

ВАШ БЕЗОПАСНЫЙ ТЕЛЕФОН:

9:41



ВАМ ПОДОЗРИТЕЛЬНЫЙ ЗВОНОК

...Ваши деньги в опасности, аккаунт взломан, оформлена доверенность...



**ПОЛОЖИТЬ
ТРУБКУ**



**ПОЛОЖИТЬ
ТРУБКУ**



НЕ СООБЩАЙТЕ НИКОМУ:

**ПАСПОРТНЫЕ ДАННЫЕ
РЕКВИЗИТЫ КАРТЫ
КОДЫ ИЗ SMS И PUSH**



НЕ СКАЧИВАЙТЕ ПРИЛОЖЕНИЯ:

**ПО ТРЕБОВАНИЯМ НЕЗНАКОМЦЕВ
ИЗ НЕОФИЦИАЛЬНЫХ ИСТОЧНИКОВ**



**НЕ ПЕРЕДАВАЙТЕ ДЕНЬГИ КУРЬЕРАМ И НЕ
ПЕРЕВОДИТЕ НА СЧЕТА ФИЗИЧЕСКИХ ЛИЦ.
С "БЕЗОПАСНОГО" СЧЕТА ОНИ НЕ ВЕРНУТСЯ!**



**ПРИ ПЕРВОМ СОМНЕНИИ ЗВОНИТЕ В
ПОЛИЦИЮ. С МОБИЛЬНОГО 102**



GosUslugi.

Была обнаружена
авторизация на
портале ГосУслуги
Если эти действия
совершали не Вы,
пожалуйста,
обратитесь в службу
поддержки:

