КАК УСТРОЕНА СХЕМА МОШЕННИЧЕСТВА В СФЕРЕ КРЕДИТОВАНИЯ

- Злоумышленник звонит и представляется от имени «сотрудника» банка и спрашивает, отправляли ли заявку на получение кредита.
- Начнет уговаривать взять кредит. В случае, когда заемщик отказывается, ему предлагают подключить программу рефинансирования со ставкой ниже и получить дополнительные средства. Злоумышленники уверяют, что программа позволит уменьшить финансовую нагрузку и вызывают заинтересованность потребителя. При такой схеме под риском хищения находится еще большая сумма, так как объединяются все кредиты жертвы в разных банках.

- После того как жертва отвечает «нет» и отказывается от получения, злоумышленник начинает действовать по другому сценарию и говорит, что за вас это сделали другие люди, замешанные в мошеннической схеме.
- Впечатленного клиента несложно убедить оформить кредиты в разных банках якобы для отмены мошеннических займов, а потом перевести на «безопасный» счет.
- В некоторых случаях чтобы вызвать доверие у собеседника, злоумышленники создают фейковые сайты, на которых якобы можно проверить, действительно ли вам звонит настоящий сотрудник банка или полиции.

МОШЕННИКИ МОГУТ ПРЕДСТАВИТЬСЯ СОТРУДНИКАМИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

- Аферисты от имени сотрудников правоохранительных органов: МВД, прокуратуры или ФСБ обзванивают людей, которые уже пострадали от рук мошенников и предлагают свою помощь.
- Подтверждают все слова, ФИО «работника» банка. Могут прислать выписки из банковского счета, удостоверения и другие подтверждающие документы, чтобы окончательно убедить, что ситуация реальная. Обманщики обещают найти преступников и наказать.
- В итоге жертвам предлагают обратиться в банк (или сразу в несколько) и подать новую заявку, чтобы аннулировать предыдущую.
- Как только жертва получает деньги, просят перевести их на новый «безопасный» счет. На самом деле данный счет принадлежит мошенникам.

КАК ПОНЯТЬ, ЧТО ЗВОНЯТ МОШЕННИКИ, А НЕ СОТРУДНИКИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Есть несколько факторов, на которые стоит обратить внимание во время разговора.

- При разговоре мошенники часто ссылаются на законы, могут начать давить чинами и специальными званиями. Мошенники это делают, чтобы вы не могли критически оценивать ситуацию.
- «Сотрудник» МВД, прокуратуры или ФСБ может сказать, что вы не имеете права рассказывать об этом звонке, потому что он под тайной следствия. Закон о неразглашении действительно существует, но работает по-другому.
- Настоящие сотрудники никогда не запрашивают конфиденциальную информацию, не станут спрашивать каким банком вы пользуетесь. Если у вас будут узнавать, на какую карту поступают денежные средства, сколько на ней на данный момент денег и когда вы последний раз выводили средства-это точно мошенники. Тем более не должны спрашивать реквизиты или CCV/CVC код банковской карты.

- Мошенники часто просят вас не вешать трубку. Жертву будут торопить, не давая времени на оценку ситуации. Они так делают, чтобы держать в напряжении.

КАК НЕ СТАТЬ ЖЕРТВОЙ И ДАЛЬНЕЙШИЕ ДЕЙСТВИЯ

Действуйте по алгоритму:

- Будьте спокойны и рассудительны. Ничего не говорите о себе, лучше узнайте кто именно вам звонит. Пытайтесь получить как можно больше информации. Спросите имя и фамилию, звание, должность «сотрудника», номер кабинета и отделение, в котором он работает.

> По 51й статье Конституции РФ вы имеете полное право не свидетельствовать против себя. Это значит, что даже настоящим сотрудникам вы можете ничего о себе не

- Повесьте трубку.

