МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ (МИНЮСТ РОССИИ)
ГЛАВНОЕ УПРАВЛЕНИЕ МИНИСТЕРСТВА ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО САНКТ-ПЕТЕРБУРГУ И ЛЕНИНГРАДСКОЙ ОБЛАСТИ

Исаакиевская пл., д. 11,
г. Санкт-Петербург, 190121
тел. (812) 679-70-31
E-mail: ru78@minjust.gov.ru

18.12.2025 № 78/06-28375/25

Председателю
комитета общего и профессионального
образования Ленинградской области

В.И. Ребровой

Уважаемая Вероника Ивановна!

Главным управлением Минюста России по Санкт-Петербургу и Ленинградской области во исполнение пункта 1.8 решения протокола заседания координационного совещания по обеспечению правопорядка в Ленинградской области от 21.10.2025 № 4 направляет электронную версию учебно-методического пособия «Стоп, мошенники» под редакцией Д.В. Гурьева и В.А. Гуреева для последующего распространения и использования при проведении работы по правовому просвещению и правовому информированию в образовательных организациях Ленинградской области.

Приложение: на 96 л. в 1 экз.

И.о. начальника

Минюст России ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00B80BB08AE6343F55DDA8E41D1D1B88D0
Владелец: **Васильева Татьяна Александровна**
Действителен: с 25.04.2025 по 19.07.2026

ильева

Погорелов Михаил Юрьевич
(812) 679-70-31 (доб. 804)

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Всероссийский государственный университет юстиции
(РПА Минюста России)»

БИБЛИОТЕКА ЖУРНАЛА
ВЕСТНИК
РОССИЙСКОЙ ПРАВОВОЙ АКАДЕМИИ

СТОП, МОШЕННИКИ!

Учебно-методическое пособие

Москва – 2025

Издательство «Деловой Стиль»

УДК 343.72
ББК 67.408
С81

Под редакцией
Дмитрия Владимировича Гурьева, кандидата экономических наук, доцента, первого проректора ВГУЮ (РПА Минюста России);
Владимира Александровича Гуреева, доктора юридических наук, профессора, проректора по научной работе ВГУЮ (РПА Минюста России).

Авторский коллектив:
Марина Николаевна Илюшина, доктор юридических наук, профессор, заведующая кафедрой гражданского и предпринимательского права ВГУЮ (РПА Минюста России), заслуженный юрист РФ; **Земфира Мухарбиевна Казачкова**, доктор юридических наук, профессор, заведующая кафедрой административного, финансового и информационного права ВГУЮ (РПА Минюста России); **Екатерина Васильевна Кирсанова**, старший научный сотрудник центра научных исследований ВГУЮ (РПА Минюста России); **Ирина Михайловна Колосова**, кандидат юридических наук, доцент, заведующая кафедрой уголовного процесса и криминалистики ВГУЮ (РПА Минюста России); **Арина Михайловна Макеева**, помощник ректора ВГУЮ (РПА Минюста России); **Владислав Юрьевич Панченко**, доктор юридических наук, доцент, заведующий кафедрой теории, истории государства и права ВГУЮ (РПА Минюста России); **Бадма Владимирович Сангаджиев**, доктор юридических наук, профессор, заведующий кафедрой конституционного и международного права ВГУЮ (РПА Минюста России); **Наталья Павловна Семенова**, кандидат биологических наук, проректор по учебной работе, заведующая кафедрой гуманитарных, социальных и общих дисциплин ВГУЮ (РПА Минюста России); **Борис Викторович Яцеленко**, доктор юридических наук, профессор, заведующий кафедрой уголовного права и криминологии ВГУЮ (РПА Минюста России), заслуженный юрист РФ.

С81 **Стоп, мошенники!** : учебно-методическое пособие. – Москва : Деловой Стиль, 2025. – 96 с.

ISBN 978-5-6048014-2-0 (в обл.)

Учебно-методическое пособие посвящено различным видам мошенничества, методам совершения, профилактике правонарушений, предостережению граждан от опасностей, которые появляются в результате возникновения различных ситуаций общения с мошенниками, преодолению правового нигилизма, формированию правосознания и юридической культуры граждан.

Настоящее издание предназначено для широкого круга читателей.

УДК 343.72
ББК 67.408

ISBN 978-5-6048014-2-0

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Настоящее издание посвящено актуальной теме. С развитием информационных технологий способы совершения дистанционных мошенничеств изменились. Одни из самых популярных видов мошенничества сегодня – телефонные и через сеть Интернет. Злоумышленники могут представиться по телефону сотрудниками банка, правоохранительного органа, медицинскими или социальными работниками. Практически ежедневно люди становятся жертвами злоумышленников. Чаще всего пострадавшими оказываются пожилые люди и дети. Чтобы уберечь себя и своих близких, необходимо знать и помнить наиболее распространенные схемы мошенничества. Мошенники могут обладать информацией о некоторых данных паспорта, месте жительства, детализации по банковскому счету, создают сайты-клоны торговых площадок (копируют интерфейс оригинального сайта), сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в финансовую пирамиду, требуют передать деньги для лечения пострадавшего в аварии человека, сообщают о якобы ставших виновниками ДТП родственниках, предлагают решить вопрос о невозбуждении уголовного дела и т.д.

Учебно-методическое пособие подготовлено в целях повышения осведомленности о различных формах мошенничества (например, финансовые пирамиды, фишинг, мошенничество с кредитными картами), помощи в распознавании признаков мошеннических схем и предостережения от возможных рисков. Представленные материалы обучают основам безопасного поведения в сети Интернет и социальных сетях, помогают избежать распространенных ловушек и защитить граждан от финансовых потерь.

В пособии рассмотрены наиболее популярные жизненные ситуации, подробно описаны нормы нарушенного закона и ответственность для всех участников (поскольку не всегда виноваты только мошенники – это могут быть и те, кто переводит деньги, например, террористическим организациям), а также представлены комментарии и рекомендации экспертов по поводу того, как себя вести в той или иной ситуации.

При подготовке издания осуществлялся сбор материалов обучающимися и оказывалась методическая помощь преподавателями ВГУЮ (РПА Минюста России) и его институтов (филиалов), использовался опыт обращений граждан в юридические клиники, созданные на базе Университета.

Авторский коллектив выражает благодарность руководству Следственного комитета РФ за содействие в подготовке издания.

Учебно-методическое пособие «Стоп, мошенники!» предназначено для различных групп людей и служит важной цели в борьбе с мошенничеством. Издание может быть использовано в образовательных программах для повышения финансовой грамотности среди студентов и учеников; служить ресурсом для обучения сотрудников, работающих с жертвами мошенничества, для разработки стратегий по противодействию преступности, для проведения информационных кампаний и семинаров, направленных на защиту граждан от мошенничества.

СПИСОК ТЕРМИНОВ

***POS*-микрозаем** – денежные средства, предоставленные микрофинансовой организацией получателю финансовой услуги на основании договора микрозайма без обеспечения исполнения обязательств по такому договору в счет оплаты товара (работы, услуги) посредством перечисления данных денежных средств микрофинансовой организацией на банковский счет продавца (исполнителя) товара (работы, услуги).

***QR*-код** – двумерный штрихкод, который может содержать текстовую и контактную информацию.

***URL*-адрес** – путь к ресурсу в сети Интернет. Такими ресурсами могут быть сайт, отдельная веб-страница, файл, видео и любой другой объект.

Аккаунт – хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

Банк данных в исполнительном производстве – банк данных, содержащий сведения, необходимые для осуществления задач по принудительному исполнению судебных актов, актов других органов и должностных лиц, который создает и ведет, в том числе в электронном виде, ФССП России.

Биометрическая защита – способ разблокировки телефона с помощью отпечатка пальца, распознавания лица или других биометрических данных.

Бот – программа, которая автоматически выполняет определенные задачи в социальных сетях, мессенджерах или на других онлайн-платформах (приложениях).

Брутфорс – метод взлома, основанный на систематическом переборе всех возможных комбинаций символов для подбора пароля, логина, кода или ключа шифрования, в том числе с использованием специализированного программного обеспечения.

Вардрайвинг – процесс поиска и определения местоположения беспроводных сетей *Wi-Fi* с использованием мобильных устройств и транспортных средств, который может проводиться как в законных целях, например для определения зон покрытия *Wi-Fi*, так и в незаконных – для поиска уязвимых сетей и их последующего взлома.

Вербовка – поиск и привлечение лиц для участия в диверсионной деятельности.

Взлом (хакинг) – несанкционированный доступ к компьютерным системам, сетям, веб-сайтам или учетным записям с целью получения

контроля над ресурсом, кражи данных, нарушения работы системы или совершения иных противоправных действий путем эксплуатации уязвимостей в программном обеспечении, применения вредоносного программного обеспечения, использования социальной инженерии или других методов.

Взыскатель – лицо, в пользу или в интересах которого выдан исполнительный документ.

Виртуальная кража – преступление, совершенное с использованием Интернета для кражи личных или финансовых данных жертвы с намерением использовать эту информацию в преступных целях.

Воронка продаж – модель, описывающая путь, который проходит клиент от знакомства с продуктом до его покупки. В «инфоцыганстве» часто используется для заманивания покупателей через серию предложений.

Вредоносная программа – программа, любая ее часть или код, способный или целенаправленно написанный для нанесения вреда устройствам и данным, хранящимся на них.

Вредоносная программа (вирус) – тип программного обеспечения, разработанный для причинения вреда компьютерным системам, кражи данных, нарушения работоспособности программ или устройств, проникающий в систему разными способами: через электронную почту, зараженные веб-сайты, съемные носители и другие каналы.

Геймер – человек, который любит играть в видеоигры или профессионально занимается киберспортом.

Двухфакторная аутентификация (*2FA*) – дополнительная мера защиты для идентификации личности с помощью одноразового кода, который отправляется на мобильный номер телефона через *SMS*-сообщение или электронную почту.

Диверсант – лицо, совершающее диверсию.

Диверсионная группа – группа лиц, совместно осуществляющих подготовку или совершение диверсий.

Диверсионное сообщество – устойчивая группа лиц, объединенная для осуществления диверсионной деятельности.

Диверсия – преднамеренное действие, направленное на разрушение или повреждение чего-либо, чаще всего в контексте военных или террористических действий.

Дипфейк – технология, которая представляет собой создание и использование реалистичных, но искусственно сгенерированных искусственным интеллектом (нейросетью) медиаданных (например, видеозаписей, аудиозаписей или фотографий).

Договор микрозайма – договор займа, сумма которого не превышает предельный размер обязательств заемщика перед займодавцем по

основному долгу, установленный законом (должен четко определять, какая сумма денежных средств передается заемщику, иначе он может быть незаключенным).

Долевое строительство – форма строительства объекта недвижимости, при которой застройщик получает денежные средства от покупателя, а взамен обязуется предоставить ему квартиру в установленный срок, определенного качества.

Должник – лицо, обязанное по исполнительному документу совершить определенные действия или воздержаться от них.

Дроппер (дроп) – лицо, используемое преступниками для вывода денежных средств с банковских счетов или иных платежных систем, полученных в результате противоправных действий.

Жалоба – просьба гражданина о восстановлении или защите его нарушенных прав, свобод или законных интересов либо прав, свобод или законных интересов других лиц.

Застройщик – юридическое лицо, легально осуществляющее строительство объектов недвижимости.

Искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их.

Исполнительное производство – совокупность процессов и действий, направленных на принудительное исполнение вступивших в законную силу исполнительных документов.

Киберпреступность – совокупность преступлений, совершаемых с использованием информационных технологий и компьютерных сетей, включая несанкционированный доступ к данным, кражу личных сведений, фишинг, распространение вредоносного программного обеспечения и другие виды противоправной деятельности в киберпространстве.

Кладмен/Закладчик – лицо, которое за вознаграждение делает тайники с наркотиками, например, зарывает в землю для того, чтобы в последующем другой человек их забрал для употребления.

Коучинг – наставничество или обучение, предлагающее помощь в достижении личных или профессиональных целей. В контексте «инфоцыганства» может быть не всегда качественным и эффективным.

Кэтфишинг – разновидность интернет-мошенничества (кибермошенничества), которая представляет собой создание и использование ненастоящей личности в социальных сетях, мессенджерах или на других онлайн-платформах (приложениях).

Легализация денежных средств – придание похищенным денежным средствам законного характера.

Лид-магнит – бесплатное предложение для привлечения потенциальных клиентов, например бесплатный вебинар или книга. Часто служит начальной точкой для вовлечения в дальнейшие продажи.

Маркетплейс – онлайн-платформа, на которой продавцы размещают свой товар, а покупатели могут его приобрести. Тем самым маркетплейс служит между ними посредником.

Меры принудительного исполнения – действия, указанные в исполнительном документе, или действия, совершаемые судебным приставом-исполнителем, в целях получения с должника имущества, в том числе денежных средств, подлежащего взысканию по исполнительному документу.

Мессенджер – компьютерная программа для обмена сообщениями в реальном времени через Интернет.

Микрозаем – заем, предоставляемый займодавцем (юридическим/физическим лицом) заемщику на условиях, предусмотренных договором займа, в сумме, не превышающей предельный размер обязательств заемщика перед займодавцем по основному долгу, установленный законом.

Микрофинансовая организация – компания, которая определяет механизм выдачи займов: небольшие суммы на короткий срок под высокий процент.

Многопользовательская онлайн-игра – онлайн-игра, в которой в одной игровой среде может играть более одного человека одновременно.

Мошенничество – хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Онлайн-игра – вид видеоигры, для которой необходимо постоянное подключение в сети Интернет.

Платформа вакансий – онлайн-платформа, которая собирает и систематизирует вакансии из различных источников. Она позволяет соискателям не тратить время на переходы по множеству сайтов, а сразу находить интересующие их предложения.

Подготовка диверсии – комплекс мероприятий по планированию, организации и обеспечению совершения диверсии.

Подстрекательство – активное побуждение к совершению диверсии.

Пособничество – оказание помощи в совершении диверсии, но без непосредственного участия в ней.

Продающий вебинар – онлайн-презентация, цель которой – продать курс или услугу. Может содержать манипулятивные техники для убеждения аудитории в необходимости предлагаемого продукта.

Расписка – документ, удостоверяющий в письменной форме, что лицо, давшее расписку, получило от другого лица деньги, вещи, материальные ценности и обязуется их вернуть.

Резервное копирование – создание копии данных на другом устройстве или в облачном хранилище для их сохранности в случае утери телефона.

Рейдерство аккаунтов – процесс захвата доступа к учетным записям без ведома пользователя.

Скимминг – вид мошенничества с банковскими картами, который представляет собой считывание информации с их магнитной полосы с помощью специального технического устройства, или скиммера. Мошенники также пытаются узнать *PIN*-код жертвы. Получив данные карты, ее можно скопировать и вывести с нее все деньги.

Скриншот – снимок экрана компьютера или мобильного устройства, изображающий то, что было на нем в момент его создания.

Скрытый майнинг (майнер) – вирус, который предназначен для тайной добычи криптовалюты с помощью устройства.

Служба поддержки – центр связи компании, где клиенты могут найти помощь в решении вопросов или проблем.

Содействие диверсии – любые действия, которые помогают или способствуют совершению диверсии (вербовка, финансирование, предоставление информации и т.д.).

Соучастие – участие нескольких лиц в совершении преступления.

Социальная инженерия – манипуляция, которая представляет собой создание и использование психологических приемов (обман или злоупотребление доверием) с целью получения денежных средств или доступа к персональным данных.

Спам – массовая рассылка корреспонденции лицам, не выражавшим желания ее получить.

Специализированная платформа для сбора средств – онлайн-сервис, выступающий в качестве посредника для взаимодействия организаторов сбора средств и благотворителей.

Судебный приказ – судебное постановление, вынесенное судьей единолично на основании заявления о взыскании денежных сумм или об истребовании движимого имущества от должника.

Счет эскроу – специализированный счет, предназначенный для учета, хранения и блокирования денежных средств в целях передачи другому лицу при наступлении определенных условий (например, исполнение договора).

Техподдержка платформы – сервисная служба, которая помогает решать проблемы в использовании продукта и организовывать рабочие процессы.

Троянец-стиллер – вирус, который предназначен для тайного сбора доступа к персональным данным с помощью устройства.

«Угон» аккаунта – несанкционированный доступ к цифровой учетной записи, осуществляемый без согласия или ведома законного вла-

дельца, с целью получения контроля над аккаунтом, кражи личных данных, совершения противоправных действий или иного неправомерного использования.

Удаленная блокировка – возможность заблокировать утерянное устройство через Интернет с помощью другого устройства.

Участник долевого строительства – лицо, заключившее с застройщиком договор долевого строительства.

Финансовая пирамида – мошенническая схема, в которой выплаты участникам осуществляются за счет привлечения новых вкладчиков, а не за счет реальной инвестиционной или предпринимательской деятельности.

Фишинг – вид интернет-мошенничества, направленный на получение доступа к конфиденциальным данным пользователей (логинам, паролям, номерам банковских карт и т.д.) путем рассылки фальшивых электронных писем, сообщений, перенаправляющих на поддельные веб-сайты, имитирующие интерфейс легитимных ресурсов. Цель фишинга – заставить жертву добровольно предоставить свои данные преступнику.

Фишинг-атака – попытка кражи данных через подключенные устройства. Атака может быть проведена вручную или с помощью инструмента, который автоматизирует процесс. Это также может быть комбинация: скрипт прокладывает дорогу хакеру, который завершает атаку вручную.

Фишинговая ссылка – гиперссылка, ведущая на поддельный веб-сайт, который имитирует интерфейс легитимного ресурса, с целью кражи конфиденциальной информации пользователя (логина, пароля и др.), распространяемая через электронную почту, сообщения в социальных сетях или мессенджерах.

Фишинговый сайт – сайт, который предназначен для сбора доступа к персональным данным.

ДОНИМАЮТ ЗВОНКИ И *SMS*

Цель телефонных мошенников – выманить личные данные, *CVC/CVV*-коды карт (три цифры на задней стороне карты), логины и пароли от банковских приложений. Они предлагают перейти на фальшивые сайты, платежные порты в Интернете.

КОММЕНТАРИЙ

Злоумышленники используют различные тактики, чтобы запугать или манипулировать жертвами, часто выдавая себя за представителей банков, государственных учреждений или популярных компаний. Они, как правило, звонят с незнакомых номеров или сходных номеров банков и других юридических лиц. Началом разговора обычно является «байка», что у человека возникли проблемы с его счетом, либо предлагаются «выигрыши» в конкурсах, в которых жертва не участвовала, либо мошенник хочет напугать собеседника неожиданной новостью о разных неприятностях, которые якобы случились с последним либо с его близкими. Такие звонки могут начаться с простого вопроса, чтобы установить доверие, психологический контакт, после чего мошенник начинает воздействовать на эмоции собеседника и в конечном счете убеждает жертву раскрыть персональные данные.

ОТВЕТСТВЕННОСТЬ

Статья 159 УК РФ «Мошенничество».

Кроме уголовной ответственности телефонные мошенники также могут подвергаться гражданской ответственности. Пострадавшие от мошенничества имеют право подать иск на возмещение убытков. В некоторых случаях суды могут присуждать компенсации жертвам, даже если уголовное дело не было возбуждено.

РЕКОМЕНДАЦИИ ЭКСПЕРТОВ

1. Не выполняйте указания неизвестного лица и не вводите под диктовку коды на своем телефоне. Необходимо проверить информацию, перезвонив в абонентскую службу своего оператора связи, банка и т.д.

2. Всегда внимательно читайте условия и стоимость предоставления сервисов, которыми пользуетесь, не ставьте автоматически галочку напротив строки «Я согласен», иначе Вы можете добровольно подписаться на сервисы, которые не заказывали, и при этом с Вас будут списываться суммы, о которых Вы не подозреваете.

3. Не поддавайтесь первому импульсу и старайтесь проверять информацию, поступившую от неизвестных лиц. Стоит помнить, что сотрудникам банков запрещено пытаться узнать по телефону информацию о реквизитах банковских карт клиентов. Получив подобное сообщение, постарайтесь проверить поступившую от неизвестных информацию, позвонив в колл-центр своего банка.

4. Для того чтобы распознать обман и не лишиться крупной суммы денег, постарайтесь связаться с родственником напрямую либо через друзей и знакомых; попросите звонящего описать внешность Вашего родственника и ответить на вопросы личного характера.

5. Крупные агентства по подбору персонала, от имени которых действуют мошенники, предоставляют информацию обо всех вакансиях бесплатно, и, скорее всего, после отправки *SMS* Вам придет информация о вакансии, размещенной в свободном доступе в Интернете.

6. Если Вам кажется, что помощь требуется Вашему родственнику, знакомому, другу, постарайтесь связаться с ним по известному Вам номеру.

7. Получив *SMS* или *MMS* от неизвестного отправителя с предложением перейти по ссылке, отнеситесь к этому с осторожностью. Вряд ли кто-то из Ваших друзей и знакомых станет делать Вам анонимные подарки.

8. Телефоны с такими операционными системами, как *Android* и *iOS* (*iPhone*), являются уязвимыми с точки зрения вирусных атак. Не следует открывать *MMS* от неизвестного отправителя, переходить по ссылкам в Интернете, пришедшим с неизвестных номеров, а также устанавливать на мобильное устройство неизвестное программное обеспечение.

9. Не выполняйте действий под диктовку неизвестного Вам человека, как бы правдоподобно он ни описывал условия акции. Перезвоните в абонентскую службу Вашего оператора связи и проверьте информацию.

10. Не отдавайте телефон в руки незнакомца. Если Вы хотите помочь, предложите самостоятельно набрать нужный номер и передать информацию.

11. На большинстве современных телефонов есть возможность блокировки нежелательных номеров. Используйте эту функцию для защиты себя от повторяющихся звонков и *SMS*-уведомлений.

12. Если Вы столкнулись с телефонным мошенником, обязательно и немедленно сообщите об этом в правоохранительные органы. Это поможет предотвратить подобные случаи в будущем и оперативно задержать виновное лицо.

ВНИМАНИЕ! Если у Вас выманили обманным путем определенную сумму денег, то незамедлительно обратитесь по телефону 02, с мобильных телефонов – 102, 112 либо с письменным заявлением в полицию (см. примерный образец заявления в Приложении 1).

ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА, МОЖНО ПРЕДЛОЖИТЬ СЛЕДУЮЩИЕ ДЕЙСТВИЯ:

1. Постарайтесь получать как можно больше информации из прессы и интернет-источников о возможных способах обмана при помощи телефонных звонков и *SMS*-уведомлений. Мошенники становятся все более изобретательными, однако их схемы быстро становятся известными. Ваша задача – вовремя узнавать о них. Спектр возможных хитростей злоумышленников весьма велик – от псевдо-звонков от имени известных компаний до предложений подарков. Не стесняйтесь ставить под сомнение подобную информацию, если она напрямую касается Вас.