+7 991 866

+7 988 920



Сообщение

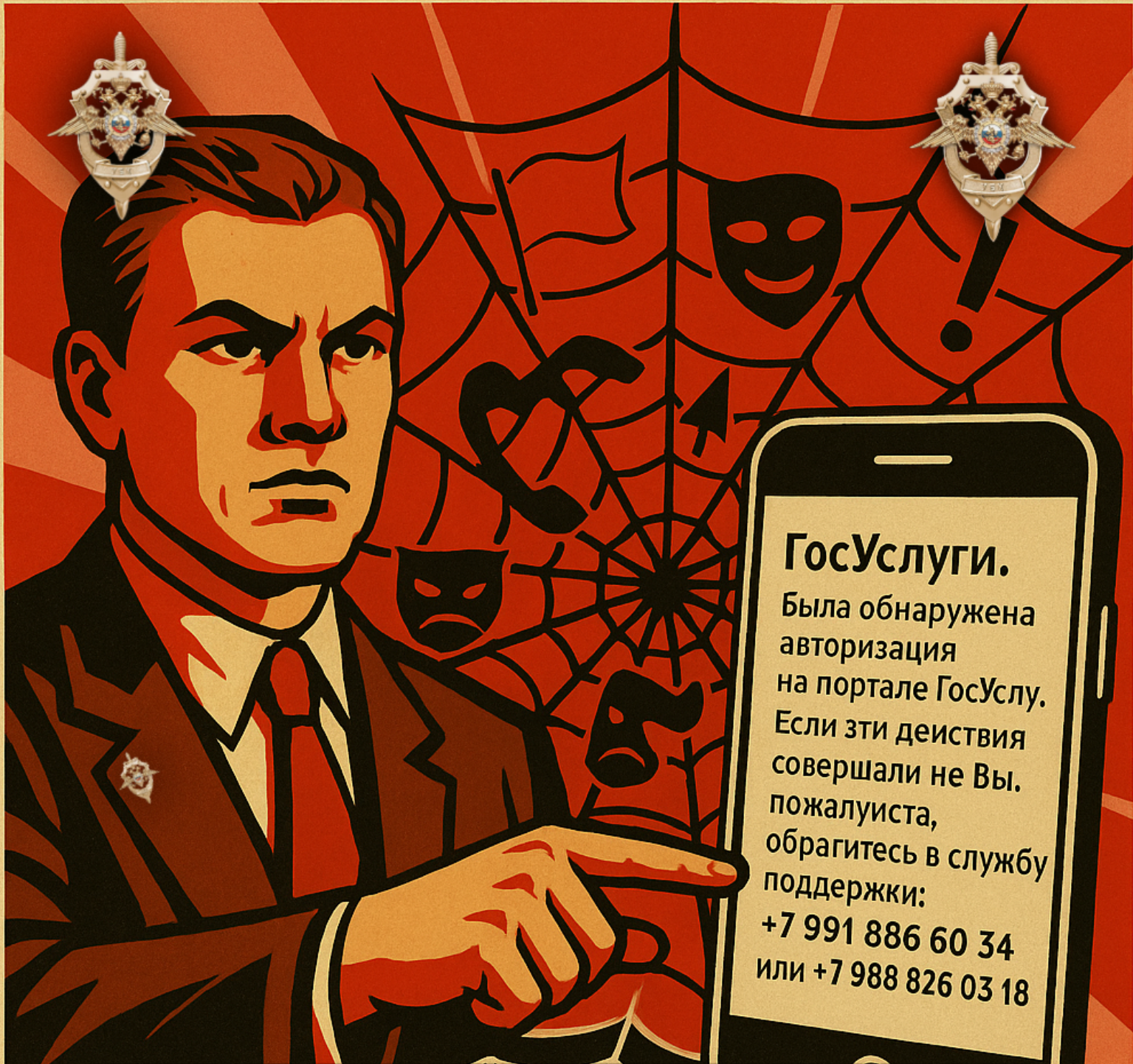


Сообщение

0%
ДОВЕРИЯ



@CYBERPOLICE_RUS



Госуслуги.

Была обнаружена авторизация на портале ГосУслу. Если эти действия совершали не Вы, пожалуйста, обратитесь в службу поддержки:
+7 991 886 60 34
или +7 988 826 03 18

КИБЕРПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ:

«Госуслуги» не направляют такую информацию в СМС и мессенджерах!

Роскомнадзор, МВД, ФСБ, Почта России не рассылают сообщения в мессенджере!

НИКТО не в праве требовать у вас коды из СМС!

Звонит незнакомай и та услышал:



ПРО КОД ИЗ СМС

ПРО БЕЗОПАСНЫЙ СЧЕТ

ПРО ОБНОВЛЕНИЕ
ПРИЛОЖЕНИЯ

ПРО УЧАСТИЕ В
РАССЛЕДОВАНИИ

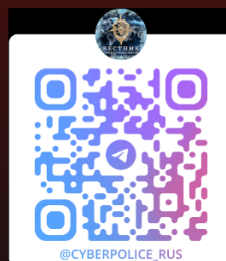
ПРО ЛЕГКИЙ ЗАРАБОТОК

Осторожно, товарищ, это мошенник!

Защити себя — положи трубку!

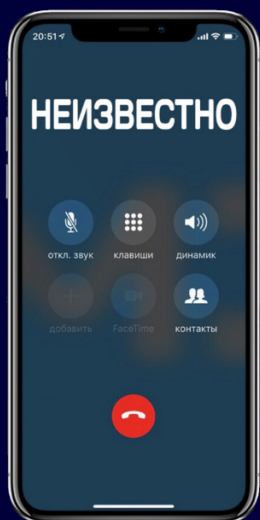


Управление по организации
борьбы с противоправным
использованием информационно-
коммуникационных технологий
МВД России



Подписаться
на Киберполицию
России

ОНИ БУДУТ ПУГАТЬ И ЗАСТАВЛЯТЬ ВАС:



Перевести накопления на безопасный счет, чтобы их не изъяли в рамках уголовного дела.



Установить приложение, которое спасет вам здоровье, жизнь и уменьшит квартплату.



Передать личные данные, банковские реквизиты и код из СМС.

ОСТОРОЖНО - МОШЕННИКИ!

ОНИ ПОПЫТАЮТСЯ СТАТЬ ВАШИМИ ДРУЗЬЯМИ И УБЕДИТЬ:



Перевести предоплату за несуществующий товар.



