Глава 5

Остапы Бендеры наших дней

Киберпреступники прекрасно знают, что самым слабым звеном любой системы остается человек: «взломать» его проще, чем обойти технические средства защиты. Социальная инженерия — это психологическая атака, с помощью которой злоумышленник заставляет вас делать то, чего вы делать не должны.
В этой главе мы рассмотрим различные сценарии использования социальной инженерии и способы противодействия им.

Великому Комбинатору наше время наверняка бы понравилось. Его род занятий в современных терминах можно определить именно как социальную инженерию — метод психологического воздействия на человека с целью вынудить его совершить то, что выгодно злоумышленнику. Остап Ибрагимович оценил бы достоинства цифровых технологий: когда нет прямого контакта с потенциальной жертвой, то нет и риска получить шахматным конем по голове, если обман раскроется.

И последователи Остапа Бендера весьма преуспевают на этом поприще, ибо люди все также доверчивы и готовы отдать «ключ от квартиры, где деньги лежат» первому встречному, который по-общается с ними дружелюбно и авторитетно.

> *Увы, стопроцентной защиты от профессиональных обманщиков нет — даже специалисты по информационной безопасности иногда попадаются на их уловки, не говоря уже об обычных пользователях.*

Секрет успеха социальных инженеров в том, что они ловко используют против нас наши же чувства и эмоции: жадность, страх, любопытство, сострадание, альтруизм и даже любовь. Моральных барьеров для них не существует; нет такой подлости, на которую они не пойдут ради наживы. Они могут выманивать последние деньги у стариков, вовлекать подростков в торговлю наркотиками и сдавать их после этого полиции, или давить на жалость, собирая пожертвования якобы на операцию тяжелобольному ребенку.

Чаще всего интерес преступников носит чисто коммерческий характер. Их цель, выражаясь их же языком, — «развести» человека на деньги, поэтому дети обычно представляют для этой

публики меньший интерес, чем взрослые. Но успокаиваться было бы ошибкой. Во-первых, дети вырастут, заведут собственные счета в банках и тоже станут объектом охоты, а, значит, они должны быть подготовлены к взрослой жизни. Во-вторых, монетизация социальной инженерии может быть и не столь прямой, но куда более циничной и опасной. Например, некто может уговорить девочку-подростка всего на одну фотографию в обнаженном виде — и эта фотография сломает ей жизнь, как это случилось с Амандой Тодд[1].

Некто может уговорить девочку-подростка всего на одну фотографию в обнаженном виде — и эта фотография сломает ей жизнь.

Увы, несмотря на все усилия полиции в разных странах, рынок детской порнографии существует, и кто-то зарабатывает на этом. Целью может быть и вербовка в экстремистские организации и деструктивные сообщества, что тоже хорошо оплачивается заинтересованными политическими структурами.

Тем не менее, руки опускать не стоит. Соблюдая ряд простых правил, можно значительно снизить риск пополнить статистику жертв компьютерных преступлений, совершаемых при помощи социальной инженерии. Для этого следует познакомиться с их основными приемами и научиться постоянной бдительности. Главное — не стать при этом законченным параноиком. Сложно? Да! Мир чрезвычайно усложнился, но надо учиться в нем жить.

«Доверяй, но проверяй» — советует эксперт по информационной безопасности Алексей Лукацкий:

1 *См. главу про кибербуллинг.*

«В сфере безопасности доверие — именно та точка, с которой начинается провал. Сейчас среди специалистов в этой области широко распространена концепция Zero Trust Security — «безопасность с нулевым доверием». Мы изначально исходим из того, что никакого доверия быть не должно, и рассматриваем протоколы и программы, исходя из того, что против нас действует враг, который может подменить кого-то, выдать себя за кого-то и т.п. Подобную стратегию я рекомендую и обычным пользователям. Конечно, это работает далеко не всегда: ведь человеку присуще испытывать доверие, и именно этим пользуются киберпреступники. А если не доверять никому, то жить становится неинтересно, грустно и тяжело»[1].

На жадину не нужен нож

В 1990-х годах, когда все пользовались, в основном, наличными деньгами, а не карточками, уличные мошенники широко практиковали такой сценарий: вы идете по оживленной улице, и вдруг неожиданно вам под ноги падает тугая пачка долларов. В ту же секунду появляется случайный прохожий, который восклицает: «Вот нам повезло!», — и предлагает поделить деньги. Даже если у вас и были моральные терзания из серии «А, может, отдать хозяину?», ваш новый знакомец быстро их гасит и настойчиво предлагает отойти в укромное место, чтобы пересчитать добычу. В этот момент появляется «потерпевший»

1 *Алексей Лукацкий. «Не заклеивайте камеру!» 8 правил кибербезопасности для всех. // Идеономика (**ideanomics.ru**), 23 января 2018.*

(как правило, не один), и, даже если вы готовы с радостью вернуть пропажу, вы все равно «попали» на деньги, потому что мошенник утверждает, что в пачке было больше, чем вы отдали, а поскольку перевес в физической силе на его стороне, то спорить бесполезно — приходится выворачивать карманы якобы для более точного пересчета. Тут-то вас и обчистят.

> *Встречалось множество вариаций этой схемы, но итог был один — вы в минусе, преступники в плюсе. Нехитрый спектакль разыгрывали на улицах до тех пор, пока большинство людей не узнали о ловушке и не перестали в нее попадаться. Доходность промысла упала, и жулики переключились на другие способы обмана граждан.*

Помню, как-то раз и мне выпала такая «удача» на Манежной площади, но я проигнорировал свой шанс немного разбогатеть, несмотря на уговоры внезапно материализовавшегося возле меня товарища, чем его очень расстроил. Не то чтобы я был такой умный и проницательный, просто несколькими днями раньше мне попалась статья о таком способе обмана, и вовремя полученное знание уберегло меня от неприятностей.

Даже когда здравый смысл кричит «Это ловушка!», жадность шепчет «Все получится!» — и человек отдает деньги.

Тогда основным источником информации были газеты и «сарафанное радио», теперь — интернет и социальные сети. Казалось бы, все фокусы жуликов давно описаны и разобраны по шагам, но люди все равно продолжают попадаться на самые примитивные «разводки». Причина, по-видимому, заключается в том, что почти все мы в какой-то мере инфицированы вирусом

жадности, вакцину от которого так и не изобрели. Даже когда здравый смысл кричит «Это ловушка!», жадность шепчет «Все получится!» — и человек отдает деньги, порой весьма немалые, ловким пройдохам просто потому, что они сочинили красивую сказку, в которую так и хочется поверить.

