Осторожно, мошенники!

ПАМЯТКА
о распространенных способах дистанционного мошенничества

Старая сим-карта — это не то, что можно просто взять и выбросить.

При смене номера телефона:

- ✓ **Отвяжите его от всех онлайн-сервисов**
- ✓ **Настройте двухфакторную аутентификацию через push-уведомления**
- ✓ **Регулярно меняйте пароли на своих учетных записях**

Важно! Мошенники скупают неиспользуемые симки у сотовых операторов, чтобы получить доступ к личным кабинетам пользователей.

Осторожно, мошенники!

ПАМЯТКА
о распространенных способах дистанционного мошенничества

Подозрительные ссылки!

Мошенники в мессенджерах могут направить вам сообщение, содержащие ссылку на скачивание фотографии с текстом:

«Посмотри, это ты на фото?» /«Архив фото»

или под другими разными предлогами вас будут убеждать пройти по ссылке!

Последствия перехода:

- **Установка вирусов**
- **Кража денег**
- **Оформление кредитов**
- **Контроль над вашим телефоном**

НИКОГДА не переходите по сомнительным ссылкам!

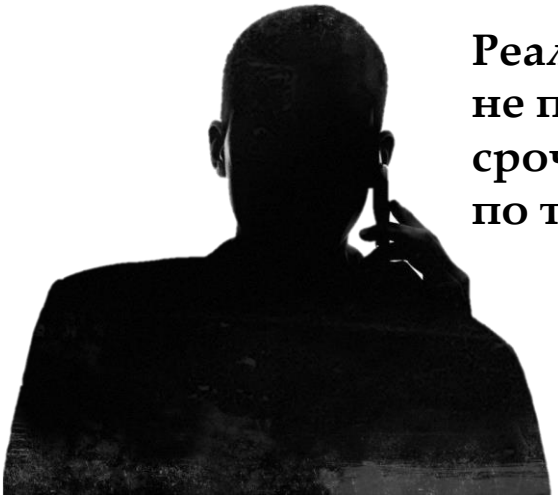
Осторожно, мошенники!

ПАМЯТКА
о распространенных способах дистанционного мошенничества

Нельзя верить в истории с продлением договора на обслуживании сим-карт!

Помните: у сим-карт нет срока действия, а договор с оператором связи бессрочный!

Если вам звонят с требованием продлить номер, продиктовать код из СМС или паспортные данные — это мошенники! СРАЗУ КЛАДИТЕ ТРУБКУ!



Реальные операторы связи НИКОГДА не просят коды из СМС и не требуют срочного продления номера по телефону!

Осторожно, мошенники!

ПАМЯТКА
о распространенных способах дистанционного мошенничества

Мошенники предлагают поменять электросчетчики

Мошенники звонят с предложением поменять счетчики, а после того как граждане соглашаются, мошенники сообщают, что домой придет мастер, только надо сообщить номер квитанции.

Работники энергосбыта НИКОГДА не просят такие данные и не отправляют ссылки!

При звонках о замене счётчиков не сообщайте персональные данные и коды из SMS – это мошенники!

При подобных звонках сразу прекращайте разговор!

Осторожно, мошенники!

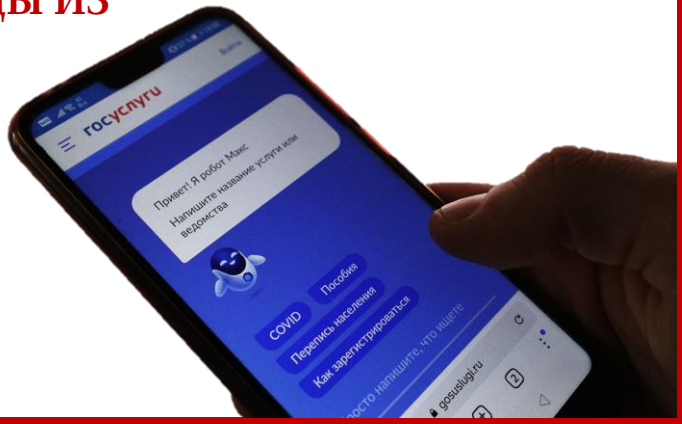
ПАМЯТКА
о распространенных способах дистанционного мошенничества

Взломанные Госуслуги

Мошенники, представляясь специалистами и сотрудниками различных организаций и даже специалистами портала «Госуслуг» могут сообщить о взломе личного кабинета.

Чтобы защитить данные или установить новые пароли преступники будут требовать назвать коды из смс-сообщений, а иногда и говорить об утечке данных из госуслуг, оформлении кредитов посторонними лицами.

НИ В КОЕМ СЛУЧАЕ НЕЛЬЗЯ НИКОМУ ПО ТЕЛЕФОНУ НАЗЫВАТЬ КОДЫ ИЗ СМС-СООБЩЕНИЙ!



Если вы не смогли зайти в личный кабинет «Госуслуг» необходимо обратиться в МФЦ и в отделение банка для подтверждения аккаунта и смены пароля.

Осторожно, мошенники!