# ПРОКУРАТУРА КРАСНОЯРСКОГО КРАЯ

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

# ПО ПРОТИВОДЕЙСТВИЮ КИБЕРМОШЕННИЧЕСТВУ

г. Красноярск 2025 г.

## Введение

Потерпевшими от киберпреступлений являются граждане абсолютно всех категорий, включая как социально-незащищенные слои населения (инвалиды, пенсионеры, несовершеннолетние), так и люди, занимающие руководящие посты в организациях (предприятиях) всех форм собственности, имеющие несколько высших образований.

Злоумышленниками используются изощренные способы «выманивая» денежных средств, для чего используются различные «легенды», посредством изложения которых оказывается психологическое воздействие на граждан, которые под его воздействием выполняют все команды злоумышленников. Многие из потерпевших в дальнейшем в ходе общения с сотрудниками правоохранительных органов сообщают, что действовали «под гипнозом», в результате профессиональной манипуляции со стороны преступников.

В ходе совершения преступлений злоумышленники используют звонки с номеров, визуально приближенных к номерам телефонов правоохранительных органов, служб банков (например звонки на Ватсап с номера +900, 9ОО, тогда как официальный номер Сбербанка 900).

**Распространенные способы совершения преступлений:**

**1. Поддельный QR-код или приложение.**

Многие научились не поддаваться на распространенные схемы обзвонов, мошенники это учли, добавили в свой арсенал более изощренные методы.

Теперь они уже не требуют номер карты, а просят перейти по присланному QR-коду, который может привести на фишинговый сайт, либо содержит в себе вредоносный файл, заражающий смартфон. Еще одна разновидность – установка потенциальной жертвой по просьбе мошенника стороннего приложения. Предлог может быть любым – подтвердить запись к врачу, факт оплаты товара, заявку на участие в конференции и пр.

В результате злоумышленники получают доступ как к мобильному устройству, так и банковским приложениям, установленным на смартфоне жертвы, списывают деньги с банковского счета и даже оформляют кредиты.

**Что делать в этой ситуации:**

- не пользоваться QR-кодами и не устанавливать приложения, ссылки на которые получены от неизвестных, подозрительных источников;

- обращать внимание на ссылки, которые отображаются при сканировании кода. Если наименование сайта вызывает подозрение, лучше найти сайт самостоятельно в сети Интернет, либо скачать приложение через официальный магазин;

- прежде чем сканировать QR-коды с рекламных плакатов, вывесок, нужно убедиться, что оригинальное изображение не заклеено картинкой с подложным кодом;

- использовать антивирусные программы проверки QR-кодов, которые анализируют код на наличие вредоносного содержимого;

- не публиковать в социальных сетях личные документы с QR-кодами.

**2. Взлом аккаунта в Госуслугах**

Потерпевшему поступает смс или сообщение в мессенджере якобы от службы безопасности Госуслуг с уведомлением о подозрительной активности в аккаунте, для проверки просят связаться по указанному номеру телефону, по которому отвечает лже-представитель портала. А дальше все по сценарию – средства под угрозой в связи с оформлением третьими лицами заявок на кредиты, к работе подключаются псевдо-представители службы безопасности банка или ЦБ РФ, правоохранительных органов. Для их аннулирования заявок просят перевести личные накопления на «безопасный счет», а после – оформить заявки на кредиты.

**Что делать в этой ситуации:**

- не перезванивать на указанный в сообщении номер;
- зайти на официальный сайт Госуслуг, где указаны контакты, по которым можно связаться с представителем (номер телефона 8 800 100-70-10, либо с мобильного номер 115) для уточнения информации, либо обратиться в МФЦ.

**3. Установка вредоносного программного обеспечения**

Участились случаи обращения в правоохранительные органы потерпевших, которые сообщают о списании денежных средств с банковской карты на счета третьих лиц по неизвестным причинам (никто не звонил, доступа третьих лиц к телефону с установленным приложением банка не было). В ходе расследования устанавливается, что за некоторое время до совершения преступления потерпевший перешел по ссылке или QR-коду (например, проголосовал по просьбе знакомого в мессенджере, поучаствовал в розыгрыше), в результате на смартфон установилось вредоносное ПО, предоставившее удаленный доступ злоумышленникам к банковскому приложению.

**Что делать в этой ситуации:**

- устанавливать антивирусное ПО, своевременно обновлять его;
- не переходить по ссылкам, полученным из неизвестных источников.

**4. СМС от работодателя.**

Потерпевшему поступает СМС сообщение или сообщение в мессенджере от работодателя. О том, что с ним в ближайшее время свяжется сотрудник ФСБ или иной организации и следует с ним пообщаться, а также направляет ссылку в мессенджере Телеграм по которой нужно пройти.