2. Внимательно изучайте любые предложения, которые звучат слишком хорошо, чтобы быть правдой, и всегда проверяйте информацию через официальные источники, чтобы не попасться на уловки мошенников. Данные предложения необходимо перепроверять несколько раз, если они поступили якобы от банков (**сотрудники Сбербанка**, например, **звонят с номера 900**, не отправляя сообщения ни в каких мессенджерах).

3. Прежде чем что-либо делать, Вам необходимо убедиться в достоверности информации, полученной по телефону от неизвестных, представившихся сотрудниками полиции, радиостанции, операторами сотовой связи, Вашими родственниками или знакомыми. Сотрудники полиции, как правило, вызывают граждан повесткой, но не звонят на их личные телефонные номера.

4. Если Вы получаете какое-либо выгодное предложение, связанное с непредвиденными затратами, обязательно осведомитесь обо всех условиях акции (если ее так можно назвать). Ставьте под сомнение слишком большие скидки или неожиданные выигрыши, особенно если Вы не принимали участия ни в каких розыгрышах и лотереях за определенный период времени. Никогда не соглашайтесь вносить предоплату за призы (в качестве налога на выигрыш или любого другого платежа), поскольку это не что иное, как уловки телефонных мошенников.

5. Не разглашайте без необходимости свою персональную информацию. Не выкладывайте слишком много фотографий и сведений в социальных сетях, не вводите номера карт, паспортные данные и адреса на сомнительных ресурсах, не копируйте и не отправляйте документы без тщательной проверки. Старайтесь не пересылать слишком важ-

ные документы или коммерческие данные по электронной почте, так как ее могут взломать.

6. Если Вам звонят с просьбой перевести деньги за «родственника, находящегося в плену», сначала уточните информацию у других членов семьи и ни в коем случае не передавайте данные своих банковских карт! Помните, что мошенники часто используют эмоциональные уловки, поэтому доверяйте только проверенным источникам, а при необходимости обращайтесь в правоохранительные органы.

7. Если телефонные мошенники обращаются к Вашим детям с просьбой оформить кредит на паспортные данные родителей, используя различные манипуляции и запугивания, то предостерегите детей не делать этого. Объясните им, что это мошенники, которым нельзя доверять, и необходимо сразу же отключать телефон, если будут предлагать кредит или денежную сумму за выигрыш в лотерее.

Обман при телефонном мошенничестве – это преднамеренное введение жертвы в заблуждение с целью получения ее личных данных, денежных средств или других ресурсов.

Телефонное мошенничество – это одна из форм мошенничества, при которой злоумышленники используют телефонные звонки или текстовые сообщения для обмана людей с целью получения денежных средств или личной информации. Существует множество видов телефонного мошенничества, включая «*SMS*-мошенничество», «звонки из банков», «снятие кредитов», «звонок и визит из социальных служб», «переводы по картам» и др.

Фальшивые звонки от служб поддержки представляют собой один из наиболее распространенных видов телефонного мошенничества, при котором злоумышленники выдают себя за сотрудников компаний, таких как банки, интернет-провайдеры или техническая поддержка. Они могут звонить жертве под предлогом решения проблем с аккаунтом, сообщать о подозрительных транзакциях или предлагать помощь по техническим вопросам. Часто такие звонки происходят в спокойной обстановке, что создает у жертв ощущение доверия.

Мошенничество с выигрышами – это форма телефонного мошенничества, при которой злоумышленники информируют жертву о том, что он (она) выиграл(а) приз в лотерее или конкурсе, в котором на самом деле никогда не участвовал(а). Мошенники часто используют привлекательные предложения, такие как крупные суммы денег, дорогие подарки или бесплатные путевки, чтобы привлечь внимание и вызвать интерес у потенциальной жертвы. В большинстве случаев они прибегают к эмоциональным уловкам, чтобы создать у человека ощущение счастья и удачи.

Схемы «помощи» представляют собой тип телефонного мошенничества, при котором злоумышленники пытаются обмануть жертву, представляясь ее родственниками или друзьями, попавшими в чрезвычайную ситуацию. Мошенники часто используют эмоциональные уловки, заявляя, что им срочно нужны деньги на лечение, оплату штрафа или помощь в решении других неотложных проблем. Такие звонки могут вызвать сильные эмоции и панику у жертвы, что делает ее более подверженной манипуляциям.

Фишинг через *SMS* представляет собой технику мошенничества, при которой злоумышленники отправляют жертвам текстовые сообщения с целью получить личные данные или финансовую информацию. Эти сообщения могут выглядеть очень убедительно и часто содержат поддельные ссылки на фальшивые веб-сайты, которые имитируют легитимные сервисы, такие как банки, интернет-магазины или службы доставки. Мошенники используют различные уловки, чтобы вызвать у получателя чувство срочности, например, предупреждая о блокировке аккаунта или необходимости подтвердить транзакцию.

Неизвестные звонки с просьбой подтвердить информацию представляют собой распространенный метод мошенничества, при котором злоумышленники обращаются к жертве под предлогом проверки данных, связанных с ее аккаунтом, кредитной картой или другой чувствительной информацией. Мошенники могут представляться сотрудниками банков, страховых компаний или других организаций и утверждать, что им нужно обновить информацию для обеспечения безопасности. Зачастую такие звонки начинаются с вопросов о личных данных, таких как номер паспорта, адрес или сведения о финансах.

Социальная инженерия. Основной принцип социальной инженерии заключается в манипуляции человеческими эмоциями и доверием с целью получения конфиденциальной информации или денежных средств. Мошенники тщательно изучают своих потенциальных жертв, собирая информацию из открытых источников, таких как социальные сети, что позволяет им создавать убедительные сценарии для телефонных разговоров.

Создание ложной срочности. Мошенники способны сообщать жертве о несуществующих проблемах, таких как блокировка банковского счета, угроза судебного преследования или необходимость немедленной выплаты долгов. Эти устрашающие сценарии заставляют человека почувствовать необходимость действовать быстро, без возможности тщательно обдумать ситуацию.

Использование технологий подмены номера. Современные технологии позволяют злоумышленникам изменять номер телефона, с которого они звонят, так, что на экране жертвы может отображаться номер,

принадлежащий известной компании, банку или даже государственному учреждению. Это создает иллюзию доверия и легитимности, заставляя людей считать звонок безопасным и не требующим проверки.

Заведомо ложная информация. Чаще всего мошенники при звонках абонентам выдают себя за представителей банков, государственных учреждений или других авторитетных организаций и сообщают жертве ложную информацию о ее счете, кредитной истории и т.д. Например, они могут утверждать, что на счету обнаружены подозрительные транзакции, требуя от жертвы немедленно подтвердить свои личные данные для предотвращения финансовых потерь.

Скрытые платежи или подписки. Данный метод считается изощренным, телефонные мошенники используют его для обмана жертв, заставляя их согласиться на ненужные услуги или продукты, о которых они не были должным образом информированы. Мошенники могут представляться сотрудниками известных компаний и предлагать «бесплатные» пробные версии товаров или услуг, которые на самом деле требуют финансовых затрат через скрытые условия. Жертвы, поддавшись соблазну, могут предоставить свои платежные данные, не осознавая, что в итоге они будут автоматически списываться с их счета после окончания пробного срока.

ВАМ НАПИСАЛ/ПОЗВОНИЛ БОТ

Услугами чат-ботов пользуются миллионы людей. Искусственный интеллект во многом облегчил жизнь современного человека. Однако в руках мошенников, которые используют его под видом магазинов, медицинских организаций, фирм и т.д., он превращается в глобальную угрозу.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация 1. «Поздравляем! Вы выиграли бесплатную премиум-подписку на месяц! Чтобы ее получить, отправьте одноразовый код из *SMS*-сообщения мобильного номера телефона», – написал мужчине в мессенджере неизвестный бот. Не задумываясь, человек сразу ввел запрашиваемые персональные данные. Через несколько часов, когда мужчина решил войти в личный кабинет, оказалось, что его аккаунт был взломан.

Ситуация 2. Алину Сергеевну при помощи бота мошенники заманили на сторонний сайт, внешне копирующий «*Lamoda*», и предложили промокод на покупки на 10 тыс. руб. Женщина связалась с «личным менеджером» через мессенджер и лишилась доступа к своей учетной записи и конфиденциальным данным.

КОММЕНТАРИЙ

Данные ситуации являются примером мошенничества с помощью бота (*bot*) – программы, которая автоматически выполняет определенные задачи в социальных сетях, мессенджерах или на других онлайн-платформах (приложениях). Боты (*bots*) работают в автономном режиме, без человеческого вмешательства.

Распродажа в магазине, акция от фирмы-производителя, лечение зубов со скидкой в Вашей клинике – это лишь малый перечень того, о чем Вас может известить бот, предлагая перейти по ссылке или запрашивая код.

ОТВЕТСТВЕННОСТЬ

Ущерб, причиненный в результате совершения этого деяния, соответствует составу преступления, предусмотренного ст. 159 УК РФ «Мошенничество», т.е. хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

ЧТО ДЕЛАТЬ, ЕСЛИ ВАС ОБМАНУЛИ ИЛИ ВВЕЛИ В ЗАБЛУЖДЕНИЕ?

1. Обратитесь в правоохранительные органы с заявлением о возбуждении уголовного дела с приложением всех имеющихся у Вас данных (например, переписки, чеков о перечислении денежных средств).

2. Перезвоните в банк или другую кредитную организацию, чтобы остановить перечисление денежных средств и заблокировать банковский счет.

3. Обратитесь за консультацией в юридические организации.

КАК НЕ СТАТЬ ЖЕРТВОЙ БОТА?

1. Проверьте информацию. Если Вам пришло сообщение от магазина, предлагающего купить товар с большой скидкой, или предложение от частной клиники, куда Вы обращаетесь за медицинской помощью, не стесняйтесь перезвонить и узнать о том, действительно ли проходит акция.

2. Используйте надежные ресурсы.

3. Настройте параметры конфиденциальности. Ограничьте доступ к персональным данным на всех своих аккаунтах.

4. Не переходите по подозрительным *URL*-ссылкам. Они могут переадресовывать на фишинговые или вредоносные сайты, которые могут применяться для сбора доступа к персональным данным или повреждения устройства соответственно.

5. Не скачивайте подозрительные файлы. Они могут содержать вредоносные программы – вирусы (например, скрытый майнинг (майнер) или троянец-стиллер, которые могут применяться для добычи криптовалюты или сбора доступа к персональным данным с помощью устройства соответственно).

6. Скачайте антивирусные программы. Они могут защитить устройство от вредоносных программ.

7. Настройте двухфакторную аутентификацию (*2FA*). Это дополнительная мера защиты для идентификации личности с помощью одноразового кода, который отправляется на мобильный номер телефона через *SMS*-сообщение или электронную почту.

8. Придумайте сложный пароль. Комбинируйте строчные и прописные буквы, цифры и специальные символы при регистрации в социальных сетях, мессенджерах или на других онлайн-платформах (приложениях). Отключите функцию «автоматическое сохранение паролей» в браузере или приложениях.

ЛОЖНАЯ ТЕХПОДДЕРЖКА

В последнее время наблюдается рост числа мошеннических схем, связанных с ложной технической поддержкой. Злоумышленники, выдавая себя за сотрудников служб поддержки, используют фишинговые письма, в которых персонализируют сообщения, адресуя конкретным сотрудникам, и ведут себя от имени реальных сервисов, используемых в коммерческих компаниях, а также самый распространенный способ – звонки для получения конфиденциальной информации и доступа к финансовым ресурсам граждан и организаций. Согласно статистике ВЦИОМ только телефонному мошенничеству в 2024 г. были подвергнуты более 67% россиян.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация. «Добрый день, Мария Ивановна, Вам звонят из ... банка! Мы предлагаем Вам установить новое защитное приложение», – раздалось в телефонной трубке. Мария Ивановна согласилась установить программу, которая в действительности оказалась программой удаленного доступа, с помощью которой мошенники похитили с ее счета все сбережения.

КОММЕНТАРИЙ

В настоящее время на фоне быстрорастущей популярности маркетплейсов и интернет-магазинов отмечается и рост мошенничества, связанного с просьбой подтвердить учетные данные из-за возможной утечки данных или для проверки платежа, а также с покупкой товара на сайте-двойнике.

ОТВЕТСТВЕННОСТЬ

Описанные мошеннические схемы, которые связаны с переводом средств на счет человека или организации, могут подпадать под действие уголовного закона. В первую очередь подобные действия квалифицируются по ст. 159 УК РФ «Мошенничество», поскольку злоумышленники вводят потерпевших в заблуждение и незаконно завладевают их средствами.

ЧТО ДЕЛАТЬ, ЕСЛИ НАТКНУЛИСЬ НА МОШЕННИКОВ?

1. Сохраняйте спокойствие и не поддавайтесь панике – мошенники часто используют психологическое давление, создавая ощущение срочности или опасности (например, сообщают о блокировке карты, подозрительных операциях, возможной утечке данных).

2. Как можно быстрее зайдите в свой онлайн-банк. Большая удача, если платеж еще не прошел. Тогда Вы сможете отменить транзакцию или обратиться в банк с просьбой проверить транзакцию. Это актуаль-

но, если речь идет о мошенничестве, при котором Вы перевели деньги на чью-то карту или электронный кошелек.

3. Позвоните в свой банк на горячую линию и сообщите о факте мошенничества. Спросите, что Вам делать. По сути, банки не обязаны ничего предпринимать, но некоторые все же проводят какие-то расследования, дают советы, проверяют мошенника, в редких случаях могут заблокировать его карту за подозрительные операции.

4. Соберите доказательства отсутствия умысла. Подготовьте документы, подтверждающие, что Вы не знали о целях использования средств: переписку с получателем, где обсуждалась «легальная» цель перевода (например, помощь, оплата услуг); ссылки на сайты или соцсети, которые ввели Вас в заблуждение (если перевод был через фальшивый благотворительный фонд).

5. Подайте заявление в полицию.

ВНИМАНИЕ! Согласно ст. 205.1 УК РФ «Содействие террористической деятельности» лицо, добровольно сообщившее о переводе средств террористам и способствовавшее предотвращению преступления, освобождается от уголовной ответственности, если в его действиях нет иного состава преступления. Это важно, если Вы узнали о связи получателя с террористами после перевода и готовы сотрудничать со следствием.

КАК ИЗБЕЖАТЬ ПОДОБНОЙ СИТУАЦИИ?

Если Вам звонит «техподдержка», но у Вас есть сомнения в ее подлинности, стоит немедленно прервать разговор в следующих случаях:

1. Просят назвать код из *SMS* или банковские данные. Настоящие службы поддержки никогда не запрашивают коды подтверждения, *CVV*-коды, *PIN*-коды или пароли.

2. Сообщают о взломе аккаунта и требуют срочных действий. Мошенники часто давят на страх и предлагают «немедленно защитить» аккаунт, но это ловушка.

3. Звонят из неизвестного сервиса, которым Вы не пользуетесь. Если Вам предлагают помощь от компании, где у Вас нет аккаунта, это обман.

4. Используют подменный номер или просят установить сторонние приложения. Если звонок якобы из банка, но номер не совпадает с официальным или предлагают скачать «защитную программу», это 100% мошенничество.

5. Говорят, что Вам звонят из банка, и угрожают последствиями. Настоящие сотрудники таких организаций не требуют перевода денег или передачи данных по телефону.

Лучший выход – сразу повесить трубку и перезвонить в реальную службу поддержки по официальному номеру с сайта компании.

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ

Отвергая нормы морали и права, мошенники стремятся похитить сбережения и ценности граждан, придумывая все более сложные схемы отъема денег.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация. Вам позвонили от имени близкого человека и сообщили, что он попал в аварию, за решетку или в больницу и за него нужно внести залог, штраф, взятку или денежную компенсацию? В последние годы мошенники все чаще используют телефонные звонки как способ обмана граждан.

КОММЕНТАРИЙ

Как показывает статистика, чаще всего в сети телефонных мошенников «попадают» пожилые или доверчивые люди. Каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.

ОТВЕТСТВЕННОСТЬ

Ущерб, причиненный в результате совершения данного деяния, соответствует составу преступления, предусмотренного ст. 159 УК РФ «Мошенничество», т.е. хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Однако ответственность может наступить не только для мошенников, но и для самих потерпевших, если в результате перевода денег оказывается, что они поступили на счета террористических или экстремистских организаций. В таком случае речь идет о ст. 205.1 УК РФ «Содействие террористической деятельности» и ст. 282.3 УК РФ «Финансирование экстремистской деятельности».

ЧТО ДЕЛАТЬ, ЕСЛИ ВАС ОБМАНУЛИ ИЛИ ВВЕЛИ В ЗАБЛУЖДЕНИЕ?

1. Перезвоните в банк или другую кредитную организацию, чтобы остановить перечисление денежных средств и заблокировать банковский счет.

2. Обратитесь за консультацией в юридические организации.

3. Обратитесь в правоохранительные органы с заявлением о возбуждении уголовного дела с приложением всех имеющихся у Вас данных.

КАК ПРЕДОТВРАТИТЬ ПОВТОРЕНИЕ ТАКИХ СИТУАЦИЙ?

1. Будьте настороже. Первый признак мошенничества – это внезапный звонок с плохими новостями. Если Вам звонят и сообщают о несчастном случае с Вашим родственником или другом, сохраняйте спокойствие и не поддавайтесь панике. Мошенники часто используют эмоциональное давление, чтобы заставить жертву действовать быстро и безрассудно.

2. Проверяйте информацию. Если Вам сообщили о несчастном случае, первым делом постарайтесь проверить информацию. Позвоните своему родственнику или другу, чтобы убедиться, что с ним все в порядке. Если Вы не можете до него дозвониться, попробуйте связаться с другими членами семьи или общими знакомыми. Не доверяйте информации от незнакомцев, даже если они утверждают, что работают в правоохранительных органах или медицинских учреждениях.

3. Не предоставляйте личные данные. Мошенники могут пытаться выведать у Вас личные данные под предлогом необходимости помочь Вашему близкому. Никогда не сообщайте свои адреса, номера телефонов, данные банковских карт или другую личную информацию незнакомцам. Настоящие представители служб экстренной помощи никогда не будут запрашивать такую информацию по телефону.

4. Избегайте спешки. Мошенники часто пытаются заставить Вас принять решение быстро, чтобы Вы не успели подумать и проверить информацию. Если Вам говорят, что нужно срочно перевести деньги или оплатить какие-либо услуги, остановитесь и подумайте. Не позволяйте эмоциям управлять Вашими действиями.

5. Уточняйте детали. Если Вам сообщают о несчастном случае, задавайте уточняющие вопросы: где произошел инцидент, какие услуги необходимы, кто именно Вам звонит и т.д. Мошенники могут не иметь четкой информации и запутаться в своих ответах. Если ответы выглядят неубедительно или противоречат друг другу, это может быть признаком мошенничества.

6. Используйте независимые источники. Если Вам говорят о несчастном случае, который произошел в каком-то учреждении (например, больнице или полиции), постарайтесь самостоятельно найти контактные данные этого учреждения и позвонить туда. Не используйте номера телефонов, которые Вам предоставил звонящий.

7. Сообщайте о подозрительных звонках. Если Вы столкнулись с подозрительным звонком, обязательно сообщите об этом в правоохранительные органы. Это поможет предотвратить мошенничество в будущем и защитить других людей от подобных ситуаций.

8. Обучайте своих близких. Обсудите с родственниками и друзьями возможные сценарии мошенничества. Чем больше людей будет осве-

домлено о методах мошенников, тем меньше шансов у них обмануть кого-либо из вас. Убедитесь, что Ваши близкие знают, как действовать в случае получения подобного звонка.

9. Используйте технологии. Существуют приложения и сервисы, которые помогают блокировать нежелательные звонки и идентифицировать потенциальные мошеннические номера. Установите такие приложения на свой телефон для дополнительной защиты.

Следуя этим рекомендациям, Вы сможете защитить себя и своих близких от мошеннических схем при звонках о несчастных случаях.

МОШЕННИЧЕСТВО ПРИ ПОИСКЕ РАБОТЫ

В современном мире Интернет стал основным инструментом для поиска работы. Каждый день сотни тысяч россиян занимаются поиском работы. Однако вместе с удобством возросла и угроза столкнуться с мошенниками. Около одной четверти объявлений о вакансиях размещаются мошенниками, по данным статистики ГУ МВД России за 2024 г.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация. Злоумышленники размещают в Интернете вакансии и ждут отклика кандидатов. Соискателя принимают, присылают ему договор и просят сказать номер карты, а затем и код из *SMS* – якобы для перечисления гонорара. Однако на деле это лишь уловка, чтобы похитить деньги.

ОТВЕТСТВЕННОСТЬ

Ущерб, причиненный в результате совершения данного деяния, соответствует составу преступления, предусмотренного ст. 159 УК РФ «Мошенничество», т.е. хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

ЧТО ДЕЛАТЬ, ЕСЛИ ВАС ОБМАНУЛИ ИЛИ ВВЕЛИ В ЗАБЛУЖДЕНИЕ?

1. Обратитесь в правоохранительные органы с заявлением о возбуждении уголовного дела с приложением всех имеющихся у Вас данных.
2. Перезвоните в банк или другую кредитную организацию, чтобы остановить перечисление денежных средств и заблокировать банковский счет.
3. Сообщите об этом на специализированные сайты, где пользователи могут делиться информацией о мошенниках. Это поможет другим избежать подобных ситуаций.

КАК ПРЕДОТВРАТИТЬ ПОВТОРЕНИЕ ТАКИХ СИТУАЦИЙ?

1. Исследуйте компанию. Перед тем как откликнуться на вакансию, проведите тщательное исследование компании. Посетите ее официальный сайт, изучите информацию о деятельности, ценностях и репутации. Обратите внимание на наличие контактной информации, включая адрес и телефонный номер. Если компания не предоставляет такую информацию или она выглядит подозрительно, это может быть первым сигналом о мошенничестве.

2. Будьте осторожны с предложениями о работе. Если Вам предлагают работу, которая кажется слишком хорошей, чтобы быть правдой (например, высокая зарплата за минимальные усилия), будьте настороже. Мошенники часто используют заманчивые предложения, чтобы привлечь внимание соискателей. Проверяйте информацию о вакансии на независимых ресурсах и форумах.

3. Не отправляйте деньги. Никогда не отправляйте деньги работодателю под предлогом оплаты за обучение, страховку, оборудование или любые другие расходы. Надежные компании никогда не требуют предварительных платежей от соискателей. Если Вас просят перевести деньги, это явный признак мошенничества.

4. Используйте проверенные платформы. При поиске работы используйте известные и проверенные платформы для размещения резюме и поиска вакансий (например, *LinkedIn*, *HeadHunter*, *Indeed*). Такие сайты часто имеют механизмы проверки работодателей и могут помочь избежать мошенничества.

