

# Как обезопасить себя от действий мошенников

## ПАМЯТКА

о порядке действий при обнаружении признаков мошенничества в отношении сотрудников БПОУ ОО «Медицинский колледж», совершаемого с использованием (применением) информационно- телекоммуникационных технологий, средств телефонной связи или в сфере компьютерной информации (фишинговых (поддельных) сайтов, рассылки сообщений без согласия получателя, размещения опасных вредоносных ссылок и прочего)

Никто не застрахован от действий злоумышленников, будь то обычные граждане или представители власти, независимо от должности, от звания, от ученой степени.

Поэтому важно всегда помнить о мерах предосторожности и соблюдать элементарные правила безопасности!



# Отдельная банковская карта для повседневных расчетов

**Не привязывать** основную карту к электронным платежным системам

**Не расплачиваться** основной картой в магазинах

**Не расплачиваться** основной картой на маркетплейсах и сайтах, предлагающих услуги



# Опасайтесь фейковых (фишинговых) сайтов

## Как защититься от фишинга:

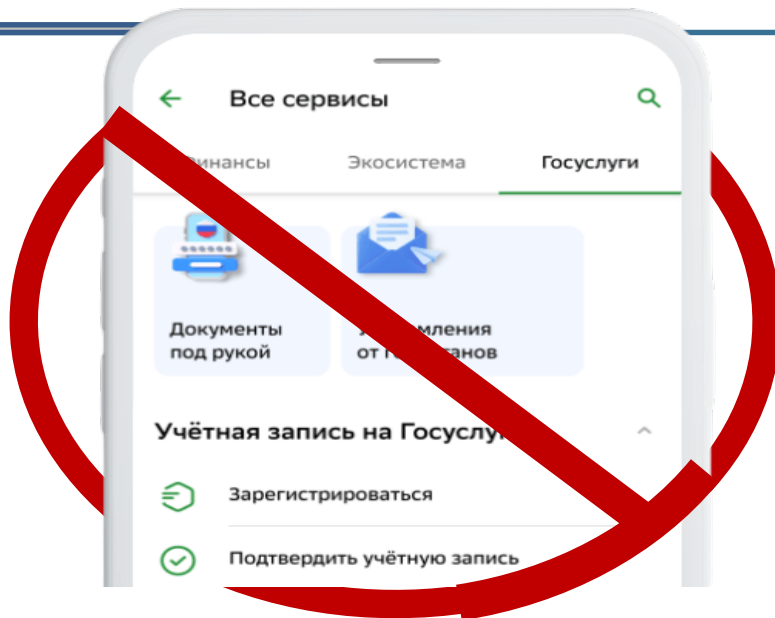
- Не переходите по ссылкам от неизвестных отправителей
- Не покупайте товары по явно заниженной цене
- Сохраняйте в избранное адреса сайтов, которые вы часто используете для платежей;
- Не используйте для оплаты на сайтах основную карту
- Не забывайте про живое общение - звоните, связывайтесь, уточняйте данные и очень аккуратно переводите куда-то деньги



# НЕ связывайте воедино все электронные сервисы

Сейчас банки в своих онлайн-кабинетах приглашают соединить свой банковский кабинет с порталом Госуслуг.

**НЕ делайте ЭТОГО!**



# НИКОГДА НЕ сообщайте НИКОМУ НИКАКИХ ДАННЫХ из СМС

Для того, чтобы получить доступ к Вашему личному кабинету на портале Госуслуг злоумышленники могут позвонить и представиться:

Сотрудниками Поликлиники, где Вас записали на прием или исследование.

Не сообщайте никакие коды, пароли, номера и иные данные – ЭТО МОШЕННИКИ!

Сотрудниками фонда ОМС, где для Вас готов новый полис, но надо лишь сказать код.

Не сообщайте никакие коды, пароли, номера и иные данные – ЭТО МОШЕННИКИ!

Сотрудниками Федеральной налоговой службы

Звонят, чтобы сверить налоговые уведомления, для этого надо сообщить код из СМС.

Не сообщайте никакие коды, пароли, номера, заявки – ЭТО МОШЕННИКИ!



# **НИКОГДА НЕ сообщайте НИКОМУ НИКАКИХ ДАННЫХ из СМС**

**Для того, чтобы получить доступ к Вашему личному кабинету на портале Госуслуг злоумышленники могут позвонить и представиться:**

**Специалистами сотовой связи  
уверяющий об окончании договора, а затем предложивший продлить  
действие услуг, для чего нужно передать смс-коды, номера заявок  
поступивших на телефон, последние цифры номера телефона и т.д.**

