Введение

Вся наша жизнь сегодня связана с ежедневным использованием средств техники будь то телефоны, компьютеры или планшеты. Мы сидим в социальных сетях, общаемся, совершаем покупки, заказываем справки и получаем новости с помощью сети интернет. Получив доступ к нашим устройствам, у преступников появляется возможность получить наши личные данные, просмотреть переписки или воспользоваться нашими денежными средствами.

Чем больше интернет и средства коммуникации входят в нашу жизнь, тем больше становится количество преступлений, совершаемых с использованием ифнормационно-коммуникационных технологий[1].

Так, за 2024 год по России зарегистрировано 765 тыс. преступлений, совершаемых с использованием ИКТ (на 2 % больше, чем в 2023 году), количество потерпевших граждан 448 900, ущерб составил 200 млрд. рублей (в 2023 году 147 млрд. рублей).

По Республике Северная Осетия-Алания преступлений данной категории зарегистрировано 3 951, количество потерпевших граждан 3219, ущерб составил 394 161 000 рублей.

Указанные данные дают основание полагать, что ущерб такого масштаба влияет не только на отдельно взятых граждан, но и на все государство в целом.

Проводя анализ, совершаемых преступлений выявлено, что совершение преступлений с использованием ИКТ невозможно без активных действий самих граждан. То есть если вы не перейдете по ссылке, не сообщите личные данные или код из СМС-сообщения в ходе телефонного разговора или не скачаете вредоносное программное обеспечение к себе в устройство преступники не смогут исполнить свой умысел.

Как нельзя кстати здесь придется пословица: «Предупрежден, значит вооружен». Зная о способах, которыми пользуются преступники для достижения своих целей, вы сможете обезопасить себя и своих близких от преступных посягательств. Вы должны уверенно пользоваться своими устройствами и постоянно повышать свою цифровую и финансовую грамотность.

---

[1] Далее - «ИКТ».

1. Основные способы мошенничеств, совершаемых с использованием информационно-коммуникационных технологий.

Для того, чтобы понять как же нам защититься от мошеннических атак на нас, необходимо понимать какими же способами преступники достигают своих замыслов и какие методы для этого используют.

Первый вид мошенничества - «**Звонки по телефону**». Используя методы социальной инженерии, мошенники звонят и пытаются получить личные данные граждан, реквизиты банковских счетов или коды из СМС — сообщения.

Второй вид — это Киберпреступления.

Киберпреступность — это преступная деятельность, в рамках которой используются либо атакуются компьютер (телефон), компьютерная сеть или сетевое устройство. Большинство кибератак совершается преступниками с целью получения финансовой прибыли, однако, целью кибератак может быть и выведение компьютеров или сетей из строя — из личных или политических мотивов.

2. Вид мошенничества - звонки по телефону.

В настоящее время уже привычным явлением для нас стали звонки от мошенников. Практически на каждом углу, а так же во всех СМИ нас предупреждают о том, что необходимо быть бдительными и не попадаться на уловки мошенников. Однако, ежедневно в полицию обращаются граждане, которые перевели свои деньги или сообщили необходимую мошенникам информацию.

Так давайте же разберемся, почему это происходит.

Для получения необходимой информации преступники используют различные психологические приемы. Существует раздел психологии который называется «Социальная инженерия».

Социальная инженерия — это раздел психологии, изучающий способы манипулирования человеком для получения желаемого результата.

Разделим этот процесс на три основные стадии.

Первая стадия - «подготовительная». Происходит сбор информации о человеке. Причем собрать информацию преступники могут как путем просмотра профилей в социальных сетях, так и непосредственно во время звонка (от самого гражданина). Для установления первичного контакта достаточно обладать поверхностной информацией о человеке (пол, возраст, место работы, ФИО, место жительства и т.д.).

Вторая стадия - «Активная» или стадия звонка. Преступниками осуществляется звонок и, исходя из собранной информации, происходит установление первичного контакта. Для того, чтобы человек не положил трубку мошенники вызывают различные эмоции, такие как:

-**Страх**. Если вы поделились своими страхами в публичном пространстве, социальных сетях, или мессенджерах преступникам может стать известно о них и они обязательно этим воспользуются.

Например:

«*Защитите свои сбережения — переведите их на* ***Безопасный счет***». Такого понятия как «Безопасный счет» не существует и мошенники заставляют Вас перевести деньги на их счет или счет посредника.

«*Ваш личный кабинет будет заблокирован — срочно поменяйте пароль*». Сотрудники банков или портала госуслуг не звонят и не сообщают такую информацию как блокировка личного кабинета. Никогда и ни при каких обстоятельствах не сообщайте свой пароль или код из СМС-сообщения третьим лицам.

«*Вы внесены в базу должников ФССП и вам будет ограничен выезд за границу*». Если Вас насторожила информация, которую вам сообщили положите трубку и самостоятельно наберите в организацию для уточнения сведений. При этом номер телефона организации необходимо взять из проверенного источника или обратиться в офис для личного приема.

-**Раздражение.** Вас могут забрасывать бесконечными сообщениями и звонками, с целью вывести Вас из равновесия и заставить совершить ошибку в виде перехода по фишинговой

ссылке или позвонив напрямую мошенникам.

Что же делать? Во первых, успокойтесь и не принимайте никаких поспешных решений. Во-вторых, вы можете заблокировать все нежелательные номера и отправить жалобы на беспокоящие Вас интернет-ресурсы.

-**Любопытство**. Злоумышленники звонят и предлагают воспользоваться новой услугой или новым тарифом у оператора. Только позвонив по указанному номеру Вам смогут сообщить детали и Вы окажетесь в числе первых кому станет доступна данная услуга. Причин может быть много, но помним всегда, что все необходимые услуги мы можем получить в офисе компании или узнать об их условиях на официальных сайтах организаций.

-**Жадность**. Еще одно свойство человека — желание получить больше при минимуме вложенных усилий. Поэтому так сложно отказаться, когда вам предлагают что либо купить или оформить подписку в 10 раз дешевле. Так, мошенники могут получить доступ к вашим платежным или учетным данным или заставить вас совершить какие-либо необдуманные действия.

Например:

«*Вы выиграли автомобиль*». Для получения выигрыша необходимо будет лишь продиктовать личные данные или код из СМС-сообщения. Также, злоумышленники могут попросить оплатить доставку или пересылку по почте.

«*Купи билеты со скидкой 90%*». Вы переведете деньги, сообщите личные данные, а билетов естественно не получите, так как это звонят мошенники.