> *Иначе как объяснить недавний случай, когда женщина из Камбоджи отдала 75 тысяч долларов выпускнику средней школы в Нигерии, который создал в Instagram* фальшивый аккаунт и прикинулся американским пилотом[1]? Все было как обычно: они познакомились в Сети, и он, что называется, напел ей про красивую жизнь летчика и большие заработки, а потом предложил вместе провернуть одно дельце: дескать, он пришлет ей дорогих вещей на 500 тысяч долларов, чтобы продать их и вложить деньги в камбоджийскую недвижимость. Но... прежде ей нужно будет оплатить пошлину. (Как можно поверить в такую чушь? Не спрашивайте!) Для вящей убедительности «летчик» подключил к афере друга из Индонезии, изображавшего сотрудника курьерской почты. За первую посылку сообщники попросили 800 долларов; потом якобы возникли трудности, и нужно было доплатить еще (как всегда), и так далее — камбоджийка все платила и платила, втянувшись в эту игру, и даже взяла кредит в банке.*

Жадность — болезнь почти неизлечимая, она поражает мозг, блокируя критическое мышление, причем не только жертвы, но и преступников. Ведь они сорвали весьма солидный

---

* *Соцсеть признана экстремистской и запрещена на территории РФ.*

1 *19-year-old impersonates American pilot, defrauds woman of N27m. // PUNCH, 29.02.2020.*

куш, на который и рассчитывать не могли! Пора было бы и остановиться — но нет. А зря!

> *В минуту просветления несчастная жертва заметила, что «американский пилот» звонит ей с нигерийского номера, и обратилась в полицию. Дальнейшее было делом техники — начинающего социального инженера отследили по SIM-карте и арестовали.*

Этого лжепилота по имени Чигемезу Арикибе можно признать достойным продолжателем национальных традиций. Его старшие товарищи рассылали знаменитые «нигерийские письма» по всему миру, начиная с 1980-х годов (в бумажном виде, разумеется). С появлением электронной почты дело поставили на поток, и вряд ли можно найти человека, ни разу не получавшего подобный спам. Обычно в таком письме рассказывается душещипательная история про принца или принцессу, томящегося в лагере беженцев, бывшего министра, убитого повстанцами, внезапно умершего богатого бизнесмена, не оставившего наследников, и тому подобное. Суть всегда одна: якобы в некоем банке зависли огромные деньги, и с вашей помощью их можно вытащить — за что вам обещают щедрое вознаграждение. То есть вам предлагают соучастие в преступлении, если называть вещи своими именами, и, как ни странно, многие соглашаются.

Сюжеты «нигерийских писем» настолько фантастичны и абсурдны, что поверить в этот бред может только абсолютно неадекватный человек, неспособный усомниться и просто погуглить, проверить: есть ли хоть крупица правды в полученном письме. За творческий подход к сочинительству авторам

«нигерийских писем» в 2005 году даже коллективно присудили Шнобелевскую премию[1] по литературе. Однако на церемонию награждения никто не явился — лауреаты предпочли остаться анонимными.

Пожалуй, наиболее блестящим образцом этого жанра можно считать историю нигерийского космонавта, застрявшего на орбите:

> *«Меня зовут Бакаре Тунде, я брат первого нигерийского космонавта, майора ВВС Нигерии Абака Тунде. Мой брат стал первым африканским космонавтом, который отправился с секретной миссией на советскую станцию «Салют-6» в далеком 1979 году. Позднее он принял участие в полете советского «Союза Т-163» к секретной советской космической станции «Салют-8Т». В 1990 году, когда СССР пал, он как раз находился на станции. Все русские члены команды сумели вернуться на землю, однако моему брату не хватило в корабле места. С тех пор и до сегодняшнего дня он вынужден находиться на орбите, и лишь редкие грузовые корабли «Прогресс» снабжают его необходимым. Несмотря ни на что, мой брат не теряет присутствия духа, однако жаждет вернуться домой, в родную Нигерию. За те долгие годы, что он провел в космосе, его постепенно накапливающаяся заработная плата составила*

1 *Шнобелевская (Игнобелевская, Антинобелевская) премия (англ. Ig Nobel Prize, от игры слов: англ. ignoble — «постыдный») — пародия на престижную международную награду — Нобелевскую премию. Десять Шнобелевских премий вручаются в начале октября, то есть в то время, когда называются лауреаты настоящей Нобелевской премии, — «за достижения, которые заставляют сначала засмеяться, а потом — задуматься» (first make people laugh, and then make them think) («Википедия»).*

15 000 000 американских долларов. В настоящий момент данная сумма хранится в банке в Лагосе. Если нам удастся получить доступ к деньгам, мы сможем оплатить Роскосмосу требуемую сумму и организовать для моего брата рейс на Землю. Запрашиваемая Роскосмосом сумма равняется 3 000 000 американских долларов. Однако для получения суммы нам необходима ваша помощь, поскольку нам, нигерийским госслужащим, запрещены все операции с иностранными счетами.

Вечно ваш, доктор Бакаре Тунде, ведущий специалист по астронавтике».

Нормальный человек посмеется над этим и пройдет мимо. Однако в столь несуразном, на первый взгляд, подходе есть свой смысл: люди даже с минимальными зачатками рационального мышления отсекаются сразу, что экономит ресурсы мошенников. Ведь если «клиент» «заглотил наживку», приходится вступать с ним в личный контакт, отвечать на его вопросы, разговаривать по телефону, а это требует времени и дополнительных расходов.

Схема стала настолько популярной, что у нее появилось собственное название — «Разводка 419» («Scam 419»), по номеру соответствующей статьи в уголовном кодексе Нигерии. Поскольку криминальное сообщество не уважает авторские права, эту схему стали использовать мошенники всех стран — разумеется, без каких-либо отчислений ее изобретателям, так что «нигерийской» считать ее можно весьма условно. Отправитель письма может находиться где угодно — в Латвии, Египте, США, Мексике, Украине, Венгрии, Малайзии, Колумбии и, само собой, в России. Нигерия больше не удерживает пальму первенства

в этом виде жульничества, но из-за общей бедности и высокого уровня коррупции для многих молодых нигерийцев такой способ заработка остается едва ли не единственно возможным и, кстати, весьма доходным — некоторым из них удается получить до 60 тысяч долларов в год. С такими деньгами в Африке действительно можно жить как принц или космонавт. И даже лучше.

Конечно же, вы не настолько наивны, чтобы принять участие в спасении Абака Тунде с борта станции «Салют», которая, как выясняется, не затонула в Тихом океане, а все летает и летает вокруг Земли с несчастным нигерийцем на борту. Означает ли это, что вас нельзя поймать на крючок жадности? Едва ли. Пусть отечественные коллеги нигерийских мошенников и не прославились литературными шедеврами, но действуют они не менее изобретательно.

> *Например, вам приходит SMS, в котором говорится о выигрыше в лотерее с новенькой Audi в качестве приза. (Мне приходило.) Но сначала вам нужно перечислить небольшую сумму, чтобы подтвердить свое участие, или просто послать ответное SMS на указанный номер, который… оказывается платным. И сколько б не твердили миру про бесплатный сыр, который бывает только в мышеловке, азарт и жадность снова выигрывают у логики.*
>
> *Бывает и проще: вам говорят (или пишут), что вы выиграли небольшой денежный приз, и просят сообщить данные банковской карты. Правда, чуть больше данных, чем нужно для перевода, зато вполне достаточно для снятия. Что удивительно, попадаются на эту разводку преимущественно мужчины среднего возраста с опытом работы в силовых*

структурах. Может быть потому, что рисковать — дело для них привычное?