- Найдите в интернете официальный номер телефона отделения, которое вам назвали. Например, отделение банка или полиции.
- Позвоните туда или на горячую линию, попросите соединить с отделом безопасности. Спросите, есть ли у них сотрудник с таким именем, и объясните ситуацию. Скорее всего вам ответят «нет», и скажут, что это были мошенники.

> Если вас все-таки обокрали мошенники, то сразу обращайтесь в банк и МВД.

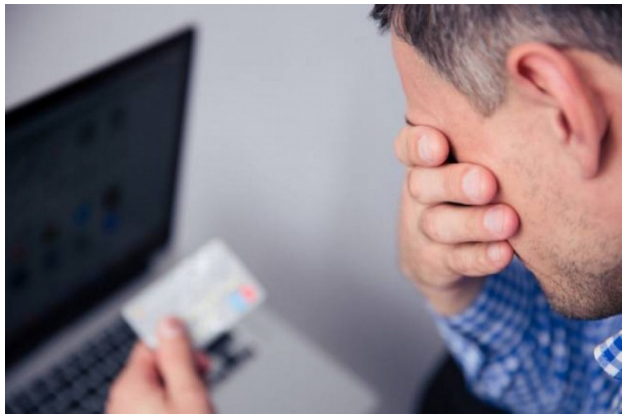
В СЛУЧАЕ СО СХЕМОЙ ПО РЕФИНАНСИРОВАНИЮ ЗАЩИТА МОЖЕТ БЫТЬ:

- Со стороны финансовой организации, который сам обеспечивает средствами на погашение рефинансируемых кредитов.
- Со стороны самого потребителя-понимание, что никто кроме его самого не может перечислять деньги.
- И конечно же, не забывать проверять кредитную историю на наличие действующих кредитов и в закрытии в полном объеме долгов и обязательств перед банком.

ГЛАВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ

- Помните, что настоящие сотрудники правоохранительных органов и банков никогда не попросят отправить деньги на «защищенный счет» или оформить встречный кредит.
- Не совершайте действия по звонку- никаких финансовых операций, кодов подтверждений и т.д. Общайтесь в отделениях с настоящими сотрудниками в форме.
- С осторожностью относитесь к звонкам с неизвестных номеров, особенно если к вам обращаются от имени службы безопасности банка или правоохранительных органов. Читать внимательно сообщения, которые направляет банк.
- Не устанавливайте на телефон посторонние программы, назначение которых вы не понимаете.
- Не общайтесь с банками в мессенджерах и проверяйте незнакомые ссылки, прежде чем переходить по ним.

ПРОКУРАТУРА РЕСПУБЛИКИ ТЫВА



КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИЧЕСТВА В СФЕРЕ КРЕДИТОВАНИЯ, МОШЕННИКИ ПОД ВИДОМ СОТРУДНИКОВ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

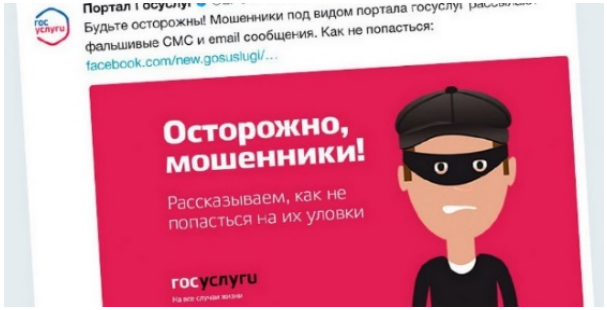
г. Кызыл
2023 г.

КАК ОБЕЗОПАСИТЬ СВОЮ УЧЕТНУЮ ЗАПИСЬ НА ПОРТАЛЕ ГОСУСЛУГ

Наши персональные данные на портале «ГОСУСЛУГИ» находятся под надежной защитой: их никому не передают без нашего согласия.

> Но к их безопасности стоит подходить серьезно, даже если вы пользуетесь ими не очень часто.

