

# 정부, 큐싱(QR코드+피싱) 피해로부터 우리 청소년들을 지키기 위해 적극 나선다

- 공공장소나 인터넷에 출처가 불분명한 QR코드는 조심! 또 조심!! -

과학기술정보통신부(장관 유상임, 이하 ‘과기정통부’), 교육부(부총리 겸 교육부 장관 이주호), 여성가족부(여성가족부장관 직무대행 차관 신영숙), 개인정보보호위원회(위원장 고학수, 이하 ‘개인정보위’), 경찰청(청장 조지호), 한국인터넷진흥원(원장 이상중, 이하 ‘KISA’)은 최근 초·중·고 학생들의 큐알(QR)코드 활용이 증가하면서 이를 악용한 큐싱(QR코드+ 피싱)으로 인해 발생할 수 있는 사이버 사기 피해에 대해 각별한 주의를 당부했다.

\* QR코드와 피싱(Phishing)의 합성어, 악성코드나 유해 웹사이트에 연결되는 QR코드를 촬영하면 스마트폰에 악성 앱이 설치되어 개인·금융정보를 탈취하거나 소액결제를 유도

특히, 복잡한 인터넷 주소 입력을 대신하거나, 필요한 앱을 바로 설치할 수 있도록 도와주는 QR코드의 편리함을 일상생활에서 자주 이용하는 학생들을 대상으로 하는 큐싱 피해가 우려되는 상황이다. 중국, 미국, 스페인에서는 QR코드를 포함한 가짜 주차위반 딱지, 공공자전거에 부착된 사기 QR코드 등 큐싱을 통해 개인정보 탈취나 사이버 사기 피해가 발생하기도 하였다. 지난 과기정통부 ICT 산하기관 국정감사(10.10.) 때 최수진 위원(국민의 힘)은 키보드 이용 시연을 통하여 신종 사기 수법인 큐싱 위험 및 선제대응 필요성에 대해 지적하였으며, 국회 과방위(위원장 최민희) 차원에서도 관련 부처가 협력하여 큐싱 예방을 위한 적극적인 조치와 홍보를 요청한 바 있다.

지금까지 국내에 확인된 큐싱 시도 유형으로는 공유형 키보드에 부착된 정상 QR코드 위에 큐싱 스티커를 덧붙이거나, 온라인 광고나 메일 본문에 큐싱을 삽입하여 안전거래 등을 위해 필요한 앱이라고 속여 설치를 유도하는 경우가 있었다. 큐싱은 육안으로는 가짜 여부를 판별하기 어려워 정보통신(IT)에 익숙한 청소년들도 속아 넘어가기 쉬운 것으로 알려져 있다.

큐싱으로 악성 앱이 설치되면 스마트폰에 있는 모든 개인정보가 탈취될 수 있고, 원격에도 내 스마트폰을 조정하여 보이스피싱, 몸캠 피싱, 개인정보 불법판매 등 다양한 피해를 입을 수 있다. 이처럼 고도화되는 사이버 피해를 사전에 예방하기 위해서는 큐싱 사기 예방 수칙을 생활화할 필요가 있다.

#### < 큐싱 사기 예방 수칙 >

- ① 출처가 불분명한 웹사이트나 모르는 사람이 보낸 이메일에 포함된 QR코드는 스캔 금지!
- ② 공공장소 QR이 덧붙여진 스티커가 아닌지 확인(공유자전거 등 이용할 때 가짜 QR코드인지 살펴보기)
- ③ QR 스캔 시 연결되는 링크 주소(URL)가 올바른지 다시 한번 확인
- ④ QR코드 접속 후 개인정보 입력을 요구하거나 수상한 앱은 설치 금지!
- ⑤ 모바일 전용 보안 앱, 스미싱 탐지 앱 설치 및 최신 버전 유지하기!

한편, 정부는 관계부처 합동으로 전국 초·중·고 학생과 학부모, 교사를 대상으로 큐싱 위험성에 대한 경각심 제고와 피해 예방, 대응 요령에 대해 교육과 홍보를 집중적으로 실시한다.

#### < 큐싱 예방 교육 및 홍보 강화 >

과기정통부는 정보보호, 소프트웨어, 인공지능 분야 인재양성 사업과 연계하여 중·고교 학생들을 대상으로 큐싱 예방 대면 교육과 교육자료 배포를 진행하고, 전국 정보보호 대학교 동아리를 활용해 청소년 대상으로 큐싱 예방 교육 봉사활동을 지원할 계획이다. 전국 5개 국립과학관과 10개 KISA지역정보보호지원센터 등을 통해 교육자료와 포스터 등 큐싱 주의사항을 홍보하고, 온라인채널(SNS·홈페이지·유튜브)를 통해 예방 캠페인도 진행한다.

교육부는 전국 시·도 교육청에 관내 학교를 대상으로 큐싱 주의 안내문을 발송하도록 요청하여 학생, 학부모, 교사에게 알리도록 할 예정이다. 경찰청은 지역별 학교전담경찰관(SPO, School Police Officer)이 담당 학교 범죄예방교육 시 큐싱 예방수칙도 함께 교육한다.

여성가족부는 전국 1,000여개 청소년수련시설과 청소년 복지시설·지원센터 등에 방문하는 청소년들을 대상으로 교육자료와 홍보물을 배포하고, 개인정보위는 전국 초·중·고 학교 대상 직접 찾아가는 개인정보 인식제고 교육에 큐싱 예방 내용을 포함하여 현장 교육을 진행한다.

## < 쿼싱 피해 또는 의심되는 경우 조치방법 >

쿼싱에 속아 악성 앱 설치가 의심되면, 즉시 스마트폰을 비행기 모드로 변경하여 통신을 차단하고 모바일 백신으로 악성 앱을 삭제하여야 한다. 금융정보 유출이 의심되는 경우, 거래하는 금융회사 영업점을 방문하거나 콜센터에 전화하여 본인 계좌에 일괄 지급정지를 요청함으로써 피해를 최소화 하고, 특히 사기 전화범에게 속아 피해금을 계좌로 송금한 경우에는 경찰청 (☎112)에 피해사실을 신고하고 범인이 돈을 옮기지 못하도록 즉시 지급 정지를 신청할 것을 당부했다.

쿼싱이 의심되는 QR코드를 발견하였거나, 악성 앱 감염 등이 의심되는 경우 ‘사기전화지킴이(경찰청·금융감독원)’에 신고하거나, 국번없이 118 상담센터 (KISA)에 연락하면 24시간 무료로 상담받을 수 있다.

담당 부서	과학기술정보통신부 정보보호기획과	책임자	과 장	김연진	(044-202-6440)
		담당자	사무관	김승열	(044-202-6441)
	과학기술정보통신부 과학기술문화과	책임자	과 장	김보열	(044-202-4840)
		담당자	사무관	김근우	(044-202-4843)
	교육부 디지털교육전환담당관	책임자	과 장	송선진	(044-203-7046)
		담당자	사무관	이경은	(044-203-7059)
	여성가족부 청소년정책과	책임자	과 장	김민아	(02-2100-6231)
		담당자	사무관	박혜원	(02-2100-6238)
	개인정보보호위원회 자율보호정책과	책임자	과 장	윤여진	(02-2100-3081)
		담당자	사무관	박미영	(02-2100-3018)
	경찰청 청소년보호과	책임자	과 장	최은정	(02-3150-2048)
		담당자	경 정	임희진	(02-3150-2148)
	한국인터넷진흥원 국민피해대응단	책임자	단 장	이동연	(02-405-6640)
		담당자	팀 장	김은성	(02-405-5363)