Какие документы предлагают продлить мошенники?

1. **Карта Банка**. Аферисты сообщают жертве, что нужно срочно продлить срок действия банковской карты. **Важно!** Эту информацию можно найти на самой карте. Банки никогда не обзванивают граждан с такими запросами.

2. **Полис ОМС**. Мошенники связываются с гражданами под видом сотрудников страховых компаний или медучреждений и сообщают о необходимости заменить полис обязательного медицинского страхования. **Важно!** Ни цифровой, ни бумажный полис ОМС (даже если он старого образца) менять **НЕ ТРЕБУЕТСЯ**.

3. **СИМ-карта или договор на услуги связи**. Злоумышленники от имени оператора сотовой связи настаивают на продлении договора или срока действия СИМ-карты. Иначе номер пользователя якобы заблокируют. **Важно!** Такие договоры не нужно продлевать. Если возникли вопросы, можно обратиться к оператору по официальным каналам связи.

4. **Полис ОСАГО.** Преступники звонят или присылают на почту автовладельцам письмо с предложением продлить страховку с большой скидкой. **Важно!** Настоящие агенты иногда и правда предлагают продолжить сотрудничество со страховой компанией. Если возникли сомнения, самостоятельно перезвоните страховщикам по официальному номеру.

Кем могут представиться мошенники?

С целью воздействия на граждан аферисты могут представляться сотрудниками правоохранительных органов, органов государственной власти, работниками банков и портала Госуслуг.

Необходимо запомнить, что:

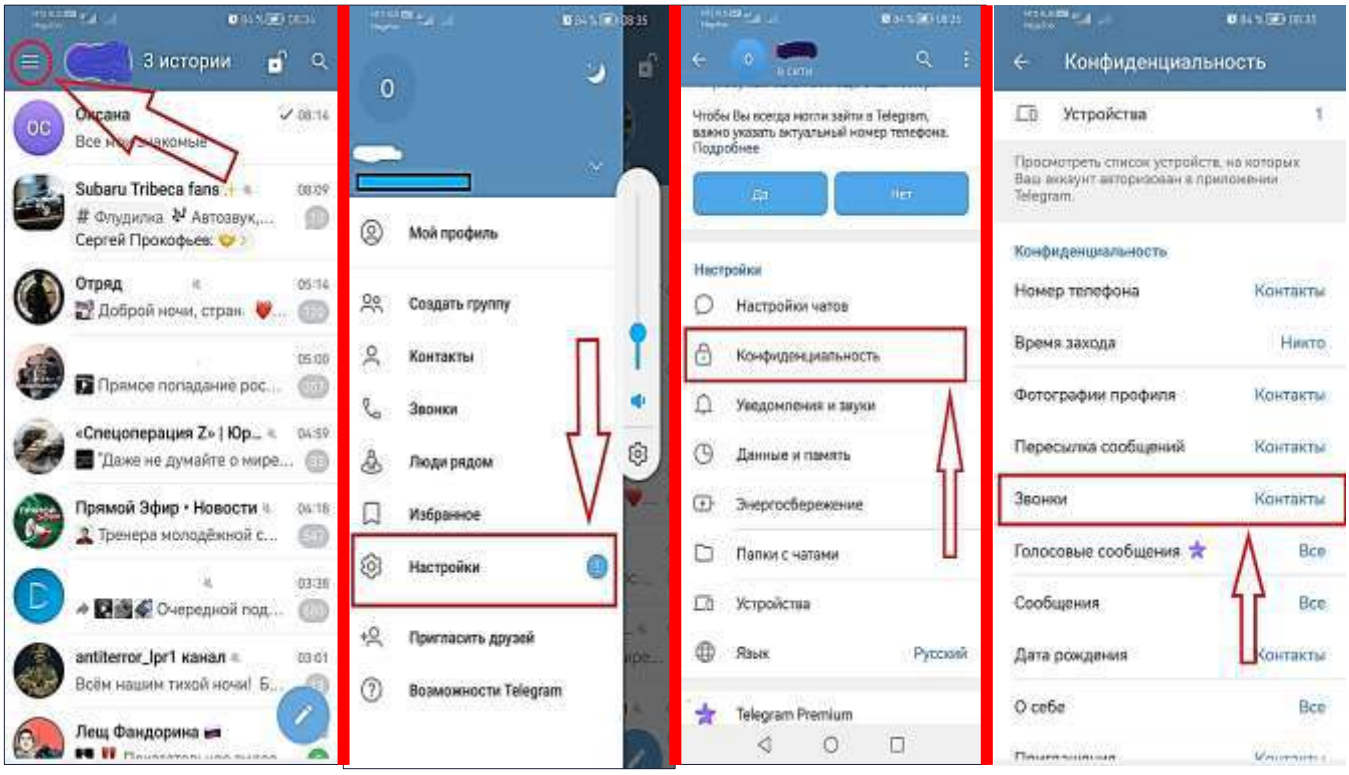
Сотрудники ведомств не звонят с помощью мессенджеров таких как «Телеграм» или «Уотсап». Доверяйте интуиции. Если какая-нибудь информация кажется вам сомнительной, неуместной или поступает по нестандартным каналам связи, задумайтесь. Задача мошенников — сбить вас с толку и заставить принять необдуманные решения. Задавайте больше дополнительных вопросов. Сомнительно, если при оказании интернет-услуги от вас требуют паспортные данные и другие конфиденциальные сведения.

