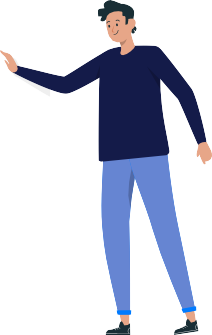
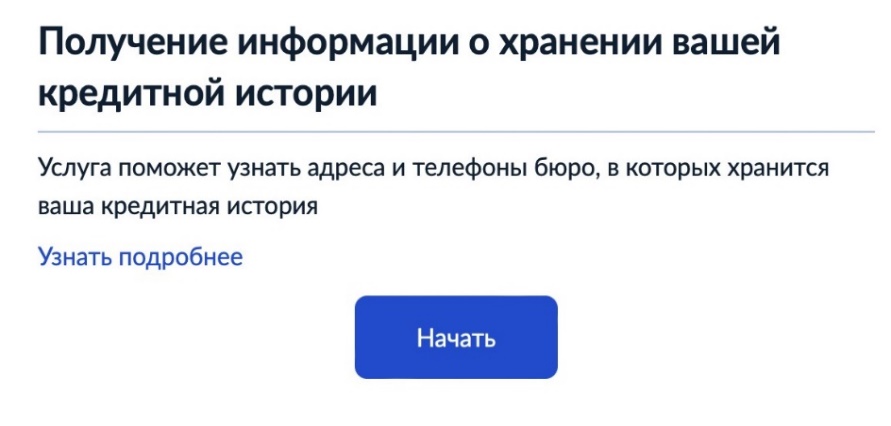
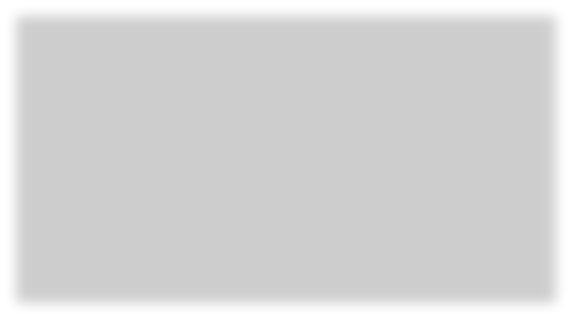


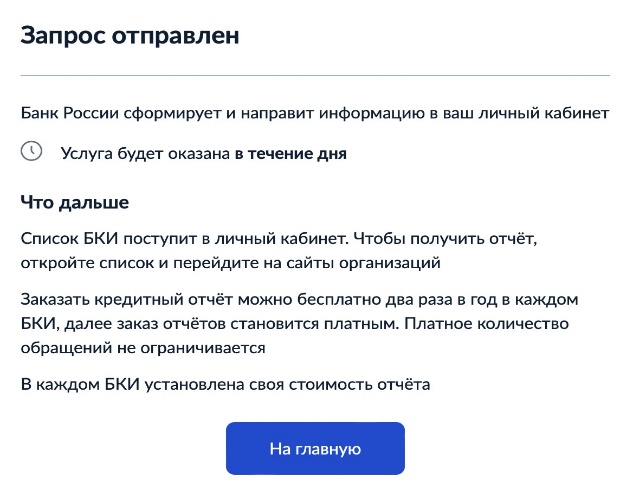
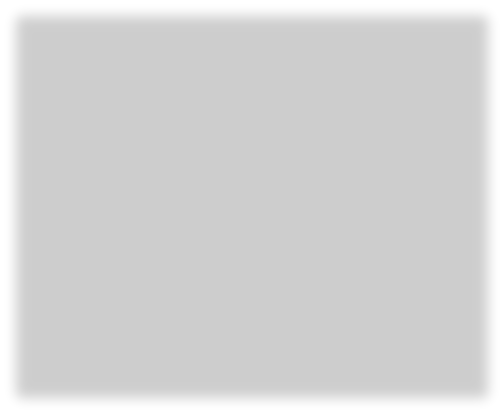
**КАК УЗНАТЬ, ОФОРМЛЯЛИСЬ ЛИ МОШЕННИКАМИ НА ВАШЕ ИМЯ КРЕДИТЫ?**

Центр правовой помощи гражданам в цифровой среде ФГУП «ГРЧЦ» рекомендует проверять свою кредитную историю. Таким образом Вы выясните, направлялись ли от Вашего имени заявки на потребительские кредиты.

