УПРАВЛЕНИЕ МВД РОССИИ ПО Г. УЛАН-УДЭ

«Профилактика преступлений, совершаемых с использованием информационно-телекоммуникационных технологий»

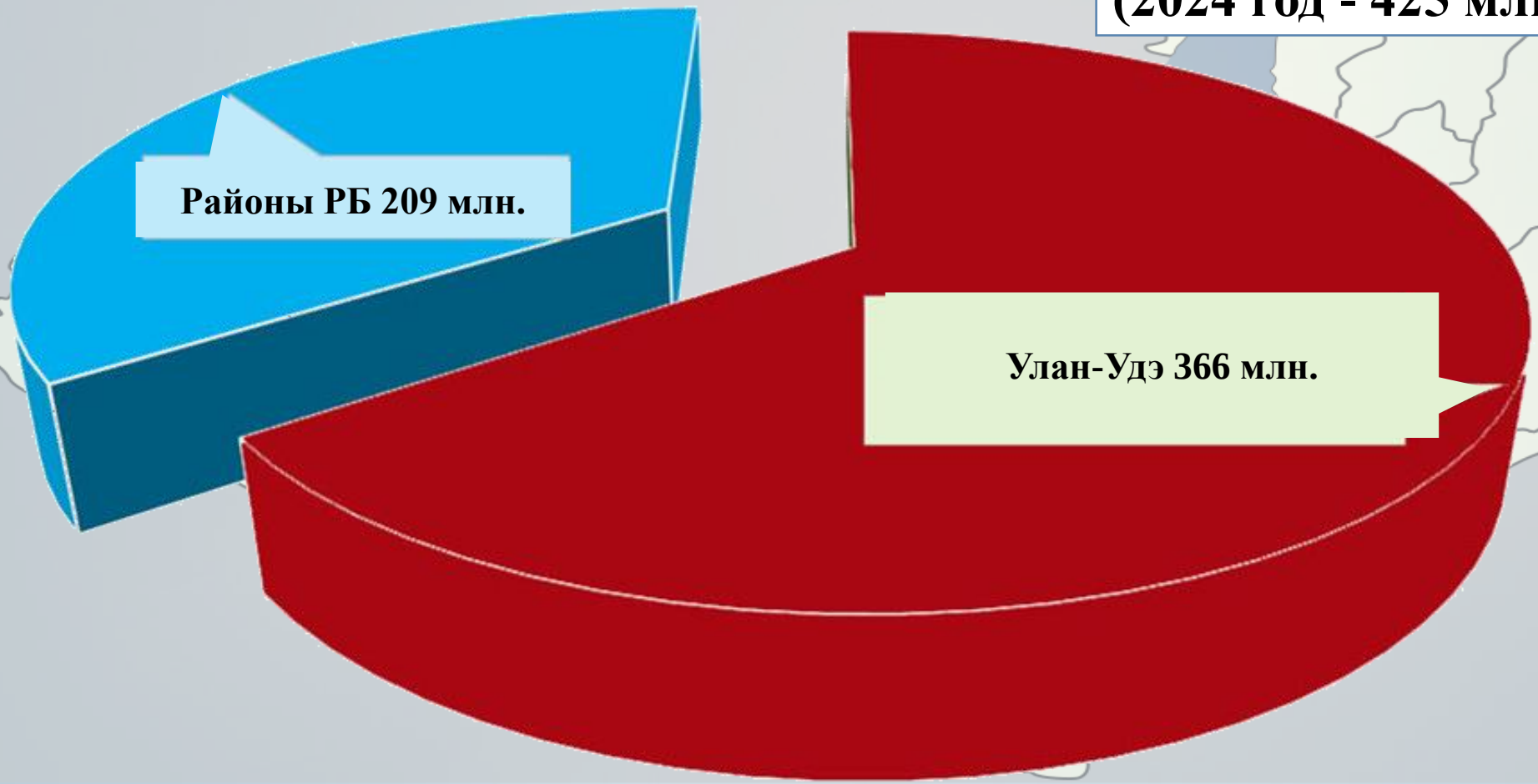
СТАТИСТИЧЕСКИЕ ДАННЫЕ ПО ИТОГАМ 2025 года

- **По Республике зарегистрировано:**
- 5775 преступлений в сфере ИТТ (снижение на 7,5%) из них:
- 3288 мошенничеств (рост на 15,5 %)
- 824 краж с банковских счетов (снижение на 16,0 %);
- 1186 взлома портала «ГОСУСЛУГИ» (снижение на 36,1 %).

- **По г. Улан-Удэ зарегистрировано:**
- 3381 преступлений в сфере ИТТ (снижение на 11,8 %) из них:
- 1857 мошенничества (рост на 8,5 %);
- 512 краж с банковских счетов (снижение на 18,1%);
- 601 взлома портала «ГОСУСЛУГИ» (снижение на 41,9 %).

Материальный ущерб по итогам 2025 года составил:

По Республике 575 млн.
(2024 год - 673 млн меньше на 98 млн.)
По г. Улан-Удэ 366 млн.
(2024 год - 425 млн меньше на 59 млн.)