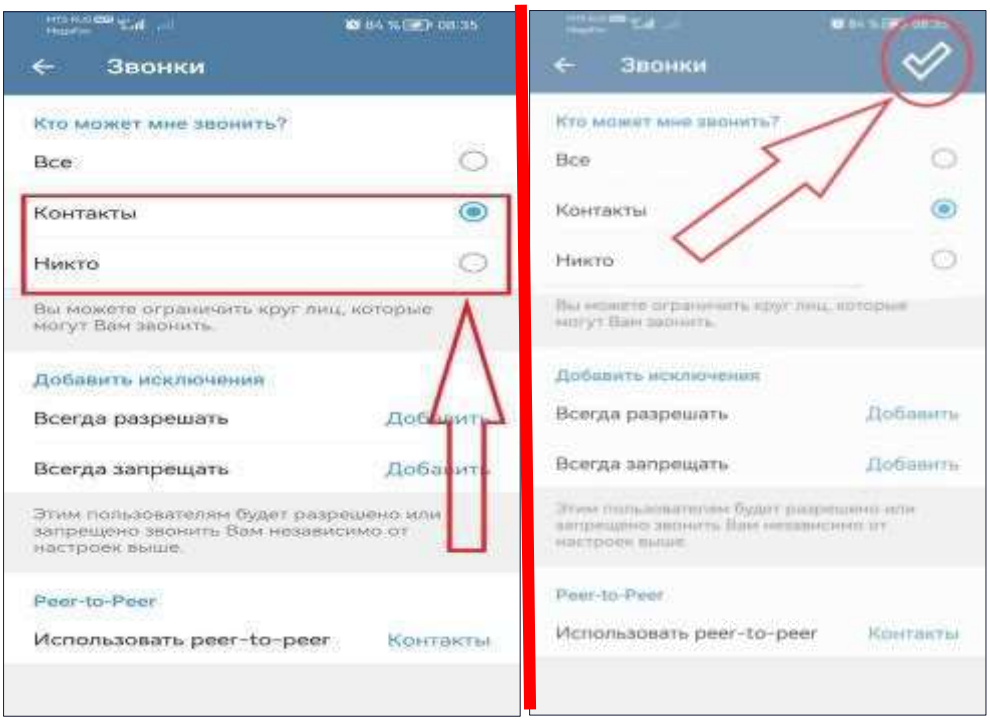
Не торопитесь доверять звонку «банковского сотрудника или сообщению от «друга» с просьбой перевести деньги. Чтобы удостовериться, точно ли с вами связались реальные люди, перезвоните в банк или знакомому и поговорите лично. Попросите собеседника подтвердить свои слова. Например, в случае звонка из правоохранительных органов можно уточнить номер телефона дежурной части. Связываются от имени организации? Узнайте у звонящего имя руководителя, юридический и фактический адрес. Затем перепроверьте всю собранную информацию.

Третьей стадией социальной инженерии будет получение желаемого мошенниками результата. Это могут быть личные данные, номера банковских карт или реквизиты счетов, а также код из СМС-сообщения от банка или с портала Госуслуг.

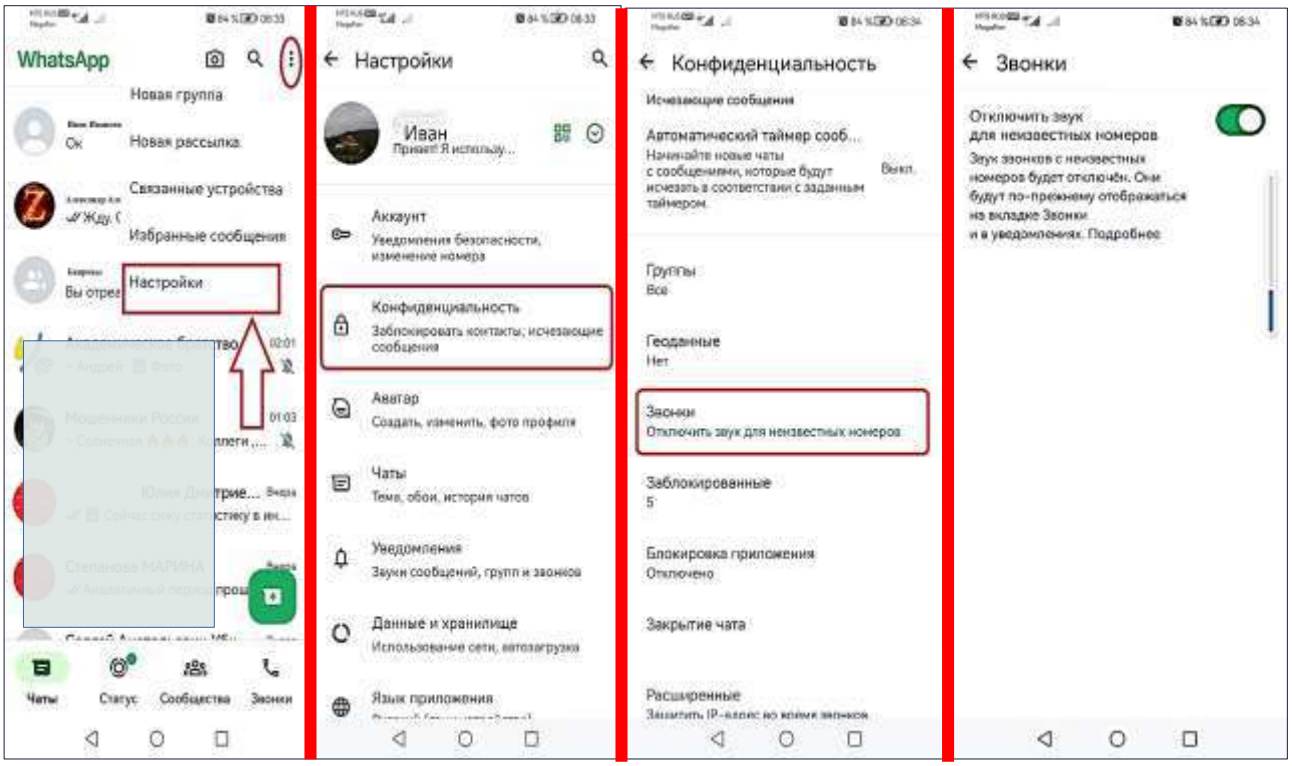
Все чаще преступники для совершения мошеннических действий начали использовать мессенджеры, такие как «Уотсапп» или «Телеграм».

«ТЕЛЕГРАМ»





«WhatsApp»



После настройки функции «Запрета звонков для неизвестных номеров», звонки от номеров, которые не сохранены в ваших контактах будут приходить пропущенными вызовами.

Будьте бдительны и помните о принципе недоверия ко всей информации, получаемой дистанционно.

3. Киберпреступления

Как мы уже говорили ранее, целями для атаки киберпреступников могут выступать компьютер (телефон), компьютерная сеть или сетевое устройство.

Основные типы киберпреступлений:

1. Мошенничество с использованием электронной почты, мессенджеров и интернета.

Согласно официальному сообщению, с января по март 2025 года почте Mail удалось заблокировать свыше 7,1 млрд спам- и мошеннических писем, в то время как в 2024 году этот показатель составлял 9,6 млрд. На это повлияло развитие антиспам-решений на основе искусственного интеллекта и применение «репутационных фильтров», блокирующих IP-адреса и домены с низким рейтингом.

Было заблокировано:

42% - предложения с фейковыми инфестициями.