Для этого нужно сначала узнать конкретное бюро кредитных историй, в котором хранится Ваша кредитная история. Сделать это можно на портале Госуслуг. Для этого необходимо выбрать раздел «Услуги», затем «Справки и выписки», потом «Сведения о бюро кредитных историй» либо вместо этого сразу ввести в строке поиска запрос «узнать своё БКИ».



Портал Госуслуг попросит Вас проверить и подтвердить Ваши персональные данные, после проверки которых следует нажатием поля «Отправить запрос» подтвердить необходимость получения такой услуги. В ответе портала Госуслуг будут указаны контакты бюро кредитных историй, Вам необходимо зарегистрироваться на его сайте (можно авторизоваться с помощью учетной записи Госуслуг) и запросить свою кредитную историю. Два раза в год ее можно получить бесплатно, далее стоимость определяется Вашим бюро кредитных историй и составляет в среднем 400-500 рублей за один отчет.



Если вы выясните, что мошенники отправляли от Вашего имени заявки на получение займов или уже заключили договоры потребительского кредита, Центр правовой помощи гражданам в цифровой среде ФГУП «ГРЧЦ» готов оказать безвозмездную правовую помощь по подготовке исковых заявлений о признании кредитных договоров недействительными и компенсации морального вреда, а также представлять интересы истцов в суде.

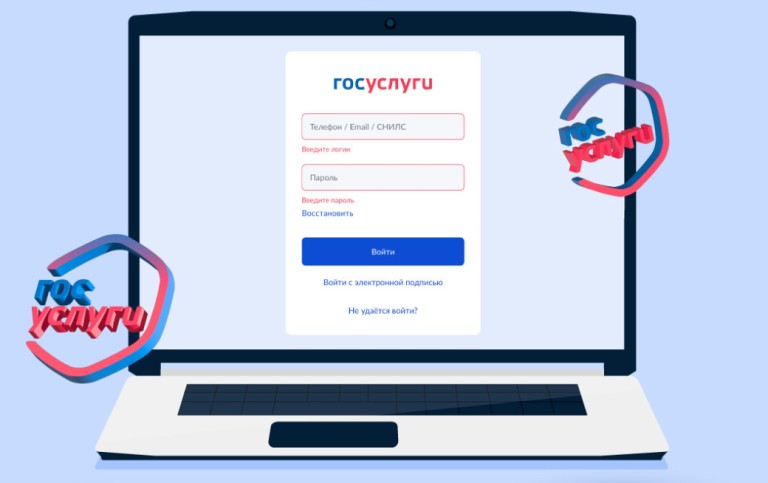
Наши контакты:

Адрес: г. Новосибирск, ул. Октябрьская магистраль, д. 4, 3 этаж

Телефон: +7 (383) 304-75-02

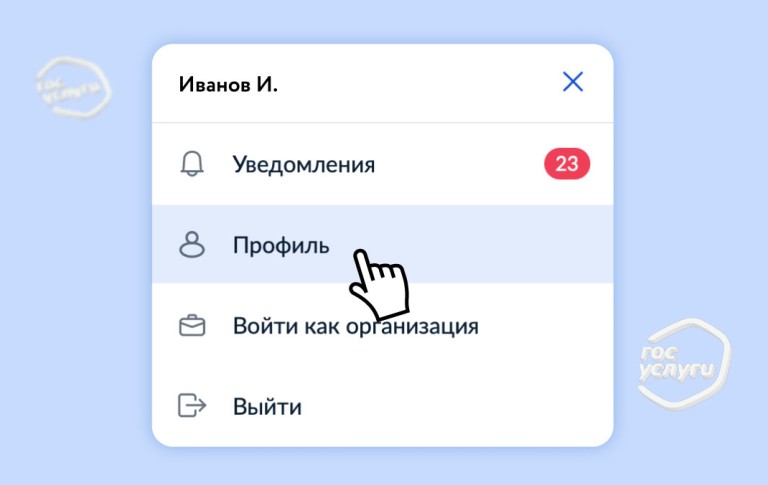
Е-mail: 4people\_54@grfc.ru

**Как проверить, входил ли злоумышленник в ваш личный кабинет на портале Госуслуг?**

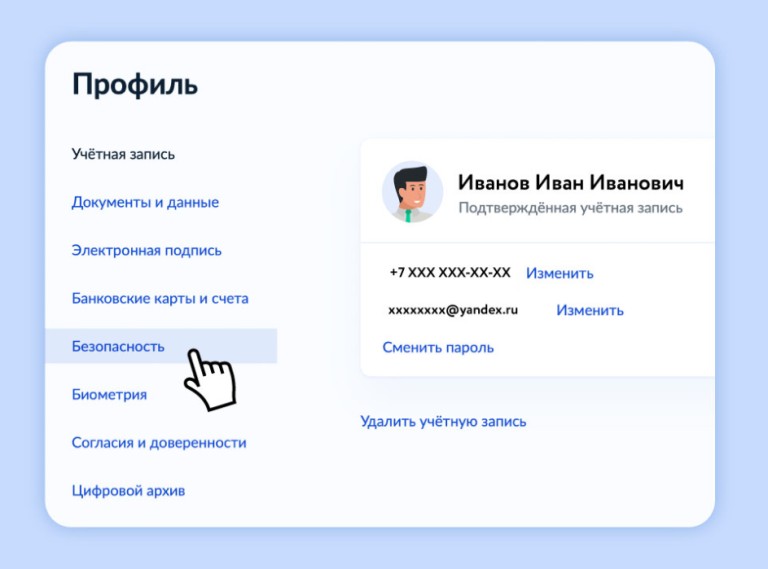


Вы можете получить информацию в профиле пользователя Госуслуг.

Для этого нужно нажать на имя пользователя и выбрать вкладку «Профиль».



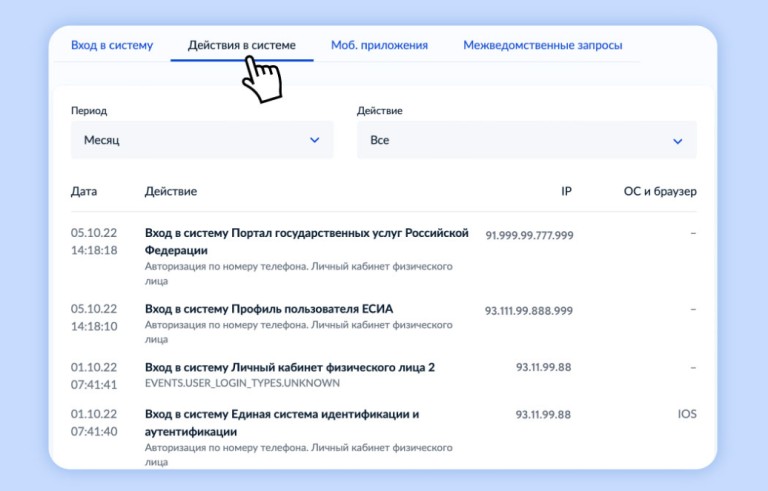
Попав в «Профиль», перейдите в раздел «Безопасность».