5. Обращайте внимание на грамматику и стиль письма. Мошеннические объявления о работе часто содержат ошибки в грамматике и орфографии. Если текст вакансии выглядит неаккуратно или неформально, это может быть признаком того, что предложение не является легитимным.

6. Не раскрывайте личную информацию. Будьте осторожны с личными данными. Никогда не предоставляйте информацию о своем банковском счете, номере социального страхования или другие конфиденциальные данные до тех пор, пока Вы не будете уверены в легитимности компании. Обычно такие данные запрашиваются только после официального трудоустройства.

7. Проводите собеседования только в безопасной обстановке. Если Вам предлагают пройти собеседование, выбирайте безопасное место – лучше всего это сделать в офисе компании или через видеозвонок на проверенной платформе. Избегайте собеседований в общественных местах или по телефону с незнакомыми людьми.

8. Доверяйте своим инстинктам. Если что-то кажется неправильным или вызывает у Вас сомнения, не игнорируйте свои чувства. Лучше отказаться от предложения, чем рисковать своими деньгами и данными.

Следуя этим рекомендациям, Вы сможете снизить риски и успешно найти работу без столкновения с мошенниками. Помните, что Ваша безопасность на первом месте!

ЗА «ЛЕГКИЕ» ДЕНЬГИ ТЯЖЕЛАЯ ОТВЕТСТВЕННОСТЬ

В настоящее время среди молодежи популярна идеология «легких» денег. С появлением многочисленных блогеров, которые не занимаются тяжелой физической работой и демонстрируют свою богатую и счастливую жизнь, физический и умственный труд обесценивается.

Молодежь стремится к богатой жизни без приложения значительных усилий. Поэтому на интернет-сайтах, в социальных сетях и мессенджерах все чаще встречаются предложения о легких подработках, которые сулят быстрый и легкий заработок.

Но, как известно, «бесплатный сыр бывает только в мышеловке», а легкий заработок оборачивается серьезными проблемами. Чаще всего жертвами «легкого заработка» становятся люди, нуждающиеся в деньгах: студенты, школьники, люди из неблагополучных семей.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация 1. Привлечение «курьера». Мошенник сулит легкий заработок, ведь необходимо всего лишь забрать в указанном адресе денежные средства у незнакомого человека и внести их через банкомат на определенный счет или передать другому лицу. Злоумышленник заранее звонит будущей жертве и под различными предлогами (взломали банковский счет, родственник попал в ДТП) вынуждает приготовить для передачи «курьеру» крупную денежную сумму, якобы для решения проблемы. Стоит отметить, что «курьеру» могут поручить прием и передачу не только похищенных денежных средств, но и поддельных документов.

Ситуация 2. «Дропперство». Для «отмывания» и снятия с банковских карт переведенных обманутыми гражданами денег мошенники привлекают дропперов (дропов). Эти люди заводят банковские карты, а злоумышленники переводят на них похищенные средства. В итоге дропы попадают в руки полиции, а мошенники выходят сухими из воды. Дропами чаще всего становятся люди, нуждающиеся в деньгах: студенты и школьники, которым родители в 14 лет оформили банковскую карту.

Ситуация 3. Работа «кладменом (закладчиком)». К сожалению, наркодилеры находят все новые способы для распространения наркотиков, вовлекая в это не только взрослых, но и молодежь. Дети соблазняются иллюзией легкого и быстрого заработка и помогают распространять наркотики среди граждан.

ОТВЕТСТВЕННОСТЬ

В погоне за легким заработком люди нарушают закон. «Курьеры», несмотря на то, что не они обманывали и таким способом похищали денежные средства, чаще всего становятся соучастниками преступления, предусмотренного ст. 159 УК РФ «Мошенничество».

«Дропперы» также могут нести уголовную ответственность по данной статье, кроме того, часто они становятся соучастниками в преступлении, предусмотренном ст. 174 УК РФ «Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем».

Наказание за преступления, связанные с оборотом наркотиков, предусматривает ст. 228 УК РФ «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». В ней несколько пунктов. К примеру, наказуемыми являются: незаконное приобретение, хранение, перевозка, изготовление, переработка без цели сбыта наркотических средств и психотропных веществ (ст. 228 УК РФ); незаконные производство, сбыт или пересылка (ст. 228.1 УК РФ); нарушение правил оборота наркотических средств или психотропных веществ (ст. 228.2 УК РФ). За преступления в сфере обращения наркотических средств предусмотрены одни из самых суровых наказаний.

ЧТО ДЕЛАТЬ, ЕСЛИ НАТКНУЛИСЬ НА МОШЕННИКОВ?

1. Если Вам предложили подобный заработок, действуйте аккуратно. Разузнайте все про работодателя. Если же заработок заведомо незаконный, то подумайте о своем будущем после совершения незаконных действий и о чувствах своих родных.

2. Не спешите отказывать. Вы вполне можете помочь правоохранительным органам в разоблачении преступника, который больше не сможет обманывать невинных людей.

3. Обратитесь в полицию и объясните ситуацию. Помните, что Ваши помощь и здравомыслие спасут немало людей от горя и бедности, потому что «легких» денег не бывает.

КАК ИЗБЕЖАТЬ ПОДОБНОЙ СИТУАЦИИ?

1. Никогда не ждите от жизни подарков в виде случайно свалившихся богатств. Помните, что честный и законный заработок всегда сопровождается огромными усилиями со стороны человека.

2. Не доверяйте даже знакомым, если у Вас появились сомнения в их порядочности. Если Вам предложили быстро подзаработать и для

этого «ничего даже делать не надо», то отнеситесь к такому предложению скептически.

3. Чтобы не стать дроппером, следует никому не сообщать данные своей банковской карты, не передавать ее третьим лицам, не соглашаться переводить и снимать в банкомате деньги по просьбе неизвестных лиц, никуда не перенаправлять деньги, которые поступили по ошибке. В последнем случае надо обратиться в банк и попросить сделать обратный перевод по реквизитам отправителя. О подозрительных просьбах необходимо сообщать в банк и в полицию.

Вот несколько признаков, по которым можно вычислить мошенников:

- не могут четко описать Ваши обязанности либо напрямую говорят, что работа связана с переводом/обналичиванием денег;
- предлагают работать неофициально;
- не сообщают адрес офиса, предлагают встретиться на улице;
- просят немедленно сообщить им личные данные и информацию о банковской карте, в том числе код из *SMS*.

4. Объясните детям, друзьям, что никому нельзя сообщать данные банковских карт и тем более давать к ним доступ. Если карта оформлена для ребенка, то стоит установить лимит на переводы и снятие наличных денежных средств. Обратите внимание ребенка на то, что только он должен пользоваться данной картой.

5. Наконец, следите не только за собой, но и за состоянием своих родственников и близких друзей, ведь именно Вы способны их защитить в таких ситуациях, так как теперь обладаете жизненно важной информацией.

Если Вам звонят с неизвестного номера и просят:

- перевести деньги на сторонний счет;
- сообщить номер карты и код на обратной стороне;
- продиктовать код из *SMS*;
- перейти по ссылке или скачать приложение;
- пополнить баланс неизвестного номера;
- перевести деньги для получения приза или компенсации;
- отправить сумму, чтобы спасти попавшего в беду,

ПРЕРВИТЕ РАЗГОВОР!

С Вами на связи мошенники!

КТО ТАКИЕ ДРОППЕРЫ, ИЛИ КАК НЕ СТАТЬ СОУЧАСТНИКОМ ПРЕСТУПЛЕНИЯ?

В число дропперов чаще всего попадают подростки и пенсионеры. Первых привлекают азарт и быстрый заработок. Обычно они «клюют» на подработку в *Telegram*. Люди старшего возраста менее информированы о том, как устроены банковские технологии, доверчивы, им сложнее обнаружить мошенническую схему.

Виды дропперов:

• «неразводные» (осведомлены о криминальной составляющей своей деятельности и действуют добровольно и умышленно);

• «разводные» (не понимают, что находятся в ловушке у мошенников, и не отдают себе отчета, что участвуют в схеме, нарушающей закон);

• «обнальщики» (самостоятельно обналичивают денежные средства);

• «транзитники» (принимают денежные средства на свой счет, а дальше переводят их сторонним лицам по указанию мошенников);

• «заливщики» (получают наличные денежные средства от других таких же дропов, вносят их к себе на счет и отправляют по цепочке «транзитнику»).

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация. 21-летний парень из Оренбурга решил подзаработать на открытии карты и переводах. Куда? Кому? Лишними вопросами он не задавался. Конечно, ему поведали об очередных крипто-проекте или бизнес-необходимости. Не откровенный криминал – и ладно. Деньги он переводил исправно, получал процент. Но однажды с ним связался следователь и сообщил, что с помощью его карты обманули пенсионерку. 216 тыс. руб. были краденными.

Конечно, парень их уже перевел, денег и след простыл, но для обвинения было достаточно установить номер карты, на который поступил перевод от обманутой пенсионерки. Прокуратура города обратилась в суд с исковым заявлением о взыскании с владельца счета суммы неосновательного обогащения чужими денежными средствами. Дроппер был признан соучастником мошеннической схемы и попал на всю сумму долга. Приставы изъяли у него 216 тыс. руб. в пользу жертвы. Вот тебе и заработал... Естественно, реальный организатор этих схем остался за кадром, в отличие от наивных подельников. Молодые парни получают сроки, а потом втягиваются в эту систему, из которой уже нет выхода.

ОТВЕТСТВЕННОСТЬ

Мошенничество (ст. 159 УК РФ). По ч. 4 ст. 159 УК РФ предусмотрено наказание в виде лишения свободы на срок до 10 лет со штрафом в размере до 1 млн руб. или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Организация преступного сообщества (преступной организации) или участие в нем (ней) (ст. 210 УК РФ). Участие в преступном сообществе наказывается лишением свободы на срок от семи до 10 лет со штрафом в размере до 3 млн руб. или в размере заработной платы или иного дохода осужденного за период до пяти лет либо без такового и с ограничением свободы на срок от одного года до двух лет.

Преступления в сфере незаконного оборота наркотиков. Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества (ст. 228.1 УК РФ), наказываются вплоть до пожизненного лишения свободы. Аналогичным образом наказывается контрабанда наркотиков (ст. 229.1 УК РФ).

Также дропперов привлекают за *неправомерный оборот средств платежей* (ст. 187 УК РФ).

В настоящее время велик риск быть вовлеченными в *террористическую* (ст. 205.1, 205.4, 205.5 УК РФ) или *экстремистскую* деятельность (ст. 282.1, 282.2, 282.3 УК РФ).

ЧТО ДЕЛАТЬ В СЛОЖИВШЕЙСЯ СИТУАЦИИ?

Если Вы случайно оказались вовлечены в незаконную деятельность, немедленно сообщите об этом в правоохранительные органы. Чем раньше Вы поймете свою ошибку, тем меньше будет риск уголовной ответственности.

КАК НЕ СТАТЬ ЖЕРТВОЙ ЗЛОУМЫШЛЕННИКОВ?

Не верьте на слово! Быстрый заработок часто скрывает преступную деятельность. Остерегайтесь подозрительных предложений и защищайте себя от ненамеренного участия в преступлениях.

При общении с незнакомыми людьми по телефону и в мессенджерах всегда нужно сохранять холодную голову, нельзя поддаваться эмоциям и давать доступ к своим счетам злоумышленникам, как бы они ни убеждали и ни угрожали.

КАК МОШЕННИКИ «ТОЛКАЮТ» НА СОВЕРШЕНИЕ ДИВЕРСИЙ ПРОТИВ ГОСУДАРСТВА?

Для совершения диверсий активно применяются компьютерные и сетевые технологии: интернет-медиа, социальные сети и мессенджеры, официальные сайты органов власти. Злоумышленники получают к ним незаконный доступ и воздействуют на население с помощью искаженной информации, угроз, предложений. В настоящее время массово распространяются предложения быстрого заработка за совершение диверсии.

Мошенники предлагают от 50 до 300 тыс. руб. за выполнение одного определенного задания. Жертв преступных схем подцепляют сообщениями о подозрительных переводах со счетов, попытками оформить кредит, предложениями помочь с поимкой преступников, угрозами человеку или его родным, а также открытыми предложениями совершить конкретные действия.

Всего с начала специальной военной операции МВД России выявило 220 фактов нападений и поджогов органов власти и военкоматов, а также зафиксировало свыше 180 случаев диверсий на железных дорогах.

На внутреннюю дестабилизацию России делается большая ставка, и схемы вовлечения российских граждан в диверсионную деятельность достаточно изощрены.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация 1. Сергей, потерявший работу и испытывающий финансовые трудности, познакомился в Интернете с человеком, который жаловался на «несправедливость власти» и предлагал «помочь восстановить справедливость». Сергею предложили «мелкое задание» – распространить листовки. Позже задания стали более серьезными и рискованными, под предлогом «борьбы за правду». Сергею пообещали, что его семья получит финансовую поддержку, если он будет «помогать движению».

Ситуация 2. Доверчивым пенсионерам предлагают, например, списать долги – казалось бы, легкий выход из сложной ситуации. Но никто не предупреждает, как будет на самом деле. В телефонном разговоре дают инструкцию и адрес места, где совершить акт диверсии.

КОММЕНТАРИЙ

Обманутые россияне уверены, что действовали по заданию сотрудников ФСБ России, МВД России или Центробанка. Эти кураторы

(на деле – мошенники) под благими предлогами, угрозами и манипуляциями заставляют готовить зажигательные смеси, а затем идти к военкоматам.

ОТВЕТСТВЕННОСТЬ

Диверсия – это уголовно наказуемое деяние, под которым понимается совершение взрыва, поджога или иных действий, которые направлены на разрушение или повреждение предприятий, сооружений, объектов транспортной инфраструктуры и транспортных средств, средств связи, объектов жизнеобеспечения населения либо на нанесение вреда здоровью людей и (или) компонентам природной среды.

В отличие от терактов диверсии совершаются скрытно, без привлечения внимания. Зачастую они представляют собой действия, которые в дальнейшем поспособствуют проведению террористического акта. Целью совершения диверсии является подрыв экономической безопасности и обороноспособности РФ.

Объектами диверсии могут стать:

1) промышленные предприятия;

2) общественные места;

3) транспортная инфраструктура;

4) общественный транспорт;

5) узлы связи;

6) объекты, отвечающие за жизнеобеспечение населенных пунктов;

7) объекты оборонного комплекса.

Диверсионные действия: взрыв; затопление; поджог; иные действия, влекущие выход из строя объекта.

Диверсии в компьютерных сетях могут представлять собой: рассылку компьютерных вирусов; взлом и проникновение в локальные вычислительные сети, подключенные к Интернету, с целью похищения, изменения или уничтожения информации; переполнение электронных почтовых ящиков; перегрузку серверов избыточным количеством обращений.

Диверсии могут приобретать различную форму:

1) экономические диверсии (демпинг, валютные махинации и др.);

2) политические диверсии (заговор, переворот, организация беспорядков и др.);

3) информационно-психологические диверсии и др.

Уголовная ответственность. За диверсию предусмотрена уголовная ответственность:

• ст. 281 УК РФ:

– за совершение диверсии наступает наказание в виде лишения свободы на срок от 10 до 20 лет;

– если диверсия совершена организованной группой или повлекла причинение значительного имущественного ущерба либо наступление иных тяжких последствий, наступает наказание в виде лишения свободы на срок от 12 до 20 лет;

– если последствием диверсии стало причинение смерти человеку, то наступает наказание в виде лишения свободы на срок от 15 до 20 лет или пожизненное лишение свободы.

• ст. 281.1 УК РФ:

– ответственность за склонение, вербовку, вооружение, финансирование в целях совершения диверсий. Наказание – от восьми до 15 лет лишения свободы со штрафом от 300 до 700 тыс. руб.;

• ст. 281.2 УК РФ:

– ответственность за прохождение обучения по подготовке диверсии. Наказание – лишение свободы от 15 до 20 лет с ограничением свободы до двух лет или пожизненное лишение свободы;

• ст. 281.3 УК РФ:

– ответственность за создание диверсионного сообщества (руководство, пропаганда и поддержка диверсий сообществом). Наказание – от 15 до 20 лет лишения свободы со штрафом до 1 млн руб. Участие в таком сообществе – колония от пяти до 10 лет со штрафом до 500 тыс. руб.

Если субъект, совершивший преступление, не достиг возраста привлечения к уголовной ответственности, к нему будут применены иные меры ответственности, такие как помещение в специальные учебно-воспитательные учреждения закрытого типа, а также привлечение законных представителей к материальной ответственности с возмещением причиненного преступлением ущерба.

Террористический акт (ст. 205 УК РФ). Совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями наказывается лишением свободы на срок от 10 до 20 лет или пожизненным лишением свободы.

Финансирование терроризма (ст. 205.1 УК РФ). Предоставление или сбор средств либо оказание финансовых услуг, заведомо предназначенных для финансирования организации, подготовки или совершения хотя бы одного из преступлений террористической направленности, наказывается лишением свободы на срок от восьми до 15 лет со штра-

фом в размере до 500 тыс. руб. либо в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового.

Государственная измена (ст. 275 УК РФ). Совершение гражданином Российской Федерации действий, направленных против безопасности Российской Федерации: шпионаж, выдача иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, либо оказание помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности Российской Федерации, наказывается лишением свободы на срок от 12 до 20 лет со штрафом в размере до 500 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет.

ЧТО ДЕЛАТЬ В СЛОЖИВШЕЙСЯ СИТУАЦИИ?

1. Оцените ситуацию. Не переходите по ссылкам, направленным Вам в *SMS*-сообщениях и социальных сетях.

Кто предлагает? Обратите внимание на все детали, которые могут помочь Вам понять мотивацию лица, предлагающего совершить какие-либо действия. Если это возможно, запишите разговор с помощью аудио или видео, сделайте заметки о внешности человека, его словах, месте и времени разговора.

Что именно предлагается? Уточните детали диверсии. Зафиксируйте информацию: запомните и отметьте все, что Вам сказали, включая время, место и способ совершения требуемых от Вас действий.

Каковы последствия? Подумайте о возможных последствиях как для Вас, так и для других людей – потенциальный материальный ущерб, травмы, смерть и наказание, которые могут повлечь предлагаемые действия.

2. Решите, что делать.

Категорически откажитесь. Ясно и твердо выразите свой отказ. Не давайте двусмысленных ответов. Важно помнить, что данное в процессе переписки согласие на выполнение тех или иных действий формально образует приготовление к преступлению. Поэтому в переписке нельзя давать согласие на совершение общественно опасных действий даже в шутку. Кроме того, сам вербовщик может позднее использовать скриншоты с таким согласием для шантажа, требуя передачи денежных средств или совершения каких-либо иных действий.

3. Обратитесь в правоохранительные органы.

Не пытайтесь самостоятельно проводить расследование. Не предпринимайте никаких действий, которые могут подвергнуть Вас опасности.

Сообщите о предложении. Свяжитесь с полицией или Федеральной службой безопасности и подробно опишите ситуацию. Предоставьте всю ранее собранную Вами информацию.

Сотрудничайте со следствием. Следуйте инструкциям правоохранительных органов и выполняйте их указания.

4. Защитите себя.

Избегайте контактов с человеком, сделавшим Вам предложение. Не отвечайте на звонки, сообщения или другие попытки связаться с Вами.

Будьте осторожны. Будьте внимательны к своему окружению и не подпускайте близко незнакомых Вам людей, избегайте подозрительных ситуаций.

При необходимости обратитесь за помощью к психологу, психотерапевту или юристу. Они могут помочь Вам справиться с переживаниями или полученной психологической травмой, а также получить необходимую юридическую консультацию по делу.

Этот алгоритм представляет собой общие рекомендации. Ваши действия могут варьироваться в зависимости от конкретной ситуации и местонахождения. Однако важно всегда действовать разумно и обращаться за помощью к компетентным органам.

5. Предупредите диверсию.

Для того чтобы избежать ситуации, в которой Вам могут предложить совершение диверсии, прежде всего стоит быть более осмотрительным и предоставлять как можно меньше личных данных в открытый доступ:

- будьте бдительны в онлайн- и офлайн-пространстве;
- развивайте критическое мышление и способность анализировать информацию;
- не доверяйте слепо всему, что видите или слышите, особенно в Интернете;
- мошенники нацелены на быстрый результат, поэтому они действуют в короткие сроки, что также создает стрессовую ситуацию для жертвы, которая способствует скорому принятию преступниками решения;
- подходите ко всему с «холодной головой», не поддаваясь провокациям и проверяя любую информацию в официальных источниках;
- следите за новостями и будьте в курсе текущей политической и общественной ситуации, так как информированность поможет распознавать потенциальные опасности;
- соблюдайте правила цифровой гигиены и используйте сложные пароли, регулярно обновляйте программное обеспечение, будьте осторожны с подозрительными ссылками и электронными письмами;
- осторожно ведите себя в социальных сетях и не делитесь личной информацией (не публикуйте данные о своей учебе, работе, местопо-

ложении, планах на будущее): вся эта информация может быть использована против Вас;

• не доверяйте незнакомцам и будьте внимательны к людям, которые чрезмерно интересуются Вашей жизнью или высказывают радикальные взгляды, избегайте открытых дискуссий на политические или провокационные темы с людьми, которых Вы плохо знаете;

• ограничьте круг общения и будьте осторожны с новыми знакомствами;

• общаясь с семьей и друзьями, рассказывайте близким о своих планах и опасениях, сообщайте о своем местонахождении, особенно если Вы находитесь в потенциально опасном месте или ситуации, чтобы они могли помочь Вам в случае необходимости;

• избегайте сомнительных компаний и мест, ограничьте общение с людьми, которые ведут себя подозрительно, имеют связи с радикальными группировками или замечены в противозаконной деятельности;

• избегайте мест, где происходят массовые беспорядки, митинги или собрания радикальных группировок;

• будьте внимательны и осторожны во время путешествий, особенно в странах с нестабильной политической ситуацией;

• знайте свои права и обязанности;

• проявляйте гражданскую сознательность и сообщайте о подозрительных действиях в полицию или другие соответствующие органы, не игнорируйте подозрительное поведение других людей и не закрывайте глаза на потенциальные угрозы;

• не устанавливайте в своих мобильных устройствах программы, которые Вас просят установить неизвестные лица;

• не соглашайтесь на предложения легкого заработка от незнакомцев.

Важно быть бдительным, осознанным и ответственным. Помните, что люди, не поддающиеся внушению, просто не представляют интереса для вербовщиков. Главное правило защиты от манипуляций – перепроверка достоверности любой получаемой информации.

КАК НЕ СТАТЬ ЖЕРТВОЙ ЗЛОУМЫШЛЕННИКОВ?

Выход здесь один – стоп: сказать себе «стоп», когда поступает звонок.