35% - сообщения с предложениями принять участие в лотереях, розыгрышах или онлайн-казино.

23% - рассылки с реферальными ссылками, маскирующиеся под представителей банков, ритейлеров и маркетплейсов.

2% - сообщения, содержащие вложения с расширением .cab. (Файл .cab (Cabinet File) — это сжатый архив, используемый Windows для установки компонентов и драйверов. Он может содержать десятки файлов и сценариев установки. Мошенники могут использовать .cab как контейнер для скрытого запуска вредоносного ПО).

Мошенники нередко скрываются в комментариях тематических роликов на видеохостингах предлагая свои услуги. Так, аферисты пишут о «личных историях» успеха, предлагая заработок, а в ответах другие аккаунты подтверждают правдивость рассказа. В этой схеме мошенники переводят диалог с жертвой в мессенджеры, а затем обманным путем добираются до личных данных человека.

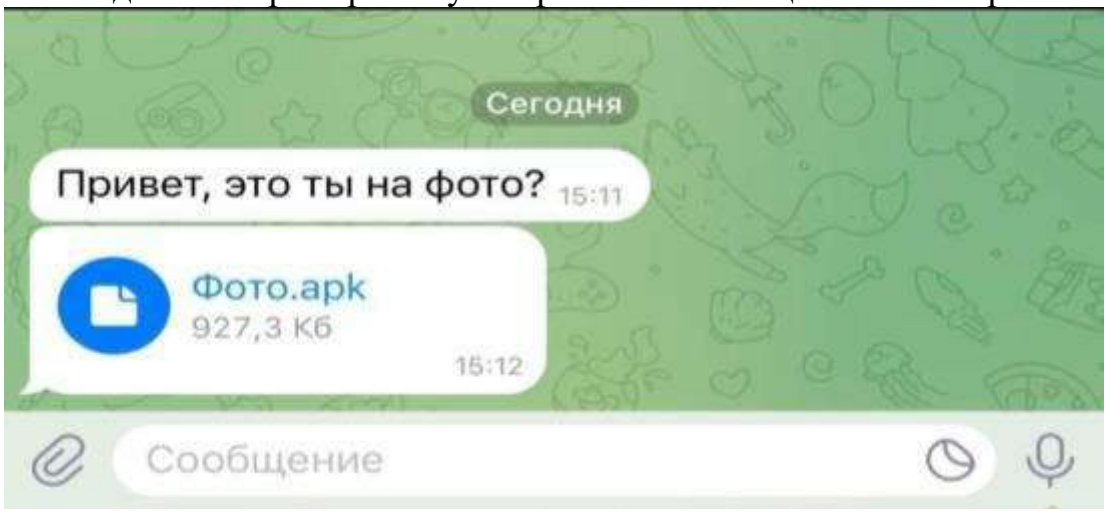
Обман с инвестициями. Эти финансовые махинации похожи на схемы

с криптовалютой, но рассчитаны на более широкую аудиторию. В комментариях мошенники рассказывают о способах быстрого заработка. Такой сценарий часто встречается под видео популярных финансовых блогеров.

Фальшивые розыгрыши и конкурсы. Мошенники создают фейковые аккаунты-копии профилей известных блогеров или подделывают логотипы брендов. От их имени проводятся акции с призами. Чтобы сбить пользователей с толку, эти аккаунты могут подделывать значки верификации.

Фишинговые ссылки. Мошенники-комментаторы предлагают перейти по ссылке «*для получения скидки*» или «*оформления предзаказа*». Такие предложения встречаются даже под видео о гаджетах и технологиях. На деле ссылки приводят на поддельные сайты, где пользователи оставляют конфиденциальные данные. Так личная информация оказывается у злоумышленников.

В последнее время участились случаи совершения мошеннических действий, с использованием фишинговых сообщений в мессенджерах типа «Телеграм» и «Уотсап». Одним из примеров служит рассылка сообщений типа .apk.



Под предлогом просмотра фото (видео) приходит сообщение с скрытым вредоносным программным обеспечением. Формат .apk (Android Package Kit) — это специальный установочный файл, содержащий код, ресурсы и параметры программы. APK-файл — это архив, внутри которого находятся все компоненты приложения. Виды вредоносных APK:

1. Фишинговые — замаскированные под легальные приложения (например Google Play Update) крадут пароли и платежные данные.

2. Троянские — получают доступ к СМ и банковским приложениям, подписывают жертву на платные услуги.

3. Шпионские — скрыто записывают звонки, отслеживают местоположение и копируют переписки.

4. Бэкдоры — позволяет хакерам удаленно управлять устройством.

Как защититься от опасных APK?

- Скачивайте приложения только из проверенных источников.

RuStore — официальный российский магазин приложений, созданный при поддержке VK и МинЦифры России. В RuStore каждое приложение проходит проверку безопасности на соответствие требованиям перед публикацией.