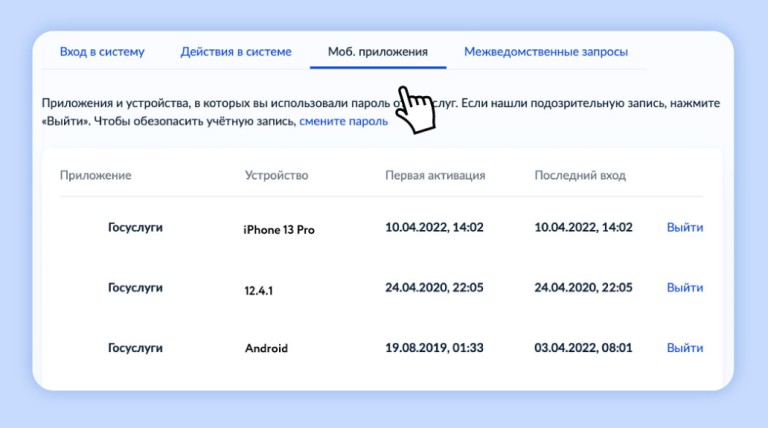
На открывшейся странице необходимая информация представлена в двух вкладках: «Действия в системе» и «Мобильные приложения».

Во вкладке «**Действия в системе**» вы можете узнать о том, к каким ресурсам был получен доступ с использованием учетной записи ЕСИА.

Если учетная запись использовалась для авторизации на сайте банка или для направления запроса на получение кредитной истории, информация об этом будет указана.



Во вкладке **«Мобильные приложения»** проверьте приложения и устройства, в которых использовался пароль от Госуслуг. Если некоторые из них Вам не знакомы, это может говорить о том, что доступ к учетной записи получили посторонние.





В случае неправомерного использования ваших персональных данных обращайтесь в Центр правовой помощи гражданам в цифровой среде, Вам окажут бесплатную юридическую помощь:

* Консультации;
* Подготовка документов в суд и правоохранительные органы;
* Представление ваших интересов в суде.

Наши контакты:

Адрес: г. Новосибирск, ул. Октябрьская магистраль, д. 4, 3 этаж

Телефон: +7 (383) 304-75-02

Е-mail: 4people\_54@grfc.ru

**Основные правила безопасности в цифровой среде**

**Как обезопасить себя и своих близких от опасностей, связанных с передачей персональных данных в цифровой среде?**

**ПРИДЕРЖИВАЙТЕСЬ НЕСЛОЖНЫХ ПРАВИЛ**



Не пересылайте Ваши персональные данные, содержащиеся в паспорте, банковской карте и других личных документах адресатам, в которых Вы не уверены. При необходимости направления скан-копий документов пересылайте их в архивах, защищенных паролями. Только адресат такого сообщения сможет получить доступ к его содержимому.

Никому и никогда не сообщайте коды для подтверждения банковских операций и CVV/CVC-коды. С помощью этой информации неизвестные лица могут списать с ваших счетов денежные средства. Если вы сообщили такую информацию, срочно уведомите об этом сотрудников банка и заблокируйте карту.



Используйте для онлайн-платежей банковскую карту, на которой храните небольшие суммы денежных средств.



При регистрации личного кабинета устанавливайте, где это возможно, двухфакторную идентификацию. На портале «Госуслуги» это сделать особенно важно, поскольку в результате взлома личного кабинета в этом приложении злоумышленник от Вашего имени может совершать действия, которые будут иметь юридически значимые последствия, в том числе оформить на Ваше имя кредит.

Если двухфакторная идентификация невозможна, используйте сложные пароли с применением букв различного регистра, цифр и символов. Не используйте пароли, содержащие Ваше имя, дату рождения и иную известную о Вас информацию. Использование простого пароля увеличивает риски взлома, входа в ваш личный кабинет и утечки ваших данных.



Перед регистрацией и использованием интернет-ресурса не забудьте ознакомиться с текстами Согласия на обработку персональных данных, Пользовательским соглашением и Политикой конфиденциальности, а также иными документами, размещенными на сайте. Так Вы сможете понять, кому Ваши персональные данные могут быть переданы.

Если Вы заходите в личный кабинет из социальной сети, электронной почты или с чужого компьютера, не забудьте выйти из своей учетной записи, чтобы ей не воспользовался злоумышленник. Пользуйтесь режимом «инкогнито», установив его в своем браузере, а также функцией «чужой компьютер» на посещаемых Вами сайтах (если такая функция имеется).