После этого звонит сотрудник с именем указанным руководителем и сообщает о попытках перевода личных сбережений на иностранные счета, либо финансирование терроризма, либо ВС Украины и т.п.

В целях пресечения преступных операций потерпевшего убеждают прервать транзакции путем перевода денег (личных накоплений или путем взятия кредита) на счет, указанный злоумышленниками.

**Что делать в этой ситуации:**

Проверить номер с которого пришло сообщение, сверить его с реальным телефонным номером абонента (работодателя).

Для проверки подлинности адресата необходимо позвонить ему

с использованием других средств связи и уточнить отправлял ли он данное сообщение.

Если нет сомнений, что это злоумышленник, то необходимо заблокировать этого абонента и удалить сообщение. Ни в коем случае не вступать в переписку и не переходить по ссылкам, содержащимся в сообщении.

В случае если вы прошли по ссылке незамедлительно измените пароль своего аккаунта в Телеграм, проверьте устройства, подключенные к вашему аккаунту. Удалите любые незнакомые устройства. Обратитесь в службу поддержки Телеграм и сообщите о произошедшем. Убедитесь, что включена двухфакторная аутентификация для дополнительной защиты вашего аккаунта. Будьте осторожны с любыми другими подозрительными ссылками и сообщениями.

**5. Злоумышленники «продают» вашу квартиру или автомобиль.**

Звонившие представляются представителями службы безопасности коммерческого банка, Госуслуг, Центрального банка России, либо правоохранительного органа.

Сообщают о том, что ваши персональные данные с личного кабинета утекли и теперь преступники могут от вашего имени продать квартиру либо автомобиль, используя электронно-цифровую подпись.

В целях защиты вас убеждают срочно их продать – перевести вырученные деньги на «защищенный канал», «безопасный счет», «резервную ячейку».

**Что делать в этой ситуации:**

Прекратить разговор и перезвонить на официальную горячую линию учреждения, проверить сообщенную информацию.

Следует обратить внимание, что учреждения не звонят с использованием мессенджеров.

**6. Перевод денег на «безопасный счет», якобы для их сохранности.**

Звонившие представляются либо представителями службы безопасности коммерческого банка, Центрального банка России, либо правоохранительного органа и сообщают, что мошенники с использованием ваших персональных данных оформляют кредиты в различных банках и для того, чтобы предотвратить хищение денег с банковского счета вам необходимо личные сбережения срочно перевести на «безопасные счета». В ходе дальнейшего общения вам сообщают о необходимости оформления кредитов и их перевода.

Следует отметить, что ваше общение со злоумышленниками может быть длительным, в некоторых случаях осуществляется в течение нескольких месяцев, используется как телефонная связь, так и общение посредством мессенджеров (Ватсап, Вайбер, Телеграм и т.д.).

Еще одна разновидность преступной схемы – когда **звонят якобы сотрудники правоохранительных органов и сообщают что в отношении вас возбуждено уголовное дело в связи с финансированием экстремисткой, террористической деятельности**, поскольку с вашего банковского счета осуществлен перевод денежных средств в недружественное государство.

В ходе общения злоумышленники могут присылать фото удостоверений, повесток, постановлений о возбуждении уголовного дела, подписок

о неразглашении следственной тайны и т.д.

**Что делать в этой ситуации:**

Прекратить разговор и перезвонить на официальную горячую линию учреждения, проверить сообщаемую информацию.

Следует обратить внимание, что учреждения не звонят с использованием мессенджеров.

Кроме того, следует помнить, что «безопасных счетов» не существует, а представители Центрального Банка России, не осуществляют работу с физическими лицами.

**7. Звонок злоумышленника под видом мобильных операторов, которые сообщают, что срок действия вашей сим-карты истек либо истекает договор обслуживания, а для его продления необходимо сообщить** код, который поступит в СМС, либо пройти по ссылке, в противном случае сим-карта будет заблокирована.

Важно знать, что у сим-карты нет срока действия, сотовые операторы перевыпускают сим-карты только по просьбе потребителей в случае физического износа, потери, необходимости другого формата.

Выполнив требования мошенников и сообщив код из СМС, либо пройдя по ссылке вы отдаете в руки злоумышленников доступ в свой личный кабинет на сайте оператора связи, после чего мошенники имеют возможность устанавливать переадресацию сообщений на нужный им номер, что позволит сменить пароль от мобильного банка и похитить денежные средства.

Вторая разновидность таких преступлений – з**вонок злоумышленника об истечении срока действия медицинского страхового полиса, а для его продления необходимо сообщить** код из СМС доступа к аккаунту Госуслуг, в дальнейшем следует оформление заявок на кредиты в банках, получение персональных данных, таких как сведения о доходах, наличие банковских счетов и т.д.