С меня просят деньги – стоп, остановись, на секунду остановись, на секунду подумай.

Прервать разговор.

Положить трубку и после сообщить о произошедшем в полицию по номеру 02 или с мобильного 102, 112.

Если Вам звонят люди, которые представляются сотрудниками спецслужб, правоохранительных органов и просят Вас что-то сделать, задайте себе вопрос: почему Вам вообще они должны звонить?

ВНИМАНИЕ! Настоящие сотрудники правоохранительных органов никогда не демонстрируют свои удостоверения в мессенджерах и тем более на заставляют совершать поджоги и другие преступления. Есть четкий и простой регламент взаимодействия полицейских с гражданами.

Сотрудник полиции, если надо, придет к Вам в форме.

Вы знаете своего участкового. Вас пригласят обязательно или в опорный пункт, или в отдел полиции, где разъяснят Ваши права, обязанности, ознакомят со всеми необходимыми вопросами. Сотрудник полиции не будет Вас привлекать для проведения каких-либо специальных операций. Для этого вполне хватает своих сотрудников. Полиция сегодня не будет на удаленном доступе по телефону просить Вас о выполнении каких-либо своих поручений.

КАК УБЕРЕЧЬ СЕБЯ И СВОИХ БЛИЗКИХ ОТ ФИНАНСОВЫХ ПИРАМИД?

Финансовая пирамида – это незаконный способ получения дохода, базирующийся на перераспределении денежных средств от нижестоящих к вышестоящим участникам пирамиды.

Главный смысл всех финансовых пирамид – это привлечение большой массы вкладчиков для незаконного обеспечения благосостояния организаторов и заинтересованных лиц.

По своей правовой природе финансовая пирамида – это преступление против собственности. Составы таких преступлений предусмотрены гл. 21 УК РФ.

(Основными видами финансовых пирамид являются многоуровневые пирамиды, построенные по типу Понци.

Первая – это та самая пирамида, где каждый вновь прибывший вносит вклад, который распределяется между вкладчиками, стоящими по иерархии выше.

Таким образом, чтобы новоприбывший вкладчик получил выплату, он в свою очередь должен привести новых желающих, которые также сделают первый взнос.

Вторая пирамида отличается от многоуровневой тем, что новому вкладчику не требуется приводить такого же нового инвестора. Требуется только первое крупное вложение, далее организатор выплачивает первому вкладчику из «собственных» денежных средств прибыль, что становится толчком для срабатывания принципа взаимного информирования.)

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация 1. Пенсионерка верит в «высокий доход». Баба Нина увидела в газете рекламу «инвестиционного фонда», обещавшего 50% годовых. Сотрудник фонда убедил ее перевести все накопления, чтобы обеспечить себе «безбедную старость». Через месяц выплаты прекратились, а «фонд» исчез.

Ситуация 2. Молодой специалист и «успешный бизнес». Андрей, стремясь к финансовой независимости, вложил все свои сбережения в «стартап», который обещал огромные прибыли от торговли криптовалютой. Его уговорил знакомый, который сам недавно вступил в эту «компанию» и хвастался своими успехами. Вскоре выяснилось, что компания не ведет никакой реальной деятельности, а выплаты первым участникам осуществляются за счет новых вкладчиков.

Ситуация 3. Мать-одиночка и «легкий заработок». Ольга, находясь в сложной жизненной ситуации, увидела в Интернете объявление о высо-

кооплачиваемой работе курьером. Ей нужно было лишь забирать посылки в разных местах и передавать их «клиентам». Впоследствии выяснилось, что она перевозила наркотики, а ее «работода-тели» – наркоторговцы.

ОТВЕТСТВЕННОСТЬ

Существует несколько норм, нарушаемых финансовыми пирамидами, включая:

- ст. 159 УК РФ «Мошенничество»: предусматривает лишение свободы на срок до 10 лет в зависимости от тяжести преступления;
- ст. 172 УК РФ «Незаконная банковская деятельность»: также устанавливает уголовную ответственность за осуществление финансовых операций без лицензии.

Для тех, кто переводит деньги мошенническим организациям, предусмотрены аналогичные статьи УК РФ, так как они могут быть признаны соучастниками таких действий.

ЧТО ДЕЛАТЬ В СЛОЖИВШЕЙСЯ СИТУАЦИИ?

1. Нельзя поддаваться панике! Убедитесь еще раз, что Вы точно попали в финансовую пирамиду, после чего принимайте меры по выводу Ваших законных средств из активов данной организации.

2. Соберите все документы, которые доказывают факт передачи Ваших денежных средств в руки мошенников. Это могут быть договоры, выписки по банковскому счету, переписки с организаторами.

3. Попробуйте связаться с организаторами финансовой пирамиды для вывода Ваших средств. Скорее всего, Вам откажут.

4. Найдите всех возможных участников данной финансовой пирамиды, а также потерпевших от ее деятельности.

Гражданско-правовые меры:

Вариант 1. Направьте в адрес компании претензию с требованием о возвращении денежных средств.

Вариант 2. Если Вам будет отказано, то Вы можете направить в адрес организации иск. Важно обратить внимание на договор, если Вы его заключали с организацией, по которому Вы передавали денежные средства, так как в данной ситуации Вы можете столкнуться со следующей проблемой: если это «профессиональные» мошенники, то в договоре они могут прописать условие, что при досрочном выводе денежных средств на вкладчика налагается денежный штраф в определенном размере. При подаче иска стоит найти всех пострадавших от данной финансовой пирамиды, а также стоит воспользоваться услугами профессионального представителя.

Уголовно-правовые меры:

Вариант 1. Обратитесь в правоохранительные органы. Обращаясь в правоохранительные органы, займите активную позицию, т.е. содей-

ствуйте следствию в полном объеме, попытайтесь осветить данную ситуацию в социальных сетях, Вы даже можете попробовать обратиться в СМИ. Все это повысит шанс быстрого реагирования защитников на Вашу проблему. Если же деятельность сотрудников будет затягиваться, Вы можете обратиться за защитой своих интересов в органы прокуратуры.

Также важно воспользоваться услугами профессионального защитника, но еще важнее найти потерпевших от незаконных действий организации людей. При подаче одиночного заявления в правоохранительные органы существует шанс, что за Вашим заявлением последует отказ со ссылкой на то, что это гражданско-правовые отношения. Но при написании не одного заявления, а, допустим, 15 заявлений, в которых будет фигурировать данная организация, Вы повышаете шанс положительного разбирательства в Вашу пользу.

Вариант 2. Пишите не просто заявление в правоохранительные органы, а заявление о возбуждении уголовного дела с требованием возбудить уголовное дело по ст. 159 УК РФ. В случае отказа воспользуйтесь услугами высококвалифицированного юриста и обжалуйте отказ в суде.

Также важно помнить, что при отказе в возбуждении уголовного дела Вы можете составить жалобу в порядке ст. 125 УПК РФ. Таким образом, в процессе рассмотрения жалобы будут участвовать сотрудники прокуратуры.

Вариант 3. Вы можете попытаться связаться с организаторами пирамиды и уведомить их, что написали заявление о возбуждении уголовного дела в органы, и не только Вы, а еще 15 потерпевших. Это может стать рычагом давления на организаторов, и, возможно, они предпримут попытку решить данную проблему, например, вернув Вам деньги.

КАК НЕ СТАТЬ ЖЕРТВОЙ ЗЛОУМЫШЛЕННИКОВ?

1. Не верьте обещаниям высоких доходов. Критически оценивайте инвестиционные предложения, которые обещают сверхприбыли за короткий срок.

2. Проверяйте информацию о компании. Узнайте, зарегистрирована ли компания, имеет ли она лицензии на осуществление финансовой деятельности, изучите отзывы в Интернете.

3. Будьте осторожны с предложениями от знакомых. Не доверяйте слепо рекомендациям друзей и родственников, особенно если они сами недавно вступили в сомнительный «проект».

4. Тщательно изучайте договоры. Прежде чем подписывать какие-либо документы, внимательно прочитайте все условия, обращая внимание на мелкий шрифт и скрытые комиссии.

5. Не вкладывайте последние деньги. Инвестируйте только те средства, которые Вы готовы потерять.

ЧТО ДЕЛАТЬ, ЕСЛИ С БАНКОВСКОЙ КАРТЫ УКРАЛИ ДЕНЬГИ?

Необходимо выяснить, точно ли списание денежных средств является мошенническим.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация 1. Часто люди, посещая какие-либо сайты или используя приложения, приобретают семидневный пробный период пользования сервисом. При этом лица, администрирующие такие сервисы, просят ввести данные банковской карты, сообщая, что это необходимо для предоставления клиенту безвозмездного периода доступа к сервису. По окончании пробного (бесплатного) периода сервис списывает с карты средства за подписку на определенный период без повторного одобрения самого человека, так как данная подписка настраивается как автоплатеж.

Вряд ли можно будет доказать, что подобные действия администраторов сервиса носят криминальный характер. Как правило, администраторы таких сервисов заявляют о том, что они предупреждали клиентов об автоплатеже. И привлечь их к гражданско-правовой ответственности будет весьма затруднительно, поскольку доступ к сервису они обеспечили. В этой связи важно проверять отключение автоплатежа.

Ситуация 2. При оплате покупки произошла ошибка, клиент ввел *PIN*-код дважды, что привело к повторному списанию средств с карты.

В таком случае необходимо обратиться в банк, после проверки банк вернет средства. Однако надо представить доказательства того, что дважды произошла оплата именно одного и того же товара.

Ситуация 3. Деньги могут быть списаны по решению суда без уведомления клиента в том случае, если у клиента имеются непогашенные обязательства по алиментам, налоги и штрафы. Если есть просроченная задолженность по кредиту, на счете достаточно средств, а договором предусмотрено безакцептное списание, то банк может удержать сумму долга.

Такими полномочиями обладает служба судебных приставов. При этом она должна информировать клиента о подобных взысканиях. В этой связи рекомендуется проверить в реестре исполнительных производств наличие задолженности на собственное имя. Для этого требуется ввести свои имя и паспортные данные.

ОТВЕТСТВЕННОСТЬ

Тем не менее в большинстве случаев завладение Вашими деньгами является преступлением. В зависимости от особенностей совершенного преступления квалифицировано оно может быть по-разному. Например, если кто-то тайно изъял Вашу карту, виновный будет нести ответственность за кражу по ст. 158 УК РФ. За кражу виновный будет привлечен и в том случае, если обналичил деньги с потерянной Вами карты. Иная квалификация содеянного будет в том случае, если Вы сами предоставили виновному свои персональные данные, используя которые преступник обналичил деньги. Ответственность в этом случае будет наступать по ст. 159 УК РФ за мошенничество. В некоторых ситуациях возможна квалификация содеянного по ст. 159.3 УК РФ, предусматривающей уголовную ответственность за обманное использование чужой банковской расчетной, кредитной или иной платежной карты. Однако сообщение о похищении Ваших денег является основанием для возбуждения уголовного производства, которое предполагает розыск преступников. Скорее всего, они уже успели распорядиться Вашими деньгами по своему усмотрению. Случаи, когда правоохранительные органы возвращают клиентам похищенные у них деньги, редки. Для возврата денег с преступников Вам придется дождаться их осуждения и предъявления иска к ним в порядке гражданского судопроизводства (либо будет необходимо заявлять гражданский иск в уголовном деле).

В некоторых случаях возможно привлечь к ответственности банк, который обслуживал счет. Как правило, это можно сделать в той ситуации, когда к совершенному хищению причастны сотрудники банка (например, были соучастниками тех лиц, которые похитили деньги, – предоставляли им информацию и т.д.). В тех случаях, когда Вы сами (пусть и в результате обмана) предоставили данные или доступ к деньгам мошенникам, банк привлечь к гражданско-правовой ответственности будет нельзя.

ЧТО ДЕЛАТЬ В СЛОЖИВШЕЙСЯ СИТУАЦИИ?

При наличии подозрительных транзакций на банковском счете или в случае потери карты действовать необходимо следующим образом:

1. Немедленно позвоните на горячую линию Вашего банка, изложите суть проблемы и заблокируйте карту. Также это можно сделать через мобильное приложение банка.

2. Если средства уже были списаны, посетите отделение банка и подайте письменное заявление по установленному образцу. Обратите внимание, что большинство банков требуют уведомить их о несанкционированной операции в течение 24 часов.

3. Ожидайте ответа: банк либо вернет средства, либо откажет в возврате. Обычно процесс рассмотрения занимает до 30 дней, однако если кража произошла за пределами страны, то этот срок может быть увеличен.

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ?

В качестве профилактики незаконного списания денег можно привести следующие методы:

1. Следите за транзакциями на своем счете. Например, включите услугу *SMS*-уведомлений для всех Ваших активных карт, чтобы мгновенно получать сообщения о каждой операции. В качестве альтернативы можно выбрать *push*-уведомления в мобильном приложении банка. Они бесплатны и не занимают память телефона, но при этом важно обеспечить постоянное подключение к мобильному Интернету. В противном случае уведомления могут приходить с задержкой, что не позволит вовремя сообщить банку о возможной краже средств.

2. Никогда не делитесь своим *PIN*-кодом, *CVC*/*CVV*-кодом (секретным кодом на обратной стороне карты), сроком действия карты и другой конфиденциальной информацией. Например, если Вам звонят якобы из службы поддержки банка или менеджер утверждает, что Ваша карта заблокирована, не рассказывайте свои данные. Настоящие представители банка никогда не потребуют у Вас секретную информацию, такую как *PIN*-код или *CVC*/*CVV*-код.

3. Не позволяйте продавцам и официантам забирать Вашу карту из поля зрения. Всегда прикрывайте рукой клавиатуру терминала или банкомата, когда вводите свой пароль. Убедитесь, что с камер наблюдения не видно, как Вы вводите *PIN*-код.

4. Посещайте только надежные сайты и избегайте нажатия на ссылки в письмах от незнакомцев. Проверяйте любую информацию о блокировке карты или об отказах в операциях, звоня по номеру горячей линии банка – только по официальным контактам. Номер для срочной связи всегда можно найти на обратной стороне карты и на сайте банка.

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА И ДРУГИХ ВИДОВ МОШЕННИЧЕСТВА?

Фишинг – форма мошеннических операций, направленных на сбор любых персональных данных, владение которыми позволит получить от Вас какую-либо выгоду. К таким данным относятся: серия и номер паспорта, данные банковских и кредитных карт, пароли для входа в социальные сети, электронную почту и др.

На почту приходит сообщение от домена, очень похожего на какую-либо социальную сеть или иной сайт, где хранятся данные пользователя. Само содержание сообщения бывает о том, что аккаунт пытаются взломать, и снизу закрепляется ссылка, перейдя по которой будет происходить фейковое восстановление профиля, а в реальности копирование данных для входа в профиль пользователя.

Один из видов фишинга – метод создания сайтов, схожих по домену и оформлению с настоящими сайтами. Это могут быть фишинг-сайты как социальных сетей, так и электронных магазинов, банков и др.

Фишинг через электронную почту. Мошеннические письма могут приходить на Вашу почту и часто содержат призыв перейти по ссылке, произвести оплату, предоставить личную информацию или открыть вложение. При этом адрес отправителя может быть схож с оригинальным, а в самом сообщении может находиться информация, которая покажется Вам личной.

Голосовой фишинг, или вишинг (vishing). Мошенники звонят Вам по телефону, выдавая себя за сотрудников реальных компаний или известных людей. Они могут использовать автоматических помощников и скрывать свой номер. Их цель – не дать Вам завершить разговор и добиться от Вас определенных действий.

ОТВЕТСТВЕННОСТЬ

За фишинг предусмотрена уголовная ответственность. Фишинг – это один из многочисленных способов совершения мошенничества. Поэтому действия виновных будут квалифицированы либо как мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ), либо как обычное мошенничество (ст. 159 УК РФ), либо как мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). Наказание по всем указанным статьям предусмотрено серьезное – до 10 лет лишения свободы.

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ ФИШИНГОВОЙ АТАКИ?

1. Немедленно прекратите взаимодействие.

Закройте подозрительные электронное письмо, веб-сайт или сообщение. Если Вы уже предоставили личные данные, такие как логи-

ны, пароли или данные банковской карты, переходите к следующим шагам без промедления.

2. Смените пароли.

Немедленно измените пароли для всех аккаунтов, к которым мог быть получен доступ, и включите двухфакторную аутентификацию на тех сервисах, где это возможно, чтобы обеспечить дополнительную защиту Ваших учетных записей.

3. Проверьте свои банковские счета и уведомите банк.

Если мошенники получили доступ к Вашим банковским данным, срочно свяжитесь с Вашим банком, сообщите о компрометации и запросите блокировку карты или учетной записи. Попросите о выпуске новой карты, чтобы предотвратить дальнейшие мошеннические действия.

4. Сканируйте компьютер и телефон.

Проведите проверку Ваших устройств на наличие вредоносного ПО с помощью актуального антивирусного программного обеспечения. Убедитесь, что все программы и операционные системы обновлены до последних версий для защиты от уязвимостей.

5. Сообщите о фишинговой атаке.

Уведомите правоохранительные органы о мошеннических действиях. Проинформируйте компанию, от имени которой была осуществлена фишинговая атака, о произошедшем инциденте.

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ?

Чтобы не попасться на уловки фишеров, рассмотрим методы по противодействию и профилактике фишинговых посягательств на данные пользователя:

1. Проверка *URL*-адресов. Всегда внимательно проверяйте *URL*-ссылки перед тем, как на них кликнуть. Убедитесь, что адрес сайта начинается с «https://» и не содержит ошибок или подозрительных символов.

2. Осторожность с письмами и сообщениями. Будьте внимательны к электронным письмам и сообщениям, особенно если они содержат вложения или ссылки. Даже если письмо пришло со знакомого адреса, то это не гарантирует его безопасность.

3. Двухфакторная аутентификация. Активируйте двухфакторную аутентификацию на всех своих аккаунтах, где это возможно. Это добавит дополнительный уровень защиты, даже если Ваш пароль будет скомпрометирован.

4. Использование надежных сетей. Избегайте доступа к важным аккаунтам, таким как онлайн-банкинг, через открытые или публичные *Wi-Fi* сети. Используйте защищенные соединения.

5. Обновление программного обеспечения. Регулярно обновляйте операционную систему, браузеры и антивирусные программы. Это поможет защитить Вас от известных уязвимостей и угроз, используемых фишерами.

НА МОЙ ПАСПОРТ ВЗЯЛИ КРЕДИТ. ЧТО ДЕЛАТЬ?

В современных условиях, когда общественные отношения становятся все более сложными, незаконное получение кредита на чужие паспортные данные представляет собой серьезную проблему. С развитием технологий и Интернета мошенники становятся все более изобретательными, находя новые способы обмана людей. Важно понимать, что мошенничество может принимать различные формы и каждый из нас может стать его жертвой, если не будет внимательным и осторожным.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация 1. Мошенники взяли кредит в МФО (микрофинансовой организации) по ксерокопии фотографии с лицом и паспортом в руках (которую украли в каршеринге) и по *SMS* на чужой телефон.

Ситуация 2. Предложения приходят через мессенджеры, электронную почту или в виде всплывающих окон. Жертва, перейдя по ссылке, оставляет свои данные на фальшивом сайте, после чего мошенники используют эту информацию для оформления кредита.

Ситуация 3. Мошенники создают иллюзию романтических отношений, что помогает установить доверительные отношения и отвлекает от реальных мошеннических действий.

Ситуация 4. Мошенники используют игры и мобильные приложения, социальные сети для манипуляций и вхождения в близкий круг общения.

КОММЕНТАРИЙ

Зачастую злоумышленники для получения персональных данных (включая паспортные данные) используют методы социальной инженерии. *Социальная инженерия* опасна тем, что позволяет манипулировать людьми с целью получения конфиденциальной информации или доступа к защищенным системам. Преступники используют доверие, страх, жадность или любопытство, чтобы заставить человека добровольно раскрыть свои данные или выполнить определенные действия. Основная цель социальной инженерии – получить доступ к системам или данным без необходимости преодолевать сложные технические барьеры.

Вот некоторые приемы социальной инженерии, которые используют мошенники:

1. Мошенники выдают себя за представителей известных компаний, сотрудников специальных служб или организаций (в том числе

банков, поликлиник, Социального фонда России, МВД России, ФСБ России и т.п.), чтобы обманом заставить людей предоставить информацию или совершить определенные действия.

2. Отправка сообщений или электронных писем с вредоносными вложениями или ссылками, а также с просьбой предоставить конфиденциальную информацию, такую как данные кредитной карты или пароли.

3. Мошенники требуют деньги или личные данные под угрозой причинения вреда или раскрытия личной информации.

4. Мошенники создают фальшивые благотворительные организации для сбора пожертвований, просят указать свои персональные данные.

5. Мошенники используют сайты знакомств и социальные сети для установления доверительных отношений с целью обмана.

6. Мошенники предлагают работу с обещанием высокой зарплаты, но просят внести плату за оформление документов или другие подобные причины.

7. Мошенники используют технологию «дипфейк» для создания поддельных видео или аудио, которые выглядят реалистично и вызывают доверие у жертв.

ОТВЕТСТВЕННОСТЬ

Действуют различные меры ответственности в сфере кредитования, включая уголовную и административную. Ключевыми критериями для различения этих видов ответственности являются размер причиненного ущерба и статус лица, получившего кредит незаконным путем.

Административная ответственность предусмотрена ст. 14.11 КоАП РФ «Незаконное получение кредита или займа».

Уголовная ответственность регулируется ст. 159.1, 176 УК РФ.

Использование чужих персональных данных для получения кредита незаконным способом можно квалифицировать как мошенничество. Ответственность за мошенничество в сфере кредитования регулируется ст. 159.1 УК РФ.

К сожалению, каждый может стать жертвой такого мошенничества, но особенно **уязвимы активные пользователи Интернета**, чьи данные могут быть украдены с различных онлайн-ресурсов, а также **те, кто недавно потерял паспорт**.

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ ТАКОГО ВИДА МОШЕННИЧЕСТВА, КАК ПОЛУЧЕНИЕ КРЕДИТА НА ВАШИ ПАСПОРТНЫЕ ДАННЫЕ?

1. Если Вы подозреваете, что мошенники оформили кредит на Ваше имя, важно первым делом обращаться не в кредитные организации,

так как они редко признают свою вину. В первую очередь необходимо обратиться в полицию и подать иск в суд.

2. Чтобы выяснить, есть ли на Вас кредиты от мошенников, нужно обратиться в бюро кредитных историй. Для этого можно выполнить следующие шаги:

• отправьте запрос в Центральный каталог кредитных историй через «Госуслуги» или на сайте Центробанка;

• запросите данные о действующих кредитах в бюро кредитных историй. Два раза в год отчет можно получить бесплатно.

