

ЗАЩИТИ СЕБЯ И СВОИХ БЛИЗКИХ ОТ КИБЕР МОШЕННИКОВ

ПАМЯТКА

МИНИСТЕРСТВО
ИНФОРМАЦИОННОГО РАЗВИТИЯ И СВЯЗИ
ПЕРМСКОГО КРАЯ

2024

САМЫЕ РАСПРОСТРАНЕННЫЕ МОШЕННИЧЕСКИЕ СХЕМЫ

- **Звонок, информирующий о том, что Ваш родственник попал в беду**

  На телефон поступает звонок, якобы родственника, который попал в опасную ситуацию. Чтобы выпутаться из передряги, естественно нужны деньги.

- **Блокировка банковской карты**

  Звонят с неизвестного номера и сообщают, что с банковской картой проблемы. Для решения просят назвать паспортные данные и информацию о банковской карте.

- **Получение внезапного выигрыша**

  Поступает звонок о выигрыше крупной суммы денег, квартиры или автомобиля. Для получения приза просят сообщить персональные данные.

- **Приглашение в МФЦ за получением «забытых» документов**

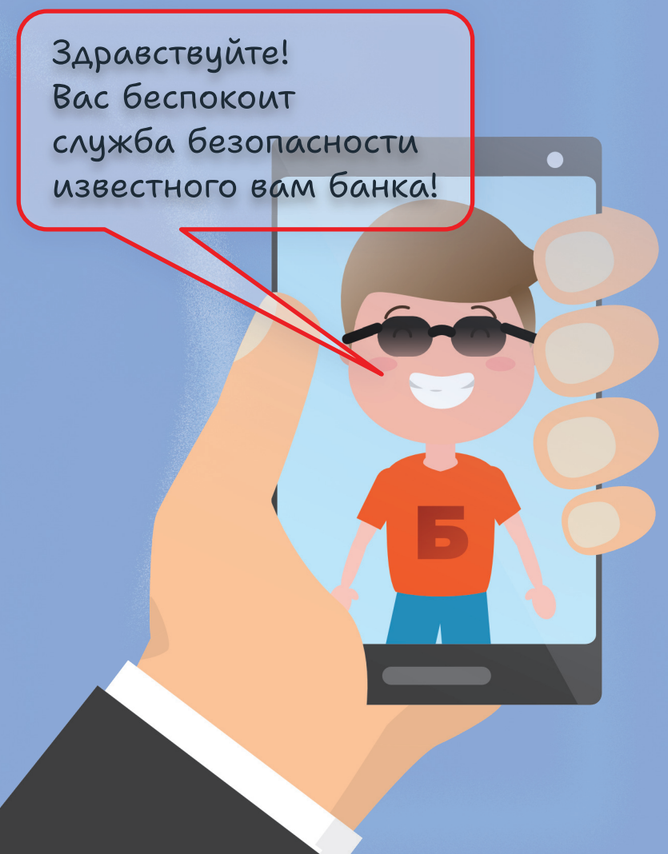
  Звонят от лица сотрудников МФЦ или других органов власти и убеждают, что на Ваше имя есть невостребованные документы, которые предлагают получить. Для подтверждения просят сообщить персональные данные.

- **Звонок оператора сотовой связи**

  Лже-оператор сообщает, что срок действия sim-карты истекает, необходимо его продлить. Мошенник присылает человеку СМС с кодом, который просит сообщить для продления договора. Как только человек отправляет код, мошенник получают доступ к личному кабинету Госуслуг.

Помните!

Никто не имеет права требовать предоставить персональные данные, пин-код банковской карты или пароль от личного кабинета на портале Госуслуг.



С МОЕЙ КАРТЫ ОБМАНОМ СПИСАЛИ ДЕНЬГИ. ЧТО ДЕЛАТЬ?

Позвоните в банк и заблокируйте карту.

Обратитесь с заявлением в полицию.



ЭТО ВАЖНО ЗАПОМНИТЬ!

- Злоумышленники по телефону могут представляться представителям банков, МФЦ, МВД, государственных органов, а также могут писать в мессенджерах и социальных сетях с поддельных аккаунтов
- Не сообщайте логины и пароли от личных кабинетов, данные банковских карт и документов, одноразовые коды из СМС по телефону, в мессенджерах и социальных сетях
- Не открывайте ссылки в письмах, мессенджерах, социальных сетях от неизвестных адресатов
- Не скачивайте файлы из непроверенных источников
- Ограничьте использование иностранных мессенджеров и социальных сетей, а также круг людей, которые имеют доступ к аккаунтам ваших соцсетей
- Ограничьте объем информации о себе в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких
- Заблокируйте автоматическое подключение гаджетов к Wi-Fi точкам
- Будьте внимательны к именам сайтов или отправителям писем. Внимательно проверьте, что адрес сайта написан верно – мошенники могут заменить всего одну букву. Лучше ввести адрес сайта вручную

КАК ЗАЩИТИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Надежные пароли необязательно сложные для запоминания

- **Длина пароля — 10 символов и более.**
- **В пароле должны быть заглавные (А, О, С) и строчные буквы (м, к, у), цифры, специальные символы (#, @, <) и знаки препинания.**

0n4$p1Wn*b?AU79

Легко запомнить фразу, связанную с жизненной ситуацией, и превратить ее в надежный пароль.