**Что делать в этой ситуации:**

Прекратить разговор.

Если вы сообщили код из СМС необходимо незамедлительно обратиться к сотовому оператору с просьбой заблокировать номер телефона.

В случае Госуслуг необходимо заблокировать свою учетную запись. Сделать это можно либо через мобильное приложение Госуслуги, либо через техподдержку МФЦ, либо лично обратиться в МФЦ.

**8. Сдача налоговых деклараций и справок о доходах.**

Звонившие представляются сотрудниками Госуслуг, управления по делам Президента России, сообщают, что в рамках декларационной кампании проверяют персональные данные лиц, сдавших налоговые декларации либо декларации о доходах.

Со слов злоумышленников – для подтверждения следует назвать паспортные данные и код из СМС. Результат – списание денег с ваших счетов, оформление на ваше имя кредита.

**Что делать в этой ситуации:**

Прекратить разговор.

Никогда не сообщайте по телефону код из СМС, а также свои персональные данные (паспорта, ИНН, СНИЛС, номера банковских карт, и т.п.)

Если вы сообщили код из СМС для подтверждения транзакции (банковского перевода) необходимо незамедлительно обратиться на горячую линию банка и сообщить о данном факте.

В случае взлома учетной записи Госуслуг необходимо заблокировать учетную запись. Сделать это можно либо через мобильное приложение Госуслуги, либо через техподдержку МФЦ, либо лично обратиться в МФЦ.

**9. Взлом либо копирование аккаунта пользователя в мессенджерах Ватсап, Вайбер, Телеграм, социальных сетей Вконтакте** и дальнейшее направление сгенерированных искусственным интеллектом (нейросетью) голосовых либо видео сообщений от имени вашего знакомого, родных, коллег и т.д. (у которых ранее взломали аккаунт), которые полностью копируют их голос и видеоизображение, используя при этом ранее отправленные видео и аудио сообщения вашего знакомого.

А дальше все по типичной схеме – у вас просят одолжить взаймы, присылают фото банковской карты для перевода денежных средств.

**Что делать в этой ситуации:**

В данной ситуации важно убедиться, что вы общаетесь именно с вашим знакомым, связавшись с ним используя другие средства связи.

Сделав это, вы обезопасите себя и предупредите вашего знакомого о том, что от его имени действуют мошенники и возможно его аккаунт был взломан.

Для того, чтобы не потерять контроль над вашим аккаунтом никогда не переходите по незнакомым ссылкам, не скачивайте программы из неподтвержденных источников, используйте двухфакторную аутентификацию ваших аккаунтов.

**10. Хищение денежных средств через систему быстрых платежей (СБП).**

Например, покупатель на сайте оставляет заявку на приобретение товара, ему поступает звонок якобы от сотрудника магазина, предлагается скидка на товар, но только при условии оплаты через СБП или QR-коду, затем злоумышленник присылает в мессенджер ссылку, ведущую на страницу с формой оплаты по QR-коду. Покупатель подтверждает платеж и денежные средства поступают на счет мошенника.

**Что делать в этой ситуации:**

Важно в такой ситуации связаться со службой поддержки онлайн-магазина, через официальный сайт или приложение. Не сохранять для оплаты в личных кабинетах банковские карты, при возможности заведите отдельную карту для оплаты покупок онлайн.

**11. Заработок на бирже, заманивание прибыльными инвестициями** – получившая широкое распространение в последнее время схема, в результате

использования которой причиняется наиболее крупный ущерб. Преступниками создается максимальная видимость того, что общение происходит с представителями крупной инвестиционной площадки, их сайты имеют видимое сходство с банковскими организациями (например, Газпром-инвестиции, РБК-инвестиции, Тинькофф-инвестиции и т.д.), назначается личный брокер, общение с которым может осуществляться даже посредством видеозвонков.

Под их руководством создается якобы личный кабинет на торговой площадке, в котором отображаются все внесенные денежные средства, и прибыль. Однако их дальнейший вывод невозможен.

**Что делать в этой ситуации:**

Игнорировать предложение. Быть бдительным и не поддаваться на манипуляции мошенников. Проверять из других источников представленную вам информацию. Следует обратить внимание на номера телефонов с которых поступило предложение, а также то, что коммерческие организации не звонят с использованием мессенджеров.

**12. Рассылка налоговых писем о выявлении подозрительных транзакций и активности налогоплательщика.**

В поддельном сообщении предлагается пройти дополнительную проверку и предоставить сведения по запросу налоговой службы. Так мошенники могут запросить кассовые документы, счета-фактуры, отчетные документы.

Далее для прохождения проверки предлагается обратиться к указанному в письме инспектору под угрозой блокировки счетов налогоплательщика.