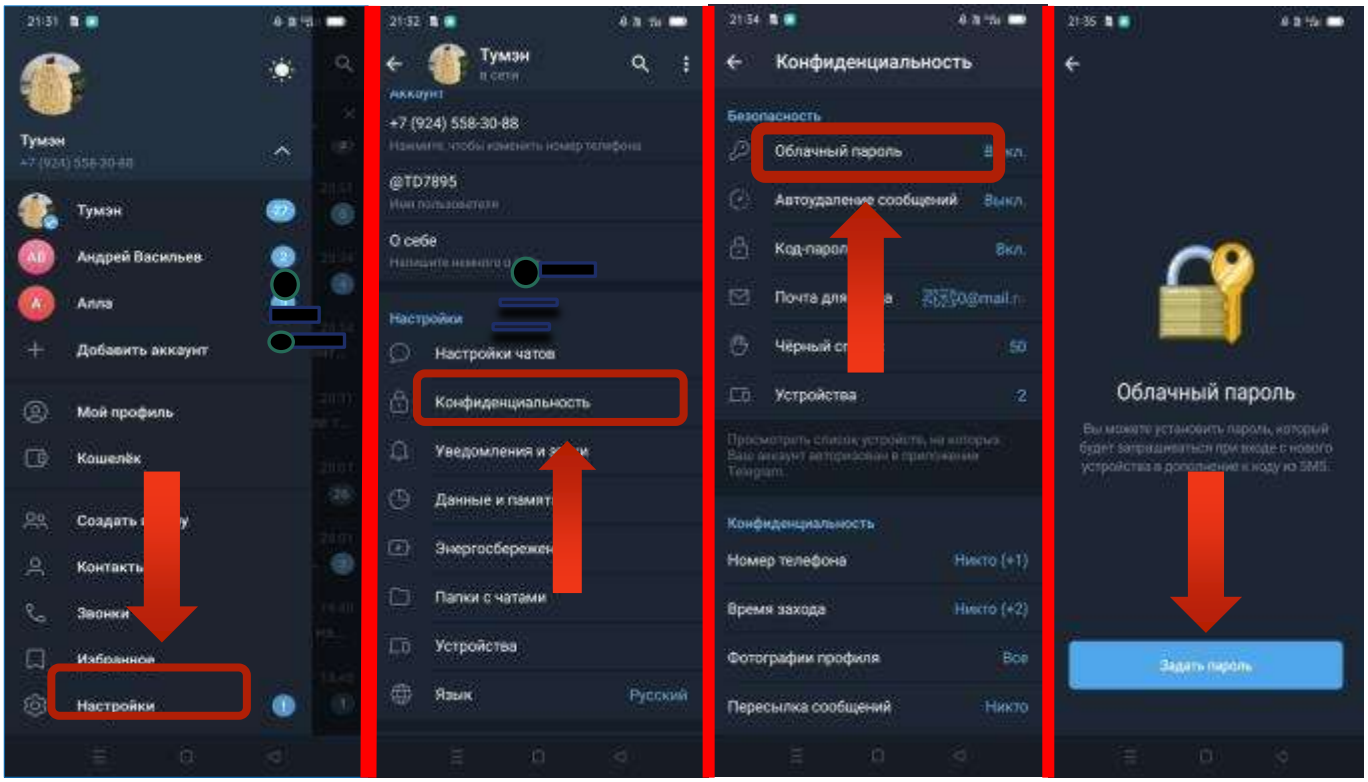
- Используйте надежное антивирусное приложение.

- Используйте сервисы анализа APK. VirusTotal, HashDroid, Checksum Calculator позволяют проверить файлы перед установкой.

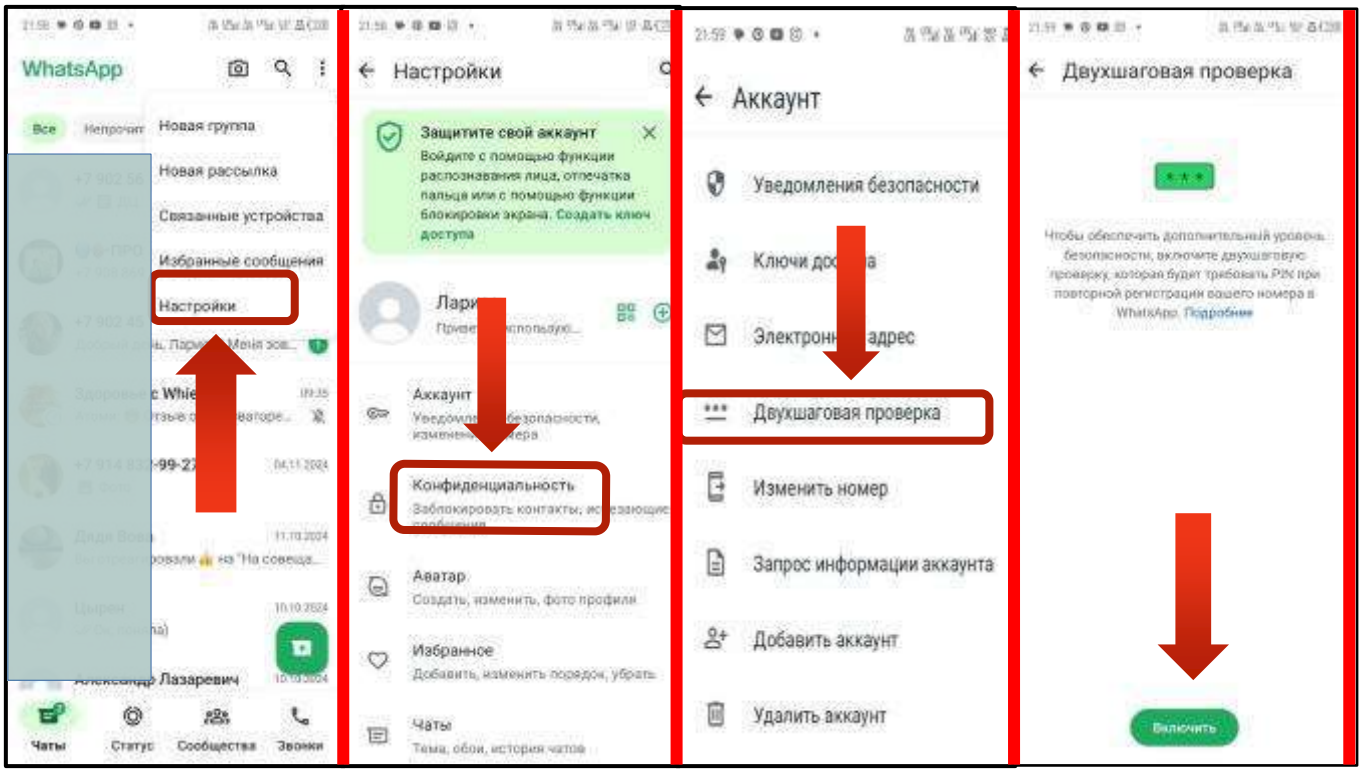
- Следите за разрешениями. Если фонарик требует доступ к контактам или камере — это тревожный сигнал.

- Установите дополнительные пароли на мессенджеры (так называемую двухфакторную аутентефиукацию).