Например: Важный шаг и надежный пароль

OnaSkazalaDA!15.02.12

Подключите двухфакторную аутентификацию

Это метод проверки личности с использованием двух различных факторов.

Где использовать?

На всех ресурсах, где содержатся важные данные или совершаются финансовые операции: при входе в аккаунты социальных сетей, порталы государственных услуг, интернет-банкинг и прочие.

КАК ПОДКЛЮЧИТЬ ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ?

Подключение двухфакторной аутентификации в личном кабинете на портале Госуслуг

Шаг 1: Зайдите в раздел «Профиль»

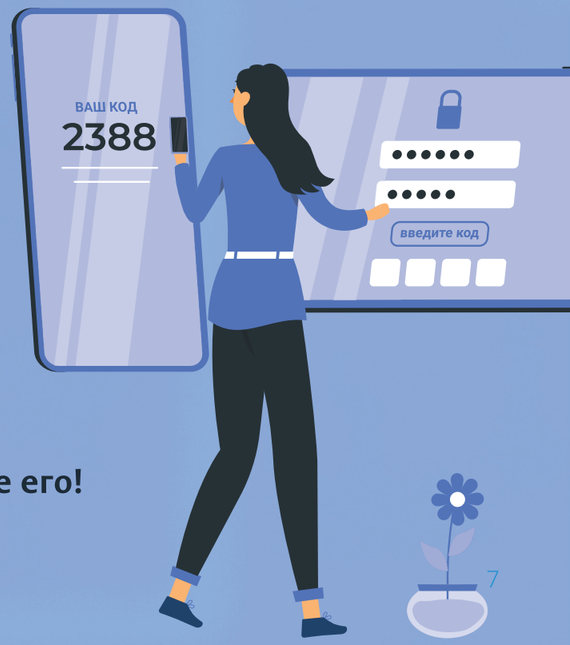
Шаг 2: Выберите вкладку «Безопасность»

Шаг 3: В разделе «Двухфакторная аутентификация» выберите пункт по коду через СМС, которое будет приходить на Ваш номер телефона

Шаг 4: Нажмите «Установить»

Шаг 5: Получите код по СМС

Шаг 6: Введите код и получите сообщение с подтверждением



Теперь при каждом входе в личный кабинет портала Госуслуг Вам будет приходить код подтверждения.
Никогда и никому не сообщайте его!

ЧТО ДЕЛАТЬ, ЕСЛИ ПАРОЛЬ ОТ «ГОСУСЛУГ» ОКАЗАЛСЯ У МОШЕННИКОВ

- **ШАГ 1. Восстановите пароль от личного кабинета**

1. Выберите близлежащий офис «Мои Документы»
2. Возьмите с собой паспорт и СНИЛС
3. Предъявите документы сотруднику и скажите, что хотите восстановить пароль от Госуслуг. Специалист проверит документы, уточнит номер телефона или адрес электронной почты и пришлёт одноразовый пароль

- **ШАГ 2. Выйдите из учетной записи со всех устройств, кроме текущего**

1. Перейдите в Личный кабинет → Профиль → Безопасность
2. Во вкладке «Действия в системе» нажмите «Выйти»
3. Во вкладке «Моб. приложения» нажмите «Выйти» из тех приложений, в которые вы не входили



- **ШАГ 3. Определите, где использовалась учетная запись**

1. Перейдите в Личный кабинет → Профиль → Безопасность→ Действия в системе
2. Проверьте, не было ли подозрительных действий в учетной записи
3. Перейдите в Личный кабинет → Профиль → Согласия и доверенности. Отзовите разрешения, которые вы не подавали
4. Проверьте список поданных заявлений и уведомления

- **ШАГ 4. Проверьте кредитную историю**

1. В личном кабинете в строке поиска введите «узнать свое БКИ» (БКИ — бюро кредитных историй»)
2. Зарегистрируйтесь на сайте каждого бюро и запросите свою кредитную историю
3. Посмотрите, какие заявки на кредиты подавались от вашего имени.
4. Если на вас взяли кредит — срочно обратитесь в банк

- **ШАГ 5. Подайте заявление в МВД**

1. Возьмите с собой копию заявления на восстановление учетной записи Госуслуг из МФЦ, снимки экрана СМС-сообщений и другие доказательства

КУДА ОБРАТИТЬСЯ, ЕСЛИ СТОЛКНУЛИСЬ С МОШЕННИЧЕСТВОМ?