**Что делать в этой ситуации:**

Игнорировать сообщение. Важно помнить, что ФНС не рассылает такого рода письма и не имеет отношения к ним, такие письма открывать не рекомендуется, как и переходить по ссылкам.

**13.** Схема «**ваш родственник попал в ДТП**». Наиболее подвержены данному виду преступлений пожилые граждане. Злоумышленник представляется либо родственником потерпевшего, либо представителем правоохранительного органа и сообщает, что для освобождения от уголовной ответственности и наказания в виде лишения свободы срочно необходимо передать денежные средства (взятку).

**Что делать в этой ситуации:**

Связаться с родственником и проверить сообщенную информацию. В случае если абонент недоступен, то ни в коем случае не предпринимать действия по передаче денежных средств, сообщить о происходящем в правоохранительные органы.

**14. Разновидность предыдущей схемы – «перевод денег на Украину,** обвинение в государственной измене». На стационарный телефон пожилого человека поступает звонок от псевдо-сотрудника МВД/ФСБ/прокуратуры и т.д., который сообщает, что от имени потерпевшего осуществляются переводы денежных средств в недружественные государства. В целях

проверки/инвентаризации необходимо передать все имеющиеся дома наличные средства курьеру/помощнику следователя. В случае отказа поступают угрозы о прибытии правоохранительных органов с обыском, в ходе которого денежные средства будут изъяты принудительно и обращены в доход государства.

**Что делать в этой ситуации:**

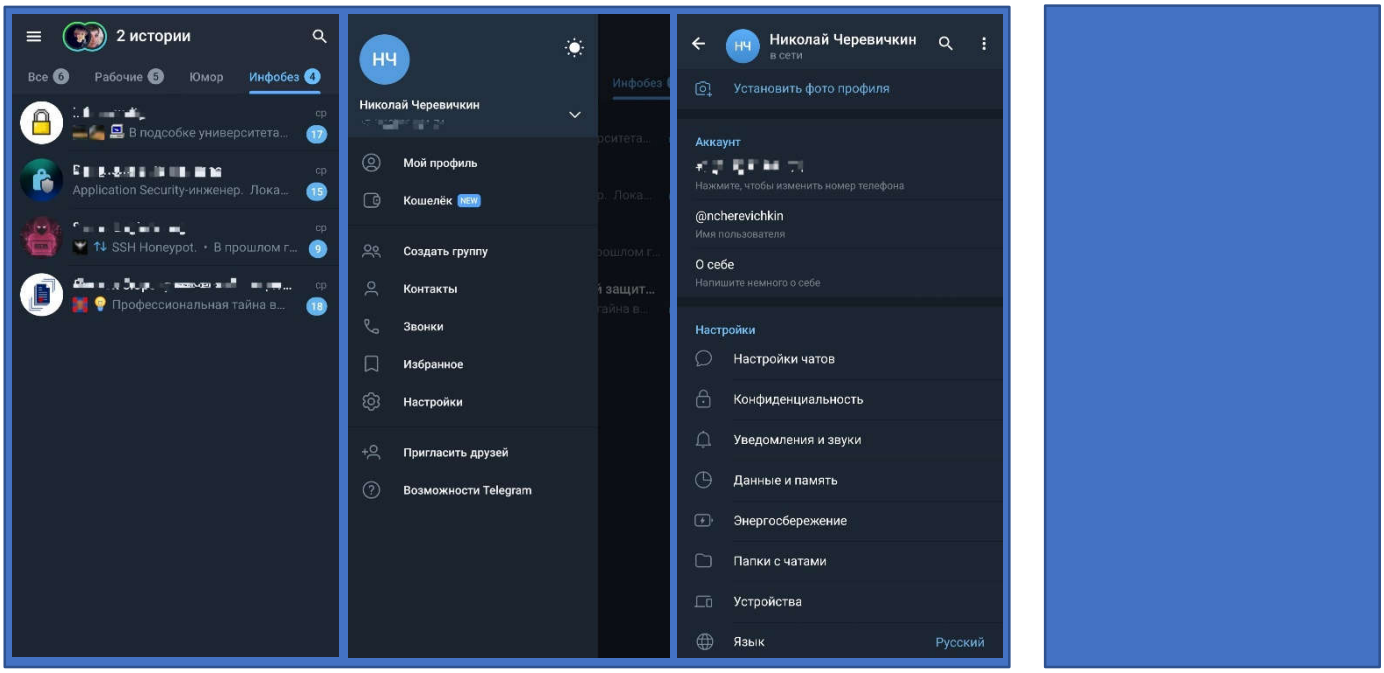
Ни в коем случае не предпринимать действия по передаче денежных средств, сообщить о происходящем в правоохранительные органы.

