МИНСТРОЙ РОССИИ

ГИС ЖКХ

госуслуги дом

ОСТОРОЖНО: МОШЕННИКИ!

ПОДДЕЛЬНЫЕ КВИТАНЦИИ ЗА ЖИЛИЩНО-КОММУНАЛЬНЫЕ УСЛУГИ

Злоумышленники раскладывают по ящикам поддельные квитанции. Визуально их трудно отличить от настоящих, а **QR-код** ведет на оплату по мошенническим реквизитам

Обычно квитанции приходят в одно и то же время, и большая их часть – в период **с 1 по 5 число каждого месяца.** Если квитанция пришла раньше или позже, это повод проявить бдительность

КАК ЗАЩИТИТЬСЯ:

1. **Зайдите в мобильное приложение «Госуслуги Дом» или на портал ГИС ЖКХ.** Здесь данные наиболее точные – отраслевые организации обязаны вносить их по закону. Сравните начисления в квитанции и на экране

2. **Проверьте получателя платежа в квитанции и его банковские реквизиты.** Сравните эти данные с информацией в приложении «Госуслуги Дом» или в ГИС ЖКХ

3. **Посоветуйтесь с соседями.** Возможно, они уже проверили квитанцию и могут подтвердить или развеять ваши опасения

4. **Оплачивайте счета онлайн.** Некоторые жители многоквартирных домов в тестовом режиме получают квитанции в электронном виде через портал «Госуслуги». А пользователи приложения «Госуслуги Дом» могут оплачивать счета в приложении, даже если сейчас они в отъезде и нет возможности заглянуть в почтовый ящик

МИНСТРОЙ РОССИИ

ГИС ЖКХ

госуслуги дом

ВИЗИТЫ САМОЗВАНЦЕВ

Иногда **мошенники** действуют под видом сотрудников коммунальных служб. Они могут прийти с проверкой коммуникаций или предложением замены счетчиков

Собственник обязан пускать в квартиру представителей управляющей организации и рабочих, только если это нужно для осмотра и ремонта коммуникаций

Помните, что **у ремонтной бригады есть документы,** подтверждающие полномочия, а собственник не должен ничего платить наличными, если не вызывал мастера сам

КАК ЗАЩИТИТЬСЯ:

1. **Вспомните, получали ли вы уведомление.** О настоящем визите коммунальные службы должны предупредить заранее, указав в уведомлении ФИО ответственного сотрудника, контактный телефон, сроки и вид работ

2. **Проверьте контактные данные.** Обратитесь в управляющую организацию, чтобы убедиться, что ее сотрудник или подрядчик планирует прийти к вам с проверкой. Актуальный номер телефона управляющей организации можно посмотреть на сайте ГИС ЖКХ

3. **Уточните цель визита.** Визит без предупреждения могут осуществить только для ликвидации аварии. Если срочный доступ нужен для осмотра коммуникаций или немедленной замены счетчиков – не открывайте

4. **Не поддавайтесь давлению.** Если вам грозят штрафами за отказ открыть дверь – это мошенники!

МИНСТРОЙ РОССИИ

ГИС ЖКХ

госуслуги дом

ПРИГЛАШЕНИЕ В ПОДДЕЛЬНЫЕ ЧАТЫ

Иногда жители многоквартирных домов обнаруживают в подъездах и на информационных стендах **приглашение вступить в чат дома**

При попытке перейти по QR-коду пользователи **теряют свой аккаунт** в мессенджере, и далее мошенники используют его для обмана других пользователей

КАК ЗАЩИТИТЬСЯ:

1. **Проверьте, есть ли в объявлении адрес вашего дома.** Если инициаторы не пишут адрес, а приглашают вступить в «чат нашего дома», скорее всего, это массовое объявление мошенников
2. **Посоветуйтесь с соседями.** Если у вас уже есть чат дома или подъезда, задайте вопрос в нем. Возможно, соседи знают настоящего создателя или уже проверили объявление на достоверность
3. **Проверяйте ссылку, по которой предлагают перейти после считывания QR-кода.** Если она подозрительная или в адресе есть очевидные ошибки, не переходите по ней
4. **Пользуйтесь официальными чатами.** Через приложение «Госуслуги Дом» вы можете вступить в чат подтвержденных собственников квартир в вашем доме. Посторонние люди и мошенники не смогут получить доступ к этому чату

МИНСТРОЙ РОССИИ

ГИС ЖКХ

госуслуги дом

ТЕЛЕФОННОЕ И ОНЛАЙН-МОШЕННИЧЕСТВО

Злоумышленники могут звонить или писать вам в мессенджер, представляясь сотрудниками управляющих или ресурсоснабжающих организаций

В звонке или переписке они будут предлагать перейти по ссылке, назвать код из сообщения или установить на смартфон новое приложение для оплаты ЖКУ

Так мошенники получают **доступ к аккаунту «Госуслуг» или смартфону** пользователя и могут похитить деньги с банковского счета или оформить кредит на его имя

КАК ЗАЩИТИТЬСЯ:

1. **Не переходите по ссылкам от неизвестных отправителей и не открывайте файлы.** Мошенники часто рассылают установочные файлы приложений под видом фотографий. Когда пользователь открывает файл, на смартфон устанавливается приложение, которое крадет пароли и платежные данные и позволяет взломщикам управлять устройством
2. **Не называйте посторонним лицам коды из SMS.** Настоящие сотрудники организаций никогда не попросят у вас код от «Госуслуг» и других аккаунтов
3. **Не принимайте решений во время разговора.** Если вас подталкивают к подозрительному действию, прекратите общение и перепроверьте информацию, а также свяжитесь со своей управляющей организацией. Актуальные контакты есть на сайте ГИС ЖКХ