по телефону горячей линии МВД 8-800-222-74-47

на сайте МВД: мвд.рф

в отделении полиции по месту вашего жительства

МОШЕННИКИ ВСЕГДА:

Звонят со скрытого
или неизвестного номера

Спрашивают данные карты

Переводят звонок «на специалиста»

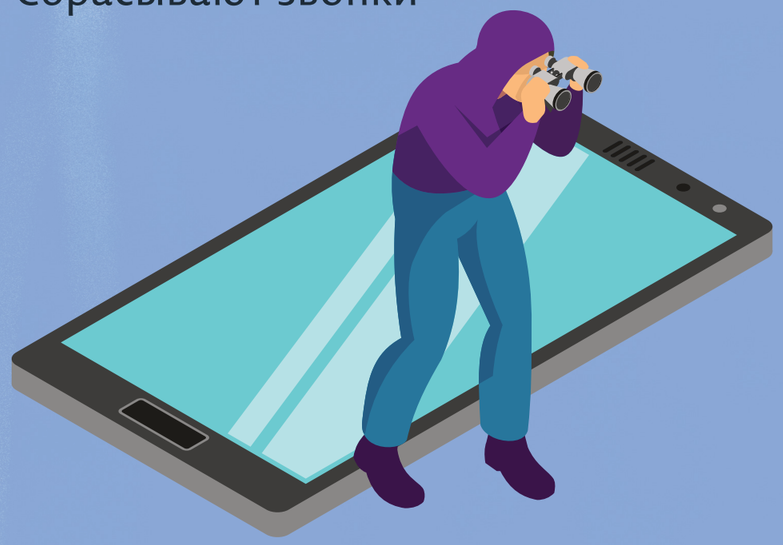
Сообщают тревожную информацию

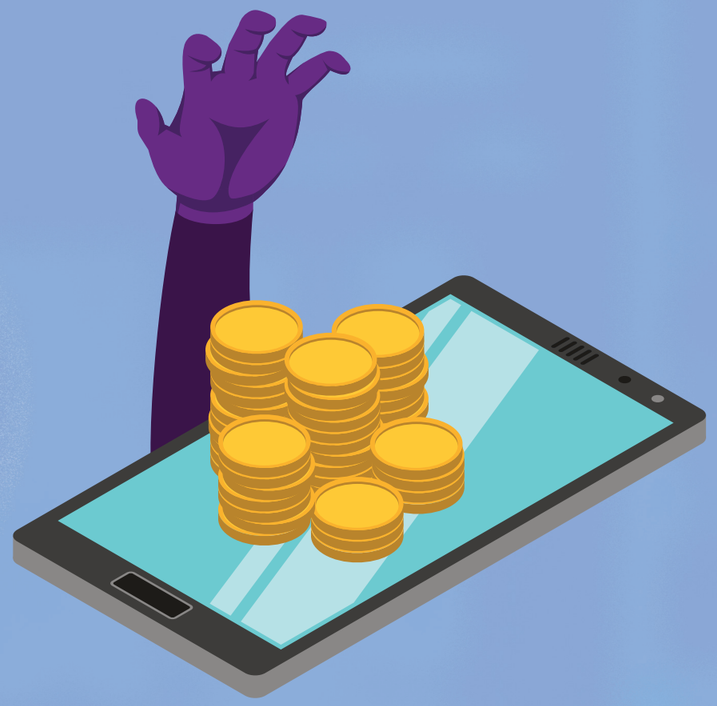
Давят на вас

Сообщают о внезапном выигрыше

Уговаривают открыть ссылку
или файл из СМС или мессенджера
(WhatsApp, Telegram, Viber и другие)

Сбрасывают звонки





ЗВОНЯТ И СООБЩАЮТ, ЧТО БЛИЗКИЙ ЧЕЛОВЕК ПОПАЛ В БЕДУ, ПРОСЯТ ПЕРЕВЕСТИ ДЕНЬГИ.

ЧТО ДЕЛАТЬ?

Успокойтесь, проясните ситуацию.

Спросите фамилию, имя звонящего, название организации, которую он представляет. Прекратите разговор и позвоните близкому человеку.

Если дозвониться не удалось, сами найдите телефон организации, от имени которой был звонок, и выясните, что случилось.

КИБЕР БЕЗОПАСНОСТЬ ЭТО ПРОСТО!

госуслуги

https://www.gosuslugi.ru/cybersecurity

МИНИСТЕРСТВО
ИНФОРМАЦИОННОГО РАЗВИТИЯ И СВЯЗИ
ПЕРМСКОГО КРАЯ