Таких сценариев множество, рассказать про все нереально. Помните, Остап Бендер говорил, что знает четыреста относительно честных способов отъема денег у населения? Он не преувеличивал. Главное, что следует уяснить: не будьте самонадеянны! Мошенники постоянно оттачивают свои приемы и изобретают новые. Не считайте себя умнее их, потому что вас могут подловить как раз на знании общеизвестных схем.

Не будьте самонадеянны! Мошенники постоянно оттачивают свои приемы и изобретают новые.

Например, в письме будет сказано, что отдел борьбы с компьютерными преступлениями полиции Нигерии арестовал шайку спамеров; в их списке рассылки обнаружен ваш адрес, поэтому вам, как пострадавшему, причитается компенсация; сообщите, пожалуйста, данные вашей карты. К гадалке не ходи: жадность снова уговорит кого-то сделать очередную глупость.

Или вот еще относительно новый прием[1], специально для технически подкованных жадин. На ваш телефон несколько раз звонят с какого-то неизвестного номера и сразу сбрасывают. Что делает заботящийся о своей безопасности человек? Правильно: он гуглит подозрительный номер и — о, чудо! — видит ссылку на страницу, где владелец номера, похоже, пытался сделать перевод в криптовалюте, но у него чуть-чуть не хватило средств для завершения транзакции — система сообщает, что на счету

1 *Высокотехнологичные нигерийские письма. // **Habr.com**, 14 июля 2019.*

должно быть минимум 2,5 биткойна. Сессия осталась открытой (вот же он лох!), нужно всего-то кинуть на этот кошелек 0,01 битка, указать свой адрес в качестве получателя и вуаля — тысяч 15–20 долларов у вас в кармане!

А на самом деле? На самом деле, сто наивных любителей халявы вроде вас — и целый биткойн в кошельке криптожуликов, причем никто не побежит жаловаться. Гениально!

«Это звонок из службы безопасности банка...»

Кроме жадности, социальные инженеры активно эксплуатируют наше чувство страха. Нет, им для этого не надо внезапно выскакивать из монитора или рассказывать на ночь леденящие душу истории типа «черной-черной ночью в черной-черной комнате...». Все куда прозаичнее: они играют на страхе человека потерять деньги.

Звонящий представляется сотрудником службы безопасности банка и говорит, что с вашего счета вот-вот уйдет крупная сумма, и если прямо сию минуту ничего не предпринять, то будет поздно. В такой ситуации человек может запаниковать и, не успев ничего сообразить, выдать мошенникам нужную им информацию. И вот тогда действительно его счет выпотрошат в ноль.

Добавит печали осознание факта, что денег вам никто не вернет. Закон в этом случае будет на стороне банка: если клиент в результате обмана или злоупотребления доверием сам нарушил условия

договора, обязывающие сохранять конфиденциальность платежной информации, и сообщил ворам номер карты, пароль, присланный в SMS, CVV-код и другие сведения, то компенсации ему не положено.

> *В 2019 г. мошенники провели около 577 000 операций с использованием электронных средств платежа без согласия клиентов банков — физических и юридических лиц. Сумма таких операций превысила 6,4 млрд руб., подсчитал ФинЦЕРТ (Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России). Средняя сумма похищенного со счетов физлиц составила 10 000 руб., юрлиц — 152 000 руб. Банки возместили клиентам 935 млн руб. — говорится в отчете, то есть примерно один рубль из семи похищенных (15%). Статистику возвратов ЦБ публикует впервые*[1].

Телефонные мошенники нашли «золотую жилу» и будут ее разрабатывать, пока денежный поток не иссякнет. Число пользователей банковских услуг растет, увеличивается и число потенциальных мишеней преступников. Остановить эту волну может только осведомленность людей о таком способе обмана.

К сожалению, пресечь на корню саму возможность телефонного мошенничества силами правоохранителей едва ли получится, ведь преступники могут находиться где угодно, необязательно в России, а телефонная сеть, в принципе, устроена так, что можно позвонить

---

1 *Мошенники в прошлом году украли у клиентов банков 6,4 млрд рублей. // Ведомости, 19 февраля 2020.*

с любого номера на любой другой. Блокировать телефоны мошенников в такой ситуации технически и юридически очень сложно.

На первых порах подпольные колл-центры организовывали в местах лишения свободы, сейчас — в обычных офисах или квартирах. Полиция может поймать одну шайку, но ей на смену придет новая. Порог входа в этот «бизнес» низкий, доходность высокая, риски небольшие. Нужно лишь найти несколько молодых людей с хорошо подвешенным языком, базу номеров для обзвона, и можно начинать. Кстати, совершенно необязательно красть базу данных из банка.

> *«По сути, для завязки разговора всего-то нужно знать номер телефона, фамилию, имя и отчество. Основной сценарий, который используют злоумышленники, кстати, не предполагает знания, в каком банке у клиента открыт счет, — говорит Артем Сычев[1], замдиректора департамента Банка России по информационной безопасности. — Человека «раскручивают» на то, чтобы он сам рассказал, в каком банке обслуживается, какие у него счета, какие операции он совершает; чтобы назвал злоумышленнику номер карты, подтвердил, что ему пришла эсэмэска с паролем. На данный момент нам известны 15 различных мошеннических сценариев. Утечки баз данных, к сожалению, действительно есть. Но информация о клиентах, утекшая из банков, — это капля в море по сравнению с тем количеством людей, которых обзванивают мошенники».*

Но есть и хорошие новости. По сравнению с 2018 годом клиенты банков стали осторожнее: тогда на социальную инженерию

1 *Телефон недоверия. // Российская газета, 16 февраля 2020.*

приходилось 97% мошеннических операций, а в 2019 — только 69%. Прогресс налицо, и если так пойдет дальше, то через год-другой эта схема станет нерентабельной.

Пока же интересно и неожиданно то, что жертвами обмана чаще всего становятся не пенсионеры, как можно было бы подумать, а экономически активные граждане в возрасте от 28 до 55 лет. Но и это вполне объяснимо: во-первых, у них есть деньги; во-вторых, они активно пользуются технологиями и в целом доверяют им — ведь если жулики позвонят какой-нибудь бабушке и даже уговорят ее сказать им пароль от интернет-банка, она все равно едва ли сможет его найти. А вот продвинутый пользователь это сделает запросто. Для особо бдительных, которые помнят, что никому нельзя сообщать пароли и пин-коды (в том числе и сотрудникам банка), предусмотрена еще одна ловушка: их переключают на «автоматизированную систему», которая, как нетрудно догадаться, есть лишь имитация настоящей.

Поэтому, хотя об этом много раз говорили, не лишним будет напомнить:

> *Если вам позвонили из банка, не пытайтесь угадать, настоящий это звонок или разводка. Уточните причину и сами перезвоните в банк по заранее сохраненному номеру на своем телефоне. Или зайдите в мобильное приложение и задайте вопрос в чате. Оба эти способа вполне надежны.*

И еще раз: все входящие телефонные звонки — какой бы номер на экране ни высвечивался — по определению считаются подозрительными. Финансовые вопросы по таким каналам обсуждать категорически нельзя!