## Настройки конфиденциальности в мессенджере «Telegram»

В целях предотвращения поступления звонков и СМС сообщений в мессенджере «Telegram» от неизвестных источников необходимо обеспечить соответствующую настройку конфиденциальности. Для этого необходимо выполнить следующий порядок действий.

1. Запускаем приложение «Telegram» и переходим в настройки конфиденциальности

Android IOS

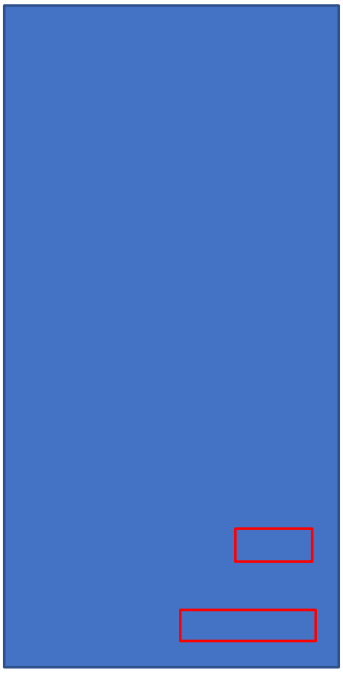



2. Для блокировки зблокировки звонков и сообщений от неизвестных номеров в настройках конфиденциальности «Telegram» необходимо ограничить круг лиц, которые могут направлять сообщения и осуществлять звонки на ваш аккаунт.

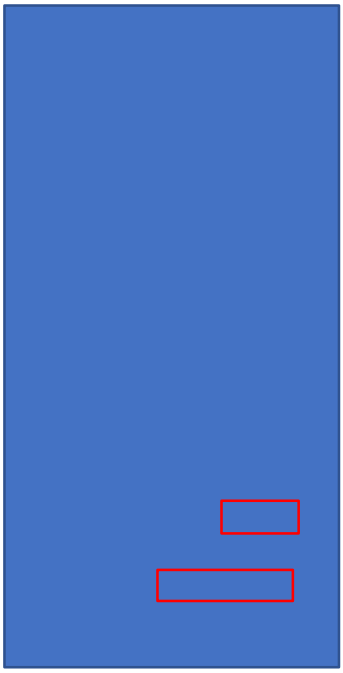
Для этого в настройках конфиденциальности в разделах «Звонки» и «Сообщения» необходимо установить разрешения только для «контактов». В этом случае осуществлять звонки и направлять СМС сообщения в мессенджере

«Telegram» смогут только абоненты, чьи номера телефонов записаны в телефонной книге Вашего мобильного устройства.

Android



IOS



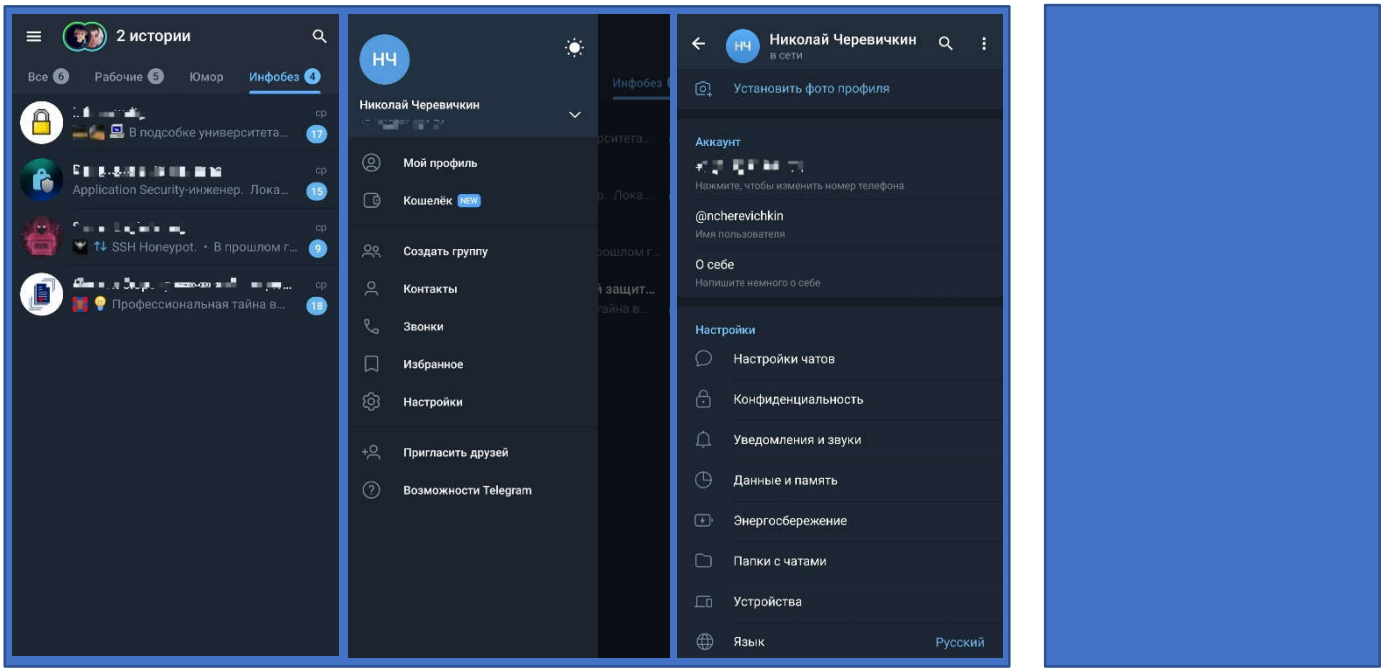
**Настройка двухфакторной аутентификации**