Категории потерпевших на территории г. Улан-Удэ

	За 2025 год	Сумма ущерба
Рабочие (в т.ч. в коммерческой сфере, гос. и муниципальные служащие)	**766**	**136 млн.**
Пенсионеры	**363**	**72 млн.**
Не работающие	**522**	**70 млн.**
Студенты	**170**	**26 млн.**
Родственники участников СВО	**12**	**20 млн.**
Работники в сфере здравоохранения	**121**	**15 млн.**
Преподаватели	**73**	**13 млн.**
Военнослужащие	**59**	**12 млн.**
Школьники	**58**	**2 млн.**

Перевела мошенникам более 7 млн. рублей

Пожилые люди остаются приоритетной мишенью для мошенников

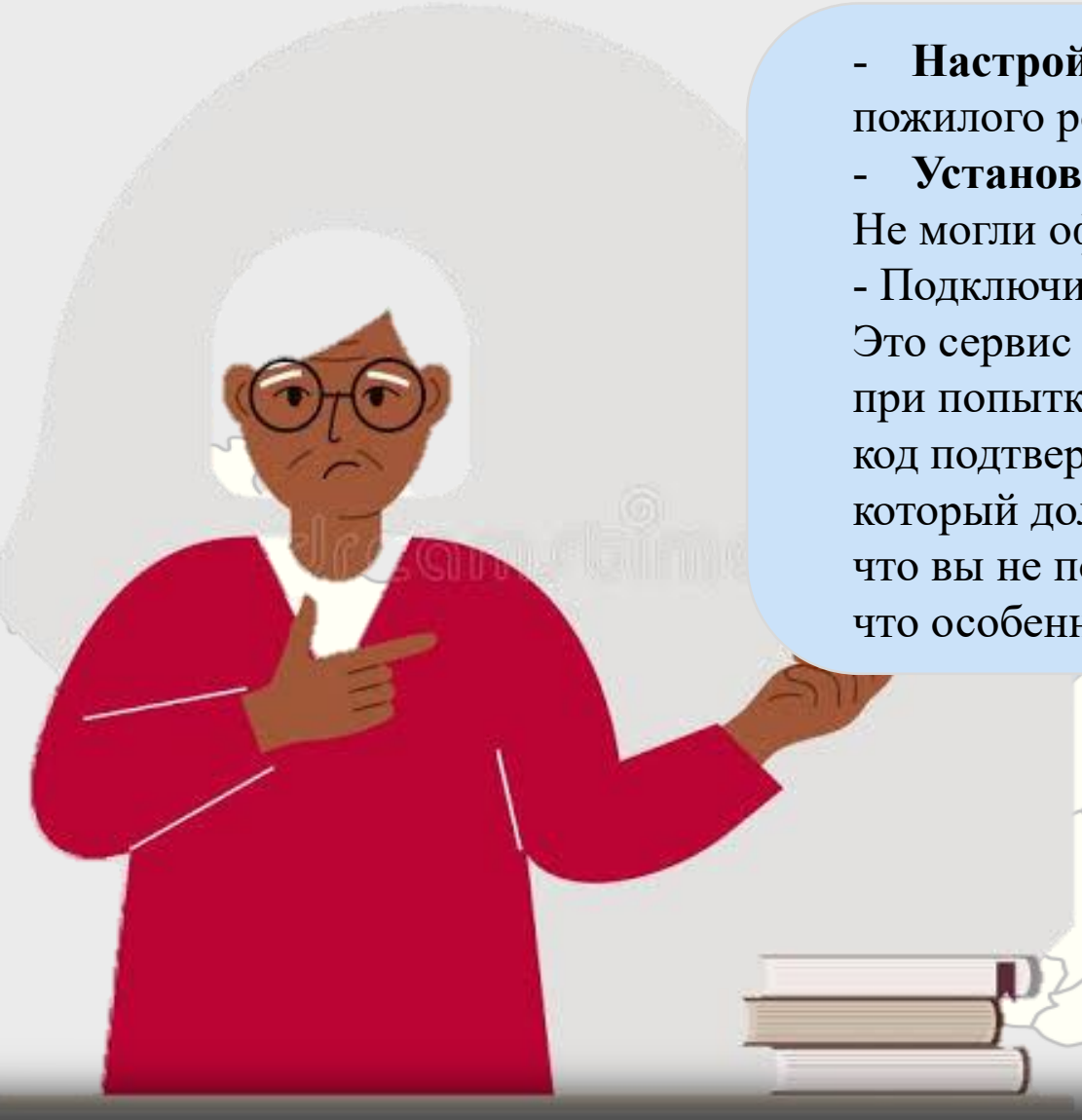
73-х летней жительнице г. Улан-Удэ поступил звонок от «сотрудника Энергосбыта», для замены электросчетчиков, попросили код из смс

Далее позвонил мужчина, представился «страховым агентом», сообщил, что ранее звонили мошенники, что могут снять все её сбережения, что бы этого не случилось, необходимо перевести деньги на «БЕЗОПАСНЫЙ СЧЕТ».

Женщина согласилась и выполнила все условия, осуществила перевод на «БЕЗОПАСНЫЙ СЧЕТ» более 2 млн.рублей

Далее по указанию мошенников продала 3-х комнатную квартиру за 5 млн. рублей, и все деньги так же перевела мошенникам.

КАК ЗАЩИТИТЬ БЛИЗКИХ?