3. Если обнаружите незнакомый кредит, обратитесь в полицию и подайте заявление в кредитную организацию, выдавшую заем.

4. Если у Вас есть подозрения, что злоумышленники получили доступ к Вашему аккаунту на «Госуслугах», необходимо незамедлительно:

• заблокировать все свои банковские счета и карты. Сделать это можно через интернет-банк, мобильное приложение Вашей кредитной организации или позвонив на бесплатный номер горячей линии, указанный на обратной стороне карты;

• попробовать восстановить доступ к своему аккаунту через многофункциональный центр (МФЦ).

5. Если мошенники взломали Ваш аккаунт на «Госуслугах» и оформили кредит, Вам следует срочно:

• связаться с кредитной организацией, выдавшей заем, и уведомить их о том, что заявку подали мошенники;

• запросить копии документов, которые были предоставлены при оформлении кредита;

• потребовать реквизиты банковского счета, на который были переведены средства;

• указанные документы и информацию предоставить сотрудникам полиции.

МИКРОЗАЕМ: КАК ЭТО РАБОТАЕТ И ЧТО НУЖНО ЗНАТЬ О ЗАЙМЕ В МФО?

Что побуждает граждан обращаться в микрофинансовые организации (МФО)? Очевидно, что простота получения денег. Вам не нужны ни поручители, ни пакет разнообразных документов. Нередко речь идет о займе «до зарплаты». Однако при этом нужно просчитывать возможные риски, в том числе связанные с действиями мошенников.

Для этого важно знать, когда целесообразно брать микрозаем, как выбрать микрофинансовую организацию, на что обратить внимание при заключении договора, оценить последствия несвоевременного возврата полученных денежных средств.

КТО ПРЕИМУЩЕСТВЕННО ВЫСТУПАЕТ В КАЧЕСТВЕ ЗАЕМЩИКА?

Очень часто микрозаймы берут молодые люди, которые обычно плохо кредитуются банками, так как не имеют кредитной истории, имеют испорченную кредитную историю либо не способны подтвердить необходимый уровень дохода, в том числе из-за серой заработной платы. Реже среди клиентов микрофинансовых организаций встречаются пенсионеры, которым не хватает пенсии на непредвиденные расходы, например на лечение или помощь детям. Кроме того, отмечаются сезонные всплески, связанные с традициями делать подарки на праздники, например на Новый год, 23 февраля и т.п. Особую категорию образуют «хронические заемщики», которые не способны соотнести уровень своего дохода с постоянно растущими потребностями, готовностью тратить значительные суммы денег на отдых, дорогие товары и т.п.

ОЦЕНИТЕ, СТОИТ ЛИ БРАТЬ МИКРОЗАЕМ

Определите, насколько неотложными являются расходы, которые Вы планируете покрыть с помощью микрозайма. Может ли это подождать до зарплаты и пенсии? ***Не совершайте спонтанных, эмоциональных покупок в долг.***

Если расходы Вы считаете необходимыми, определите, о какой сумме идет речь и какой срок возврата долга для Вас будет комфортным. Если Вам нужна небольшая сумма на короткий срок, Вы можете обратиться в микрофинансовую организацию, хотя сумма займа может достигать 1 млн руб.

Если у Вас есть в запасе время, хорошая кредитная история и Вы можете легко предоставить все нужные документы, обратитесь в банк, кото-

рый выдаст деньги на более длительный срок под процент, который будет заметно меньше, чем при займе в микрофинансовой организации.

НА ЧТО НУЖНО ОБРАТИТЬ ВНИМАНИЕ, ВЫБИРАЯ МФО?

Проверьте статус организации и следующие данные:

• организация должна быть зарегистрирована в установленном законом порядке. Необходимо проверить данные об организации в Едином государственном реестре юридических лиц на сайте Федеральной налоговой службы (https://egrul.nalog.ru/index.html): ОГРН, ИНН, полное и сокращенное наименование, адрес местонахождения МФО;

• организация должна быть внесена в государственный реестр микрофинансовых организаций. Это можно проверить на официальном сайте Банка России (https://cbr.ru/microfinance/registry/);

• организация должна быть членом саморегулируемой организации (узнать об этом можно в офисе компании или на официальном сайте микрофинансовой организации);

• наличие правил предоставления микрозаймов;

• процентные ставки по микрозаймам;

• наличие общих и индивидуальных условий договора (индивидуальные условия договора должны иметь табличную форму).

Если Вы не проверили сведения об организации, то можете оказаться жертвами мошенников, которые маскируются под легальные МФО. Они не соблюдают правил и ограничений, установленных законодательством и нормативными актами Банка России. В этом случае Вас могут обмануть, и закон не сможет Вас защитить. Заемщик, попавший к нелегальным кредиторам, рискует: не получить при заключении договора полную информацию о размере обязательств и обо всех условиях займа (полной стоимости займа); оказаться должным кредитору астрономическую сумму; стать жертвой незаконных методов взыскания долга.

НА ЧТО НУЖНО ОБРАЩАТЬ ВНИМАНИЕ, ЗАКЛЮЧАЯ ДОГОВОР?

Ознакомьтесь с правилами предоставления микрозаймов (размещаются в обязательном порядке в месте, доступном для ознакомления с ними любого заинтересованного лица, и в сети Интернет). Обратите внимание, что МФО не вправе выдавать займы в иностранной валюте.

Прочитайте общие и индивидуальные условия договора (должны быть приведены в табличной форме). Обратите внимание, что индивидуальные условия могут содержать условия о дополнительных услугах, которые увеличивают сумму, подлежащую возврату. От платных дополнительных услуг можно отказаться.

Оцените процентные ставки: хотя микрозаем выдается на короткий срок, учитывайте, что 1–2% в день – это 30–60% в месяц.

Обратите внимание, что **МФО не вправе в одностороннем порядке изменять процентные ставки и порядок их определения** по договорам микрозайма, комиссионное вознаграждение и сроки действия этих договоров.

Проверьте полную стоимость займа (в рамке в правом верхнем углу на первой странице договора). Полная стоимость не может превышать среднерыночное значение больше, чем на треть.

Не торопитесь сразу подписывать договор. У Вас есть пять дней, чтобы обдумать предложение; условия за это время измениться уже не могут. Если позволяет время, обратитесь за консультацией в несколько МФО.

Перед тем как взять микрозаем, спланируйте его погашение. Если есть возможность выбрать удобную Вам дату погашения, выбирайте дату после ожидаемой даты зарплаты, например через 3–4 дня.

Если Вы выплачиваете сразу несколько кредитов или займов, спланируйте платежи по ним в разные части месяца, чтобы распределить долговую нагрузку между авансом и зарплатой.

Не берите микрозаем, если Вы не уверены, что сможете отдать все заемные средства вовремя!

ОСОБЕННОСТИ ПОЛУЧЕНИЯ МИКРОЗАЙМА БЕЗ ПОСЕЩЕНИЯ ОФИСА

Внимательно отнеситесь к заполнению анкеты на сайте, указывая желаемую сумму и сроки погашения займа, а также предоставляя необходимые персональные данные.

Обратите внимание! При предоставлении микрозайма могут использоваться также социальные сети и мессенджеры, например *Telegram*: данная платформа позволяет удалить некоторые сообщения или удалить весь чат сразу у обоих пользователей без возможности восстановления – это делает переписку недоступной для правоохранительных органов.

Ваше согласие на получение займа может подтверждаться электронной подписью или кодом из *SMS*-сообщения после принятия положительного решения МФО о выдаче займа по итогам проверки представленной в анкете-заявлении информации, что может занять всего несколько минут.

Деньги могут быть выданы несколькими способами: наличными, перечислением на банковский счет, на пластиковую карту, на электронный кошелек, переводом через систему денежных переводов.

Способы погашения микрозайма определяет компания. Обычно платить можно банковским переводом, в салонах связи, отделениях любых банков, через терминалы. При этом платеж считается внесен-

ным только после поступления суммы на счет микрофинансовой кредитной организации, поэтому очень важно сохранять чеки и запрашивать у компании подтверждение получения средств.

О ЧЕМ НАДО ПОМНИТЬ, ЕСЛИ ВЫ ВЗЯЛИ МИКРОЗАЕМ?

• **О сроках погашения долга.** Чем быстрее Вы погасите его, тем меньше денег из своего бюджета Вам придется заплатить. Микрофинансовая организация не вправе применять штрафные санкции к заемщику – физическому лицу, за 10 дней предварительно письменно уведомившему МФО о своем намерении досрочно полностью или частично вернуть МФО сумму микрозайма.

Обязательно сохраняйте документы об оплате (чек, квитанцию или приходно-кассовый ордер). Попросите у кредитора справку о том, что Вы погасили заем (часть долга по займу).

• **О размере неустойки за просрочку.** После возникновения просрочки исполнения обязательства заемщика – физического лица по возврату суммы займа и (или) уплате причитающихся процентов МФО по договору потребительского займа, срок возврата потребительского займа по которому не превышает один год, вправе начислять заемщику – физическому лицу неустойку (штрафы, пени) и иные меры ответственности только на не погашенную заемщиком часть суммы основного долга.

Закон защищает заемщика: если Вы взяли микрозаем, общая задолженность по процентам не может превышать сумму займа более чем в три раза. Например, если непогашенная часть основного долга по просроченному договору составляет 5 тыс. руб., взимаемая с заемщика сумма, не считая штрафных санкций, не может быть больше 15 тыс. руб., которые включают сумму просроченной задолженности (5 тыс. руб.) и начисленные проценты – 10 тыс. руб. (5 тыс. руб. х2). Если Вы не погасили микрозаем вовремя, придется заплатить еще и штраф, который не может превышать 20% годовых (если на микрозаем еще идут проценты) или 0,1% в день от суммы просроченной задолженности (если проценты не начисляются). Неустойка (штрафы, пени) может начисляться только на сумму основного долга, но не может начисляться на просроченные проценты.

При этом МФО сможет вновь начать начисление процентов только после частичного погашения задолженности (уплаты причитающихся процентов и (или) основного долга), но будет обязана прекратить начисление процентов, как только они достигнут двукратного размера оставшейся непогашенной суммы основного долга.

Закон защищает Ваши права при принудительном взыскании долга, определяя порядок взаимодействия с Вами. Не допускаются направ-

ленные на возврат просроченной задолженности действия кредитора или представителя кредитора, связанные в том числе с:

1) применением к должнику и (или) иным лицам физической силы либо угрозой ее применения, угрозой убийством или причинения вреда здоровью;

2) уничтожением или повреждением имущества либо угрозой таких уничтожения или повреждения;

3) применением методов, опасных для жизни и здоровья должника и (или) иных лиц;

4) оказанием психологического давления на должника и (или) иных лиц, использованием выражений и совершением иных действий, унижающих честь и достоинство должника и (или) иных лиц;

5) введением должника и (или) иных лиц в заблуждение относительно:

а) правовой природы и размера неисполненного обязательства, причин его неисполнения должником, сроков исполнения обязательства;

б) передачи вопроса о возврате просроченной задолженности на рассмотрение суда, последствий неисполнения обязательства для должника и (или) иных лиц, возможности применения к должнику мер административного и уголовно-процессуального воздействия и уголовного преследования;

в) принадлежности кредитора или представителя кредитора к органам государственной власти и органам местного самоуправления;

6) любым другим неправомерным причинением вреда должнику и иным лицам или злоупотреблением правом.

Помните о возможности передачи права требования по Вашему долгу коллекторам.

Если Ваши права нарушены, помните, что надзор за соблюдением МФО требований законодательства осуществляет Центральный банк РФ (Банк России) – в его структуре создана Служба по защите прав потребителей финансовых услуг и миноритарных акционеров. Кроме того, Ваши права как потребителя финансовых услуг защищает Роспотребнадзор. Если взыскание осуществляет профессиональный взыскатель, реестр которых есть на сайте ФССП России, или коллектор, не включенный в реестр (нелегальный коллектор), то обращаться нужно в ФССП России.

ПОМНИТЕ О ТОМ, ЧТО ВЫ МОЖЕТЕ СТОЛКНУТЬСЯ С МОШЕННИЧЕСКИМИ СХЕМАМИ

Какими они могут быть?

1. **Ложные обещания низких процентов** при фактическом навязывании скрытых комиссий, установлении дополнительных платежей и других условий, ставящих должника в тяжелое положение (это могут

быть навязывание договора страхования, установление платы за обслуживание счета и т.д.).

Что предпринять? Всегда внимательно изучайте договор, даже если сумма займа кажется незначительной.

2. **Автоматическое продление займа**, если заемщик не уведомил организацию о своем намерении погасить задолженность вовремя. Из-за этого сумма долга увеличивается и начисляются дополнительные проценты.

Что предпринять? Настаивайте на исключении из договора условия об автоматическом продлении срока займа. Если Вам в этом отказали, вообще не заключайте такой договор.

3. **Подделка документов или незаконное использование персональных данных заемщика**, в том числе путем взлома личного кабинета «Госуслуг» посредством направления гражданину сообщения с фишинговой ссылкой (к примеру, это могут быть файл, картинка, аудиодорожка), переход по которой открывает мошеннику доступ в личные кабинеты банковских приложений, в аккаунты мессенджеров и т.д.

Что предпринять? Никогда не предоставляйте незнакомым людям или организациям свои личные данные, такие как номер кредитной карты, пароли или идентификационные номера. Внимательнее относитесь к личной кибербезопасности: не переходите по подозрительным ссылкам, не открывайте чаты с неизвестными людьми, не вступайте с ними в диалог. Не доверяйте телефонным переговорам: если речь идет о денежных переводах, обратитесь в офис банка и обсудите это в очном формате. Установите двухфакторную аутентификацию во всех приложениях, где есть Ваши личные данные. Создавайте сложные пароли и меняйте их регулярно. Используйте разные пароли для разных учетных записей. Не публикуйте слишком много личной информации в социальных сетях, так как это может быть использовано мошенниками.

КАК НЕ ДОПУСТИТЬ ВЗЫСКАНИЯ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ ВАШЕГО ВЕДОМА?

1. Периодически отслеживайте, не было ли в отношении Вас возбуждено исполнительное производство. Проверить это можно на сайте «Госуслуг».

2. С 1 марта 2025 г. граждане могут установить в своей кредитной истории самозапрет на заключение с ними банками и микрофинансовыми организациями договоров потребительского кредита (займа). Сделать это можно будет на «Госуслугах», а с 1 сентября 2025 г. – и в МФЦ.

3. Если Вы сомневаетесь в каких-либо предложении или ситуации, не стесняйтесь обратиться за советом к специалистам.

ЧТО ДЕЛАТЬ, ЕСЛИ ДЕНЬГИ УЖЕ ВЗЫСКАЛИ?

1. Выяснить, куда ушли денежные средства. Для этого нужно написать обращение в банк с просьбой о представлении выписки по операции по счету.

2. Если деньги были взысканы по судебному приказу, в течение 10 дней Вы можете обратиться в суд и отменить судебный приказ. После его отмены нужно обратиться в суд с поворотом в исполнении судебного решения. Далее необходимо обратиться к судебному приставу-исполнителю с просьбой о возврате денежных средств на Ваш счет.

3. Вы можете предъявить иск о неосновательном обогащении к лицу, на счет которого были перечислены денежные средства.

ЧТО ДЕЛАТЬ, ЕСЛИ ВАШИ ПРАВА НАРУШИЛИ?

1. **Обращение в полицию.**

Если Вы стали жертвой мошенников, необходимо обратиться в полицию. Например, если без Вашего ведома на Вас оформили микрозаем, украли деньги с Вашего счета или совершили по отношению к Вам иные преступные действия. Также обращение в полицию актуально, если коллекторы угрожают нанесением вреда Вам, Вашим близким или Вашему имуществу.

Обратиться следует в территориальный отдел полиции. Его выбор зависит от адреса, по которому зарегистрирована МФО.

Заявление о преступлении рассматривается в течение 10 дней. После этого выносится решение о возбуждении уголовного дела либо об отказе. Если Вам отказали и Вы с этим не согласны, то решение можно обжаловать, обратившись в прокуратуру.

2. **Претензия и суд.**

Если по отношению к Вам были совершены действия, пусть и не являющиеся преступлением, но все же нарушающие Ваши права, Вы можете обратиться в МФО с досудебной претензией. В ней необходимо указать свои требования. Если организация с Вами не согласится и откажет Вам, Вы можете обратиться в суд с исковым заявлением.

3. **Защита персональных данных.**

Если Вы регулярно получаете спам-звонки или рассылку от МФО, Вы имеете право предъявить данной организации заявление о том, что Вы отзываете свое согласие на обработку персональных данных. Пишется такое заявление в свободной форме. Если же МФО не будет исполнять его, Вам следует подать на нее жалобу в Роскомнадзор.

КОЛЛЕКТОРЫ ИЛИ ПРИСТАВЫ ДЕЙСТВУЮТ НЕЗАКОННО

Если Вас днем и ночью донимают коллекторы, Вы можете пожаловаться на них в Федеральную службу судебных приставов (ФССП России). Когда взыскатели звонят должникам после 22:00, без разрешения общаются с их родственниками, пытаются унижать и запугивать собеседников, они нарушают Закон о коллекторской деятельности и должны за это отвечать.

Когда Ваши права нарушают судебные приставы, такие ситуации также разбирают в ФССП России. Например, туда можно жаловаться, если пристав незаконно присвоил деньги и отказывается их возвращать. Проще всего подавать заявления в ФССП России через интернет-приемную ведомства.

КАК БЫСТРО ДОЛЖЕН ПРИЙТИ ОТВЕТ ОТ ГОСУДАРСТВЕННОГО ВЕДОМСТВА?

У всех госорганов стандартные сроки рассмотрения обращений – 30 дней со дня регистрации в ведомстве. Если для ответа нужны какие-то дополнительные документы от человека или финансовой организации, срок может увеличиться до 60 дней. Но на некоторые типовые вопросы ответы нередко приходят в течение нескольких часов или даже минут.

Если Вы все же ошиблись и направили обращение не в то ведомство, Вашу жалобу перенаправят в нужную инстанцию, но это увеличит сроки – на пересылку у госоргана есть семь дней со дня регистрации обращения.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация. Видел рекламу компаний, которые обещают решить мою проблему. Можно ли им доверять?

В Интернете много сайтов, на которых предлагают юридическую помощь клиентам финансовых организаций. Обычно там готовы проконсультировать Вас, составить и отправить обращение в госорганы от Вашего имени. При желании можно воспользоваться их услугами. Но крайне важно убедиться, что выбранные специалисты действительно могут оказывать подобную помощь. Заранее наведите о них справки, поищите отзывы в Интернете. Уточните тарифы на их услуги – возможно, траты окажутся неоправданными для Вашей ситуации. К тому же написать заявление в госведомство бывает не так уж сложно, как кажется.

ВАЖНО! Ветераны, инвалиды I и II групп, семьи с доходом ниже прожиточного минимума и другие льготные категории граждан имеют право обратиться в центры бесплатной юридической помощи – их адреса можно посмотреть на сайте Министерства юстиции РФ.

Проверять специалистов нужно обязательно, так как велика вероятность наткнуться на нелегалов. Псевдоюристы часто обещают уменьшить или даже списать долги, вернуть деньги, которые Вы вложили в финансовую пирамиду или потеряли на фондовом рынке. Они часто маскируют свои страницы под сайты государственных органов, гарантируют 100%-ный результат и завлекают эффектной рекламой, но на самом деле просто стараются заполучить доступ к Вашим персональным сведениям или банковским данным, чтобы затем обчистить Ваши счета или оформить на Вас кредиты.

С одной стороны, приставам предоставили довольно широкие полномочия, и не всегда должник понимает, какие действия можно считать законными, а какие – неправомерными. К тому же нередко приставы сами превышают данные полномочия. С другой стороны, основная часть поступающих жалоб касается бездействия приставов.

Бездействие – судебным приставом-исполнителем не принимаются меры по взысканию, выносится постановление о прекращении или приостановлении исполнительного производства без законных оснований. Например, пристав оканчивает исполнительное производство и устанавливает, что у должника нет возможностей для оплаты задолженности, не обратившись в налоговые или регистрирующие органы.

Противоправные действия – судебным приставом-исполнителем превышаются полномочия или незаконно возбуждается исполнительное производство (например, наложение незаконного ареста на недвижимое, движимое имущество должника, банковские счета с удержанием заработной платы, пенсий, пособий в размере 100%).

ИНЫЕ НЕЗАКОННЫЕ ДЕЙСТВИЯ ПРИСТАВОВ

1. Наложение ареста на банковские счета должника до истечения срока для добровольного погашения задолженности.

Проблемой является то, что данный срок (пять дней) сам по себе является довольно коротким. При этом пять дней отсчитываются со дня получения должником постановления о возбуждении исполнительного производства или с момента доставки извещения о размещении сведений о возбуждении исполнительного производства в «Банке данных исполнительных производств», а соответственно его легко пропустить.

2. Действия приставов не соответствуют размеру долга.

В течение срока для добровольного исполнения должником требований пристав вправе наложить арест на имущество. Такая мера подразумевает запрет распоряжаться имуществом (например, нельзя будет квартиру продать, обменять, подарить жене и т.п.), а при необходимости – ограничение права пользования имуществом (например, нельзя будет кого-то в квартиру вселить) или его изъятие. Чтобы узнать об этом подробнее, ознакомьтесь со ст. 80 Закона об исполнительном производстве.

Подобные действия пристава должны соответствовать размеру взыскиваемой задолженности. Допустим, человек должен 500 тыс. руб., а стоимость его квартиры – 15 млн руб. Пристав выносит постановление о запрете распоряжаться жилым помещением. Такое постановление можно оспорить, если должник готов постепенно выплачивать сумму задолженности.

3. Приставы списывают все доходы и денежные средства, хранящиеся на банковских счетах должника.

Неправомерным будет снятие всех денежных средств со счета должника. Это противоречит ст. 99 Закона об исполнительном производстве. Так, удержать могут не более 50% доходов. В некоторых случаях, например при наличии долга по алиментам, удержание не может превышать 70%. Средства будут списывать ежемесячно до полного погашения долга. Но эти ограничения не применяются, если средства списываются со счета, куда поступает зарплата. В таком случае ограничения распространяются только на последний платеж.

Кроме того, не на все доходы должника может быть обращено взыскание. Неприкосновенные доходы перечислены в ст. 101 Закона об исполнительном производстве.

4. Приставы списывают все денежные средства, не оставляя средств для прожиточного минимума.

С 2022 г. у должников появилась возможность защитить сумму прожиточного минимума от ежемесячного списания. Для этого нужно было подать заявление в подразделение судебных приставов при личном визите или направить его по почте. Однако порой даже после подачи должником нескольких заявлений средства списывались в прежнем объеме.

Сохранить прожиточный минимум не получится только в нескольких случаях: если образовался долг по алиментам, если должник не возместил вред здоровью или причиненный преступлением ущерб, если он не компенсировал смерть кормильца (ч. 3.1 ст. 99 Закона об исполнительном производстве).

