ПОЛИНА ЗИНОВЬЕВА

Сила нравственных ориентиров

← Начало на стр. III

Анастасия Подковыркина, куратор газеты «ЗавтраК», гимназия №210 «Корифей», г. Екатеринбург:

? Если подумать логически, то это были очень явные, провокационные вопросы. Используют ли их интернет-вербовщики в реальной жизни?

Елена ДОКУЧАЕВА:

– На самом деле, все так и есть. Пишут объявления типа: «Требуются люди без опыта, пишите». И когда им отвечают, практически в лоб сразу говорят, что необходимо поджечь, например, военкомат. Или совершить другое преступление. В открытую. Кто готов – тот готов. Работают именно с теми, кто среагировал. Мы уже упоминали о том, что очень часто играют, в том числе на желании популярности. Говорят подростку: «Ага, ты хочешь популярности? Мы тебе поможем. Сделай, как мы подскажем».

Егор ГОРБУНОВ:

– Важно понимать: вербовщики не сидят в подполье. Это люди, которые находятся за границей, и ответственности не опасаются. У них десятки сим-карт, десятки аккаунтов, с них пишут нон-стопом разные люди, которые меняются. Работает простой принцип отбора: написали тысячам – из них пятеро согласились. Всё отлично, план выполнен.

«ОГ»:

? Как понять, что именно сейчас тобой манипулируют в сети и продолжать общение потенциально опасно?

Елена ДОКУЧАЕВА:

– Самой жертве это сделать практически невозможно. Манипуляторы всегда ищут слабые точки. Мы выделили основные крючки и назвали эту концепцию ФИШ. Почему ФИШ? Это аббревиатура из начальных букв трех главных «наживок» – финансы, идея, шантаж, на которые рыбка («фиш») чаще всего попадается.

Первый крючок – «Ф», финансовый. Когда предлагают деньги, это должно сразу настораживать. Да, бывают легальные истории, но относиться к этому нужно предельно внимательно. Наш эксперимент показал: люди очень активно ведутся на такие манипуляции.

Второй крючок – «И», идея или игра на чувстве собственной важности. Человеку говорят: «ты уникальный», «только с тобой мы сможем изменить ход истории», «у тебя особая миссия, об этом напишут в учебниках». На этом крючке в первую очередь могут оказаться те, кто ведет замкнутую жизнь в онлайне, кому не хватает живого общения или отношений. Такие люди рады обманываться. У нас даже были случаи, когда жертвы влюблялись в своих кураторов, делая всё, чтобы оценил «любимый».

И третий крючок – «Ш», шантаж. Это прямой сигнал немедленно прекращать общение. Шантажировать могут чем угодно: от денег до личных данных, переписок и фотографий. Здесь важно понять: шантаж никогда не заканчивается. Если ты уступил один раз, на этом всё не остановится. Изменить ситуацию можно только одним способом – обратиться к тому, кто поможет. К родителям, наставникам, педагогам. И, конечно, надо идти за помощью в правоохранительные органы.

Мария Калистратова, ученица 8 класса, гимназия «Корифей»:

? Сейчас блокируют разные социальные сети и приложения, объясняя это тем, что там много мошенников. Как вы считаете, откуда ждать следующей опасности после очередной блокировки?

Елена ДОКУЧАЕВА:

– Везде, где мы появляемся, за нами следуют мошенники. Мы были у домашнего телефона – мошенники были в домашнем телефоне. Мы вышли на улицу – мошенники появились на улице. Мы сейчас в Интернете, во «ВКонтакте» – значит, мошенники будут во «ВКонтакте». Мы в Telegram – они там же. Мы в Max – и они там тоже. Всё сетевое медиапространство может быть небезопасным. Нужно просто принять это. И быть начеку.

Егор ГОРБУНОВ:

–Онлайн-среда и офлайн-среда одинаково опасны с точки зрения преступности. Просто, возможно, еще не для всех это очевидно. В реальной жизни, если вас позовет какой-нибудь подозрительный дядя из подворотни, вряд ли вы подойдете. А в Интернете почему-то идут. А ведь это ровно то же самое. В сети есть всё то же самое, что и в реальности, – преступники и мошенники в том числе. Не надо думать, что это абсолютное пространство безопасности, которое вы под себя настроили, и там всё будет только так, как вам надо.

«ОГ»:

? Если человек увидел противоправный контент, что ему делать? Обращаться в полицию?