Если друг оказался вдруг... взломан

«Не имей сто рублей, а имей сто друзей» — гласит пословица, известная всем со школы. В трудную минуту мы обращаемся к друзьям за помощью и готовы ответить им тем же.

А где сейчас все наши друзья? Правильно, в мессенджерах и соцсетях. Этим и пользуются мошенники: взломав чей-либо аккаунт, они начинают рассылать просьбы перечислить денег по всему списку контактов. А нас же учили, что «друг в беде не бросит, лишнего не спросит», правда? 500 рублей на телефон? Надо так надо, не приставать же с расспросами, когда у человека и так проблемы. И сумма эта вовсе не предел — иногда люди отдают злоумышленникам куда больше, поверив в легенду, которую им подсунули.

Казалось бы, все знают и про этот прием социальной инженерии, и про то, что лучше позвонить и удостовериться: друг ли это обращается к вам или мошенник. Но мы настолько привыкли к общению в текстовом формате, что этот нехитрый трюк часто срабатывает. Задним умом крепки все, но прежде, чем упрекать кого-то в излишней доверчивости, вспомните: социнженеры — хорошие психологи, они прекрасно понимают, что один-единственный звонок раскроет их обман, и придумают дюжину убедительных причин, почему пообщаться голосом никак невозможно, а дело срочное.

Например, человек находится в другой стране, телефон украли, пишет он вам с чужого компьютера, и единственный пароль, который смог вспомнить, это пароль от Skype. Ваши действия? Здравый смысл подсказывает, что все выглядит подозрительно,

и что именно Skype чаще всего и взламывают. Но что, если ваш приятель действительно попал в беду?

Прежде чем расстаться с деньгами, постарайтесь проверить, кто же на самом деле с вами общается.

Прежде чем расстаться с деньгами, постарайтесь проверить, кто же на самом деле с вами общается. Первое, что приходит на ум, — задать вопрос, ответ на который знает только ваш друг. Так в фильме «Гостья из будущего» Коля Герасимов проверял, точно ли перед ним его друг Фима, а не космический пират:

— Как прозвище нашего физкультурника?
— Илья Муромец.
— А, это ты, Королёв.
— Честное пионерское.

Хороший способ, но есть одна проблема: если вы закончили школу лет 10–20 назад, то можете и не вспомнить прозвище вашего физкультурника. А как быть, если ваш друг тоже его забыл? Да и вообще, трудно сходу придумать уникальный вопрос для каждого — нас ведь связывают с разными друзьями очень разные вещи.

Поэтому лучше обратиться к опыту капитана Алехина из романа Владимира Богомолова «В августе 44-го».

> *В кульминационный момент его группа встречает в лесу опаснейшего немецкого агента в сопровождении двух пособников. Все трое — в советской форме, документы у всех в порядке, отвечают уверенно, держатся естественно. Мо-*

жет, и вправду свои? Чтобы вывести врага на чистую воду, Алехин как бы невзначай задает вопрос о несуществующем персонаже — некоей поварихе, якобы служившей в том госпитале, где он якобы лежал, и где, судя по документам, лечился подозреваемый.

«Нет, не знаю, — после некоторой, пожалуй, излишне затянутой паузы угрюмо сказал старший лейтенант. — Я поварихами не интересовался!»

А что тут ответишь с ходу? Сказать: «Знаю», — а вдруг это вопрос-ловушка, и никакой такой поварихи там нет? Сказать: «Не знаю», — а если это опять же ловушка, и она там — местная знаменитость, которую не знать просто невозможно?

Алехин же, провоцируя «лейтенанта», просто внимательно следил за его реакцией. И того выдала излишняя напряженность в ответе на второстепенный, казалось бы, вопрос. Потому пользуйтесь приемом особистов СМЕРШа, если у вас возникли даже малейшие сомнения в вашем собеседнике. «Бдительностью дело не испортишь!» — говорил капитан Алехин, и, безусловно, был прав.

Бывает и так, что взломали ваш аккаунт, а ваши друзья оказались не столь бдительны и откликнулись на ложный призыв о помощи. Ситуация неловкая: с одной стороны, они сами виноваты; с другой — вы пусть и невольная, но причина их финансовых потерь. Возмещать им понесенный урон или нет? Формально вы не обязаны. Не поддавайтесь первому порыву, обдумайте случившееся спокойно, а потом уже решайте.

Ловись, рыбка, большая и маленькая

Любопытство и невнимательность — еще два свойства человеческой натуры, тянущие нас в западни, расставленные социальными инженерами. Принцип действия таких ловушек чрезвычайно прост: пользователь получает письмо или сообщение с интригующим содержанием, открывает вложенный файл или кликает по ссылке — и он попался! Его данные утекают к злоумышленникам, которые даже не потрудились взломать систему или расшифровать пароль.

Такой способ кражи логинов и паролей, телефонов, номеров кредитных карт и других конфиденциальных данных называется **фишинг** и считается одним из методов социальной инженерии, требующим также и технических навыков.

> *Английский термин "phishing" — это неологизм, образованный как омофон (то есть звучит одинаково, а пишется по-разному) от слова "fishing" (по-русски — «рыбалка»), что довольно точно передает суть явления: хакер забрасывает наживку и ждет, пока пользователь «клюнет», то есть откроет зараженный файл или перейдет по ссылке.*
>
> *Происходит этот термин от сочетания слов "phreak" и "fishing". В свою очередь, "phreak" родилось из "phone" и "freak" — в 1970-х так называли технически продвинутых фриков, которые взламывали телефонные сети ради бесплатных звонков или других фокусов.*
>
> *Само же исходное слово "freak" имеет богатую и запутанную историю, уходящую корнями в XVI век. По-русски можно сказать «чудак», но это не передаст всех смыслов оригинала.*

Есть три варианта фишинга. В первом происходит заражение вирусом-троянцем, который спрятан во вложенном файле или на сайте, куда ведет ссылка. Этот троянец установит на ваше устройство бэкдор[1], который превратит компьютер в узел ботнет-сети, и кейлоггер[2], который украдет ваши логины и пароли, и майнер криптовалют[3] — все, чего пожелает взломщик.

Во втором варианте ссылка ведет на поддельный сайт — например, государственного органа, где вас попросят ввести свои данные. Визуально подделка выглядит точь-в-точь как настоящий сайт, и едва ли вы что-то заподозрите. Например, в почту вам пришло уведомление о штрафе от ГИБДД. Если у вас есть машина, то вы захотите узнать, где именно вы нарушили правила, а если нет — возмутиться и сообщить об ошибке. Но сначала вас попросят авторизоваться — как на настоящем сайте Госуслуг. Чаще всего подделывают сайты банков, авиакомпаний, государственных учреждений, интернет-магазинов и так далее — то есть те, где ввод платежных и персональных данных выглядит естественно.

