로 돈을 요구하는 사례가 대부분이므로 협박에 따라 돈을 송금하는 것은 해결방안이 아님

#. 해킹을 이용해 동영상을 삭제해 주겠다고 돈을 요구하기도..

- 범죄자가 운영하는 관리자홈페이지를 해킹해서 피해자의 동영상을 삭제해 유포 피해를 막아주겠다고 피해자에게 접근해서 돈을 요구하는 사례도 있음
- 이런 경우 대개 선급금을 요구하는데, 시간만 허비해서 추가 피해만 발생할 뿐, 이 또한 해결방안이 아님

3

예방수칙

가. 몸캠피싱 피해를 예방하는 방법

- 스마트폰의 '환경설정' 메뉴에서 '출처를 알 수 없는 어플의 설치를 차단'해 둬으로써 스마트폰의 보안설정을 강화시키세요.
※ 보안설정 강화 방법 : 환경설정 → 보안 → 디바이스관리 → '알 수 없는 출처(소스)' 에 체크 해제(스마트폰 제품에 따라 메뉴 명칭은 일부 상이)
- 특히, 출처 불명의 실행파일(*.apk)을 스마트폰에 다운받은 후 이를 스마트폰에 설치하는 행위는 절대 하지 마세요.
※ 출처 불명이란 : 공식 '앱 스토어' (구글 플레이 스토어, T스토어 등)가 아닌, 문자 · 모바일 채팅 등을 통해 URL에 접속해서 내려받는 경우
- 「랜덤 채팅」에서 낯선 미모의 여성과 대화할 때, 언제든지 이러한 범죄의 표적이 될 수 있음을 유의하셔야 합니다.
※ '랜덤 채팅'은 익명성 보장을 이유로 개인 정보와 채팅 내용을 저장하지 않으므로, 몸캠피싱 외에 '조건 만남 계약금 사기' 등 여러가지 범죄의 시발점이 됨
- 물론, 그 전에 '음란 채팅'을 하지 않는 것이 가장 중요하겠습니다.

나. 만약 피해를 당했다면

- 범인들의 송금 요구에 절대 응하지 마세요. 범인들은 돈을 받았다고 해서 약속을 지키지 않습니다. 오히려 '돈 사람'이라 생각해서 추가로 더 돈을 요구하며 더 이상 돈을 보내지 않으면 결국 동영상 배포해 버립니다. 돈을 송금하는 것은 해결방안이 아닙니다.
- 협박 문자나 전화를 받은 즉시, 채팅 화면을 캡처하고 송금 내역 등 증거자료를 준비한 후, 즉시 가까운 경찰서에 신고하세요.

※ 범피자는 여러 개의 채팅 계정과 대포 통장을 이용하기 때문에 적극적인 신고가 중요

- 신고 후에는 추가 피해를 방지하기 위해 스마트폰을 초기화하시거나, 설치된 악성 프로그램(앱)을 삭제하세요.
- 또한, 악성 프로그램(앱)으로 인해 유출된 정보에는 주소록(전화번호)정보 이외에 피해자의 각종 개인정보가 포함되어 있을 수 있으므로, 스마트폰에 연동되어 있던 각종 계정은 탈퇴한 후 새롭게 개설하시고 아이디, 패스워드 등도 변경하세요.

☐ 출처 : 경찰청 사이버안전국/예방수칙/몸캠피싱

<http://cyberbureau.police.go.kr/>

2020. 03. 30.

군 산 월 명 중 학 교 장-직인생략-