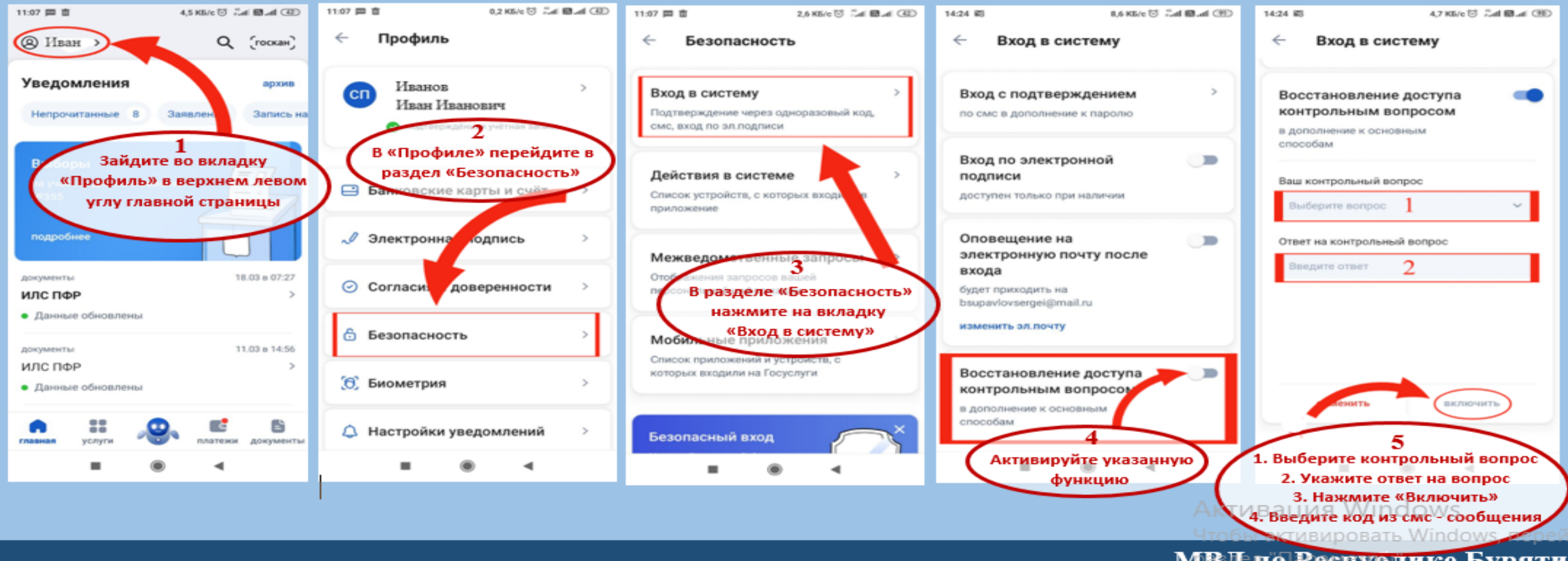


- **Настройте безопасность:** установите на телефон пожилого родственника защиту аккаунтов на портале «ГОСУСЛУГИ»;
- **Установите самозапрет** на оформление займов, что бы мошенники Не могли оформить кредиты и микрозаймы;
- Подключите функцию **«Доверенное лицо»** в портале «ГОСУСЛУГИ»: Это сервис дополнительной зашиты аккаунта от мошенников: при попытке восстановления пароля или смены данных код подтверждения приходит не только вам, но и доверительному лицу, который должен его подтвердить, убедившись, что вы не под влиянием злоумышленников, что особенно полезно для детей и пожилых людей.

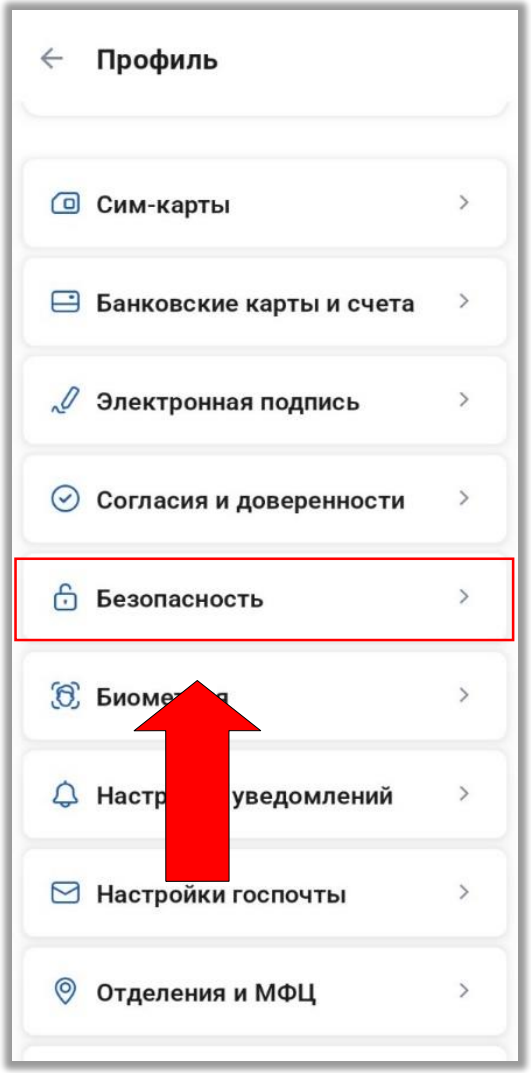
МЕРЫ ЗАЩИТЫ ОТ ВЗЛОМА ЛИЧНОГО КАБИНЕТА ПОРТАЛА «ГОСУСЛУГИ»:

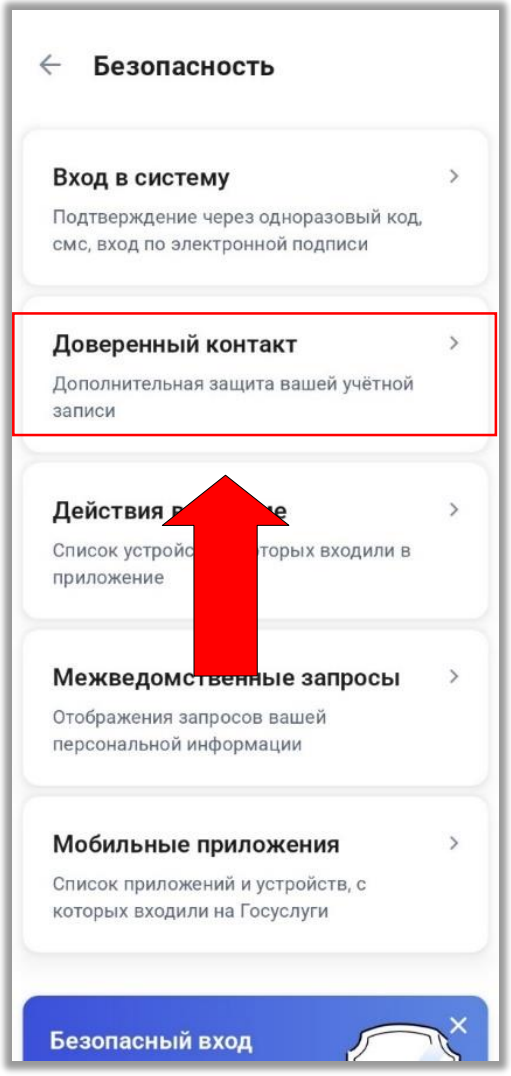
1. НАСТРОЙТЕ ФУНКЦИЮ «ВОССТАНОВЛЕНИЕ ДОСТУПА КОНТРОЛЬНЫМ ВОПРОСОМ»;
2. НИКОМУ НЕ СООБЩАЙТЕ КОДЫ ИЗ СМС-СООБЩЕНИЙ, ПОСТУПИВШИХ ОТ ПОРТАЛА «ГОСУСЛУГИ»;
3. В СЛУЧАЕ ДЛИТЕЛЬНОГО НЕИСПОЛЬЗОВАНИЯ ИЛИ ИЗМЕНЕНИЯ АБОНЕНТСКОГО НОМЕРА ОТКРЕПИТЕ ЕГО ОТ ЛИЧНОГО КАБИНЕТА ПОРТАЛА «ГОСУСЛУГИ».

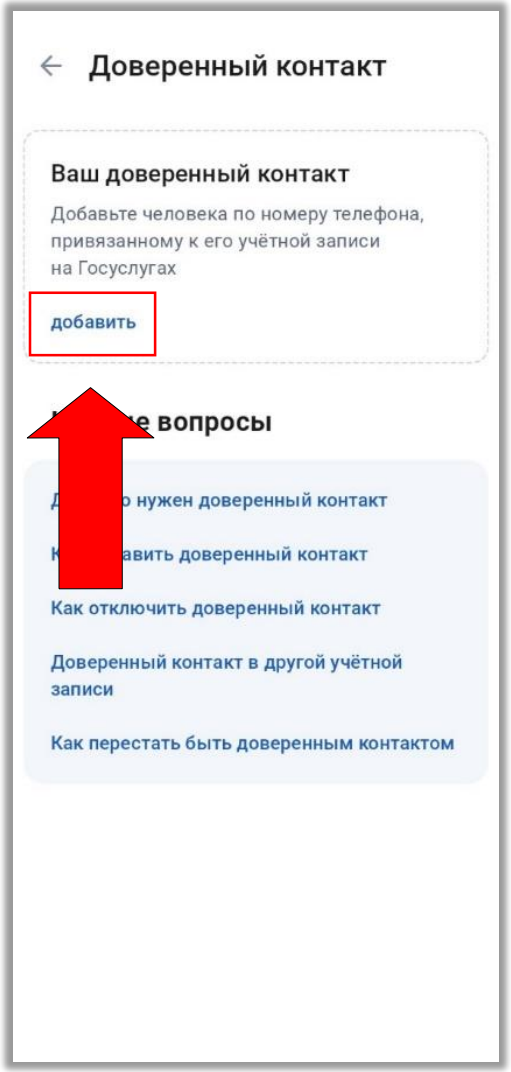
ПОШАГОВАЯ ИНСТРУКЦИЯ ПОДКЛЮЧЕНИЯ ФУНКЦИИ «ВОССТАНОВЛЕНИЕ ДОСТУПА КОНТРОЛЬНЫМ ВОПРОСОМ»:



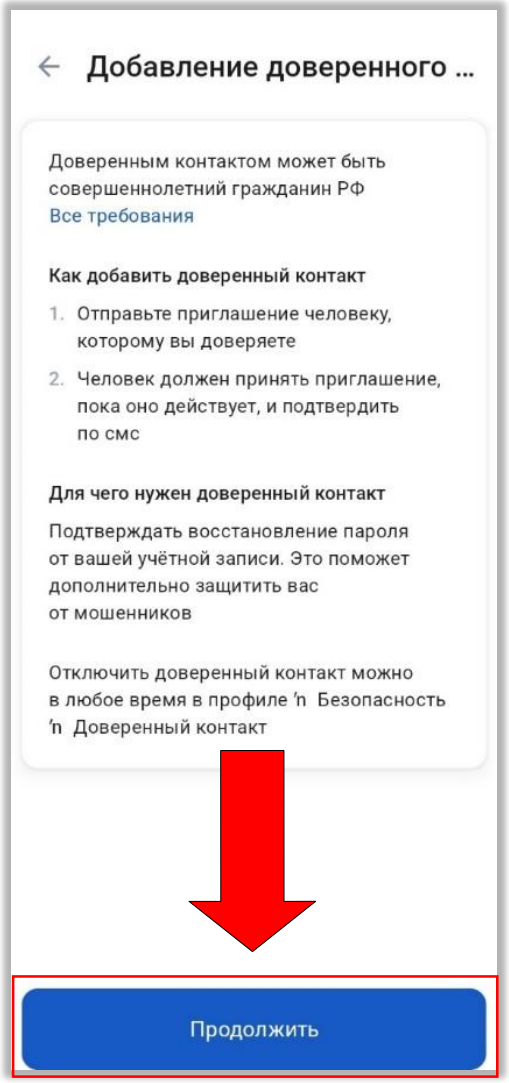
Как подключить «Доверенный контакт» в «Госуслуги»

