

После теракта в «Крокусе» в Сети активизировались вербовщики. Они пишут российским школьникам и предлагают совершить диверсию за несколько сотен тысяч рублей. В случае отказа начинают угрожать ребенку и его семье.

Вербовка детей

Вербовщики начали писать российским детям и подросткам и склонять их к терроризму и другим преступлениям. После теракта в «Крокус Сити Холле» школьники стали получать сообщения с предложением устроить диверсии в разных регионах.

За это им предлагают разные суммы: от 250–300 тыс. рублей до миллиона. Некоторым ребятам за совершение преступления просто обещают купить наркотики или алкоголь. В ответ на отказ преступники угрожают детям расправой. «Ты очень об этом пожалеешь», «Пострадаешь не только ты, но и твои родственники», — пишут неизвестные.

Чаще всего такие вербовщики ищут детей в социальных сетях и мессенджерах, игровых чатах. Обычно подростки ведут свои страницы открыто — им можно написать, представившись кем угодно. Дети публикуют много личной информации, делятся своим мнением и ярко реагируют на события.

Соцсети позволяют провокаторам свободно собирать интересующие их данные и еще на этапе планирования «вербовки» анализировать личные страницы жертв и выбирать подходящих (обычно тех, кто демонстрирует активность, и в то же время не имеет четких личностных позиций).

Вербовщики, которые действительно подталкивают детей к терактам, это обычно тонкие психологи, обученные техникам и методикам воздействия на психику людей. Для них не существует «грязных» методов — способами воздействия на детей и подростков могут быть как психологические манипуляции, так и прямые угрозы, шантаж.

Большая часть таких сообщений поступает с Украины. Их отправляют, чтобы дестабилизировать общество и усилить состояние тревоги. Родителям необходимо рассказать детям о таких рисках и научить, как правильно вести себя: игнорировать вербовщика, рассказать взрослым, а потом обратиться в полицию.

«Команды» для школьников

Сигналы о манипулировании сознанием школьников через соцсети стали поступать задолго до трагедии в «Крокусе» — более двух лет назад. И под угрозой оказались не только подростки, но и дети младшего возраста.

С детьми связываются неизвестные и дают им «задания», которые могут меняться в зависимости от повестки. И быть очень жестокими.

Среди «заданий» были поджоги, звонки о минировании. Детей помладше склоняли к бытовым, очень опасным действиям, например манипуляциям с газовым оборудованием и электроприборами.

Бывали и случаи, когда детям диктовали необходимость вынести из дома все ценности и вещи — якобы, чтобы помочь родителям, спасти их от чего-либо. После этого семья теряла все сбережения, а у ребенка оставалась серьезная психологическая травма (особенно, если взрослые отругали его).

Преступники выбирают детей по простой причине — они легко внушаемы. А тинейджеры — восприимчивы из-за своего возрастного психоэмоционального состояния. У многих из них еще нет критического мышления, нет достаточного жизненного опыта, но есть резкие реакции на посылы — например, они могут сильно испугаться и выполнить «команду».

Кроме того, современные школьники живут в цифровом пространстве — они постоянно общаются с незнакомцами в Сети. И всё больше склонны доверять не близким людям, живущим рядом, а именно онлайн-друзьям.

В переписках преступники используют специально разработанные скрипты для влияния на сознание таких неокрепших умов. Родным становится всё сложнее выяснить, с кем общается ребенок, о чем переписывается с «другом». Подросток оберегает свое личное пространство и запрещает любое вмешательство в виртуальный мир.

Способы вовлечения

Дети в возрасте от шести до 12 лет часто становятся жертвами телефонных мошенников, предлагающих взять смартфон или банковскую карту родителей и под разными предлогами предоставить доступ к личному кабинету клиента банка — например, через вредоносное приложение или фишинговый сайт.

Иногда преступники выходят на ребят через чаты в играх — и могут, например, убедить подключить доступ к экрану. Такое бывает, когда ребенок играет с телефона родителей — многие привыкли бесконтрольно отдавать свои гаджеты, и их вообще не интересует, как используется техника.

Детей постарше, в возрасте 12–17 лет, часто вовлекают в виртуальные криминальные сообщества, обещая легкий заработок.

Именно поэтому немалый процент «воркеров», занимающихся мошенничествами на маркетплейсах, равно как и посетителей тематических телеграм-каналов, составляют именно несовершеннолетние.

Кроме того, детей часто вербуют в закладчики наркотиков. Такие объявления массово встречаются в Telegram и даркнете. Юным закладчикам предлагают неплохие деньги, забывая упомянуть, что обычно таких «работников» задерживают в течение первого же месяца.

Отдельный интерес у преступников вызывают подростки с банковскими картами. Их могут использовать как соучастников легализации денег, полученных преступным путем. За это дают какое-то небольшое вознаграждение.

В таких схемах злоумышленники делают акцент не только на возможности заработка, но и на «крутости» происходящего — ведь можно почувствовать себя настоящим хакером или участником криминального синдиката. К сожалению, подростки не осознают, что «невинная шалость» может обернуться реальным уголовным делом и лишением свободы.

Последняя угроза, это sextortion — шантаж на сексуальной почве. Преступники могут представляться сотрудниками модельных агентств — или просто флиртовать онлайн, выдавая себя за таких же подростков. А потом, получив фотографии или видео интимного характера, начинают вытягивать из жертвы либо деньги, либо новые фотографии и видеоролики.

В этом случае опасность кроется еще и в том, что подросткам крайне тяжело перенести подобную ситуацию: опасаясь того, что интимные фотографии будут преданы огласке, они становятся готовы буквально на всё, лишь бы их близкие или одноклассники не узнали об этом.

Защита детей

Для того чтобы защитить ребенка от любых провокаторов, прежде всего, объяснить ему правила безопасности в Сети. Например, закрыть профиль и убрать общедоступные фото в мессенджерах, не добавлять в друзья незнакомцев и поставить запрет на отправку сообщений и звонки от тех, кого нет в списке

контактов. Не отвечать на сомнительные предложения и настораживаться, если собеседник (особенно незнакомец или взрослый) требует сохранить тайну переписки и не сообщать ничего родителям.

Технически можно использовать встроенные программы родительского контроля и настройки сетевого доступа (запрет на переход по определенным ссылкам, просмотр контента, требующего более высоких возрастных ограничений).

Программа родительского контроля поможет ограничить доступ к нежелательному контенту и оставить, например, только нужный для учебы.

Можно установить временные интервалы, в течение которых будут доступны только основные функции устройства, а развлекательные приложения или социальные сети заблокированы.

При этом, все подобные программы — лишь дополнительный инструмент, задействованный в воспитательном процессе. Школьник без труда найдет возможности обхода любых технических ограничений, и чем сильнее родители станут контролировать его, тем больше он будет закрываться и сопротивляться этому.

Поэтому самый действенный метод — это выстраивание доверительных отношений внутри семьи. Ребенок должен доверять родителям и не бояться обратиться к ним с проблемой, рассказывать о тех же странных сообщениях в мессенджерах. А взрослые, в свою очередь, должны повышать уровень компьютерной грамотности и обеспечивать цифровую гигиену.

Помимо того, родителям важно следить за поведением и интересами ребенка. Насторожить может как отказ от них, так и резкие изменения: если, например, школьник начал увлекаться оружием или стрельбой, депрессивной литературой. Тревожным сигналом может стать и выполнение заданий, полученных в Сети, — даже если они, на первый взгляд, кажутся безобидными.

Отдел профилактики терроризма и правонарушений