Для дополнительной защиты аккаунтов в социальных сетях, мессенджерах и иных интернет-ресурсах необходимо использовать двухфакторную аутентификацию. Это позволит минимизировать риски взлома аккаунтов, а также позволит обеспечить безопасное восстановление доступа к аккаунту.

Для настройки двухфакторной аутентификации в мессенджере «Telegram» необходимо выполнить следующий порядок действий:

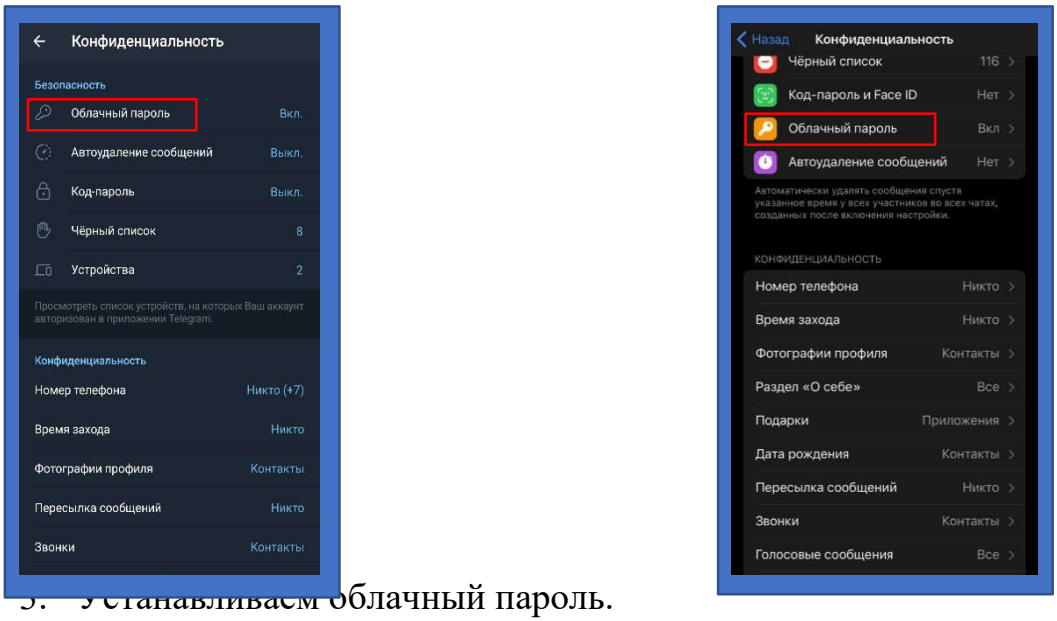
1. Запускаем приложение «Telegram» и переходим в настройки конфиденциальности

