1학년 5반 학부모님, 학생 여러분께

최근 밝혀진 끔찍한 디지털 성범죄 사건(조직적 성착취 영상거래 사건 등)의 피해자 중에는 어린 학생들이 많습니다. 범죄자들은 카톡 등 메신저, 게임, 게임채팅 을 포함해, 학생들이 일상적으로 사용하는 모든 온라인/인터넷 서비스를 이용해 학생들에게 접근하고 있습니다.

여성가족부 십대여성인권센터 및 영유아 성평등 교육 서비스 우따따의 제공자료를 참고하여 실제 피해 사례를 정리해 보았습니다. 아이와 함께 읽고 대화하시면서, 디지털 성범죄 피해를 예방할 수 있도록 지도해 주시길 부탁드립니다.

먼저 한 가지 강조하고 싶습니다. 디지털 성범죄를 포함해 모든 범죄와 폭력의 책임은 피해자가 아니라 가해자에게 있습니다. 보호자와 학생 모두 피해자에게도 잘못이 있다는 생각이나 말을 하지 않도록 주의해 주세요. 그런 생각은 도덕적으로 옳지 않습니다. 또한, 자신과 주변에서 범죄 피해를 겪었을 때 문제 해결을 방해합니다. 가해자가 협박에 이용하는 것은 바로 피해자를 향한 손가락질입니다. 자신이 잘못해서 그런 일이 생겼다는 생각이나 야단 맞을까봐 무서운 마음 때문에 보호자에게 알리지 못하는 것이 대표적인 예입니다. 피해자를 탓하는 것은 가해자 편에 서는 일입니다.

보호자는 지금 아이에게 진심으로 약속해 주십시오. 무슨 일이 생겨도 아이 편에서 학생을 지키고 보호하겠다고 약속하십시오. 야단치지 않겠다고 약속하십시오. 선생님도 약속합니다.

학생 여러분도 보호자와 저에게 약속해 주십시오. 어려운 문제가 생겼을 때 혼자 끙끙대지 말고 도와달라고 이야기하겠다고. 누구나 피해자가 될 수 있습니다. 당한 사람의 잘못이 아닙니다.

대표적인 피해 사례
"문상 나눔합니다~!" 게임 아이템을 살 수 있는 문화상품권을 공짜로 주겠다고 한 뒤, 상품권을 받으려면 학교 이름이나 친구 이름을 알려달라고 하는 사례.
"이거 네 얘기 아니야? 네 사진이 인터넷에 돌아다니고 있어!" "누가 님 사진 합성해서 성인 사이트에 올렸어요." 이런 메시지를 받으면 누구나 깜짝 놀라고 불안할 거예요. 정말인지 확인하고 싶을 수밖에 없습니다. 그래서 링크를 클릭하거나 자주 가던 사이트에 로그인하게 만들어서 개인 정보를 빼가는 사례.
"너 진짜 00 맞아? 사기지? 너 사기죄로 신고한다." 메신저나 SNS계정이 진짜 자기 계정인지 증명하라고, 셀카나 신분증 사진을 보내라고 하는 사례. 사진을 보내지 않으면 사기 계정으로 신고하겠다고 겁주는 사례.
"나도 여자야. 너랑 동갑이고." 또래 여자라고 안심하게 하거나, 비슷한 관심 또는 고민에 대해 이야기하며 친근하게 다가와서 개인 정보를 빼가는 사례. 프로필 사진이 여자 어린이 사진이어도, 말투 등이 여자처럼 느껴진다고 하더라도 믿지 마세요.
"저는 변호사입니다. 00님을 도와주고 싶어요." 먼저 학생이 SNS에 올린 말과 행동에서 잘못된 점을 꼬투리를 잡습니다. 그리고 그런 잘못을 경찰에 신고하고 소문내겠다고 겁을 줍니다. 그런 뒤에, 무서워하는 학생에게 변호사로서 도움을 주겠다며 친절한 모습으로 다가오는 사례.