---

1 *Бэкдор (от англ. back door — «черный ход», буквально «задняя дверь») — дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом.*

2 *Кейлоггер (англ. keylogger) — программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя, — нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т. д.*

3 *Под скрытым майнером подразумевается программа-вирус, которая использует ресурсы вашего компьютера для добычи криптовалют. Делается это в автоматическом режиме без ведома пользователя и каких-либо предупреждений.*

При появлении фишинговой страницы счет идет на часы, иногда — на минуты, поскольку пользователи несут серьезный финансовый, а если это компания, то еще и репутационный ущерб. Некоторые фишинговые страницы менее чем за сутки нанесли ущерб на суммы от миллиона рублей[1].

Есть еще и третий вариант, когда фишинговый сайт или приложение создаются под видом полезного ресурса. Особенно фишеры любят маскироваться под бесплатный антивирус — программу для оптимизации работы компьютера — и тому подобное. Более того, иногда они даже работают. Самый анекдотичный, но вполне реальный случай — сайт, предлагающий проверить, есть ли ваша кредитная карта в базе данных хакеров. Вы вводите номер и другие реквизиты — и теперь ваша карта точно у них есть. Как это ни смешно, находятся те, кто им верит.

Можно ли защититься от фишинга техническими средствами? От первого варианта — практически нет. Человек сам принимает решение открыть файл или перейти по ссылке, то есть открывает дверь злоумышленникам. Можно только уповать на то, что антивирус отследит подозрительную активность троянца, или что браузер предупредит о небезопасном сайте, но это уже вторая линия обороны, и она тоже может пропустить атаку.

Популярный совет «Не открывать подозрительные файлы и ссылки» в реальной жизни помогает мало.

1 *Деньги на ветер: почему ваш антифишинг не детектирует фишинговые сайты, и как Data Science заставит его работать? // **Habr.com**, блог Group IB, 31 августа 2018.*

Популярный совет «Не открывать подозрительные файлы и ссылки» в реальной жизни помогает мало. Потому что никто вам не скажет, чем (в общем случае) подозрительная ссылка отличается от неподозрительной. Правильным будет считать подозрительными все спам-рассылки и сообщения от незнакомцев, но письмо может прийти от кого угодно — в том числе от вашего друга, почту которого взломали. И текст будет абсолютно правдоподобным, разве что вас немного удивит фраза «Вот фотки с корпоратива, которые я обещал», а вы ничего такого не припоминаете. Но любопытство вполне может пересилить чувство осторожности... Так что нам остается полагаться только на интуицию и здравый смысл. И — что ж поделать — быть немного параноиками.

Чтобы снять опасения, разумнее всего переспросить отправителя, что именно он вам послал и с какой целью. Причем сделать это желательно по другому каналу связи (и держа при этом в уме, что, возможно, вам отвечает злоумышленник, — вспомним предыдущий раздел). Если ответ вас удовлетворит, открывайте послание.

> *Кстати, когда вам нужно переслать кому-то файл или ссылку, не поленитесь написать несколько слов о том, что это и зачем, чтобы ваш адресат тоже не терзался сомнениями. Считайте это обязательным правилом цифрового этикета.*

Со вторым вариантом, когда мы потенциально сталкиваемся с сайтом-подделкой, немного проще: тут можно подстраховаться техническими средствами. Понятно, что человеческий глаз не обратит внимания на небольшое отличие в веб-адресе: допустим, вместо **moi-lyubimyi-bank.ru** будет **moi-lyubimyi-bank.su**. Но менеджер

паролей[1] обнаружит эту разницу и не подставит автоматически ваши данные в форму авторизации, даже если внешнее сходство подделки с оригиналом будет идеальным.

> *Полезный совет: если вместо интернет-банка пользоваться мобильным приложением, то на удочку фишеров вы не можете попасться в принципе, потому что приложение само помнит правильный адрес.*

Это касается и всех других сервисов, где надо осуществлять платежи или передавать персональные данные. Но используйте только официальные приложения!

Что касается третьего варианта с мнимо полезными сайтами, то здесь нам отчасти приходят на помощь разработчики браузеров — встроенные средства антифишинговой защиты есть в Chrome, Firefox, Opera, Microsoft Edge, Internet Explorer и других приложениях для веб-серфинга. Когда вы пытаетесь перейти по какому-либо адресу, браузер проверяет, нет ли его в списке фишинговых. Если проверка проходит успешно, открывает его. Внимательный читатель сразу заметит брешь: такая защита эффективна только против известных угроз. А как быть с новыми, если адрес еще не успели внести в базу? Ответ донельзя прост: соблюдать осторожность и не ходить куда попало.

Чтобы оценить масштаб проблемы, обратимся к цифрам. По данным Anti-Phishing Working Group за 4-й квартал 2019 года было выявлено 162 тысячи уникальных фишинговых сайтов, причем каждый такой сайт может использовать тысячи веб-

---

1 *См. главу о паролях.*

адресов, ведущих в итоге на один источник угроз. Для сравнения — в мире регистрируется порядка 20 миллионов доменных имен в квартал[1]. То есть 1-2% всех веб-адресов принадлежат фишерам. И протокол **https** больше не является гарантией безопасности.

> *Среди советов по цифровой гигиене можно встретить и такой: лучше посещать только сайты, работающие по протоколу* ***https****, где буква «s» значит «secured» («безопасный»). То есть те, у которых адресная строка начинается с* ***https://*** *(или видна иконка закрытого замка), например,* ***https://google.com****. А если адрес начинается просто с* **http://** *без буквы «s» (или на иконке замок разомкнут), то это может быть фишинговый сайт.*
>
> *В наши дни этот совет устарел. По данным на конец 2019 года три из четырех фишинговых сайтов использовали защищенный протокол* ***https***[2]*. Несмотря на то, что это дополнительные расходы — сертификат безопасности стоит до нескольких сотен долларов, киберпреступники идут на это, чтобы вводить пользователей в заблуждение. Так что наличие буковки «s» больше не говорит о безопасности.*

Фишеры очень оперативно реагируют на актуальную повестку. Как только весь мир заговорил о коронавирусе, тут же, как грибы, стали вырастать мошеннические сайты. Ки-

---

1 *По данным за 3-й квартал 2019 г. 100+ Internet Statistics And Facts For 2020. //* ***websitehostingrating.com****, 17 июня 2020.*

2 *Phishing Activity Trends Report 1th Quarter 2020. // APWG.org, 11 мая 2020.*

берпреступники используют интерес к глобальной эпидемии для распространения своей злонамеренной активности. По данным Check Point Software Technologies[1] вероятность того, что домены, связанные с коронавирусом, представляют киберугрозу, на 50% выше, чем опасность любых других доменов, зарегистрированных в течение того же периода. Это, кстати, относится к любым другим доменам, связанным с «сезонными» темами, которые хакеры обычно используют для кибератак.

> *Эксперты по информационной безопасности советуют пользователям быть внимательными при работе с веб-площадками, в URL-адресе которых фигурируют такие ключевые слова как «coronavirus», «covid», «vaccine», «корона», «ковид», «вирус».*

Аналогичным образом злоумышленники эксплуатируют и другие сезонные темы. Так, в преддверии Дня святого Валентина отмечается 200% рост вредоносных веб-сайтов, посвященных этому празднику. Только за первую неделю февраля 2020 года мы увидели более 10 тысяч доменов со словом «Valentine», к которым обращались пользователи по всему миру. Угрозы на таких веб-сайтах могут различаться, и включают в себя онлайн-мошенничество, кражу учетных или платежных данных, а также заражение вредоносным ПО[2].