**Не сообщайте никакие коды, пароли, номера и иные данные – ЭТО  
МОШЕННИКИ!**



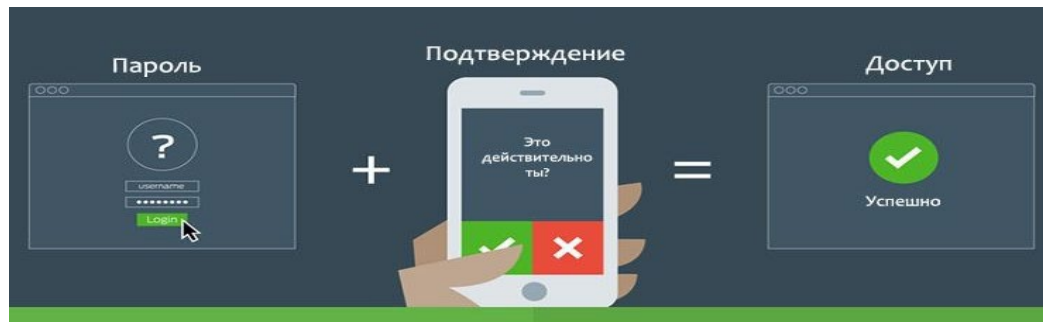
**Специалистами с портала ГОСУСЛУГИ**

**Не сообщайте никакие коды, пароли, номера и иные  
данные – ЭТО МОШЕННИКИ!**

**НЕ меняйте с такими специалистами никакие пароли!**

# Подключите двухфакторную аутентификацию во ВСЕХ СЕРВИСАХ И ПРИЛОЖЕНИЯХ

Двухфакторная аутентификация — это метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов: 1 – логин и пароль, затем 2 – например, код из СМС.



Установите пароль /  
символ / отпечаток  
пальца на включение  
телефона

## Подключите где возможно УВЕДОМЛЕНИЯ О ВХОДЕ В ЛИЧНЫЙ КАБИНЕТ (электронная почта, аккаунты)



# Запретите on line операции с недвижимостью на Госуслугах

The screenshot shows the Gosuslugi website interface. At the top, there is a navigation bar with the logo "госуслуги" and a dropdown menu "Гражданам". To the right, there are links for "Услуги", "Документы", "Заявления", "Платежи", "Помощь", a search icon, and a user profile icon labeled "РН". Below the navigation bar, there is a blue header area with a "сегодня" button and a "Старый поиск" button. A search bar contains the text "Привет! Найду информацию или расскажу об услуге". A red oval highlights a button labeled "запрет на операции с недвижимостью". Below this, there is a text box with the question "Вот что я могу предложить по запрету на действия с недвижимостью без личного участия собственника". A button labeled "Порядок наложения запрета" is visible. The main content area lists the steps to apply for a ban:

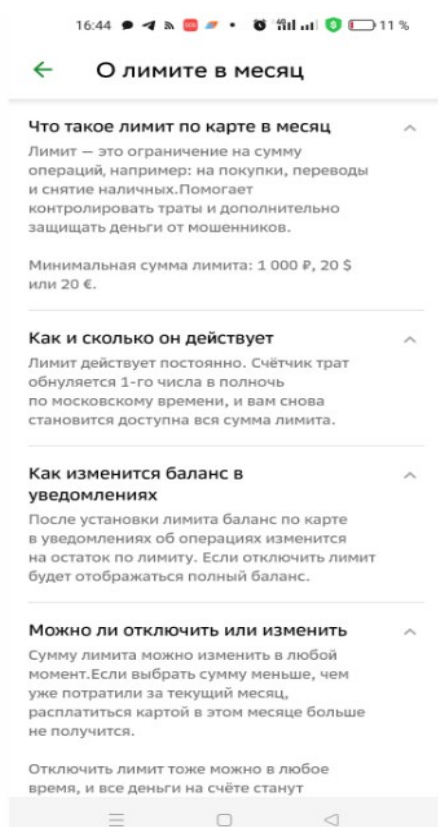
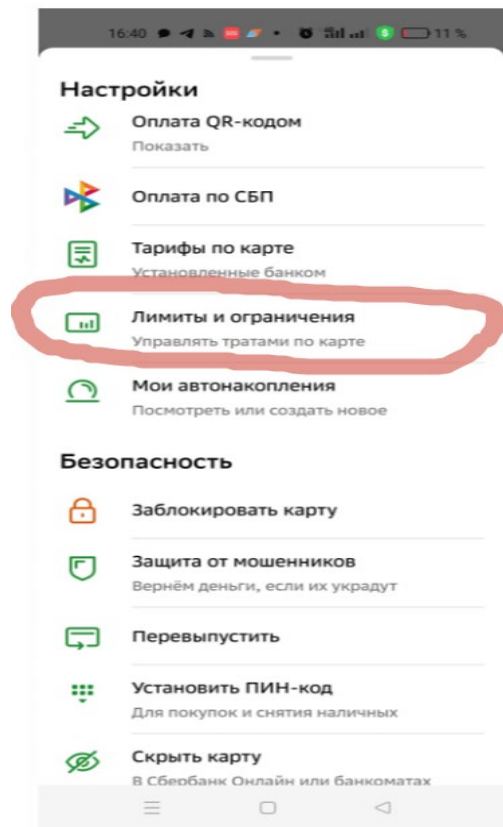
1. Подайте заявление о запрете государственной регистрации перехода, прекращения, ограничения права и обременения объекта недвижимости без личного участия собственника. Это может сделать сам собственник или его законный представитель. У заявителя должна быть подтверждённая учётная запись на Госуслугах.  
Понадобятся:
  - паспортные данные заявителя
  - ИНН заявителя
  - кадастровый номер объекта недвижимости
2. Подпишите заявление усиленной квалифицированной электронной подписью через приложение «Госключ» в течение 24 часов с момента отправки
3. Запись о запрете регистрации внесут в ЕГРН в течение 5 рабочих дней со дня приёма заявления. Уведомление об этом придёт в личный кабинет. После этого Росреестр не будет рассматривать заявления от других людей без вашего участия