Изучайте отзывы о компании в Интернете, рейтинг сайта, при необходимости проверяйте наличие лицензии у компании и иные документы. Это позволит Вам избежать входа на фишинговые сайты, не столкнуться с фирмами-однодневками и иными недобросовестными источниками информации.

Не переходите по подозрительным ссылкам. Злоумышленники копируют дизайны известных сайтов для получения Ваших персональных данных и использования их в противоправных целях. Обман достигается путем введения в заблуждение о подлинности интернет-ресурса вследствие сходства доменных имен, оформления или содержания информации. Отличительным признаком такого сайта может быть, например, малозаметная ошибка в доменном имени (yandax вместо yandex; vkontakte.ru и vkonlakte.ru и т. п.).

Установите и обновляйте антивирусные программы, сканируйте компьютер на наличие вредоносного программного обеспечения. Устаревшие версии антивирусных программ не могут гарантировать защиту устройства, поскольку новые угрозы информации появляются ежедневно.

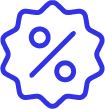


Не скачивайте файлы, в происхождении которых Вы не уверены, не устанавливайте и не запускайте неизвестные Вам приложения. Они могут как «троянский конь» содержать вредоносные и шпионские программы.

Избирательно подходите к предоставлению доступа приложениям к хранящимся на Ваших устройствах документам, фотографиям и видео, а также микрофону и камере. Используйте для этого в Вашем устройстве функцию «Настройки».



Не отвечайте на спам-сообщения, не переходите по ссылкам, указанным в таких сообщениях, не скачивайте приложенные файлы. При поступлении подозрительного сообщения удалите его со всех устройств

Не откликайтесь на слишком выгодные предложения, скидки, бесплатные услуги, взамен на которые Вы сначала должны сообщить телефон, отправить сообщение, перевести незначительную сумму денег. Так с вашего счета могут списать внушительную сумму, номер телефона станет общедоступным, а данные Вашей банковской карты станут известны мошенникам.



ПОМНИТЕ! Банки, магазины и иные добросовестные сервисы никогда не рассылают письма с просьбой перейти по ссылке, изменить свой пароль, ввести номер банковской карты и секретный код подтверждения, а также другие личные данные. Такие письма приходят от мошенников!



С периодичностью запрашивайте выписки из бюро кредитных историй через портал «[Госуслуги](https://www.gosuslugi.ru/)».



Проверьте, какие устройства подключены к Вашим мессенджерам, при обнаружении не принадлежащих Вам устройств, отключите их.



Не используйте бесплатный Wi-Fi при передаче личной информации.

ГЛАВНЫЕ РЕКОМЕНДАЦИИ:

Воспользуйтесь предложением банков, операторов сотовой связи или известных разработчиков по определению телефонных номеров мошенников.

При поступлении Вам звонка с такого номера будет видна надпись «Есть жалобы на номер».

При звонках из банков, правоохранительных органов, прокуратуры, суда и иных органов власти попробуйте прервать разговор, поинтересовавшись, на какой номер телефона можно перезвонить. Если собеседник Вам сообщит, что ни в коем случае разговор прерывать нельзя, закончите общение с ним. Это мошенник!

Перепроверяйте сообщения от родственников и знакомых с просьбой срочно выслать денег. Сначала перезвоните ему и удостоверьтесь, что просьба действительно направлена от него. Злоумышленники могут через взломанный аккаунт рассылать сообщения с просьбами выслать деньги.

Говорите с ребенком и пожилыми родственниками о безопасности в Интернете. Объясните, что не вся информация в нем достоверна, и попросите советоваться с Вами по любому непонятному вопросу!

Наши контакты:

Адрес: г. Новосибирск, ул. Октябрьская магистраль, д. 4, 3 этаж

Телефон: +7 (383) 304-75-02

Е-mail: 4people\_54@grfc.ru