---

1 *Update: Coronavirus-themed domains 50% more likely to be malicious than other domains. // Check Point Software, 5 марта 2020.*

2 *Valentine's & Chocolate Don't Always Equal Love. // Check Point Software, 12 февраля 2020.* ***https://novayagazeta.ru/articles/2016/05/16/68604-gruppy-smerti-18***

«Синий кит», «красная сова» и все-все-все

В мае 2016 года в «Новой газете» вышла статья[1] Галины Мурсалиевой о существовании в сети «ВКонтакте» некой игры, финальной целью которой является совершение самоубийства, и что, по информации редакции, жертвами организаторов этого сообщества стали 130 подростков в разных городах России. Чтобы попасть в игру, нужно было вступить в одну из так называемых «групп смерти» и выполнять все более и более разрушительные для психического и физического здоровья задания «кураторов», в итоге приводящие игрока к гибели.

> *Символом одной из таких групп был синий кит — этот образ, растиражированный СМИ, мгновенно приобрел вирусную популярность. Почему кит? Потому что киты выбрасываются на берег, совершая самоубийство. Иногда массово. Почему синий? Потому что синий — цвет грусти. Какие-либо конкретные биологические особенности голубого полосатика (по-латыни Balaenóptera músculus) значения для игры не имеют.*
>
> *Статья о «группах смерти» набрала более 1,5 миллиона просмотров за два дня, информация разлетелась по родительским чатам, и встревоженные мамочки донесли ее до каждого ребенка — даже до того, кто ни о чем таком не то что не помышлял, а и слыхом не слыхивал. В результате паника взрослых оказалась настолько заразительной, что возымела обратный эффект. Дошло до того, что в Екатеринбурге девочка пыталась покончить с собой*

1 *Галина Мурсалиева, Группы смерти (18+) // Новая газета, 16 мая 2016.*

после школьной лекции о «Синемките»[1] — ее буквально сняли с крыши.

После публикации статьи Следственный Комитет начал проверку по изложенным фактам и возбудил уголовное дело. Спустя несколько месяцев в подмосковном Солнечногорске арестовали 21-летнего безработного Филиппа Будейкина, известного в интернете под ником «Филипп Лис», предполагаемого администратора «Группы смерти». Собственно, он и не прятался — все лето и осень Лис раздавал интервью и хвастался своими «успехами», пожиная плоды хайпа, к которому так стремился.

Всего Будейкину хотели инкриминировать 15 эпизодов доведения подростков до самоубийства — об этом сообщил в интервью[2] «Новой газете» руководитель первого следственного отдела первого управления по расследованию особо важных дел ГСУ СК по Санкт-Петербургу Антон Брейдо. Однако ни по одному из них связь с обвиняемым доказана не была.

Кроме того, в деле была одна попытка совершения суицида, в которой фигурировала единственная конкретная потерпевшая — ее удалось спасти. Но и тут все оказалось неоднозначно: девочка с 12 лет «слышала голоса», была подписана на несколько сотен групп суицидальной тематики и уже пыталась совершить самоубийство годом ранее.

---

1 *В Екатеринбурге девочка пыталась покончить с собой после школьной лекции о «Синем ките». // Росбалт, 22 марта 2017.*

2 *Галина Мурсалиева. Биомусор // Новая газета, 12 декабря 2016.*

Мнения экспертов-лингвистов и психиатров по поводу того, насколько повлияло на ее поступок участие в «Группе смерти», разошлись. Психолого-лингвистическая экспертиза показала разрушительное воздействие постов и сообщений Лиса на психику девушки. Психиатры же на вопрос о способах психологического манипулирования, которому подвергался ребенок, ответили, что не существует общепризнанных каким-либо сообществом теорий и тем более методик психологического давления и манипулирования.

Следовали допросили и других участников игры, не пытавшихся совершить суицид. Одни говорили, что всем была понятна ее шуточная природа, другие признавались, что воспринимали пропаганду суицида серьезно, она вызывала у них мысли о самоубийстве и подавленное состояние.

Тем не менее, в июне 2017 года суд приговорил Будейкина к 3 годам и 4 месяцам колонии-поселения. Он освободился в марте 2019-го. Сегодня Филипп работает администратором в тренажерном зале и уверяет, что в интернете почти не сидит: времени нет[1].

Тогда же, в июне 2017-го, был принят закон[2] об ужесточении уголовной ответственности за побуждение детей к суициду,

---

1 *Сергей Хазов-Кассиа. «Че, малыши, когда суицидимся?» За что Филипп Лис сел в тюрьму // Сайт Радио Свобода, 15 июня 2019.*

2 *Федеральный закон от 7 июня 2017 г. № 120-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению».*

чтобы исправить несовершенство статьи 110 УК РФ «Доведение до самоубийства», по которой организаторам «синих китов» и других подобных игр было трудно предъявить обвинения.

Понятно, что нам хочется оградить детей от контента, который им не по возрасту, и закон здесь на нашей стороне: согласно Федеральному закону №436-ФЗ[1], запрещается распространять среди детей информацию, побуждающую к причинению вреда своему здоровью, самоубийству; способную развить порочные наклонности (алкоголизм, наркоманию, занятие проституцией, бродяжничеством или попрошайничеством). Распространяемые среди детей сведения не должны оправдывать насилие и жестокость, противоправное поведение; отрицать семейные ценности; содержать нецензурную брань и порнографию.

Роскомнадзор начал действовать, и за один только 2017 год заблокировал 14 тысяч страниц и сообществ, имевших хотя бы намек на отношение к зловещей игре. Мониторинг ведется постоянно, и теперь новые «группы смерти» блокируются сразу, не успев набрать популярность. Казалось бы, можно праздновать победу, отныне дети защищены.

Или нет?

Одни лишь запретительные меры никогда не помогают, а молодежь всегда придумает обходные пути.

---

1 *Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».*

«Киты, единороги, бабочки, крокодилы, тараканы и орангутанги? — Завтра будут другие символы, вы их не успеете и заметить. Раннее утро, 4.20? — будет другое время икс. Вы не успеете за нами, если зациклитесь на конкретных деталях», — так написала на своей странице в «Фейсбуке» одна школьница[1], обращаясь к взрослым, и была совершенно права.*

«Это не решение проблемы, а лишь возможность сделать ее невидимой для старшего поколения и надзорных институтов. Решение проблемы — в офлайне, в семейном воспитании, в умении работать с новым типом сознания, навыке понимания», — объясняет руководитель социологического центра «Платформа» Алексей Фирсов[2].

Действительно, тотальная зачистка информационного поля не помогла. Не прошло и года, как «синий кит» вернулся — на этот раз в образе «красной совы». Теперь «ВКонтакте» блокируют страницы, если написать «Сова никогда не спит» — это новый код-заявка на участие в игре. Снова таинственные кураторы, опасные задания и новая фишка — не спать несколько суток, постоянно быть онлайн и смотреть шокирующие видео.