Отдельной темой обращения в интернет-приемной на официальном сайте ФССП России является тема **«Я двойник!»**. Это связано

с тем, что довольно распространенным было взыскание денег с граждан, у которых фамилия, имя, отчество и дата рождения полностью совпадали с данными должников. При этом в отношении них не было судебных дел и возбужденных исполнительных производств.

Получив исполнительный документ о взыскании денежных средств, судебный пристав направляет запросы в банки. Автоматизированная система банка выдает данные клиентов по ФИО и дате рождения, соответственно ввиду того, что место рождения и паспортные данные в ответе банков не отражаются, пристав, недостаточно внимательно проведя идентификацию должника, списывает денежные средства с постороннего лица, не имеющего отношения к задолженности.

Теперь в исполнительном документе отражаются дополнительные идентификаторы должника: СНИЛС, ИНН, ОГРН, серия и номер паспорта.

Наиболее часто встречающейся проблемой для взыскателей является **бездействие судебных приставов**.

Решением проблемы является правильный и последовательный порядок действий взыскателя: обжалование бездействия судебного пристава-исполнителя в порядке подчиненности или в судебном порядке. Для начала необходимо обратиться к старшему судебному приставу с жалобой на бездействие судебного пристава-исполнителя, не возбудившего исполнительное производство. Обычно начальник даже не отвечает на заявление взыскателя, однако отметка о получении заявления (жалобы) судебными приставами будет служить доказательством бездействия при дальнейшем обращении взыскателя в Главное управление ФССП России в субъекте и в суд с административным исковым заявлением.

МОШЕННИКИ НА МАРКЕТПЛЕЙСАХ: КАК НЕ ПОПАСТЬ В ЛОВУШКУ?

Маркетплейсы уже довольно основательно вошли в жизнь большинства граждан, так как разнообразие предлагаемых товаров, удобство их выбора, экономия времени ценятся практически всеми потребителями.

Пользоваться маркетплейсами становится быстро, просто и удобно, потому что:

• маркетплейс – посредник между продавцами: площадка собирает товары разных продавцов в один заказ – так получать покупки удобнее;

• маркетплейс предлагает оплату бонусами или Сплитом, разбивая стоимость заказа на части;

• маркетплейс предлагает широкий ассортимент товаров из разных категорий – все, что нужно, можно купить разом;

• маркетплейс увеличивает лояльность пользователей с помощью акций, специальных предложений и кешбэка.

Тем не менее, несмотря на очевидные преимущества в работе маркетплейсов, существуют **риски, связанные с покупками на маркетплейсах и наиболее распространенными мошенническими схемами:**

1. **Недобросовестность продавца.**

Необходимо знать, что недобросовестных продавцов предостаточно, поэтому необходимо проверить рейтинг продавца и отзывы на сайте.

Нельзя переходить по сторонним ссылкам, которые присылает продавец в личный чат.

Торговля должна вестись строго на базе маркетплейса.

Товар должен находится на официальном складе и выдаваться в пунктах выдачи.

Помните, что за безопасность сделок, совершенных вне официального сайта или приложения, маркетплейс ответственности не несет.

2. **Фишинг – использование сайтов-двойников.**

Бывают ситуации, когда люди открывают сайт маркетплейса и сразу же поверх него всплывает другой, происходит переадресация на точно такой же на первый взгляд сайт. В некоторых случаях мошеннический сайт может выглядеть как диалоговое окно службы поддержки маркетплейса.

Пользователя просят ввести логин и пароль снова, хотя до этого он и так регистрировался. После этого его данные «сливаются» конкурентам или мошенникам для использования в различных схемах.

3. **Рассылка так называемых выгодных, или горячих, предложений**, где предлагаются огромные скидки, вакантные рабочие места и т.д. от имени маркетплейса по почте, *SMS* в мессенджерах либо же всплывающим окном.

Переход по таким ссылкам, введение паролей, промо-кодов чреваты утечкой персональных и банковских данных пользователя и его денежных средств с привязанной банковской карты.

Например, Вы получаете рассылку от маркетплейса о распродаже в «черную пятницу», в ней содержится ссылка на нужный товар, который давно искали и вбивали в поиске в Интернете.

По ссылке из письма перешли на страницу с товаром, положили товар в корзину и собираетесь оплатить. Однако открывается форма, где нужно вбить данные карты. Вы удивляетесь, ведь карта уже привязана к личному кабинету, но решаете, что просто сбились настройки. Вводите реквизиты, код подтверждения – деньги списались.

Однако в приложении или на сайте маркетплейса покупка не отображается, техподдержка отвечает, что заказа не было. По чеку онлайн-банка можно выяснить, что оплата произведена не маркетплейсу, а мошенникам с похожим названием.

4. **Взлом аккаунта.**

Мошенники путем направления специальных ссылок могут взломать аккаунт электронной почты и войти через нее в аккаунт на маркетплейсе, сменив пароль потребителя.

Мошенники могут сделать множество фейковых заказов на небольшие суммы (до 1 тыс. руб.), чтобы не требовался код подтверждения от банка, и оплатить их через аккаунт потребителя.

5. **Кража денег с карты маркетплейса.**

Маркетплейсы нередко предлагают дополнительные скидки при оплате картой партнерского банка.

В некоторых случаях мошенники предлагают оплатить доставку через такую карту, причем запрашивают код подтверждения либо в чате техподдержки, либо в чате с продавцом. Таким образом, они получают доступ к номеру телефона (логину для авторизации на маркетплейсе) и коду для авторизации в личном кабинете.

Одновременно мошенники запрашивают данные для онлайн-банка, и потребитель может решить, что направляет код для банка-партнера маркетплейса, а на самом деле предоставляет код от интернет-банкинга привязанной карты.

6. **Быстрый и легкий заработок на маркетплейсе.**

Нередко в Интернете можно увидеть рекламу и предложения быстрого и легкого заработка на маркетплейсе: регистрировать заказы и отменять их, комментировать отдельные позиции, якобы это повы-

шает рейтинги выбранных продавцов и самой торговой площадки, и маркетплейс готов оплачивать такие услуги.

Мошенники предлагают зарегистрироваться на маркетплейсе по специальной ссылке, внести депозит (он должен увеличить прибыль работника) и увеличивать последний, чтобы получить больший процент от выполняемой работы.

Нужно понимать, что мошенники будут убеждать человека, что работа настоящая, могут поначалу даже перечислить ему небольшую «зарплату». Но как только жертва пополнит «депозит» на крупную сумму, эти деньги уже не вернутся.

ЧТО ДЕЛАТЬ В СЛОЖИВШЕЙСЯ СИТУАЦИИ? РЕКОМЕНДАЦИИ ДЛЯ ЗАЩИТЫ НА МАРКЕТПЛЕЙСЕ

1. Обратитесь в службу поддержки маркетплейса. Опишите характер своей проблемы, по возможности сделайте скриншоты с экрана компьютера или сотового телефона, в которых отражается информация о Вашей переписке с мошенником, страницы с Вашим заказом.

2. Если заказы оформлены от Вашего имени на настоящем маркетплейсе, можно их просто отменить. Если Вы вообще не делали заказ, напишите в поддержку и подробно расскажите, что произошло. Требуйте проверить поставщика и полностью вернуть оплату.

3. Внимательно проверяйте реквизиты для перевода денежных средств.

4. Не переходите по дополнительным ссылкам на товар, проверьте его в приложении или на сайте маркетплейса и только после этого производите оплату.

5. Не вводите в дополнительные формы реквизиты банковских карт, производите оплату через приложение или сайт маркетплейса.

6. Используйте для электронной почты сложный пароль. Лучше брать комбинации не меньше восьми символов – с цифрами, прописными и строчными буквами. Для каждого аккаунта на сайтах магазинов, банков и других организаций создавайте свой пароль.

7. Заведите отдельную карту для интернет-покупок и каждый раз переводите на нее нужную сумму прямо перед оплатой. Или вообще не сохранять данные карты для оплаты в разных сервисах и магазинах – просто вводите их перед каждой покупкой.

8. Если с карты списали деньги без Вашего согласия, немедленно свяжитесь со своим банком и просите ее заблокировать. На всякий случай смените пароль от интернет-банка, если он у Вас есть.

9. Когда в Ваш аккаунт на маркетплейсе вошли посторонние, поищите в настройках личного кабинета опцию «Завершить сессии на подключенных устройствах» или «Выйти на всех устройствах» и вос-

пользуйтесь ею. Как можно скорее сообщите о происшествии в техподдержку маркетплейса. Если не получится отключить мошенников самостоятельно, это сделают сотрудники сервиса.

10. Попросите маркетплейс помочь Вам вернуть деньги. Возможно, он сам свяжется с продавцами-мошенниками и убедит их добровольно компенсировать Вам украденное или сообщит Вам их данные, чтобы Вы обратились в полицию и сразу приложили к заявлению все известные реквизиты преступников.

11. Когда выбираете товары, обращайте внимание, давно ли продавец работает на этой площадке, высок ли его рейтинг, какие отзывы от покупателей. Лучше никогда не переходить на общение с продавцами в мессенджерах и соцсетях. Но если маркетплейс предлагает Вам связаться насчет доставки с партнерами напрямую, ни в коем случае не называйте им никакие коды и пароли.

12. Всегда внимательно читайте, что за коды Вам приходят и от кого. Получив код, который не запрашивали, не сообщайте его никому ни под каким предлогом.

Если у Вас есть личный кабинет в этой организации, как можно скорее зайдите в него через сайт или приложение, прекратите все сеансы на сторонних устройствах и смените пароль.

Не получится сделать это самостоятельно – обратитесь в техподдержку организации. Контакты берите только на официальном сайте компании.

13. На некоторых интернет-площадках есть возможность оплачивать товар не заранее, а при получении – используйте эту опцию.

14. Не верьте обещаниям высокого заработка за неквалифицированный труд без опыта работы. Обращайте внимание на список обязанностей: расплывчатые формулировки – явный признак обмана.

15. Если потенциальный работодатель выходит с Вами на связь в мессенджере или через соцсети, уточните, есть ли информация о вакансии на сайте компании или популярных ресурсах для поиска работы. Впрочем, иногда даже на известных рекрутинговых сайтах попадаются ненастоящие объявления, так что не теряйте бдительности на собеседованиях.

16. Не связывайтесь с людьми и компаниями, которые просят внести плату за регистрацию в их сервисах, перечислить «страховой взнос» или купить что-то, чтобы начать работать. Почти наверняка это мошенники.

17. Вы можете подать заявление в полицию, ведь кража и мошенничество являются уголовными преступлениями. Сделать это можно как непосредственно в отделении полиции, так и направив жалобу дистанционно – через портал «Госуслуги». Но в любом случае Вы долж-

ны быть готовы к очной встрече с сотрудником правоохранительного органа, которому необходимо все подробно изложить.

18. Отношения между продавцами и покупателями регулируются Законом о защите прав потребителей, поэтому Вы можете подать жалобу в Роспотребнадзор. Сделать это можно на его официальном сайте.

Но такой способ защиты Ваших прав может сработать только в том случае, если Вам пришлось столкнуться с недобросовестным продавцом. Если же таким продавцом оказался мошенник, намеренно вводящий всех без исключения продавцов в заблуждение, то, вероятнее всего, Роспотребнадзор не в силах будет Вам помочь.

19. В случае, если все перечисленные способы не помогли, но Вы обладаете достоверной информацией о месте нахождения (юридическом адресе) продавца, обратитесь в суд с исковым заявлением. В нем Вы можете изложить суть нарушенного права, приложить доказательства и потребовать возмещения нанесенных убытков.

БЛАГОТВОРИТЕЛЬНОСТЬ: ПОДВОДНЫЕ КАМНИ

Сталкивались ли Вы когда-либо с объявлениями о благотворительности, размещенными в сети Интернет? А знаете ли Вы, что бóльшая часть таких «новостей» о сборе денежных средств – «обманка»? В современном мире благотворительность становится все более популярной, но вместе с тем растет и количество мошенников, использующих добрые намерения людей в своих целях.

Среди распространенных схем обмана в сфере благотворительности – перевод денег на личные карты или использование подставных аккаунтов нуждающихся людей или организаций, сбор пожертвований в общественных местах с высокой проходимостью, нецелевое использование полученных средств и многое другое. Злоумышленники воздействуют на эмоции, пытаются вызвать жалость и взывают к чувству справедливости, манипулируют сжатыми сроками и не дают возможности принять взвешенное решение.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация. «Саше срочно требуются деньги на операцию», – прочитала пост в одной из социальных сетей Ирина. С фотографии на нее смотрел белокурый малыш с глазами, полными слез. Желание людей поддержать нуждающихся, готовность оказать добровольную и безвозмездную помощь им – это то, чем часто пользуются мошенники.

ОТВЕТСТВЕННОСТЬ

Ущерб, причиненный в результате совершения данного деяния, соответствует составу преступления, предусмотренного ст. 159 УК РФ «Мошенничество», т.е. хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Однако ответственность может наступить не только для мошенников, но и для самих потерпевших, если в результате перевода денег оказывается, что они поступили на счета террористических или экстремистских организаций. В таком случае речь идет о ст. 205.1 УК РФ «Содействие террористической деятельности» и ст. 282.3 УК РФ «Финансирование экстремистской деятельности».

ЧТО ДЕЛАТЬ, ЕСЛИ НАТКНУЛИСЬ НА МОШЕННИКОВ?

Если Вы столкнулись с мошеннической схемой, сообщите об этом в правоохранительные органы и на специализированные сайты, чтобы предупредить других.

КАК ИЗБЕЖАТЬ ПОДОБНЫХ СИТУАЦИЙ?

Если Вы не хотите стать жертвой мошенничества при перечислении денежных средств на благотворительность:

1. Проверяйте организации. Перед тем как сделать пожертвование, убедитесь в легитимности благотворительной организации. Изучите ее сайт, проверьте наличие лицензий и регистрационных документов. Можно обратиться к независимым рейтингам и обзорам.

2. Изучайте отзывы. Читайте отзывы о благотворительных проектах на независимых платформах. Обратите внимание на мнения людей, которые уже сделали пожертвования.

3. Не доверяйте незнакомцам. Будьте осторожны с просьбами о помощи от незнакомых людей в социальных сетях или мессенджерах. Мошенники часто используют эмоциональные истории, чтобы вызвать жалость.

4. Проверяйте ссылки. Не переходите по подозрительным ссылкам. Мошенники могут использовать поддельные сайты, похожие на настоящие. Всегда вводите адрес сайта вручную.

5. Избегайте спама. Если Вы получили электронное письмо или сообщение с просьбой о помощи, проверьте отправителя. Не отвечайте на сомнительные сообщения и не отправляйте деньги без предварительной проверки.

6. Используйте безопасные методы оплаты. При пожертвовании выбирайте проверенные методы оплаты, такие как кредитные карты или специализированные платформы для сбора средств.

7. Будьте осторожны с личной информацией. Никогда не раскрывайте свои личные данные, такие как номер телефона или адрес, если это не требуется для оформления пожертвования.

ИНТЕРНЕТ-ЗНАКОМЫЕ: КТО НАСТОЯЩИЙ?

В современном информационном и цифровом обществе появились новые способы взаимодействия, которые, с одной точки зрения, предоставляют возможности для общения, а с другой – «открывают двери» для мошенничества.

Такие ситуации, которые возникают из-за «воздушных замков» и «земных обещаний», могут стать причиной серьезных финансовых и психологических последствий.

Не забывайте: новый знакомый не всегда подарок судьбы!

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация. «Привет, это Владимир. Помнишь, мы с тобой познакомились неделю назад в чате? – написал Александру в мессенджере его новый знакомый. – Помнишь, я рассказывал, что занимаюсь криптовалютой? У меня сейчас хорошая возможность для инвестиций, но моя банковская карта заблокирована. Не мог бы ты помочь мне с небольшой суммой? Обещаю все вернуть с процентами уже завтра!». Не задумываясь, Александр сразу перечислил Владимиру 5 тыс. руб. на его текущий банковский счет. Через день, когда Александр решил перейти на страницу Владимира, оказалось, что его аккаунт был удален, а все переведенные им денежные средства исчезли без следа.

Данная ситуация является примером мошенничества, которое часто называют «кэтфишинг» («*catfishing*»), – это разновидность интернет-мошенничества (кибермошенничества), которая представляет собой создание и использование ненастоящей личности в социальных сетях, мессенджерах или на других онлайн-платформах (приложениях). Основная цель кэтфишеров (*catfish*) – получение денежных средств или доступа к персональным данным.

ОТВЕТСТВЕННОСТЬ

Ущерб, причиненный в результате совершения данного деяния, соответствует составу преступления, предусмотренного ст. 159 УК РФ «Мошенничество», т.е. хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Однако ответственность может наступить не только для мошенников, но и для самих потерпевших, если в результате перевода денег оказывается, что они поступили на счета террористических или экстремистских организаций. В таком случае речь идет о ст. 205.1 УК

РФ «Содействие террористической деятельности» и ст. 282.3 УК РФ «Финансирование экстремистской деятельности». Даже если человек действовал по указанию мошенников, переводя деньги «по ошибке», то правоохранительные органы могут рассматривать его действия как участие в незаконных финансовых операциях, но при условии прямого умысла: переводивший деньги должен осознавать, что они пойдут террористам; должны быть доказательства, которые могут подтвердить причастность человека.

ЧТО ДЕЛАТЬ, ЕСЛИ ВАС ОБМАНУЛИ ИЛИ ВВЕЛИ В ЗАБЛУЖДЕНИЕ?

1. Обратитесь в правоохранительные органы с заявлением о возбуждении уголовного дела с приложением всех имеющихся у Вас данных (например, переписка, чеки о перечислении денежных средств).

2. Перезвоните в банк или другую кредитную организацию, чтобы остановить перечисление денежных средств и заблокировать банковский счет.

3. Обратитесь за консультацией в юридические организации.

КАК ПРЕДОТВРАТИТЬ ПОВТОРЕНИЕ ТАКИХ СИТУАЦИЙ?

1. Проверьте личную информацию об онлайн-собеседнике. Поищите аккаунт пользователя в других социальных сетях, мессенджерах или на других онлайн-платформах (приложениях). «Пустой» профиль в социальных сетях, мессенджерах или на других онлайн-платформах (приложениях), минимальное количество или отсутствие друзей, подписчиков, публикаций, лайков (отметок «нравится»), комментариев и т.д. – все это может быть связано с тем, что аккаунт пользователя был создан недавно. Также это может быть «закрытый» профиль: персональные данные будут доступны только после подтверждения запроса на добавление в друзья или подписки. Применяйте также обратный поиск изображений (например, через сервисы «поиск по изображению» («*search by image*») в *Google* или Яндекс.Картинках и т.д.), чтобы подтвердить подлинность фотографий.

2. Не разглашайте онлайн-собеседнику всю личную информацию: ФИО, дату рождения, номер мобильного или домашнего телефона, адрес электронной почты, место проживания, место работы или учебы, номер банковской карты, *PIN*-код и другие сведения, которые могут использоваться для идентификации личности, чтобы предотвратить возможное злоупотребление ими.

3. Не отправляйте деньги по просьбе новых знакомых, если это выглядит подозрительным.

4. Не переводите деньги, если счета связаны с подозрительными регионами.

5. Настройте параметры конфиденциальности. Ограничьте доступ к персональным данным на всех своих аккаунтах.

Чтобы распознать кэтфишинг, необходимо обратить внимание на следующие признаки:

1. «Слишком хорошо, чтобы быть правдой»: для этого долго создается ложная эмоциональная связь, которая полностью соответствует ожиданиям и желаниям (например, повышенный интерес к жизни, комплименты и т.д.). Данные способы социальной инженерии – склонность к доверию и подтверждение своей точки зрения могут использоваться для манипуляции.

2. Неправдивая или противоречивая личная информация: факты могут быть вымышленными или не соответствующими действительности (например, нестыковки в биографии и т.д.), чтобы создать ложный образ.

3. Отказ от голосовых сообщений, видеосообщений или личных встреч: новый знакомый оправдывается разными причинами (например, техническими проблемами, личными обстоятельствами и т.д.), чтобы не участвовать в «открытом» общении.

4. Возникшая срочная необходимость в финансовой помощи или предоставлении личной информации.

ОСТОРОЖНО – ДИПФЕЙК!

Услышав знакомый голос или увидев на экране телефона видеообращение от близкого человека, мы не задумываемся о том, что современные технологии, которые взяли на вооружение и мошенники, могут легко сделать нас жертвой обмана.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация. «Мама, привет! – услышала она в телефонной трубке. – Я в больнице, мне нужно срочно оплатить лечение. Можно тебя попросить, пожалуйста, отправить 10 тыс. руб. моему другу? Я тебе потом перезвоню и все расскажу!». Женщина, узнав голос дочери, не стала задавать вопросы и сразу же перечислила денежные средства на текущий банковский счет. Позже, позвонив ей, она услышала: «Мама, я не была ни в какой больнице!». Так, выяснилось, что видеозвонок был подделкой.

Данная ситуация является примером мошенничества, которое обычно называют «дипфейк» («*deepfake*»), – это технология, которая представляет собой создание и использование реалистичных, но искусственно сгенерированных искусственным интеллектом (нейросетью) медиаданных (например, видеозаписей, аудиозаписей или фотографий). С ее помощью можно сделать так, будто человек «говорит» или «делает» то, чего на самом деле не было.

ОТВЕТСТВЕННОСТЬ

Ущерб, причиненный в результате совершения этого деяния, соответствует составу преступления, предусмотренного ст. 159 УК РФ «Мошенничество», т.е. хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Уголовная ответственность в отношении лица, достигшего 16-летнего возраста, за причинение вреда на сумму от 2500 руб. наказывается штрафом, обязательными, исправительными, принудительными работами или лишением свободы на срок до двух лет.

ЧТО ДЕЛАТЬ, ЕСЛИ ВАС ОБМАНУЛИ ИЛИ ВВЕЛИ В ЗАБЛУЖДЕНИЕ?

1. Обратитесь в правоохранительные органы с заявлением о возбуждении уголовного дела с приложением всех имеющихся у Вас сведений (например, переписки, скрина экрана, чеков о перечислении денежных средств).

2. Перезвоните в банк или другую кредитную организацию, чтобы остановить перечисление денежных средств и заблокировать банковский счет.

3. Обратитесь за консультацией в юридические организации.

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ УСЛЫШАЛИ ЗНАКОМЫЙ ГОЛОС ИЛИ ПОЛУЧИЛИ ВИДЕООБРАЩЕНИЕ?