«ТЕЛЕГРАМ»



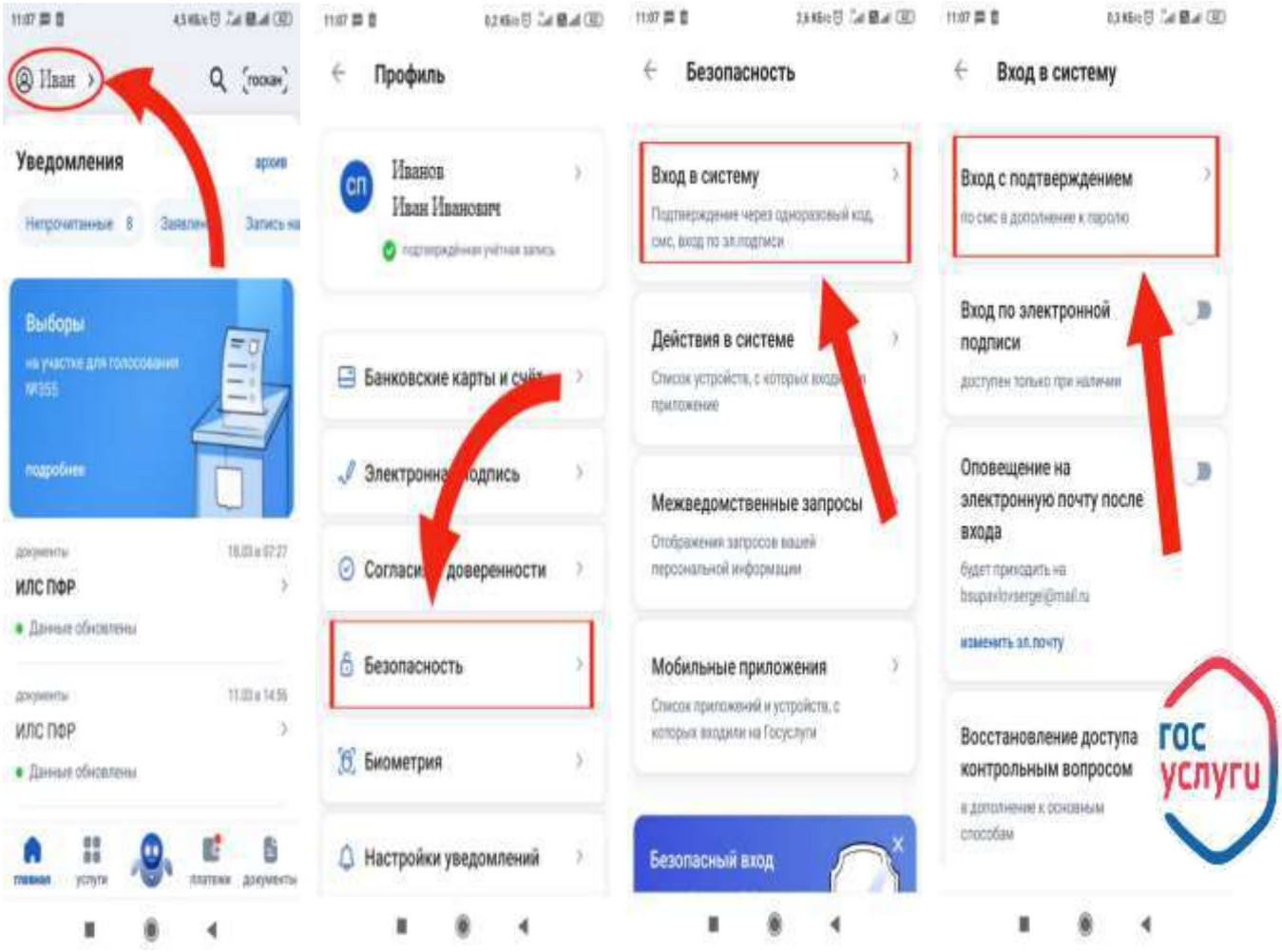
«WhatsApp»



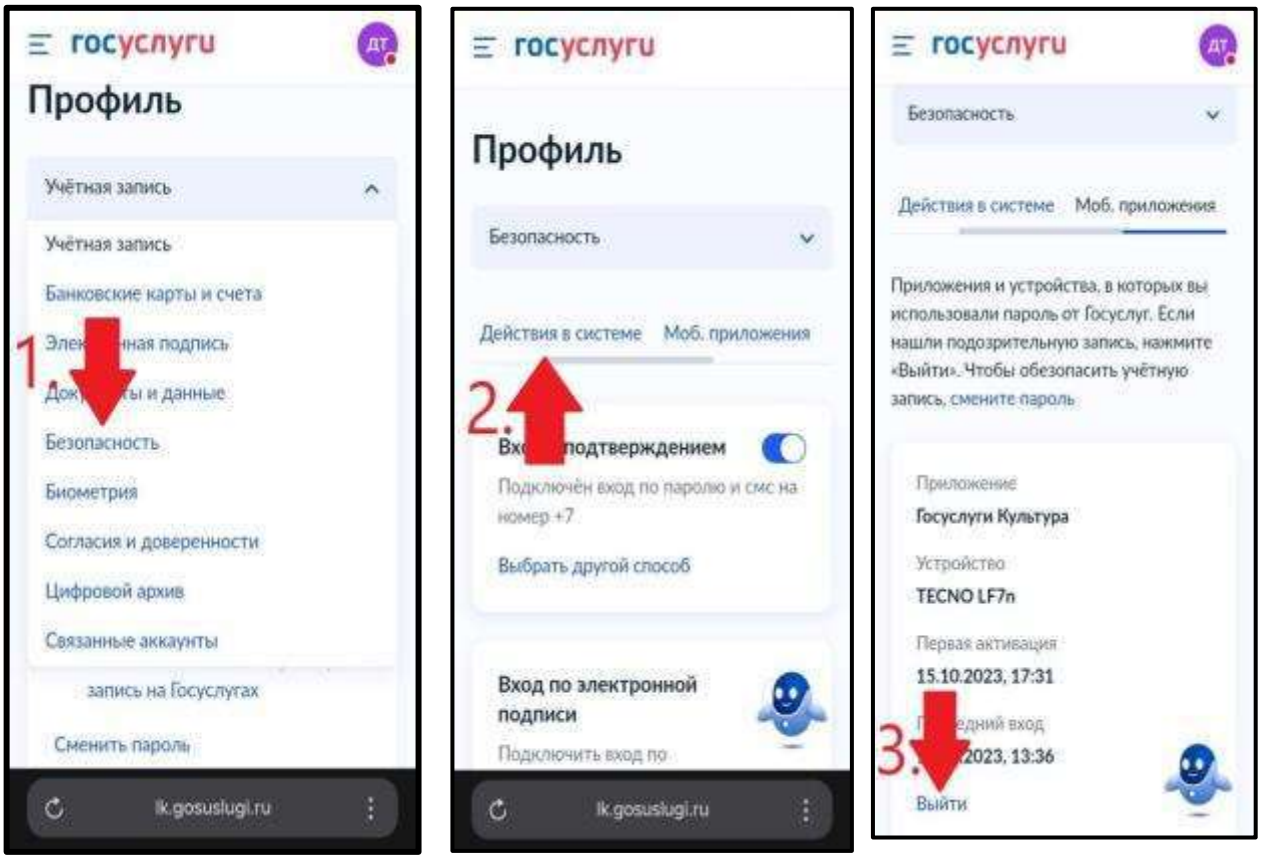
Распространенным способом мошенничества стало создание фейковых аккаунтов от лица госслужащих, звезд и иных публичных личностей. Создается фейковая страница и происходит общение с подчиненными сотрудниками или с населением с целью получения необходимой информации или с просьбой о переводе денежных средств от публичного лица. Также, нередко случается кража аккаунтов в соц. сетях, мессенджерах и Госуслугах. Мошенники используют украденные аккаунты для рассылок фишинговых сообщений,а также сообщений содержащих вредоносное программное обеспечение. Могут создаваться дипфейки с участием хозяина аккаунта, в котором он просит перевести денежные средства.