디지털 성범죄 접근의 특징
1) 학생의 개인정보를 요구합니다. 여기서 개인정보는 사진, 이름, 주소, 전화번호, 학교, 메신저/SNS 아이디와 비밀번호, 친구 이름, 알림장 사진 등으로 우리가 흔히 생각하는 것보다 훨씬 더 범위가 넓습니다.
2) 당황하게 만들거나 약점을 잡아 겁을 줍니다. 약점은 대부분 개인정보와 관련됩니다. 예전에 SNS에 올린 정보 등을 이용하기도 합니다.
3) 안심하게 만들고 선물이나 도움을 주겠다고 합니다. 겁을 준 다음 다른 사람인 척 도움을 주겠다고 하기도 하고, 안심하게 만든 다음 약점을 잡아 무섭게 굴기도 합니다.

Q&A

1) 저는 한 번도 몸 사진을 찍거나 인터넷에 올린 적이 없어요. 평범한 얼굴 셀카만 올리는 것도 안 되나요?
*평범한 얼굴 사진을 범죄자들이 다른 사람의 알몸 사진과 합성하여 퍼뜨리는 경우가 많습니다.

2) 제 이름은 제 개인 정보지만, 친구 이름은 아니지 않나요? 가짜로 이름을 지어내서 말하면 되지 않을까요?
*친구 이름을 알려주면, 개인정보보호법 위반으로 신고하겠다고 하거나 친구 부모님께 알려서 고소하겠다고 겁을 줄 것입니다. 가짜 이름에 대해서도 사기죄로 신고하겠다고 할 수 있습니다. 처음부터 그런 요구를 들어주지 말고, 아무 대답도 하지 말고 보호자에게 알리세요.

3) 만약 진짜로 제 정보나 사진이 인터넷에 돌아다니고 있으면 어떡하나요? 클릭해 보기 전에는 거짓말인지 알 수 없잖아요. 진짜로 제가 잘못한 일 때문에 경찰에 고발당하면 어떡하죠?
*무섭고 걱정되는 것이 당연합니다. 하지만 그럴수록 더욱 침착해야 하고 보호자에게 알려서 도움을 받아야 합니다. 지금 보호자와 함께 신호를 미리 정해 두세요. '이상한/무서운 연락을 받았어요' 정도면 충분합니다. 보호자의 도움을 받기 어려우면 학교에 전화하세요. 밤이라면 다음 날 아침에라도 학교에 전화하세요.

보이스피싱에 대해서 들어봤을 거예요. 어른들도 비슷한 상황에 처하면 속아 넘어가기 쉽습니다. 그래서 경찰이나 정부기관, 은행에서는 절대로 비밀번호를 물어보거나 전화로 돈을 보내라고 하거나, 메신저, 전화로 고발한다고 겁주지 않습니다.

만약 진짜로 여러분의 사진이 인터넷에 퍼져 있더라도 마찬가지입니다. 보호자의 도움 없이 잘 알지도 못하는 사람이랑 여러분이 그 문제를 해결할 수 없습니다. 반드시 보호자와 함께 정부 기관의 도움을 받아야 합니다. 그것이 그나마 가장 안전하고 확실한 방법입니다. 범죄자는 해결해 주는 척하면서 여러분의 약점을 이용하려고 합니다.

4) 자주 가던 사이트에 로그인을 하게 해서 개인 정보를 빼간다는 게 무슨 뜻인가요?
*메신저, SNS, 인터넷 사이트마다 로그인 페이지가 있습니다. 그런데 범죄자들이 그런 로그인 페이지를 진짜와 똑같은 모양으로 만들어서 개인 정보를 빼가는 경우가 많습니다. 학생의 아이디와 비밀번호를 이용해서 로그인한 뒤 비밀번호를 바꿔 버리고 나쁜 짓을 하거나, 그렇게 하겠다고 겁을 주는 것입니다. 가짜 페이지를 구별하는 방법이 있지만 완벽한 방법은 없고 학생들이 구별하는 것은 더 어렵습니다. 따라서 의심스러운 상황에서, 친구나 아는 사람을 포함해 누군가로부터 받은 링크에서 로그인을 하지 않는 것이 좋습니다. 가짜 페이지에 속지 않더라도 해킹될 수도 있습니다. 친구가 해킹을 당했을 수도 있고요. 그러니 처음부터 인터넷에 개인정보와 자세한 자기 이야기를 올리지 않는 것이 좋습니다.