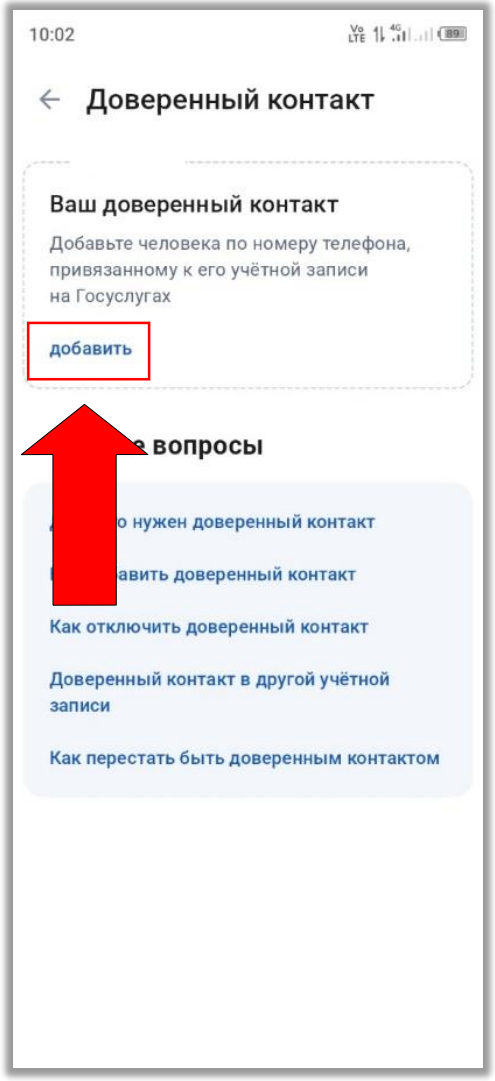


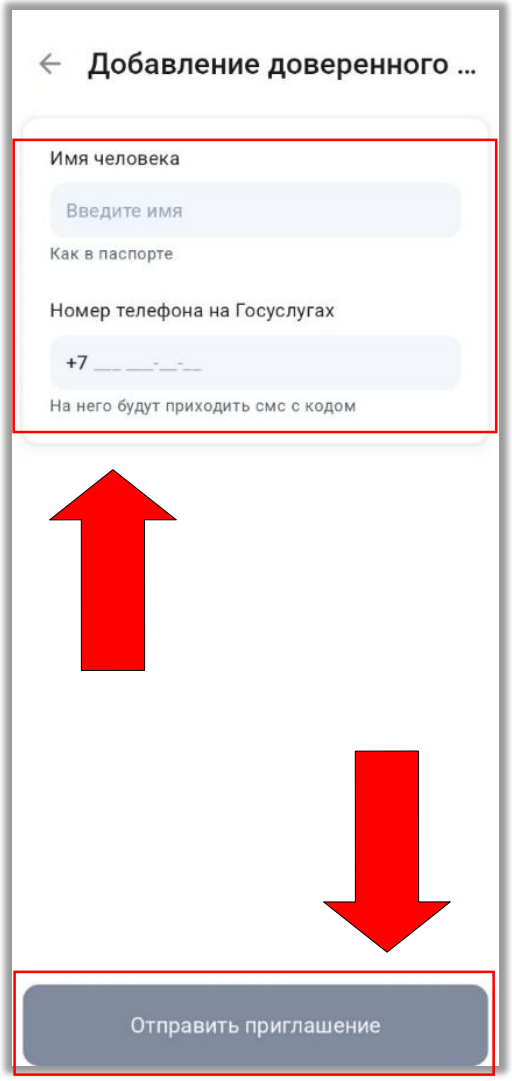


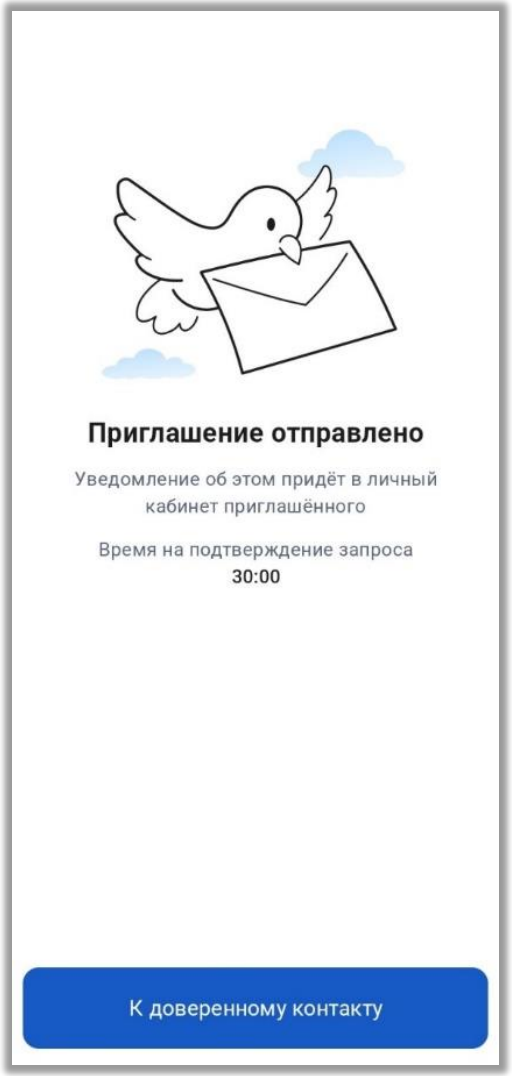


Как подключить «Доверенный контакт» в «Госуслуги»