Отдельно хотелось бы поговорить о защите личного кабинета на Едином портале Государственных услуг (ЕГПУ). Важность сохранения в безопасности личного кабинета в Госуслугах нельзя переоценить, так как там хранятся наши личные данные, документы (паспорт, снилс, ИНН и др.). Завладев доступом к нашему акканту злоумышленники могут оформить кредиты и микрозаймы от нашего имени.

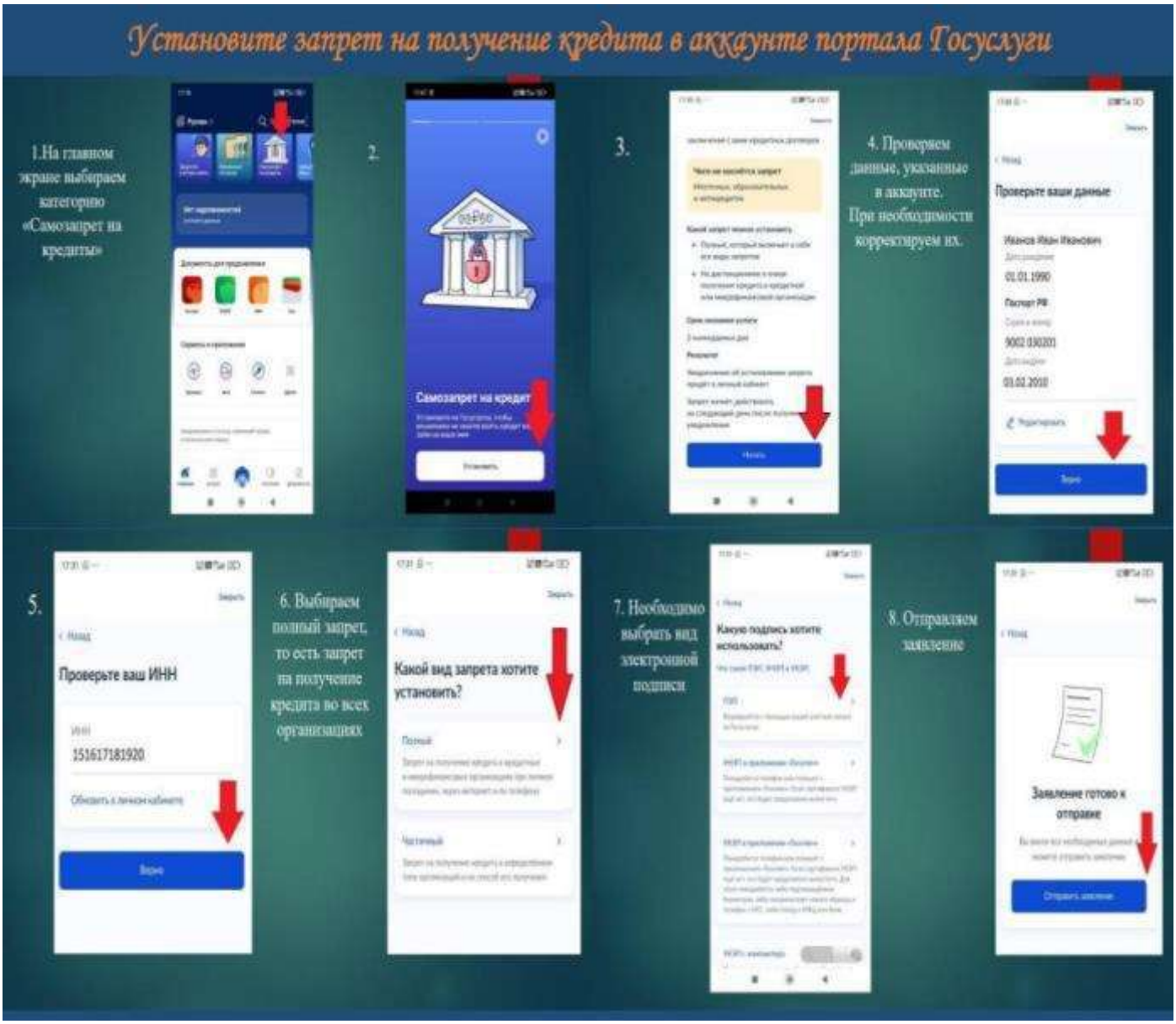
Чтобы избежать этого необходимо установить все имеющиеся виды защиты.



Если у Вас возникли подозрения, что личный кабинет в Госуслугах взломали необходимо проверить сеансы а также подключенные устройства.



Необходимо постоянно ознакамливаться с новыми функциями, которые помогают уберечься от мошенников. Так, можно установить самозапрет на получение кредита. Это не убережет ваш акааунт от взлома, но помешает злоумышленникам оформить на вас кредиты или займы.



4. Родительский контроль или как уберечь несовершеннолетних от преступных посягательств в цифровой среде.

Человек все больше времени проводит в общении со своими цифровыми устройствами, и дети не исключение. Молодежь общается в социальных сетях, и мессенджерах, проводит много времени в онлайн играх и серфит в интернете.

Правила поведения, которые мы объясняем детям в процессе воспитания, тоже должны быть актуальны и злободневны.