Пройти по поддельной ссылке и ввести логин и пароль от банковского приложения.



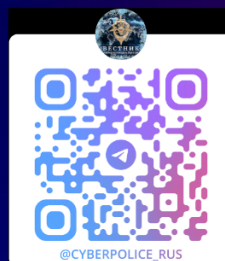
На фальшивой бирже вложить ваши деньги ради пассивного дохода.



ЗАЩИТИ СЕБЯ - ПОЛОЖИ ТРУБКУ!



Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России



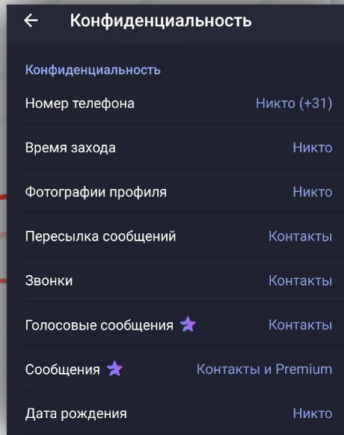
Подписаться на Киберполицию России

ЗАЩИТИТЕ СЕБЯ В МЕССЕНДЖЕРАХ

Telegram:

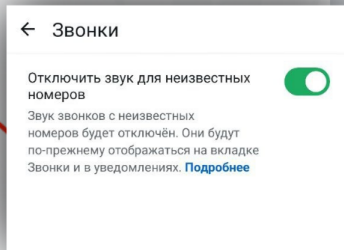
Настройки →
Конфиденциальность →
Звонки →
Мои контакты.

Так мошенник не сможет
вам позвонить.



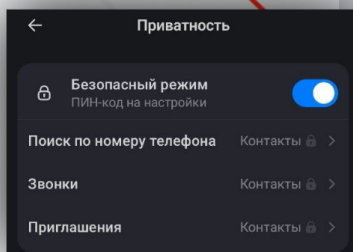
WhatsApp:

Настройки →
Конфиденциальность →
Звонки →
Отключить звук для
неизвестных номеров.



MAX:

Настройки →
Приватность →
Безопасный режим.



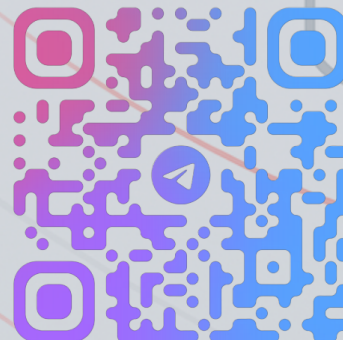
ПРИ МАЛЕЙШИХ
ПОДОЗРЕНИЯХ,
ЧТО С ВАМИ ГОВОРIT
МОШЕННИК - ЗВОНИТЕ
С МОБИЛЬНОГО 102

ЗА БЕСПЛАТНОЙ
ПРАВОВОЙ ПОМОЩЬЮ
МОЖНО ОБРАТИТЬСЯ

+7 (499) 550-80-03

Центр правовой помощи гражданам
в цифровой среде

ХОТИТЕ ЗНАТЬ БОЛЬШЕ?
ПОДПИШИТЕСЬ
НА КИБЕРПОЛИЦИЮ
РОССИИ



@CYBERPOLICE_RUS



КИБЕРПОЛИЦИЯ
РЕКОМЕНДУЕТ

ПРОСТЫЕ НАСТРОЙКИ –
МАКСИМУМ ЗАЩИТЫ

В этом буклете мы
обобщили **простые**
советы, которые
значительно **усложнят**
жизнь мошенникам.

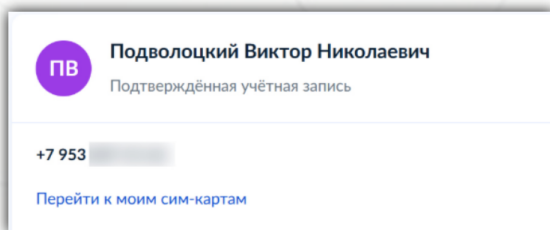


Потратьте немного времени
сейчас – сэкономьте нервы
и средства в будущем.