1. Чтобы распознать дипфейк, обратите внимание на следующие признаки:

• неестественные движения тела или лица. Они могут быть дергаными, зеркально-симметричными или синхронизированными;

• размытое или искаженное изображение. Оно может быть «плавающим», с размытыми границами, а отдельные зоны лица (например, вокруг рта, глаз, волос и т.д.) выглядят нечеткими или плохо прорисованными, с нарушенными пропорциями или неестественными переходами между текстурами;

• искажения в освещении или тенях на изображении. Блики и отражения могут не соответствовать другим объектам, а переходы между яркими и темными зонами – выглядеть размытыми или резкими;

• неестественные интонации голоса. Они могут быть «роботизированными», монотонными (без эмоций), с необычными паузами, что отличается от естественного «живого» звучания человеческой речи.

2. Проверьте личную информацию. Задайте вопросы о фактах или событиях, которые знаете только Вы и собеседник. Можно заранее выбрать кодовое слово или придумать контрольный вопрос, которые Вы можете озвучить или задать собеседнику, чтобы понять, действительно ли Вы разговариваете именно с ним.

3. Перезвоните собеседнику по мобильному или домашнему номеру телефона, чтобы убедиться, что ему нужна помощь.

4. Примените специальные программы (например, *Microsoft Video Authenticator*, *Deepware* и т.д.), чтобы подтвердить подлинность медиаданных (например, видеозаписей, аудиозаписей или фотографий).

5. Настройте параметры конфиденциальности. Ограничьте доступ к персональным данным на всех своих аккаунтах.

6. Не отвечайте на звонки с незнакомых мобильных или домашних номеров телефона и не перезванивайте на них.

7. Не переходите по прикрепленным к голосовым сообщениям *URL*-ссылкам, пока не удостоверитесь в том, что именно Ваш близкий прислал их. Они могут переадресовывать на фишинговые или вредоносные сайты, которые могут применяться для сбора доступа к персональным данным или повреждения устройства соответственно.

8. Не скачивайте присланные файлы, пока не удостоверитесь в том, что именно данный человек Вам их прислал. Файлы могут содержать вредоносные программы – вирусы (например, скрытый майнинг (майнер) или троянец-стиллер, которые могут применяться для добычи криптовалюты или сбора доступа к персональным данным с помощью устройства соответственно).

ЧТО ТАКОЕ «ИНФОЦЫГАНСТВО» И КАК ОНО ЗАРОЖДАЛОСЬ?

«Инфоцыгане» – это люди, которые продают свои информационные продукты (курсы, гайды, тренинги, марафоны и книги), не имеющие никакой практической ценности. Сами «инфоцыгане» могут позиционировать себя как бизнес-тренеры, коучи, мотиваторы, специалисты по продвижению.

В докладе члена Совета по правам человека при Президенте РФ И.С. Ашманова на заседании Государственной Думы ФС РФ говорится, что «инфоцыгане» сначала «создают образ депрессивности, скуки и нищеты», убеждают «в необходимости реализовывать мечты», а затем дают весьма банальные советы, например «полюбить себя», научиться «быть в ресурсном состоянии».

Возрастной категорией, наиболее склонной к трате денежных средств на онлайн-образование, являются респонденты от 26 до 37 лет; в зависимости от статуса занятости к покупке курсов более склонны люди со средним профессиональным образованием. Наиболее распространенными причинами участия являются получение эмоциональной поддержки, а также необходимость повышения профессиональных компетенций.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация 1. Курсы личностного роста, например «Марафон желаний» Елены Блиновской. Этот марафон представляет собой серию онлайн-занятий и упражнений, направленных на то, чтобы участники смогли «научиться» исполнять свои желания. Основная идея заключается в визуализации своих целей и позитивном мышлении. Подобные проекты могут использовать непроверенные методы, не имея научной основы, и слишком упрощенно подходить к вопросам достижения целей и успеха. Кроме того, за участие в таких марафонах может взиматься значительная плата, что вызывает сомнения относительно их реальной ценности. Это делает «Марафон желаний» примером «инфоцыганства» для некоторых обозревателей и экспертов.

Ситуация 2. Бизнес-курсы, например курсы, основанные Аязом Шабутдиновым, представляют собой тренинги для начинающих предпринимателей, направленные на развитие навыков и компетенций в области бизнеса и личностного роста. Курсы создают впечатление, что благодаря им можно быстро и легко достичь успеха в бизнесе. Это часто приводит к завышенным ожиданиям у участников. Акцент дела-

ется больше на мотивации и личных историях успеха, нежели на практическом обучении и конкретных навыках.

ОТВЕТСТВЕННОСТЬ

Осуществляя предпринимательскую деятельность в сфере оказания услуг, «инфоцыгане» зачастую не являются субъектами предпринимательской деятельности в РФ (не работают через ИП или ООО, без регистрации в налоговой), не указывают свое настоящее имя (используют псевдоним) и фактический адрес, куда можно отправить официальную претензию о возврате денег в случае недовольства качеством их продуктов, а также могут быть юридически оформлены в другой стране.

В практике судопроизводства есть немного случаев, когда «инфоцыган» привлекали к уголовной ответственности по ст. 171 и 159 УК РФ.

ЧТО ДЕЛАТЬ В СЛОЖИВШЕЙСЯ СИТУАЦИИ?

С «инфоцыганами» довольно сложно бороться на уровне закона, так как они чаще всего не являются субъектами предпринимательской деятельности, работают под псевдонимом и не указывают адрес, куда можно в случае чего направить официальную претензию о возврате денег за некачественные услугу или товар. Кроме того, многие «инфоцыгане» физически находятся в других странах, что сильно усложняет процедуру возбуждения уголовного дела. Однако попытаться с ними справиться все же можно.

Есть несколько шагов, которые можно предпринять:

1. Обозначьте свою позицию – четко и внятно расскажите, почему Вам не понравился курс, чем конкретно Вы недовольны и почему хотите вернуть деньги.

2. Найдите таких же пострадавших клиентов и составьте коллективный иск. Кроме того, оставляйте негативные отзывы о лжеспециалистах на всех доступных площадках.

3. Расскажите о Вашей истории в СМИ. Огласка поможет обратить внимание на проблему и сдвинуть дело с мертвой точки. Так Вы подорвете репутацию плохого эксперта.

Например, если обманутые клиенты начинают объединяться в группы и жаловаться на страницу мошенника в соцсетях, то ее могут заблокировать. Иногда мошенники все же выплачивают деньги тем, кто подавал иск. Однако в одиночку довольно трудно добиться, чтобы «инфоцыгане» вернули Вам средства, – они будут всячески уверять Вас, что курс не подошел конкретно Вам либо же что возврат денег не предусмотрен.

КАК ИЗБЕЖАТЬ НЕПРИЯТНОСТЕЙ?

1. Узнайте больше о наставнике. Изучите информацию в открытых источниках, биографию, данные об образовании, наличие экспертных статей в СМИ. Поинтересуйтесь у тех, кто уже проходил обучение, какие результаты это дало. Изучите отзывы не только на сайте самого курса, но и в других источниках.

2. Обращайте внимание на отзывы участников, и, если они содержат фразы в стиле «заплатить какие-то 100 тыс. руб.», «я взяла кредит на три миллиона и была так счастлива», включайте внутренний режим подозрительности – перед Вами яркие «красные флаги» и манипулятивные техники.

3. Проверьте чистоту сделки при покупке. Узнайте, какой договор с Вами заключат; если его нет, это признак отсутствия лицензии на образовательную деятельность. Посмотрите, что прописано в договоре, можно ли вернуть деньги и будет ли в конце обучения выдан диплом установленного образца или сертификат с печатью или подписью преподавателя на официальном бланке организации.

4. У организации, продающей курсы, должна быть лицензия на образовательную деятельность. Проверить наличие лицензии можно на сайте Рособрнадзора.

5. Ознакомьтесь с программой обучения. Прочитайте ее внимательно, чтобы понимать, чему Вас научат, проанализируйте план – как долго будет идти обучение, будет ли практика.

6. Обратите внимание на шаблонные фразы, например «Вы узнаете инструменты повышения продаж», – они сигнализируют о поверхностности знаний, которые Вам будут давать.

7. Недобросовестные игроки часто дают размытое представление об итогах обучения и не готовы предоставить развернутую информацию о содержании программы. И это первый сигнал, на который стоит обратить внимание.

«УГОН» АККАУНТА

В современном мире наши цифровые аккаунты стали неотъемлемой частью жизни. Они хранят личную переписку, фотографии, данные банковских карт и другую конфиденциальную информацию. Когда злоумышленники получают доступ к аккаунту без разрешения владельца, это называется «угоном», подобно угону автомобиля.

Последствия «угона» аккаунта могут быть крайне серьезными. Преступники могут использовать Ваш аккаунт для мошенничества, вымогательства денег у Ваших знакомых, распространения вредоносных программ или кражи персональных данных. Особенно опасен доступ к аккаунтам государственных услуг, через которые злоумышленники могут оформить кредиты или совершить другие противоправные действия от Вашего имени.

Важно понимать, что «угон» аккаунта – это не просто неприятность, а серьезное преступление, которое может привести к значительным финансовым потерям и даже уголовной ответственности для владельца аккаунта, если он поддастся на требования преступников.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация 1. Поддельный (фишинговый) сайт.

Мария работала бухгалтером в небольшой компании. Однажды она получила письмо, якобы от налоговой службы, о срочной проверке. В письме была ссылка на «официальный портал» для загрузки документов. Сайт выглядел точно так же, как настоящий портал налоговой, и Мария ввела свои учетные данные. На следующий день она обнаружила, что с корпоративного счета были выведены значительные суммы, а доступ к бухгалтерской системе был заблокирован.

Ситуация 2. «Социальная инженерия» через мессенджеры.

Работнику популярного ресторана Андрею в *WhatsApp* написал «поставщик продуктов» с предложением срочной закупки по выгодной цене. Для оформления заказа требовалось перейти по ссылке и авторизоваться через «корпоративный портал». После ввода данных мошенники получили доступ к бизнес-аккаунту ресторана и разослали всем клиентам из базы фальшивые акции с просьбой предоплаты.

Ситуация 3. Вредоносные программы.

Дизайнер Екатерина скачала «бесплатную» версию графического редактора с неофициального сайта. Через неделю она заметила, что от ее имени в соцсетях публикуются рекламные посты криптовалютных пирамид. Оказалось, что вместе с программой установился кей-

логгер – специальный код, который записывал все нажатия клавиш и отправлял их мошенникам.

Ситуация 4. Атака через *Wi-Fi*.

Павел любил работать за чашкой кофе в торговом центре. Однажды он подключился к бесплатному *Wi-Fi* с названием «*Coffee_Free*». Через этот поддельный роутер мошенники перехватили его данные авторизации на рабочем портале. В результате злоумышленники получили доступ к корпоративной сети его компании.

Ситуация 5. Взлом через ботов в *Telegram*.

Владелица косметического магазина Анна создала *Telegram*-канал для клиентов. Ей написал «маркетолог» с предложением установить бота для аналитики подписчиков. После добавления бота в администраторы канала мошенники заблокировали доступ Анны и начали рассылать подписчикам фишинговые ссылки на фальшивый магазин.

Ситуация 6. QR-код на плакате.

Студент Дмитрий увидел в торговом центре плакат с *QR*-кодом и обещанием скидки 90% на новый *iPhone*. Просканировав код, он попал на поддельный сайт, где ввел данные своего *Telegram*-аккаунта. В результате мошенники получили доступ к его аккаунту и стали рассылать его контактам просьбы о срочных денежных переводах.

Ситуация 7. Взлом «Госуслуг».

Пенсионерке Валентине Петровне позвонили якобы из Пенсионного фонда, сообщив о положенной доплате к пенсии. Для ее получения попросили продиктовать код из *SMS* «для подтверждения личности». После этого мошенники получили доступ к ее аккаунту на «Госуслугах» и оформили на ее имя кредит в микрофинансовой организации.

ОТВЕТСТВЕННОСТЬ

Статья 137 УК РФ «Нарушение неприкосновенности частной жизни».

Преступник, получив доступ к чужой учетной записи, незаконно собирает информацию о частной жизни владельца аккаунта, изучая его фотографии, переписку, финансовые данные и иные сведения, составляющие личную или семейную тайну.

Статья 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений».

Преступник, получив доступ к чужому аккаунту, незаконно знакомится с личной перепиской, электронными письмами, сообщениями в мессенджерах и иными формами частной переписки.

Статья 159 УК РФ «Мошенничество».

Применяется в случае завладения мошенниками денежными средствами третьих лиц обманным путем с использованием аккаунта.

Статья 163 УК РФ «Вымогательство».

Применяется, если при требовании передачи имущества владельца аккаунта имела место угроза применения насилия либо уничтожения или повреждения чужого имущества, распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам владельца аккаунта или его близких.

Статья 179 УК РФ «Принуждение к совершению сделки или к отказу от ее совершения».

Применяется, если сделка была совершена под влиянием угроз применения насилия либо уничтожения или повреждения чужого имущества, а равно распространения сведений, которые могут причинить существенный вред правам или законным интересам владельца аккаунта или его близких.

Статья 272 УК РФ «Неправомерный доступ к компьютерной информации».

Преступник, получив несанкционированный доступ к чужой учетной записи, совершает действия, направленные на изменение или удаление информации, блокирование доступа к аккаунту, а также несанкционированное копирование личных данных.

Статья 272.1 УК РФ «Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения».

Применяется в случае незаконного способа завладения персональными данными в электронном виде и незаконных действий, связанных с их распространением одновременно.

МОЖЕТ ЛИ НАСТУПАТЬ УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ, ЕСЛИ ВЫ ВЫПОЛНИЛИ ТРЕБОВАНИЯ ЛИЦ, «УГНАВШИХ» АККАУНТ?

1. **Перевод денежных средств на определенный счет.**

Преступники могут указать счета, использующиеся террористическими, экстремистскими и иными организациями, оказывающими помощь в совершении преступлений.

2. **Совершение действий, связанных с насилием или причинением вреда третьим лицам.**

Преступники, получив доступ к аккаунту в социальной сети, где пользователь выкладывал свои фотографии, присылают ему сообщение, в котором угрожают опубликовать интимные снимки в открытом доступе, если он не подожжет двери военкомата по указанному адресу (взорвет торговый центр, причинит вред здоровью указанных лиц).

3. **Передача информации или различных предметов.**

Преступники могут потребовать:

• сообщить информацию о работе родственника – инженера оборонного предприятия;

• указать место расположения видеокамер в помещении, например государственном ведомстве (у его сотрудника); передать им информацию о системе видеонаблюдения в здании, угрожая в противном случае опубликовать компрометирующие материалы;

• передать пакет с неизвестным содержимым;

• забрать пакет с деньгами и отвезти по указанному адресу.

Такие действия могут квалифицироваться по статьям, предусматривающим ответственность за причинение вреда здоровью (ст. 111, 112, 115 УК РФ), мошенничество (ст. 159 УК РФ), умышленное уничтожение или повреждение имущества (ст. 167 УК РФ), террористический акт (ст. 205 УК РФ), участие в террористической деятельности (ст. 205.1 УК РФ), вандализм (ст. 214 УК РФ), а также за преступления против основ конституционного строя и безопасности государства (ст. 275–284.3 УК РФ) или по другим соответствующим статьям УК РФ, в зависимости от конкретных обстоятельств дела.

В случаях, когда владелец аккаунта под принуждением совершает противоправные действия, важно учитывать положения гл. 8 УК РФ, устанавливающие обстоятельства, исключающие преступность деяния. Наличие состояния крайней необходимости (ст. 39 УК РФ), физического или психического принуждения (ст. 40 УК РФ) исключает уголовную ответственность, а при нарушении условий их правомерности – смягчает наказание (п. «е» и «ж» ч. 1 ст. 61 УК РФ).

ЧТО ДЕЛАТЬ, ЕСЛИ ВАШ АККАУНТ ВЗЛОМАЛИ?

Если Вы обнаружили признаки взлома аккаунта, следуйте этому алгоритму действий:

1. Немедленно смените пароль от взломанного аккаунта, используя другое устройство.

2. Включите двухфакторную аутентификацию, если она доступна.

3. Проверьте и отключите все подозрительные устройства, имеющие доступ к аккаунту.

4. Просканируйте устройство антивирусом для выявления вредоносных программ.

5. Предупредите всех лиц из списка Ваших контактов о взломе и возможных мошеннических сообщениях.

6. Обратитесь в службу поддержки сервиса для восстановления доступа.

7. Подайте заявление в правоохранительные органы, если был причинен материальный ущерб.

КАК ЗАЩИТИТЬ СВОЙ АККАУНТ?

Предотвратить «угон» аккаунта намного проще, чем бороться с его последствиями. Следуйте этим правилам безопасности:

1. Используйте сложные пароли длиной не менее 12 символов, содержащие буквы разных регистров, цифры и специальные знаки. Создавайте разные пароли для разных сервисов.

2. Никогда не переходите по подозрительным ссылкам в письмах и сообщениях. Проверяйте адрес сайта, убедитесь, что он соответствует официальному.

3. Включите двухфакторную аутентификацию везде, где это возможно. Используйте для этого отдельное приложение-аутентификатор вместо *SMS*.

4. Регулярно проверяйте историю входов в Ваши аккаунты и немедленно сообщайте о подозрительной активности в службу поддержки.

5. Не сообщайте никому коды подтверждения, которые приходят в *SMS* или электронных письмах, даже если собеседник представляется сотрудником банка или технической поддержки.

КАК ОБЕЗОПАСИТЬ ДАННЫЕ НА СЛУЧАЙ ПРОПАЖИ ТЕЛЕФОНА?

В эпоху цифровых технологий мобильный телефон превратился в универсальный ключ к нашей жизни. Он хранит доступ к банковским счетам, государственным услугам, рабочей документации и личной информации. Современный смартфон содержит больше конфиденциальных данных, чем когда-либо хранилось в домашних сейфах: от паролей к социальным сетям до документов, удостоверяющих личность. Информация, хранящаяся на телефоне, может быть во много раз ценнее, чем он сам.

Особую тревогу вызывает тот факт, что большинство пользователей даже не осознают масштаб возможных последствий от потери телефона. Они продолжают хранить в устройстве критически важную информацию без надлежащей защиты: автоматически сохраняют пароли в браузерах, держат в заметках данные банковских карт, хранят сканы паспортов и других документов в общедоступной галерее фотографий.

Ситуация усугубляется тем, что современные мошенники научились молниеносно использовать утерянные телефоны для получения незаконной выгоды. В их арсенале появились инструменты, способные в считанные минуты преодолеть стандартную защиту устройства и получить доступ к конфиденциальной информации. При этом географическая удаленность злоумышленников и использование ими современных технологий существенно затрудняют их поимку и привлечение к ответственности.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация 1. Молодая мать Анна оставила телефон в коляске во время прогулки с ребенком в парке. Спустя несколько минут злоумышленники успели войти в ее банковское приложение, где был сохранен пароль, и вывести все средства с карты. Более того, через привязанную к телефону электронную почту они получили доступ к ее рабочим документам, содержащим коммерческую тайну.

Ситуация 2. Пенсионер Михаил Петрович забыл телефон в такси, на котором его отправил домой из гостей его сын. Прежде чем он успел прийти в офис оператора связи и заблокировать *SIM*-карту, мошенники от его имени оформили онлайн-кредит через приложение банка, где были сохранены все его данные. В результате пенсионер столкнулся не только с потерей денег, но и с необходимостью доказывать в суде, что кредит был оформлен не им.

Ситуация 3. Студентка Мария потеряла телефон в торговом центре. Не имея установленной блокировки экрана, устройство стало легкой добычей для злоумышленников, которые получили доступ к ее аккаунту в социальных сетях и начали рассылать просьбы о финансовой помощи всем ее контактам, включая преподавателей университета и родственников со стороны бабушки.

ОТВЕТСТВЕННОСТЬ

Утеря телефона может привести к нарушению целого комплекса правовых норм. В первую очередь речь идет о ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», предусматривающей наказание до семи лет лишения свободы. Если злоумышленники используют полученные данные для кражи денежных средств, их действия квалифицируются по ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации», санкция которой также предполагает длительные сроки заключения.

Отдельного внимания заслуживает вопрос ответственности владельца утерянного телефона. Если через его устройство или аккаунты были совершены платежи в пользу запрещенных организаций, он может быть привлечен к ответственности по ст. 205.1 УК РФ «Содействие террористической деятельности» или ст. 282.3 УК РФ «Финансирование экстремистской деятельности». При этом доказать свою непричастность к совершению данных преступлений бывает крайне сложно.

В случае утечки персональных данных третьих лиц (например, коллег или клиентов) владелец телефона может быть привлечен к ответственности по ст. 137 УК РФ «Нарушение неприкосновенности частной жизни». Если речь идет о служебной информации, применяется ст. 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну».

Важно понимать, что даже неумышленное содействие преступникам может повлечь серьезные правовые последствия. Например, если через утерянный телефон были совершены действия, причинившие ущерб третьим лицам, владелец устройства может стать ответчиком в гражданском процессе о возмещении вреда. При этом суд может признать его действия (в частности, отсутствие надлежащих мер защиты конфиденциальной информации) проявлением грубой неосторожности, что существенно усложнит правовую защиту.

АЛГОРИТМ ДЕЙСТВИЙ ПРИ УТЕРЕ ТЕЛЕФОНА

При обнаружении пропажи телефона критически важна скорость реакции. В первые минуты после обнаружения пропажи необходимо немедленно связаться с оператором сотовой связи для блокировки

SIM-карты. Желательно заранее сохранить номер службы поддержки Вашего оператора на другом устройстве или записать его на бумаге. При обращении потребуется назвать паспортные данные и кодовое слово, если оно было установлено.

Следующим незамедлительным шагом должна стать удаленная блокировка устройства. Для телефонов на базе *Android* следует использовать сервис *Google Find My Device*, для *iPhone – Find My iPhone*. Эти сервисы позволяют не только заблокировать устройство, но и удалить с него все данные дистанционно. Важно помнить, что для работы этих функций телефон должен быть подключен к Интернету.

После блокировки устройства необходимо срочно сменить пароли от всех критически важных аккаунтов. Начинать следует с электронной почты, поскольку через нее часто настроено восстановление доступа к другим сервисам. Затем следует сменить пароли от социальных сетей, банковских приложений, государственных сервисов и рабочих аккаунтов. При смене паролей важно использовать другое надежное устройство и проверять, чтобы не было активных сессий на утерянном телефоне.

Отдельное внимание следует уделить банковской безопасности. Необходимо связаться со службой поддержки всех банков, где были установлены мобильные приложения, и сообщить о пропаже телефона. Банки могут дополнительно заблокировать доступ к онлайн-банкингу с утерянного устройства и установить особый контроль над операциями по счетам. Если есть подозрение, что мошенники уже успели получить доступ к банковским приложениям, следует немедленно заблокировать все привязанные карты.