Так, нам необходимо объяснять ребенку что такое цифровая гигиена:

- нельзя общаться с незнакомыми людьми и сообщать им информацию о себе и своих близких родственниках;

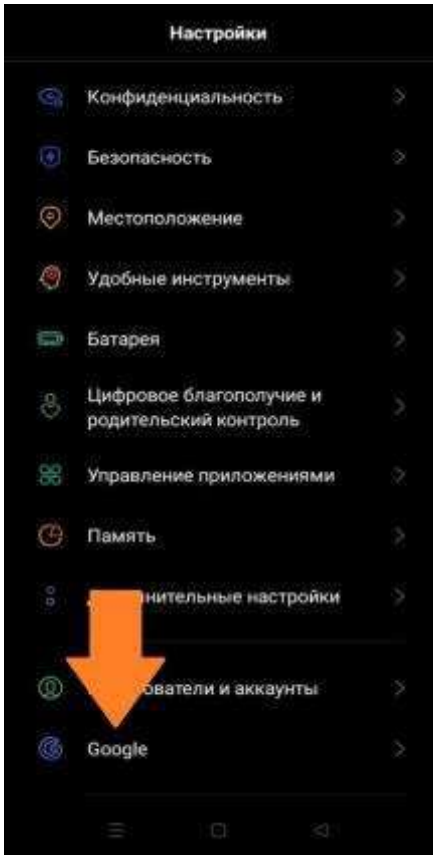
- нельзя отправлять свои личные фотографии или фотографии своих близких родственников незнакомым людям;

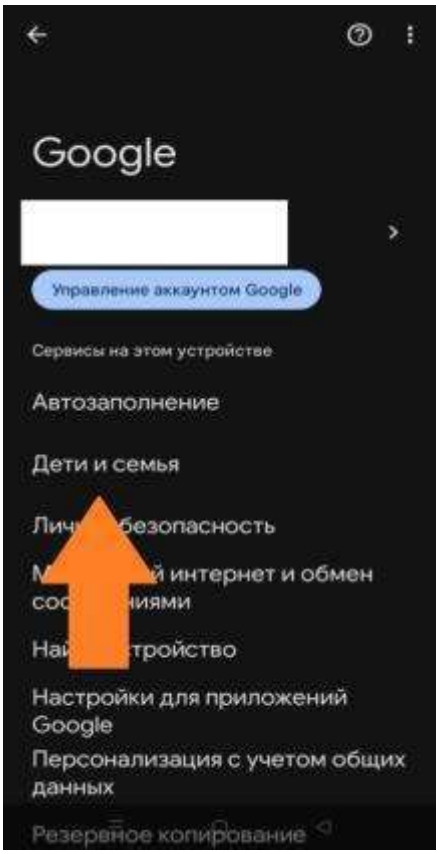
- нельзя посещать подозрительные сайты и оставлять на них свои личные данные.

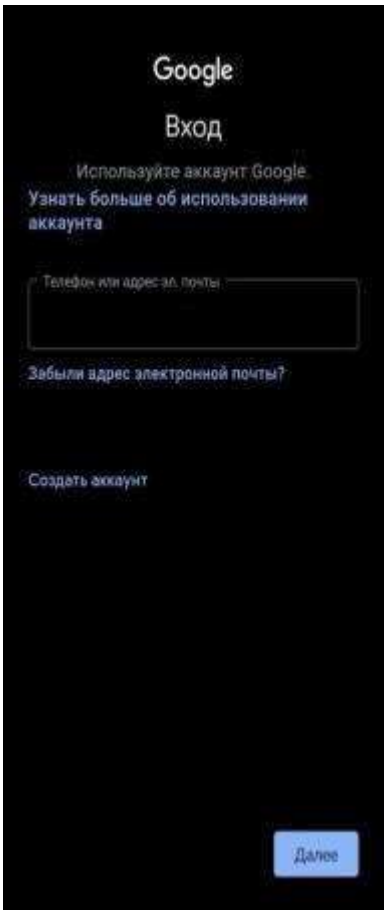
Распространенным способом мошенничества стало получение необходимой мошенникам информации в чатах онлайн игр.

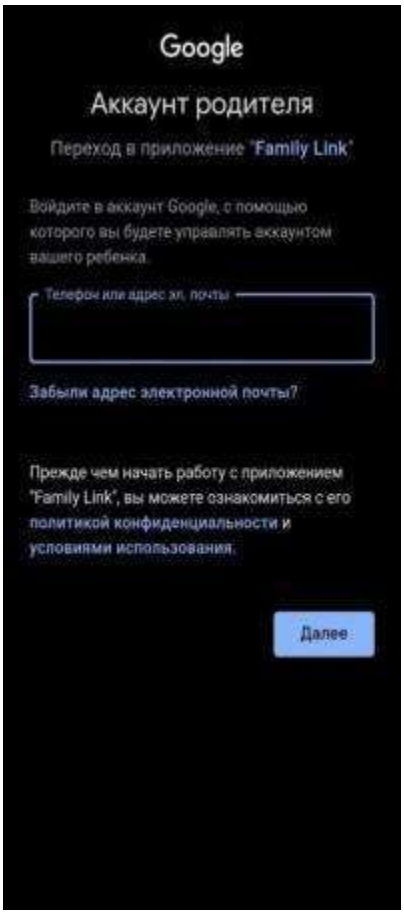
Так, мошенники знакомятся в чате с ребенком и предлагают ему купить необходимый для игры атрибут или персонажа. Ребенок диктует данные банковской карты родителей и с нее списывают средства.

Для того, чтобы контролировать ребенка необходимо настроить родительский контроль на всех устройствах.









Уделяйте больше внимания своему ребенку, чаще разговаривайте с ним, чтобы он делился с Вами о своем окружении, как прошел его день и внимательно следите за изменением в его поведении.

Контролируйте ребенка в социальных сетях, просматривайте кого он добавляет в друзья и с кем общается.

Внимательно следите за финансовыми тратами своего ребенка.

Если у него имеется банковская карта, кому и зачем он переводит денежные средства и какие осуществляет покупки.

Это простые правила помогут Вам уберечь Вашего ребенка от преступлений, совершаемых в отношении несовершеннолетних в цифровой среде.

Заключение

Изучив данные методические рекомендации вы сможете уберечь себя и своих близких от преступлений, совершаемых с использованием информационно-коммуникационных технологий, а также сможете воспрепятствовать вовлечению ребенка в преступную деятельность.

Необходимо постоянно заниматься повышением своей цифровой и финансовой грамотности, а также узнавать о новых способах мошенничества и способах защиты от них.

В этом Вам поможет официальный «Телеграм» канал Управления по борьбе с киберпреступлениями МВД по Республике Северная Осетия-Алания «**Кибервестник Алания**». Подписаться можно, отсканировав QR-код:

Будьте бдительны, и не попадайтесь на уловки мошенников!

УБК МВД по РСО-Алания