Когда Росреестр рассмотрит заявления от других людей, несмотря на запрет

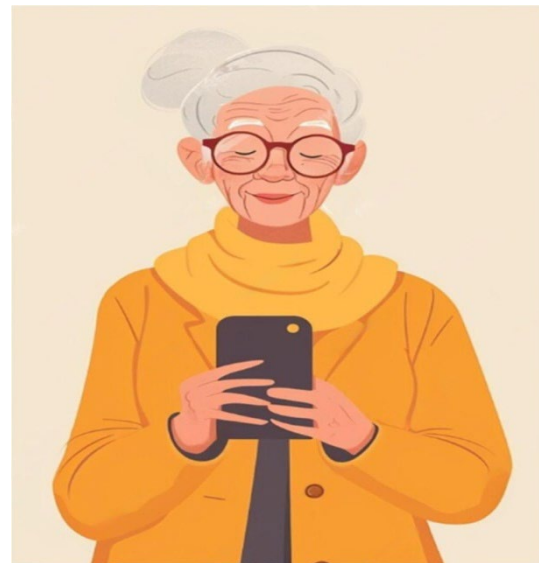
Buttons at the bottom: "Подать заявление" and "Подтвердить учётную запись".

# Запретите on line операции с недвижимостью на Госуслугах

# Установите лимит на операции по карте в on line банке



**Особенно  
возрастным  
родственникам**



При обращении к гражданам мошенники часто представляются должностными лицами:

- органов государственной власти
- правоохранительных органов
- иных контрольно-надзорных органов

**ЗАКОНЧИТЕ РАЗГОВОР!**

**НЕ отвечайте на незнакомые номера**

**НЕ переписывайтесь**

Сотрудники ФСБ и УМВД  
с плохими вестями **приходят лично!**

Если Вам звонят от лица руководства Министерства здравоохранения или от лица вашего руководителя - все, что нужно сделать, это **отключиться от звонка** и **сообщить руководству** об инциденте.



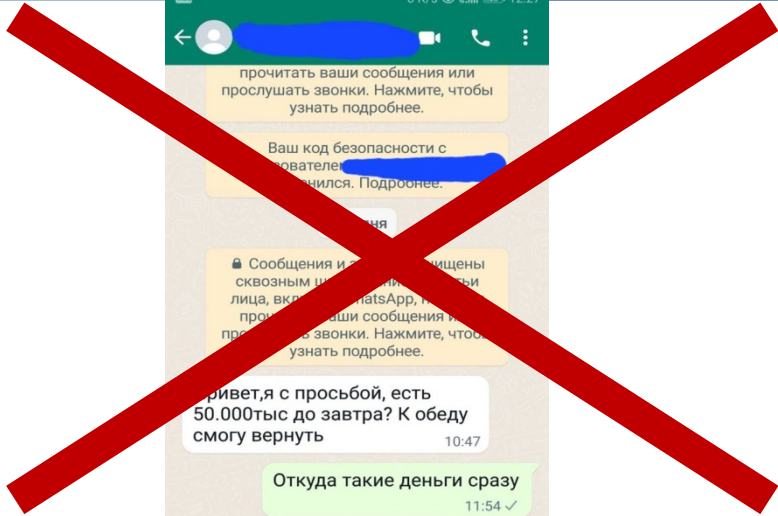
# ОБРАТИТЕ ВНИМАНИЕ!

на то, какие приложения и сервисы  
устанавливают Вам и себе на телефон Ваши  
несовершеннолетние дети и внуки!

Объясняйте детям об опасности  
общения с мошенниками!



не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, мессенджерах, возможно мошенники взломали его аккаунт, сначала свяжитесь с этим человеком и узнайте, действительно ли он просит у вас деньги



## Проверяйте связанные устройства!

# НЕ устанавливайте «ускорители» для Ютуб

Эти вредоносные программы для атаки на  
российских пользователей!

Бесплатные сервисы VPN  
могут быть опасны!

You Tube





**Вестник киберполиции  
России**



**Официальная группа «ВКонтакте»  
УМВД России по Омской области**