В случае обнаружения несанкционированных операций или попыток доступа к аккаунтам необходимо обратиться в правоохранительные органы. Заявление можно подать как лично в отделении полиции, так и через портал государственных услуг. К заявлению следует приложить максимум информации: данные устройства, время и место пропажи, детали подозрительных операций или действий.

ПРОФИЛАКТИЧЕСКИЕ МЕРЫ ЗАЩИТЫ

Защита данных начинается задолго до возможной утери телефона. Первым уровнем защиты должна стать надежная блокировка экрана. Рекомендуется использовать комбинацию биометрических данных (отпечаток пальца или распознавание лица) и сложного пароля длиной не менее восьми символов. *PIN*-коды из четырех цифр и простые графические ключи легко подсмотреть и воспроизвести.

Критически важно настроить двухфакторную аутентификацию для всех значимых аккаунтов. При этом второй фактор аутентификации

не должен завязываться только на *SMS* – лучше использовать специальные приложения-аутентификаторы или физические ключи безопасности. Это особенно важно для банковских приложений и сервисов, где хранятся конфиденциальные данные.

Регулярное резервное копирование данных позволит минимизировать потери при утере устройства. Рекомендуется настроить автоматическое сохранение фотографий, контактов и документов в облачное хранилище. При этом важно использовать разные пароли для доступа к облаку и к самому телефону. Особо чувствительные данные лучше хранить в зашифрованном виде.

Следует внимательно относиться к разрешениям, которые запрашивают установленные приложения. Необходимо регулярно проверять список установленных приложений и удалять неиспользуемые, особенно те, которые имеют доступ к конфиденциальной информации. Важно также отключать автоматическое сохранение паролей в браузерах и приложениях.

КАК МОШЕННИКИ ОБМАНЫВАЮТ ЛЮБИТЕЛЕЙ ОНЛАЙН-ИГР?

Мошенники постоянно пытаются обмануть любителей онлайн-игр, так как:

• многие геймеры сами размещают личную информацию, а также могут вкладывать немалые деньги в виртуальные покупки в играх;

• онлайн-игры – это многомилионный бизнес;

• в игре существует дружественная обстановка, что делает игроков менее бдительными, чем в других онлайн-средах.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Способы мошенничества:

• фишинг в онлайн-играх;

• вредоносные программы;

• рейдерство аккаунтов;

• виртуальная кража в онлайн-играх;

• мошенничество с помощью лотерей и розыгрышей.

Ситуация 1. Мошенники выманили у школьницы Полины Храмовой в компьютерной игре «Роблокс» 58 тыс. руб. Когда ребенок перевел сумму, родители об этом сразу не узнали.

«Там была ссылка, она перешла по этой ссылке, попала в *Telegram*-канал. А дальше – запрос информации, телефона родителей, к которому привязана карта, с позиционированием таким, что ты оказалась первой, но нужно заплатить комиссию», – объяснила мама Полины.

Ситуация 2. Согласно данным опросов 39% детей в возрасте от 11 до 17 лет желают получить в подарок игровую подписку, а 29% – внутриигровую валюту. На этом желании мошенники тоже зарабатывают, предлагая школьникам «выгодно» купить монеты в той или иной онлайн-игре, например в песочнице *Roblox*.

Так, в Екатеринбурге школьница потратила 700 тыс. руб. с банковской карты матери. Она просто хотела приобрести «робуксы» в *Roblox*, а некие незнакомцы из игрового чата согласились ей в этом помочь и продать «большую сумму игровой валюты». Они даже объяснили, куда нажать в мамином смартфоне, чтобы оформить кредит и перевести средства за право быть самой крутой на сервере. Получила ли девочка что-то в игре, неясно, но даже если так, то купленные на «черном рынке» робуксы могут быть в любой момент аннулированы.

Полиция Екатеринбурга возбудила уголовное дело после обращения матери, обнаружившей крупные переводы в истории банковско-

го приложения. Подобная ситуация повторилась уже в начале 2024 г. в Якутске: 10-летний мальчик перевел мошенникам с карты отца больше 500 тыс. руб. за бонусы в *Roblox* и ничего не получил.

ОТВЕТСТВЕННОСТЬ

Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). Под таким мошенничеством понимается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. В случае если мошенничество совершено организованной группой или в особо крупном размере, то виновным грозит лишение свободы на срок до 10 лет со штрафом в размере до 1 млн руб. или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Если такое преступление повлекло тяжкие последствия или создало угрозу их наступления, то срок наказания – до семи лет лишения свободы.

Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ). Если преступление повлекло тяжкие последствия или создало угрозу их наступления, то срок наказания – до семи лет лишения свободы.

ЧТО ДЕЛАТЬ В СЛОЖИВШЕЙСЯ СИТУАЦИИ?

Если Вы стали жертвой обмана, нужно немедленно:

1. Заблокировать карты.
2. Изменить пароли.
3. Обратиться в техподдержку платформы и в правоохранительные органы.

КАК НЕ СТАТЬ ЖЕРТВОЙ ОНЛАЙН-МОШЕННИКОВ?

1. Играть только в официальные игры от проверенных издателей.
2. Не разглашать личные данные, включая пароли и коды из *SMS*.
3. Не вводить учетные данные на сторонних сайтах.
4. Использовать разные и сложные пароли.
5. Для защиты финансовых средств можно использовать отдельные банковские карты для игровых покупок с ограниченным балансом.

КАК НЕ ОСТАТЬСЯ БЕЗ КВАРТИРЫ И ДЕНЕГ ПРИ ПОКУПКЕ СТРОЯЩЕГОСЯ ЖИЛЬЯ?

Покупка жилья – важное решение в жизни каждого человека. В Российской Федерации существует множество способов приобретения жилой площади, одним из которых является покупка квартиры у застройщика во время стройки. Однако, к сожалению, жилье, приобретенное таким способом, может не попасть в распоряжение собственника.

ПРИМЕРЫ ЖИЗНЕННЫХ СИТУАЦИЙ

Ситуация 1. В г. Хабаровске директор строительной компании ООО «Ромашка» расходовал денежные средства участников долевого строительства в своих интересах, вследствие чего предприятие обанкротилось и более 400 человек остались без квартир.

Ситуация 2. Москвичи, которые приобрели жилплощадь в доме на ул. Левобережной, оказались заложниками ситуации – застройщик дом не достраивает, но и деньги вернуть они не могут, так как под действие «долевого закона», более известного как 214-й закон, они не подпадают. В результате 80 семей остались и без жилья, и без денег.

ОТВЕТСТВЕННОСТЬ

Российское законодательство регулирует отношения, возникающие между покупателем квартиры, именуемым участником долевого строительства, и застройщиком Федеральным законом от 30 декабря 2004 г. № 214-ФЗ «Об участии в долевом строительстве многоквартирных домов и иных объектов недвижимости и о внесении изменений в некоторые законодательные акты Российской Федерации». Так, в ст. 10 данного Закона установлена ответственность за нарушение обязательств по договору. Сторона, не исполнившая обязанности по договору, обязана уплатить неустойки (штрафы, пени), проценты и возместить убытки сверх неустоек. В то же время участник долевого строительства, заключивший договор исключительно для личных, семейных, домашних и иных нужд, не связанных с осуществлением предпринимательской деятельности, может получить моральную компенсацию по решению суда. Кроме того, на строительные объекты действует гарантия пять лет.

Важными гарантиями соблюдения прав дольщиков по Федеральному закону № 214-ФЗ являются: регистрация договора ДДУ в Росреестре, размещение денежных средств покупателя на счете эскроу в банке, вследствие чего деньги сохраняются на случай невозможности выполнить застройщиком обязательства перед покупателями.

Застройщиков могут привлекать к уголовной ответственности в случае, если застройщик израсходовал денежные средства участников долевого строительства на незаконные цели по ст. 159 УК РФ «Мошенничество», а также по ст. 201 УК РФ «Злоупотребление полномочиями». Наказание зависит от тяжести преступления, суммы хищения, максимально возможное – 10 лет лишения свободы.

ВЕРОЯТНЫЕ РИСКИ ПРИ ПРИОБРЕТЕНИИ ЖИЛЬЯ В НОВОСТРОЙКАХ

1. Недобросовестный продавец (застройщик, риелтор) предлагает заключить **предварительный договор купли-продажи вместо договора долевого участия в строительстве**, мотивируя это тем, что дом находится в процессе возведения. Такой договор не обеспечивает покупателю защиту, так как не подпадает под действие Федерального закона № 214-ФЗ. Денежные средства, полученные продавцом по предварительному договору, поступают в распоряжении застройщика, а не размещаются на счете эскроу банка, что гарантирует возврат по требованию в случае банкротства застройщика или иного основания прекращения его деятельности до окончания строительства.

2. Застройщик включает в договор пункт **о дополнительных взаиморасчетах в случае, если сданная квартира отличается по площади от проектной**. Если фактическая площадь квартиры больше, чем оплаченная по проекту, то необходимо будет произвести доплату. Застройщик в договоре обязан указать конкретные цифры, в пределах которых может колебаться площадь квартиры и при этом не будет изменяться ее конечная стоимость.

3. Договор участия в долевом строительстве может содержать **условия, ограничивающие действия покупателя в случае обнаружения недостатков** в сданной квартире. К примеру: «Дольщик не имеет права предъявлять никаких требований к застройщику, кроме как устранить дефекты силами застройщика». В то же время по закону, если квартира не соответствует договору, покупатель может требовать от застройщика не только устранить дефекты, но и соразмерно уменьшить цену договора или возместить расходы на устранение недостатков.

4. В договор внесены положения, **позволяющие застройщику в одностороннем порядке изменять условия договора**. Эти условия могут корректировать без согласия покупателя сроки сдачи объекта, отклонения от размеров уплаченной площади квартиры, односторонний отказ от исполнения договора. Такие условия недопустимы. В судебном порядке можно их исключить, но желательно предпринять действия по исключению подобных пунктов в договоре на стадии заключения договора.

5. **Сроки сдачи объекта по договору исчисляются не календарными, а банковскими днями**, равными пяти рабочим дням в календарную неделю. Это на порядок увеличивает сроки сдачи жилого дома и передачи квартиры покупателю.

6. Застройщик включает условие о том, что если квартира не будет передана дольщику вовремя, то застройщик направит предложение о продлении срока (**условие о дополнительном соглашении**). Подписывая дополнительное соглашение о продлении срока сдачи о квартиры, покупатель лишается возможности потребовать неустойку в связи с просрочкой.

7. **Навязывание дополнительных услуг** – частое явление при заключении договоров долевого участия. Услуги по оформлению квартиры в собственность, страхование имущества, заключение договора с управляющей компанией, чьи тарифы за коммунальные услуги могут быть повышены по сравнению с иными управляющими компаниями.

8. **Заключение договора с застройщиком на условиях рассрочки платежа.** В данном случае денежные средства покупателя не размещаются на счете эскроу, а поступают на счет застройщика. В случае прекращения строительства покупателю не гарантирован возврат уплаченных денег.

9. **Недостоверная информация о застройщике или продавце квартиры.** Для привлечения покупателей и охвата широкой аудитории застройщики заключают договоры с посредниками (риелторами) с правом использования средств индивидуализации застройщика – наименования, знаков обслуживания, маркировки. Посредники, под логотипом застройщика, размещают недостоверную информацию о цене, об условиях договора, о способах оплаты и т.д. Как правило, в подобных случаях суд встает на сторону покупателя, но данные обстоятельства затягивают покупку, вынуждая затрачивать дополнительные ресурсы на защиту своих прав.

10. **Нередко крупные застройщики создают компании под строительство конкретного объекта.** Регистрируют такие фирмы незадолго до строительства жилого комплекса, а поэтому невозможно оценить их репутацию. Формально эти застройщики входят в состав группы крупного девелопера, но в случае просрочки сдачи объекта привлечь к ответственности «материнскую» компанию или других «дочек» невозможно.

11. **Продажа квартиры через посредника посредством уступки права требования к застройщику.** Посредник, приобретя квартиру по договору долевого участия в строительстве, перепродает квартиру с наценкой. При этом сумма, размещенная на счете эскроу, будет соответствовать первоначальной цене покупки посредником, а не той, что уплатил покупатель. При расторжении договора с застройщиком в случае его банкротства или иных негативных причин покупатель может рассчитывать вернуть со счета эскроу только ту сумму, которая была внесена посредником.

КАК ИЗБЕЖАТЬ НЕПРИЯТНОСТЕЙ НА СТАДИИ ЗАКЛЮЧЕНИЯ ДОГОВОРА?

1. **Тщательно проверяем информацию о застройщике.** По ИНН или ОГРН застройщика можно проверить ***на сайте ФНС***, который выдаст выписку из ЕГРЮЛ с полной юридической информацией о компании. На сайте застройщика должен быть показан ход строительства всех объектов, над которыми он работает на данный момент.

2. **Проверяем актуальность контактной информации.** Должны быть указаны юридический адрес, адрес офиса, ИНН, ОГРН, активный номер телефона, адрес электронной почты.

3. **Изучаем репутацию застройщика.** Прежде всего ориентируемся на крупные компании, давно работающие на рынке. Можно воспользоваться следующими ресурсами:

• *Единая информационная система жилищного строительства*. Это полный каталог новостроек, информация о застройщиках и список проблемных объектов;

• *Единый ресурс застройщиков*. Здесь есть рейтинг застройщиков, а также список лучших компаний и объектов. Проверяем в электронной картотеке арбитражных дел, в каких делах компания участвовала как ответчик, чтобы избежать вероятности последствий банкротства застройщика. Читаем отзывы о застройщиках и об объектах.

4. **Проверяем документы ЖК: разрешение на строительство и проектную декларацию.** В проектной декларации застройщик указывает основную информацию об инвестиционно-строительном объекте: характеристики и его описание, сроки реализации; предоставляет результаты государственной экспертизы проектной документации, перечисляет возможные риски и называет ключевых подрядчиков. Наличие декларации можно проверить на сайте Минстроя России.

Важной представляется информация об источниках финансирования объекта строительства.

5. **Тщательно вычитываем договор о долевом участии.** В ДДУ должны быть четко прописаны все параметры приобретаемой недвижимости. Во-первых, формат недвижимости – жилая ли она вообще. Например, некоторые покупают апартаменты, а потом удивляются невозможности прописаться или другим ограничениям. Во-вторых, проверяем площадь и стоимость, в том числе стоимость квадратного метра. В-третьих, изучаем расположение и планировку квартиры, состояние помещения и коммуникаций (с отделкой или без). Особенно тщательно нужно проверить все характеристики объекта, если он сдается с отделкой под ключ.

Далее, изучаем указанные в договоре сроки ввода дома в эксплуатацию и сроки передачи ключей. Как правило, это две разные даты, что надо учитывать при планировании ремонта и переезда в новую квартиру.

Следующий важный пункт, на который нужно обратить внимание, – это обязательства застройщика по устранению строительных дефектов и гарантийные обязательства на объект недвижимости и коммуникации. В случае возникновения проблем собственник может апеллировать к застройщику именно на основании этого пункта, а также характеристик передаваемого объекта, указанных в ДДУ.

Необходимо изучить положения, касающиеся обязанностей самого дольщика, и других условий сделки. Например, здесь может быть прописана необходимость согласования условий переуступки ДДУ с застройщиком.

В целом надо ориентироваться на содержание самого договора, а не на то, что указано в рекламе.

ЧТО ДЕЛАТЬ, ЕСЛИ ЗАСТРОЙЩИК ОСТАНОВИЛ СТРОЙКУ И НЕ ВОЗВРАЩАЕТ ДЕНЬГИ?

В данной ситуации необходимо расторгнуть договор в судебном порядке, который предусмотрен в случае прекращения или приостановления строительства; в случае существенного изменения проектной документации; в случае изменения назначения объекта недвижимости и т.д.

В случае расторжения договора застройщик обязан возвратить участнику долевого строительства денежные средства, уплаченные им в счет цены договора, а также уплатить проценты на эту сумму за пользование указанными денежными средствами в размере $^{1}/_{300}$ ставки рефинансирования Центрального банка РФ. Если участником долевого строительства является гражданин, указанные проценты уплачиваются застройщиком в двойном размере.

Расторжение договора в суде содержит следующий порядок действий:

1. **Направляем претензию застройщику.**

Претензия составляется по форме искового заявления, в ней указываются:

1) обстоятельства, при которых были нарушены интересы дольщика;

2) список требований, предъявляемых к застройщику;

3) ссылки на документы и нормативные акты, подтверждающие права и обязанности участников спора.

Если одним из требований является выплата компенсации, пени или возврат денежных взносов, то в обращении необходимо указать расчетный счет и его реквизиты для перечисления средств. В противном случае застройщик может сослаться на их отсутствие и отказать в выполнении требований дольщиков.

Закон не обязывает участников спора принимать попытки досудебного урегулирования. Однако предъявление претензии может сократить срок

разрешения конфликта или более качественно подготовиться к обращению в суд. Ответ на претензию обычно поступает в течение 7–10 дней.

ВАЖНО! Претензию необходимо направлять по юридическому адресу застройщика, указанному в ЕГРЮЛ.

Если застройщик отказывается выполнять требования, содержащиеся в претензии, переходим к следующим действиям.

2. **Направляем жалобу в Роспотребнадзор.**

Структура жалобы должна в себя включать следующую информацию:

1) шапка: наименование организации, куда подается жалоба и ее почтовый адрес;

2) от кого жалоба: ФИО заявителя, его почтовый адрес и адрес электронной почты, номер телефона;

3) суть проблемы с временем произошедшего, данные должностных лиц, которые нарушили закон; нормы закона, которые были нарушены (опционально);

4) требования, какие меры должны принять, например провести проверку, вернуть денежные средства, привлечь виновных к ответственности;

5) доказательства нарушения, например документы, фото, видеозаписи, копии чеков, показания свидетелей;

6) дата, подпись, ФИО заявителя.

3. **Если стройка была остановлена в результате мошеннических действий застройщика, необходимо обратиться с заявлением полицию.**

4. **Составляем исковое заявление в суд.**

В верхней части заявления указываются реквизиты суда, в который подается иск, информация об истце и ответчике с почтовыми реквизитами и телефонами.

Затем формулируется название иска исходя из перечисленных в нем требований (например, «О расторжении договора дольного строительства, взыскании компенсации за невыполнение условий договора долевого строительства, возмещении морального вреда»).

Для составления описательной части необходимо:

- указать лиц, между которыми был заключен договор участия в долевом строительстве, а также права и обязанности сторон, иные существенные условия договора, нарушенные одной из сторон;
- указать, в чем выразилось нарушение прав истца;
- указать документы, подтверждающие факт нарушения условий договора одной из сторон;
- произвести расчет суммы исковых требований;
- указать нормы права, положения заключенного договора, на которых истец основывает свое требование, а также нормативные документы, определяющие вид правоотношений, возникших между истцом и ответчиком;

• указать наименование штрафных санкций, которые могут быть применены к ответчику, нормы действующего законодательства, регулирующие применение штрафных санкций, произвести их расчет.

В заявлении должны быть указаны конкретные сведения о реквизитах договора, подписанного между застройщиком и дольщиком, дате передачи квартиры в собственность, ее площади и стоимости. Также должны быть приложены копии договоров и платежных документов, подтверждающих факт оплаты.

В какой суд необходимо обратиться? По месту регистрации компании-застройщика; по месту нахождения объекта строительства; по месту жительства истца; по месту регистрации компании-посредника, участвовавшей в подписании договора. Таким образом, заявителю предоставляется право ***самостоятельно*** определить суд для подачи иска исходя из различных обстоятельств (удаленность суда от места жительства истца, количество рассматриваемых исков и пр.).

5. **Ожидаем вынесения решения суда.**

КАК НЕ ОСТАТЬСЯ БЕЗ КВАРТИРЫ И ДЕНЕГ ПРИ ПОКУПКЕ СТРОЯЩЕГОСЯ ЖИЛЬЯ?

1. Выбрать добросовестного застройщика. Для этого необходимо проверить следующие условия:

• разрешение на строительство объекта недвижимости;

• опубликованная проектная декларация;

• зарегистрированное право на земельный участок для строительства;

• отсутствие процедуры ликвидации/банкротства;

• отсутствие сведений о застройщике в реестре недобросовестных поставщиков и в реестре недобросовестных участников аукциона по продаже земельных участков;

• отсутствие судимости у руководителя и главного бухгалтера застройщика за экономические преступления;

• наличие поручительства банка или страхового полиса, обеспечивающих возврат денежных средств в случае неисполнения застройщиком своих обязанностей.

2. Осуществить оплату через **счет эскроу**. Денежные средства поступают на специальный счет, но застройщик получает их только после сдачи объекта, т.е. после исполнения договора.

Приложение 1

ОБРАЗЦЫ ЗАЯВЛЕНИЙ

Начальнику ОВД

_____

(указать ФИО, должность)

от _____.

проживающего по адресу:

_____

(индекс, город, улица,
дом, квартира, контактный телефон)

Заявление

Прошу Вас привлечь к уголовной ответственности неустановленное лицо (если лицо известно, то указать его ФИО, место проживания или нахождения, особые приметы, места появления, другие существенные признаки), которое «____»_____ 20__года _____ (описать события, при которых совершено мошенничество, время, место, каким образом, имеющиеся доказательства совершенного преступления).

Указанным преступлением мне причинен значительный ущерб в размере _____ рублей.

Учитывая изложенное, руководствуясь статьей 141 УПК РФ, прошу Вас дать указание о возбуждении уголовного дела по факту совершения указанного преступления.

Об уголовной ответственности по статье 306 УК РФ за заведомо ложный донос предупрежден(а).

Подпись: _____

«_____» _____20__года.

кому_____
от _____
(ФИО заявителя)
проживающего: _____
(адрес места жительства)
паспорт: _____,
(номер паспорта, дата выдачи, кем и когда выдан)
контактный телефон: _____
адрес для корреспонденции _____

Заявление

Прошу провести проверку настоящего заявления по факту незаконного завладения принадлежащими _____ денежными средствами в размере _____. Указанные денежные средства были переданы в _____ на основании _____.

Факт незаконного завладения принадлежащими мне денежными средствами был выявлен мною при _____.

На основании изложенного прошу Вас провести необходимые оперативно-розыскные мероприятия для выявления виновных лиц и привлечь их к уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

Приложения:

1
2
3

«___» _____ 20__ г. _____

(подпись, расшифровка подписи)

Учебное издание

СТОП, МОШЕННИКИ!

Учебно-методическое пособие

Подписано в печать 27.03.2025. Формат 60×90 $^{1}/_{16}$.
Гарнитура Newton. Усл. печ. л. 6. Тираж 5000 экз.
Заказ № _____.

Издательство «Деловой Стиль»:
119330, г. Москва, вн.тер.г. муниципальный округ
Раменки, пр-кт Мичуринский, д. 6, к. 1, кв. 39
www.ds-publishing.ru

978-5-6048014-2-0
9 785604 801420