Елена ДОКУЧАЕВА:

– Если вы видите какие-то радикальные видео, что-то экстремистское, что-то, что вас смущает, и вы понимаете, что это не должно находиться в общем доступе, – на всех платформах есть кнопка «пожаловаться». Если мы говорим про подозрения в вербовке – надо обращаться в ФСБ, МВД, прокуратуру через форму обратной связи на официальных сайтах этих ведомств. Обращение обязательно будет рассмотрено. Лучше не пытаться выяснить самому, стоят ли за объявлением террористы или нет, – по ту сторону работают люди со спецподготовкой. Есть прекрасный фильм, где по сюжету журналистка вела расследование, общалась с вербовщиком, а потом радикализовалась. В нашем эксперименте, о котором я рассказывала, напомню, десять человек дошли до конца. Никто не говорит, что это точно террористы. Но для нас это показательная цифра. Люди могут начать общаться с вербовщиками по разным причинам. Начинают в шутку, а в итоге могут потерять финансы, жилье, свободу. Просто открыв какую-нибудь ссылку или вкладку на телефоне.

Алиса Климовских, ученица 9 класса, медиастудия «Спектр», г. Ревда:

? Существуют ли стопроцентно защищенные приложения? Такие, где можно общаться, не боясь взлома, и где твоя личность и данные будут абсолютно защищены?

Елена ДОКУЧАЕВА:

– Любое приложение, увы, можно взломать. Не важно, чем вы пользуетесь. Важно, соблюдаете ли вы правила цифровой гигиены. У кого из вас стоит двухфакторная аутентификация в мессенджерах и соцсетях? Вот видите, не у всех. А она должна стоять везде. Потому что если у вас ее нет, если вы не используете облачный пароль или ставите пароли из даты рождения, которую легко найти, – о какой защищенности приложения мы тогда говорим? Даете ли вы мессенджерам все разрешения, не задумываясь, для чего они нужны? Случается, да? А так быть не должно. Это касается вообще всех приложений.

Егор ГОРБУНОВ:

– Мы с вами уже давно заплатили за цифровое удобство своей приватностью. Так или иначе, о нас очень много чего известно: история поиска, запросы, подписки, социальные сети, интересы. И часто вы сами даете разрешения приложениям на сбор информации. Кто и когда в последний раз читал любое пользовательское соглашение? В Лондоне проводили исследование: чтобы подключиться к бесплатному Wi-Fi в метро, нужно было пройти стандартную процедуру: ввести номер телефона и верифицироваться. Когда человек вводил номер, ему приходило пользовательское соглашение, в котором, в качестве эксперимента, было прописано, что человек обязуется несколько месяцев мыть в этом метро туалеты. Люди не читали – и соглашались. Не надо бояться какой-то глобальной слежки, но важно быть осознанным. У кого бывает такое: зашел в мессенджер посмотреть конкретную переписку – а потом ловишь себя через полчаса и понимаешь, что просто залип в телефон? Что происходит в этот момент? Вы становитесь жертвой манипуляции. Соцсети так работают, они заточены на то, чтобы привлечь ваше внимание. Эти технологии используют как для ведения бизнеса, так и для идеологической войны.

«ОГ»:

? Есть ли статистика, в каком психоэмоциональном состоянии люди, в том числе и подростки, наиболее подвержены влиянию киберпреступников?

Елена ДОКУЧАЕВА:

– К сожалению, подростков вовлекают в самые разные преступления. Начиная от лжеминирования, попыток поджога релейных шкафов и до более серьезных. К каждому человеку вербовщик и мошенник ищут индивидуальный подход. Сейчас появились новые технологии – те же самые фейки, кружочки, сгенерированные голоса близких, аудиосообщения. И человек – оп! И попадается. Часто ведутся на деньги. Но обозначить какие-то конкретные, единые крючки не получится – для каждого все-таки находится свой. А вот эмоциональное состояние жертв бывает похожим. Они ищут поддержки, у них снижен порог критического восприятия информации. Но важно понимать и другое: детей, особенно подростков, порой начинают шантажировать не только личными данными. Играют на страхе за близких. Дети идут на преступление, потому что им объясняют: «Родителей лишат прав, тебя отправят в детский дом, всё будет плохо. Но мы тебе поможем, если ты будешь делать то, что мы скажем». Были случаи, когда шантажировали перепиской, в которой речь шла о деньгах. Сначала объясняли, что надо