Android IOS



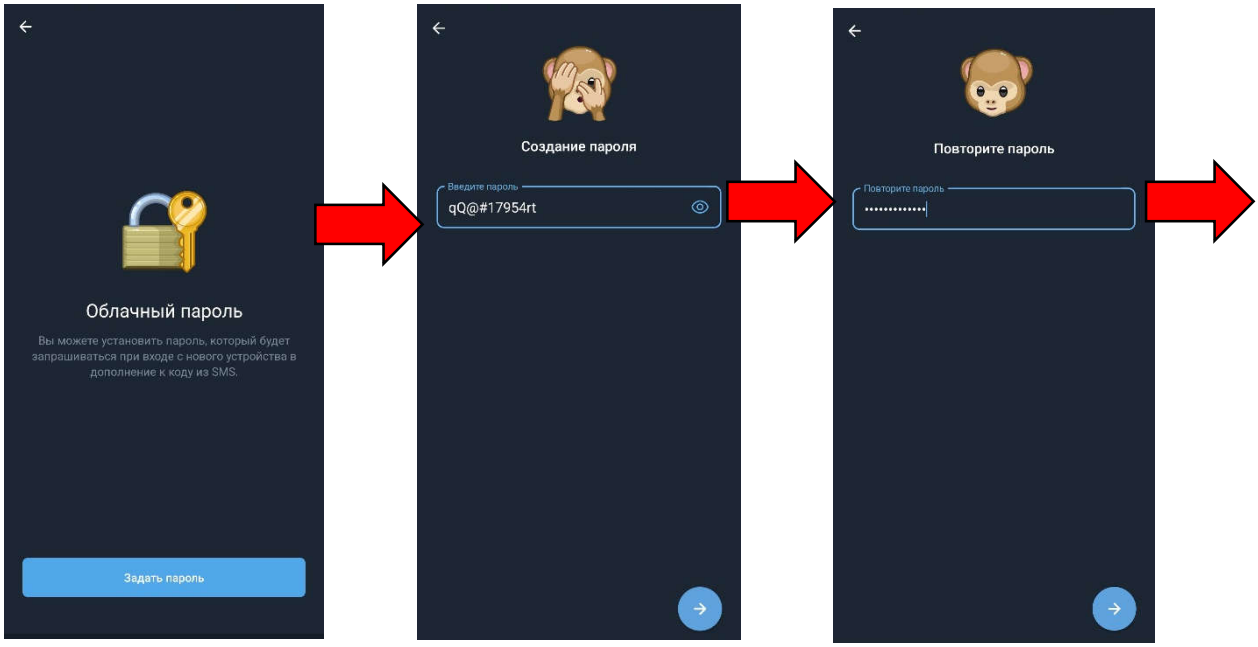

2. Переходим в 2 раздел «Облачный пароль»

Android IOS



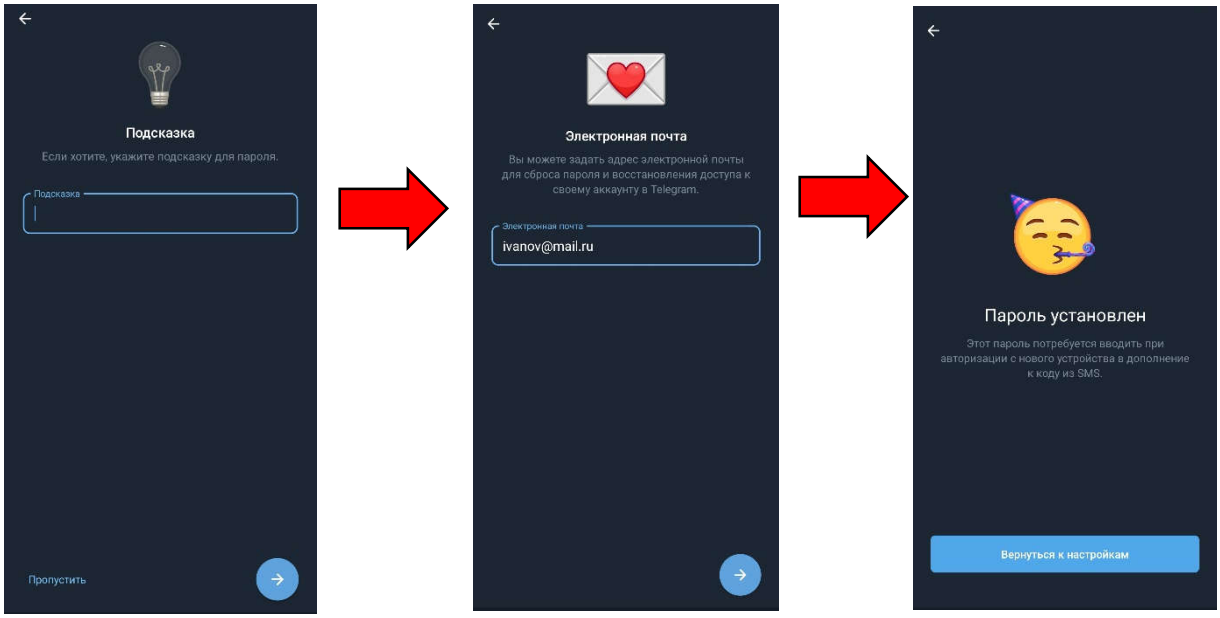

3. Устанавливаем облачный пароль.

Пароль не должен быть простым содержать имена, даты рождения и иные сведения, которые легко может вычислить злоумышленник.




Правильное использование подсказки для пароля позволяет вспомнить даже сложный пароль спустя длительное время.

Для повышения безопасности, а также упрощения возможности восстановления доступа к личному аккаунту рекомендуется указать личную электронную почту, на которую будут направляться коды подтверждения в случае сброса или смены пароля.