Ночные бдения были частью ритуала и у «синих китов». Фраза «разбуди меня в 4:20», замеченная у ребенка на его странице, явно указывала на то, что он в игре. «Эксперты» уверяли, что именно в это время мозг ребенка наиболее беззащитен, и таким образом его можно

---

* *Соцсеть признана экстремистской и запрещена на территории РФ.*

1 *Страница Елизаветы Скульской.*

2 *«Синий кит» вернулся в новом обличье. // Известия, 25 января 2018.*

подчинить воле кураторов. Это, разумеется, чушь. Но то, что ребенок перестает высыпаться и от этого становится раздражительным, невнимательным и у него падает успеваемость — это факт.

Безотносительно всяких «китов» и «сов», все гаджеты на время сна должны находиться подальше от кровати ребенка.

Поэтому безотносительно всяких «китов» и «сов», все гаджеты на время сна должны находиться подальше от кровати ребенка. А чтобы просыпаться вовремя, заведите обычный будильник — смартфон для этого совершенно необязателен. И помните, что без вашего личного примера это не работает, — с привычкой держать свой телефон под подушкой придется расстаться и вам.

«Мода» на «красных сов» сегодня уже прошла. Что будет дальше? Малиновый медведь? Фиолетовый ястреб? Фантазия детей не знает границ, обязательно появится что-то еще. Как же быть? Опять массово блокировать новые сообщества и сайты, всегда отставая от их выдумок?

В этой ситуации Следственный Комитет демонстрирует весьма взвешенную позицию по вопросу о влиянии Сети на подростков и об истинных причинах детских суицидов.

> *«Не надо демонизировать интернет», — считает старший помощник председателя СКР Игорь Комиссаров, — по нашей статистике больше всего несовершеннолетних — 800 человек — в России погибло в результате самоубийств в 2014 году. В 2017 году — 692, за девять месяцев этого года (2018) погибло 583 несовершеннолетних. Значительного роста числа самоубийств, совершенных несовершеннолетними, за последние*

годы нет и не было, несмотря на громкие заявления отдельных представителей власти, общественников и журналистов.

Мы тщательно разбирались в рамках обязательно возбуждаемого уголовного дела по каждому случаю суицида или попытки суицида у детей. И пришли к выводу, основанному, в том числе, на результатах проведенных экспертиз, что каждый раз это было обусловлено комплексом причин. И ни в одном случае нет определяющего влияния только интернета на последующие действия несовершеннолетних.

Никогда те или иные группы, содержащие деструктивный контент, не становились главной причиной детских суицидов. И не только суицидов, но и основной причиной противоправного или опасного поведения несовершеннолетних.

Нельзя убить или заставить совершить преступление по интернету. В большинстве случаев ребенок принимает решение о лишении себя жизни под воздействием сразу нескольких факторов в условиях длительной психотравмирующей ситуации и отсутствия понимания и поддержки со стороны окружающих. Проблемы в семье, часто внешне благополучной, в школе, ориентированной на показатели ЕГЭ, затруднение в общении со сверстниками, увеличение потребления школьниками наркотических и психотропных препаратов, незанятость несовершеннолетних позитивной деятельностью и так далее. А сам интернет никогда не играл в этом главную роль. Это только средство коммуникации. Не надо демонизировать его влияние»[1].

1 *Следственный комитет России: «Не надо демонизировать интернет» // Известия, 29 ноября 2018.*

Среди части взрослых весьма популярна конспирологическая версия, что все эти «группы смерти» созданы и управляются врагами нашей страны с какими-то далеко идущими политическим целями — чтобы подчинить себе молодых людей и использовать их для дестабилизации обстановки, когда это потребуется, и что «кураторы» обладают прямо-таки сверхъестественными способностями в области манипуляции сознанием подростков: вот так запросто прикажут человеку прыгнуть с крыши — и он прыгнет.

При сколь-нибудь критическом размышлении эта версия рассыпается — достаточно взглянуть на Филиппа Лиса и других горе-кураторов, чтобы понять, что социальные инженеры из них так себе, и что никакая вражеская спецслужба не даст им ни цента за их «подрывную работу».

Нормального подростка нельзя склонить к суициду, просто показывая ему какие-то картинки в интернете и отдавая приказы.

Нормального подростка нельзя склонить к суициду, просто показывая ему какие-то картинки в интернете и отдавая приказы. К сожалению, иногда обстоятельства складываются так, что юноша или девушка уже имеют психологические проблемы, и мысль об уходе из жизни засела у них в голове. Тогда любое слово может подтолкнуть к фатальному решению — будь то диалог с «куратором» или статья в газете. Это так называемый «эффект Вертера», известный еще с XVIII века, когда по Европе прокатилась волна самоубийств, вызванная публикацией романа Гёте «Страдания молодого Вертера».

Но раз эти группы существуют и создаются все новые, значит, это кому-то выгодно? Совершенно правильный вопрос!

Но он, как ни удивительно, в большинстве публикаций про «группы смерти», начиная со статьи Галины Мурсалиевой, даже не поднимается. Или того хуже — обсуждение уходит в мистическую плоскость: самодеятельные расследователи на полном серьезе демонстрируют публике договор купли-продажи души, который владелец группы якобы заключает с куратором.

Когда группа становится достаточно многочисленной, ее владелец начинает зарабатывать на рекламе.

На самом деле все гораздо проще: когда группа становится достаточно многочисленной, ее владелец, как это обычно происходит в соцсетях, начинает зарабатывать на рекламе. Именно на это рассчитывал Будейкин и его коллеги по цеху. Кроме того, практикуются в таких группах и банальные «разводки» на деньги: по словам одного участника, он трижды натыкался на кураторов, которые вторым заданием просили прислать им 200 рублей на телефон или QIWI Кошелек.

Не гнушаются такие «предприниматели» зарабатывать и на чужой крови — почти в буквальном смысле этого слова. Например, сайт памяти Рины Паленковой[1] представляет собой, по сути, интернет-магазин, где можно купить вещи «как у Рины» — тетради, барабанные палочки, одежду и прочее. Ничего личного — только бизнес.

---

1 *Рина Паленкова (настоящее имя Рената Камболина, 18 декабря 1998 – 23 ноября 2015) — студентка из Уссурийска, прославившаяся после своего самоубийства. Также с ней связан мем «Ня.Пока» из ее последней записи, ставшей своего рода предсмертной запиской. Этот пост получил более 400 тысяч лайков, а в «группах смерти» ее образ стали использовать как пример для подражания.*

Воронка вовлечения

«Синих китов» и «красных сов» можно, пожалуй, считать городской легендой: их опасность была сильно преувеличена в результате массовой паники родителей, возникшей после ряда нашумевших публикаций. Следствие не выявило никаких тайных организаторов, стоящих за созданием подобных игр, и единого центра координации.