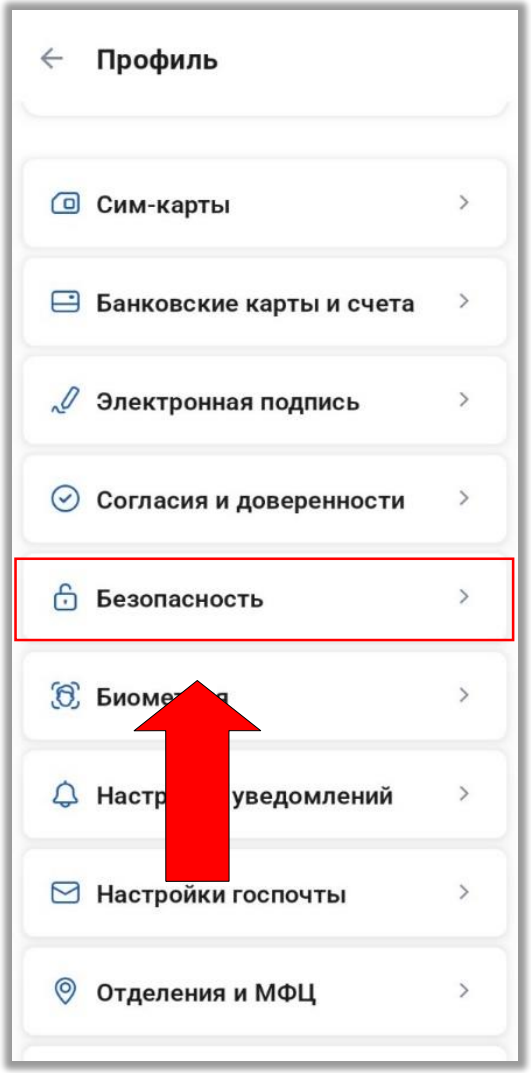


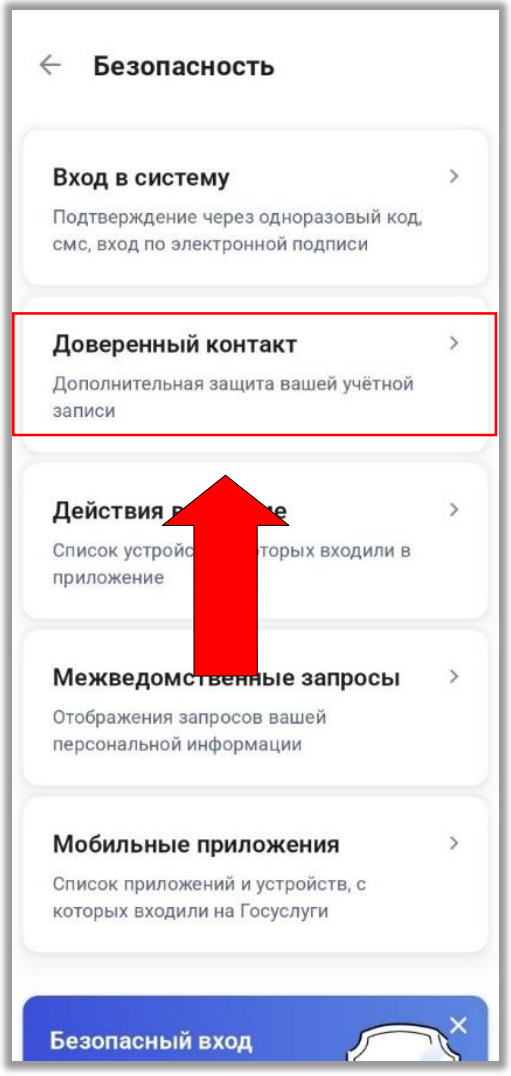


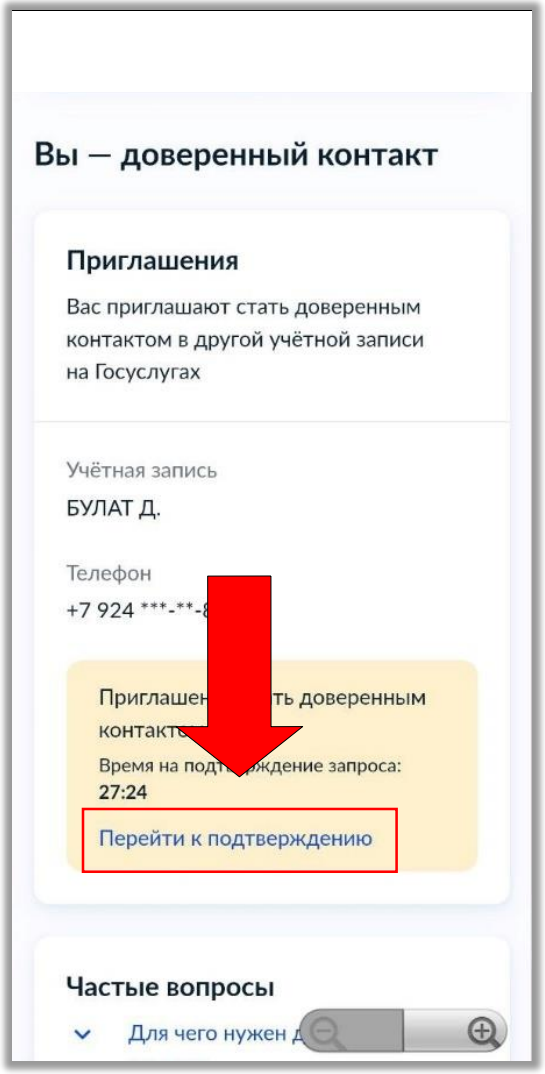




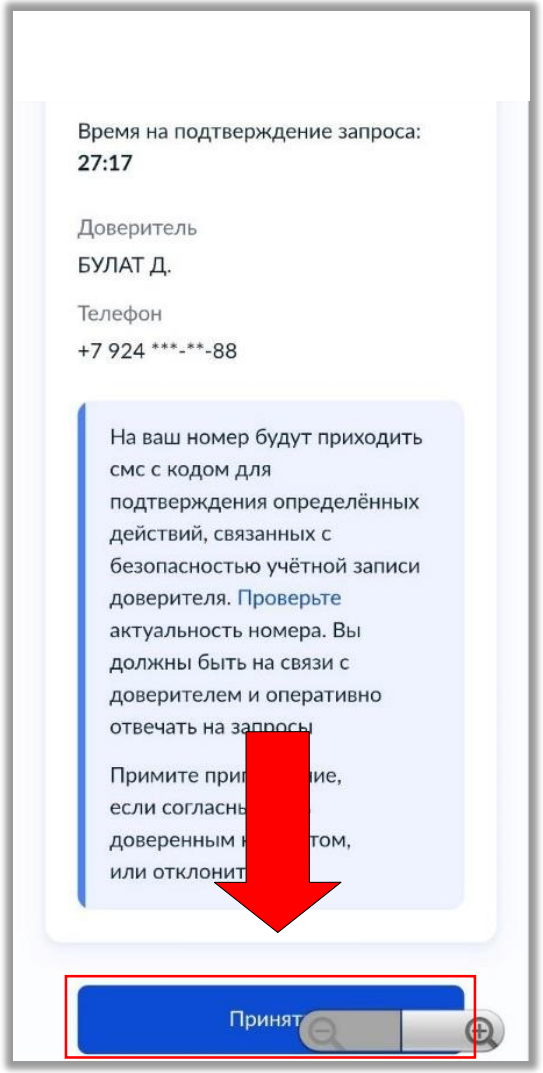
Как стать доверенным контактом в «Госуслуги»

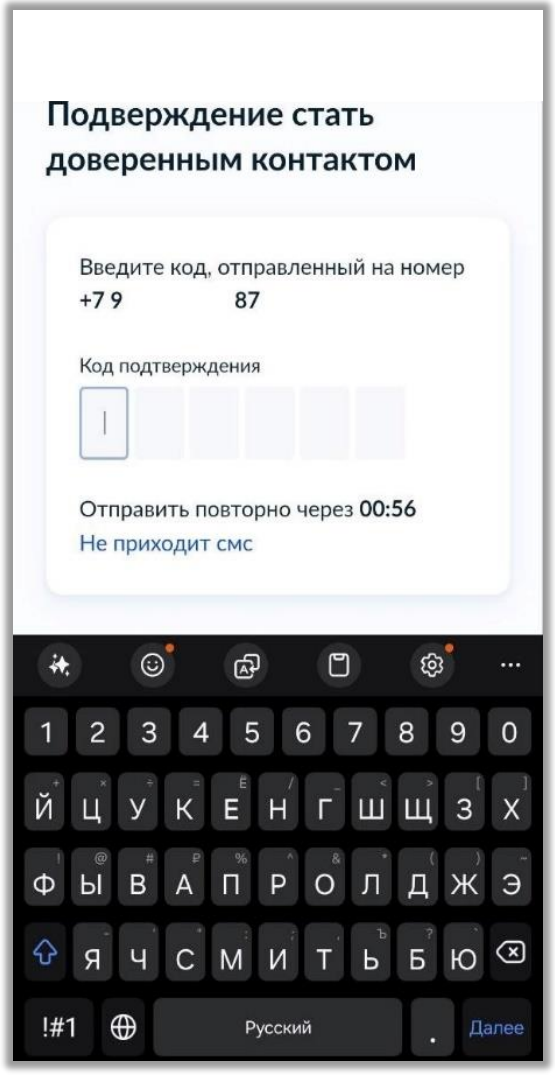






Как стать доверенным контактом в «Госуслуги»





Способы и схемы IT-преступлений

1

Телефонные мошенничества с использованием **аккаунтов руководителей, представителей учебных частей** в мессенджерах

2

Сообщение от службы доставки: **цветов, почта России, СДЭК** для получения посылки, продиктовать код из смс

3

Телефонный звонок якобы **службы замены домофонов** для получения бесплатных ключей

Мошенники сначала создают ложную, но правдоподобную угрозу, чтобы выбить человека из равновесия

- **Новый приём:** убеждают «подтвердить персональные данные, продиктовать код из смс»
- **Схема:**

звонок от **«представителя организации»** → затем **«Госуслуги»** про **«взлом»** → звонок от **«ФСБ, прокуратуры и т.д.»** с требованием срочных действий, возбуждение уголовного дела

Цель – вызвать панику и вынудить передать данные/доступ, получить ВАШИ денежные средства

ОБРАТИТЕ ВНИМАНИЕ НА КЛЮЧЕВЫЕ ФРАЗЫ, КОТОРЫЕ ИСПОЛЬЗУЮТ МОШЕННИКИ, В ХОДЕ ТЕЛЕФОННОГО РАЗГОВОРА:

1. Вы поддерживаете террористов/экстремистов,
2. Подозреваетесь в измене Родине, переводе денег на Украину.
3. Вас беспокоят из «Росфинмониторинга», «Роскомнадзора», «Центробанка», «Госуслуги» и др.
4. Вы участвуете в поимке мошенников, никому не говорите об этом, не разглашайте сведения.
5. В нашей организации проводится проверка, с Вами свяжется наш куратор сотрудник «ФСБ», «МВД» и «Следственного комитета».
6. Необходимо задекларировать имеющиеся наличные денежные средства и драгоценности.