## Общие правила и рекомендации по снижению уровня уязвимости перед угрозами со стороны IT-преступлений

1. Создавайте уникальные и надежные пароли, многофакторную аутентификацию, а также обеспечивайте регулярную смену паролей в мессенджерах, социальных сетях, государственных порталах и иных интернет ресурсах.

! Важно помнить, что взлом аккаунта в социальных сетях может осуществляться через привязанную к нему электронную почту, поэтому необходимо обеспечить надежную парольную защиту личного электронного почтового ящика.

2. Не переходите по ссылкам в письмах или сообщениях от неизвестных отправителей.

3. Проверяйте детали: опечатки в адресе сайта, странные доменные зоны и ошибки в текстах – являются признаками вредоносных страниц.

4. Не публикуйте личные данные на подозрительных сайтах, такие как номер телефона, адрес электронной почты, номер банковской карты.

5. Не стоит доверять сообщениям от неизвестных номеров, всегда проверяйте номер абонента, который Вам звонит или пишет СМС сообщение.

6. Используйте надежные спам-фильтры и определители номеров, которые позволяют выявлять и блокировать звонки от подозрительных абонентов.

Услуги антиспама предоставляют большинство сотовых операторов. Кроме того, существуют безопасные сервисы и приложения позволяющие настроить спам фильтр на самом смартфоне (определитель номера от Яндекс, Kaspersky Who Calls и т.д.).

Важно! Не используйте сервисы по определению номеров телефонов, которые запрашивают и предоставляют персональные данные о владельцах номеров телефонов («Getcontact», NumBuster, и т.д.). Использование подобных приложений и сервисов позволяет злоумышленникам идентифицировать Ваш номер телефона, а также номера телефонов, записанных в телефонной книге Вашего смартфона.

7. Периодически проверяйте свой гаджет на наличие вирусов и вредоносных программ. При обнаружении, их необходимо вылечить и обезвредить.

8. При потере или компрометации данных своей банковской карты, необходимо обратиться в банк и заблокировать карту. Не забывайте периодически следить за Вашей банковской активностью. В случае выявления подозрительных операций, которые Вы не совершали, необходимо обратиться в банк.

9. Порталом Госуслуги предоставлены возможности:

- установить самозапрет на выдачу кредитов,
- установить запрет на совершение регистрационных сделок с недвижимостью без личного участия в регистрирующем органе,
- проверить информацию о зарегистрированных на Ваше имя сим-картах, прекратить оказание услуг по неиспользуемым номерам.

## ВАЖНО ЗНАТЬ!!!

Используемые мошенниками схемы постоянно меняются, «подстраиваясь» под общественно-политическую обстановку, значимые события в государстве. Распространены также следующие способы:

- обман во время кампании по сдаче налоговых деклараций (поступление письма от злоумышленников на электронную почту от якобы сотрудников налоговой службы с требованием представить декларацию по специальной ссылке при переходе на которую необходимо ввести личные данные и реквизиты банковской карты якобы для идентификации налогоплательщика);

- хищение денег и имущества под предлогом обновления банкнот (звонок от мошенников с указанием о необходимости проверки подлинности банкнот Банка России, для чего убеждают установить стороннее приложение, посредством которого получают удаленный доступ к телефону жертвы; также используется поквартирный обход от якобы специалистов социальных служб, которые убеждают обменять денежные купюры на поддельные);

- использование ложных аккаунтов руководителей Банка России, правоохранительных органов, органов прокуратуры, содержащих реальные данные, взятые из открытых источников (фамилию, имя, отчество, фото);

- сообщение клиентам банков об утечке персональных данных;

- обещание помочь с компенсацией ранее похищенных денег;

- обмен кэшбека на рубли;

- сообщения с официального бота «Советы по безопасности» о якобы предстоящей блокировке аккаунта из-за «мошеннических действий». Они требуют перейти по ссылке в «Системный центр» для проверки, после чего ваш аккаунт может быть взломан и украден.

Все более широкое распространение получают следующие способы вовлечения несовершеннолетних в преступную деятельность:

1. трудоустройство в качестве курьеров;

2. сдача в аренду за плату аккаунтов в мессенджерах и социальных сетях.

Указанные действия могут повлечь привлечение к уголовной ответственности несовершеннолетних за совершение преступления в составе ОПГ.

Также все чаще злоумышленники звонят несовершеннолетним под видом представителей служб безопасности и вынуждают осуществить перевод денежных средств со счетов родителей на якобы безопасные счета!

Динамика распространения данных видов преступлений представляет латентную угрозу межрегионального характера, в этой связи создание эффективного противодействия является одной из первостепенных задач для правоохранительных органов региона.

## БУДЬТЕ БДИТЕЛЬНЫ!!!