> *В Сети встречаются куда более реальные угрозы, реализуемые методами социальной инженерии. Речь идет о вовлечении подростков в различные деструктивные сообщества, связанные с наркотиками, радикальными движениями, экстремизмом и терроризмом.*

Вся эта «темная сторона» обладает особым ореолом притягательности для неокрепших умов, хотя в подавляющем большинстве случаев дело, к счастью, ограничивается банальным любопытством, позерством и пустой болтовней. В общем, как у взрослых: вряд ли кто-то из них из-за прослушивания «Владимирского централа» по радио «Шансон» реально решится избрать преступный путь.

Тем не менее, нельзя сбрасывать со счетов тот факт, что криминальный мир постоянно нуждается в притоке новых «бойцов», которые становятся пушечным мясом в его войне с правоохранительными органами. Например, есть постоянный спрос на наркокурьеров-закладчиков, и молодежь идеально подходит на эту роль.

Криминальный мир постоянно нуждается в притоке новых «бойцов».

Понятно, что рекрутировать на такую «работу» в открытую сложно — страницы с наркоконтентом будут быстро заблокированы, а их владельцами заинтересуются оперативники. Поэтому преступники поступают иначе: сначала формируется максимально широкое сообщество вокруг какой-то темы, не запрещенной, но близкой по смыслу к истинной цели — например, психоделические мультики. Затем некоторым участникам высылают приглашение в закрытую группу, где намерения организаторов выражаются более явно; на следующем этапе «когорту избранных» могут пригласить в секретный чат, в котором ведутся совсем откровенные разговоры, — это уже не считается публикацией контента и под действие закона не попадает. И, наконец, с наиболее «перспективными» кандидатами начинают персонально общаться в мессенджере — чтобы завершить вербовку и дать новичку конкретное задание.

> *Судьба закладчика, как правило, незавидна: обычно они попадаются на третьей-четвертой попытке, или их сдают сами дилеры, которым дешевле набрать новых курьеров, чем платить тем, кто уже отработал какое-то время.*

За такую «работу» по статье 228 УК РФ[1] молодым людям, если им уже исполнилось 18, грозит лишение свободы на срок от 10 до 15 лет в колонии строгого режима, а несовершеннолетним — от 5 до 10.

---

1 *УК РФ Статья 228. Незаконные приобретение, хранение, перевозка, изготовление, переработка наркотических средств, психотропных веществ или их аналогов, а также незаконные приобретение, хранение, перевозка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества.*

При этом дети, которые устраиваются работать «закладчиками» (или, как их чаще называют, «кладменами»), порой даже не осознают, что это противозаконно. Они считают всякие «смеси» и «соли» вполне легальным товаром, а их родители ничего не замечают. Ну, зарабатывает ребенок через интернет, но ведь и учится при этом хорошо, и ведет себя адекватно, и выглядит нормально, то есть сам — явно не наркоман[1].

Механика вовлечения в другие преступные сообщества и группировки примерно такая же. Но вербовка далеко не всегда является целью администраторов сообществ, публикующих у себя деструктивный контент. В подавляющем большинстве случаев они хотят просто, как серферы на волне, прокатиться на модной теме, хайпануть и на этом заработать — также, как и в случае с «группами смерти».

> *Например, есть еще одна «страшилка» для взрослых — А.У.Е. Аббревиатура расшифровывается как «арестантский уклад един» (или «арестантское уркаганское единство») и представляет собой одновременно название и девиз предположительно существующего российского неформального объединения банд, состоящих из несовершеннолетних. Тренд опять задала «Новая газета»[2], резко подняв градус обеспокоенности общества процессами криминализации подростков.*

---

1 *14-летние наркоторговцы: как дети попадают за решетку. // Сайт* ***Ok-inform.ru****, 15 октября 2017.*

2 *Алексей Тарасов. Страна из трех букв // Новая газета, 16 июня 2017.*

При том, что детские банды действительно существуют, и с этим надо что-то делать, есть еще и гипертрофированное отражение реальности в интернете, которое возникает тогда, когда что-либо становится модным. Из того, что количество групп «ВКонтакте», посвященных А.У.Е. или похожей тематике, зашкаливает, вовсе не следует, что все дети вырастут уголовниками. Подавляющее большинство этих групп носит чисто коммерческий характер — их участникам предлагают купить футболки, банданы и другие предметы с соответствующей символикой. Но число их участников исчисляется сотнями тысяч, и это не может не настораживать.

Давайте сопоставим факты. По словам все той же «Новой газеты», эта молодежная субкультура наиболее распространена в Забайкальском крае и соседних регионах, которые едва ли можно назвать экономически благополучными. Напрашивается вывод: отнюдь не интернет является главным виновником распространения тюремных обычаев среди подростков, а сама среда, в которой они живут. Что же касается их более обеспеченных сверстников, то для них это просто очередная игра. Хотя, разумеется, сказанное ничуть не умаляет опасности самого явления — вне зависимости от того, насколько влияет на его распространение интернет.

По данным компании «Крибрум» на март 2019 года в деструктивные течения в Рунете были вовлечены порядка 5 миллионов аккаунтов российских подростков (35% от их общего числа в России), и количество таких аккаунтов продолжает расти.

Период с января 2018 г. по март 2019 г. характеризуется стабильно высоким, растущим деструктивным фоном. Особую опасность представляют следующие темы: наркомания, ультра-движение, анархия.

В подростковой среде в социальных медиа фиксируется стремление подростков к группам, продвигающим разрушающее поведение через темы социопатии, массовых и серийных убийств, обесценивания собственной жизни и стремления к смерти, сатанизма и псевдомистических культов, наркомании, ритуальных убийств и самоубийств, нацизма и национализма, экстремизма и радикализма[1].

Как относиться к этим пугающим цифрам и фактам? Прежде всего, уточнить, что имеют в виду под вовлеченностью аналитики «Крибрум»: участие в группе, репост или лайк, поставленный материалу деструктивной тематики. Как вы понимаете, между лайком и реальным действием — дистанция огромного размера. Разумеется, мониторинг интересов подростков может дать много полезной информации для размышления взрослым и помочь сделать так, чтобы эта дистанция не была преодолена. Но и излишне драматизировать ситуацию не стоит. Доверие — один из важнейших инструментов воспитания, а большинство детей вполне четко разграничивают игру и настоящую жизнь.

---

1 *Форум «Цифровая гигиена. Молодежь в сети», 28 марта 2019.* ***http://digital-gigiena.ru/***

Контрольные вопросы

1. Что такое социальная инженерия?
2. Какие эмоции и чувства преступники используют наиболее часто?
3. Что значит «нулевое доверие»?
4. Как работают «нигерийские письма»?
5. Как телефонные мошенники обманывают клиентов банков?
6. Почему банк не компенсирует потери в результате применения социальной инженерии?
7. Как проверить, просит помощи друг или мошенник от его имени?
8. Что такое фишинг?
9. Какие варианты фишинга вы знаете?
10. С помощью чего можно защититься от фишинга?
11. Как вы отличаете подозрительные ссылки от неподозрительных?
12. Почему надежнее пользоваться мобильными приложениями?

13. Что такое «группы смерти»? Что вы об этом думаете?

14. Что такое воронка вовлечения?