РЕГУЛЯРНО ПРОВЕРЯЙТЕ

Зарегистрированные на вас симкарты.

Для этого зайдите в свой профиль на "Госуслугах", под вашим номером телефона будет ссылка «Перейти к моим сим-картам». Отключайте не нужные и старые номера.



Надежность вашего пароля.

Проверьте ваш пароль на сайте "Лаборатории Касперского" по ссылке:

<https://password.kaspersky.com/ru/>

Обязательно используйте сложные пароли: с цифрами, буквами и специальными символами. Везде где только можно установите двухфакторную аутентификацию.

Ваши данные на предмет компрометации.

Проверить, не фигурируют ли ваши данные в выявленных утечках можно по адресу:

<https://chk.safe-surf.ru/>

ИСПОЛЬЗУЙТЕ АНТИМОШЕННИЧЕСКИЕ УСЛУГИ И АНТИВИРУСЫ

Антифрод от операторов связи

Что: Специальные платные услуги (часто называются "Антифрод", "Защита от мошенников" и т.п.).

Как: Блокируют известные мошеннические номера, SMS с фишинговыми ссылками и подозрительные звонки до того, как они дойдут до вас. Работают на уровне сети оператора.

Важно: Не блокируют все угрозы, но отсекают массовые атаки.

Антивирусы

Что: Специальные программы для устройств (смартфоны, компьютеры).

Как: Проверяют файлы, приложения, сайты и сообщения на наличие вредоносного кода, блокируют опасные действия, часто имеют встроенную защиту от фишинга.

Важно: Используйте лицензионные решения. Есть качественные бесплатные решения.

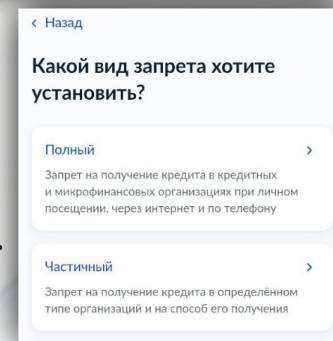
УСТАНОВИТЕ САМОЗАПРЕТ НА КРЕДИТЫ

Войдите в свой аккаунт, нажмите на соответствующую "иконку" или введите в поиске слово "самозапрет".



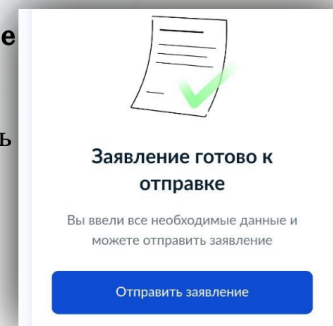
Выберите тип запрета.

Мы рекомендуем установить полный.



Отправьте заявление одним нажатием. Для этого не нужна электронная подпись

Уже более 10 млн пользователей установили запрет.





ПОЛЬЗУЙСЯ БЕЗОПАСНО!

<https://www.банк...>



Пользуйтесь официальными мобильными приложениями банка.



Проверяйте адрес банка в адресной строке, адрес должен заканчиваться только так - .ru/



Переходите в интернет-банкинг только с официального сайта банка.



Не переходите в интернет-банкинг по ссылкам в поисковых системах или в сообщениях.



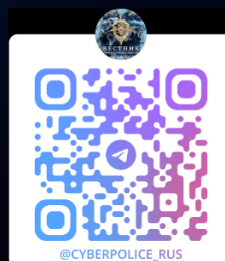
Никому и никогда не сообщайте SMS-коды из сообщений и cvv (сvc) код.



Не вступайте в диалог, если слышите про "безопасный счет"!



Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России



Подписаться на Киберполицию России



С «БЕЗОПАСНОГО» СЧЕТА ДЕНЬГИ НЕ ВЕРНУТСЯ



@CYBERPOLICE_RUS

МОШЕННИК ХИТЁР, У НЕГО ЗВЕРИНАЯ ЗЛОБА-

**СМОТРИ
В ОБА!**