Способы и схемы IT-преступлений

4

Биржевое мошенничество,
инвестирование денег,
быстрый доход

4. Биржевое мошенничество

1. Различная реклама в интернете о возможности получения высокого дохода

2. Заманивают вложить деньги в поддельных инвестиционных платформах

3. Убеждают внести больше денег под предлогом увеличения прибыли или снятия

4. «Лжеброкеры» не выходят на связь, доступ к личному кабинету закрыт

За 2025 год 54 жителя г. Улан-Удэ вложили в «инвестиции» более 40 млн. рублей.

ИТОГ таких «инвестиций» один–

ни собственные средства, ни начисленную на них «прибыль» вывести невозможно!

Инвестировал 3 млн. рублей.

Житель г. Улан-Удэ, увидел в интернете рекламу о заработке на инвестициях и решил попробовать, далее ему позвонили консультанты и изложили алгоритм действия, регулярно находились на связи, консультировали каждое действие, для того, что бы получить «максимальный доход», он оформил кредиты. Когда решил вернуть деньги и обещанную прибыль, счета оказались заблокированы.

ОБРАТИТЕ ВНИМАНИЕ НА КЛЮЧЕВЫЕ ФРАЗЫ, КОТОРЫЕ ИСПОЛЬЗУЮТ МОШЕННИКИ, В ХОДЕ ТЕЛЕФОННОГО РАЗГОВОРА:

1. Инвестиции, получение стабильного дохода (приглашение в чаты «успешных» инвесторов, их «положительные» отзывы, необходимо скачать приложение для дальнейшей работы).
2. Предложения пассивного заработка новыми знакомыми (в том числе - на сайтах знакомств) из сети Интернет.
3. Положены выплаты, компенсации, выигрыш в конкурсе и лотерее, бонусы, кэшбэк.

Основные способы и схемы IT-преступлений

5

Сообщения в мессенджерах

с вредоносными файлами формата .apk с вопросами типа «Это ты на фото/видео?»,

5. Вредоносные файлы.

Какие бывают вредоносные APK?

Фишинговые APK
- замаскированные под легальные приложения (например, «Лента»), крадут пароли и платёжные данные

Троянские APK
- получают доступ к SMS и банковским приложениям, подписывают жертву на платные услуги

Шпионские APK
- скрыто записывают звонки, отслеживают местоположение и копируют переписки

Бэкдоры
- позволяют хакерам удалённо управлять устройством

- Устанавливайте приложения только из официальных магазинов;
- Перед установкой проверяйте рейтинг, отзывы, количество скачиваний, разработчика;
- Ограничьте разрешения приложений: не давайте доступ к контактам, SMS, геолокации без необходимости;
- Проверяйте скаченные файлы с помощью антивируса и не игнорируйте предупреждения.

Основные способы и схемы IT-преступлений

6

Мошенничества

с использованием торговых интернет-площадок

(авито, вайлберис, озон)

С использованием торговых площадок

Мошенники размещают объявления, на 50-70% ниже рыночной стоимости

Входят в доверие, просят частично или полностью оплатить товар

После перевода денежных средств, объявление удаляется, продавец не выходит на связь

ЭТО ВАЖНО - не переходите по ссылкам и QR-кодам, что бы оформить заказ, не называйте СМС-код!!!

Удаленная работа на маркетплейсе: ставить "лайки", добавлять товар в избранное, описывать товары, выкупать товары и т.д.

7. Микрозаймы и кредиты

1.

Создают онлайн-платформы под видом официального сайта (фишинговые сайты).

2.

Звонят и запрашивают личную информацию, представляясь сотрудниками государственных служб

3.

При недостаточной защите учетной записи мошенники взламывают аккаунт пользователя

В результате чего мошенники получают доступ к персональным данным, что позволяет им оформить на Вас кредит и распоряжаться полученными деньгами.

- **НЕ вводите личные данные на подозрительных сайтах;**
- **НЕ переходите по подозрительным ссылкам;**
- **ВКЛЮЧИТЕ двухфакторную аутентификацию на портале «ГОСУСЛУГИ» и других онлайн-сервисах;**

Будьте избирательны при покупке в интернет-магазинах. Изучайте отзывы, информацию о продавце, внимательно сверяйте адрес сайта

Не сообщайте коды из сообщений незнакомым, а также другую важную информацию: номер карты, CVC-код и т.д.

Не вводите данные банковской карты на сомнительных сайтах

Не авторизуйтесь на незнакомых сайтах через аккаунты в соцсетях и мессенджерах.

Подключите **двухфакторную аутентификацию** для входа в свои учетные записи. Используйте разные сложные пароли для каждого аккаунта и регулярно их обновляйте

Не открывайте **подозрительные письма** и не скачиваете файлы из ненадежных источников

Не отвечайте на **звонки с незнакомых номеров.** Установите защиту от спама и определитель номера

Всегда проверяйте информацию и **не принимайте поспешных решений**

Подписывайтесь на наш канал
МВД по Республике Бурятия
в мессенджере «MAX»
@mvd03