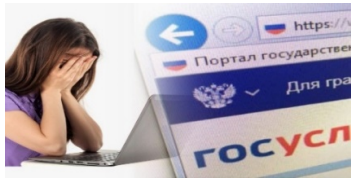
Ведь иногда злоумышленники могут получить доступ к вашему почтовому ящику или даже взломать личный аккаунт. Чаще всего это происходит из-за низкого уровня защиты и неосторожных действий самого владельца учетной записи.



Необходимо помнить, что безопасность определяется не только уровнем защиты портала, но и уровнем защиты вашего рабочего места, с которого осуществляется доступ. И если злоумышленник получит доступ к вашему аккаунту на «Госуслугах», он сможет действовать от вашего имени не только **на самом портале, но и за его пределами**.

Например:

- на вас могут оформить кредит;
- зарегистрировать на ваше имя фирму, проводящую сомнительные операции;
- распорядиться вашей собственностью на свое усмотрение.



КАК ЗАЩИТИТЬ СВОЙ АККАУНТ?

Портал «Госуслуги» предлагает несколько инструментов для защиты вашего аккаунта. Они также позволяют вам вовремя узнать о попытке взлома.

1. Используйте уникальный пароль

«Госуслуги» требуют от вас придумать длинный и сложный пароль, чтобы его было труднее подобрать. Однако сервис никак не может проверить его уникальность. Если вы воспользуетесь тем же самым паролем, которым защитили электронную почту и еще десяток аккаунтов на других сервисах, то утечка данных с любого из них поставит ваши документы под угрозу. Поэтому для такого важного аккаунта, как на «Госуслугах», не только рекомендуется, но и жизненно необходимо придумать уникальный пароль.

2. Включите оповещения о входе в ваш аккаунт Госуслуг

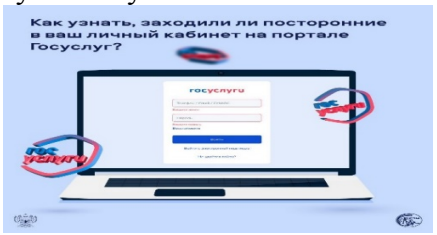
Если вы включите оповещения, то после каждого успешного входа вам придет письмо на электронную почту. Так вы узнаете, если кто-либо, кроме вас, получит доступ к аккаунту, и сможете своевременно поменять пароль. *Чтобы включить уведомления о входе:*

•Нажмите на свою аватарку и в открывшемся меню выберите Личный кабинет.

•На главной странице личного кабинета откройте вкладку Настройки.

•Нажмите Настройки безопасности.

•В блоке Оповещения о входе поставьте флажок «Присылать уведомление на электронную почту».



3. Задайте контрольный вопрос

Контрольный вопрос-это дополнительная мера защиты от попыток посторонних сменить пароль от вашего аккаунта. Но стоит помнить, что контрольный вопрос не защитит вас, если ответ на него легко угадать или найти в Интернете. Важно, чтобы его знали только вы, причем могли в любой момент его вспомнить.

Чтобы задать контрольный вопрос:

•Нажмите на свою аватарку и в открывшемся меню выберите Личный кабинет;

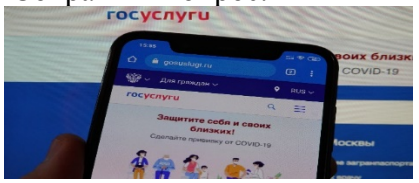
•На главной странице личного кабинета откройте вкладку Настройки;

•Нажмите Настройки безопасности;

•Выберите Задать контрольный вопрос;

•Введите вопрос, ответ на него и пароль;

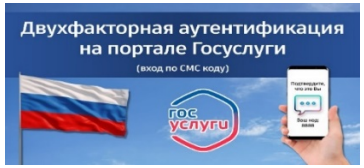
•Нажмите Сохранить вопрос.



4. Включите двухэтапную проверку входа

После включения двухэтапной проверки, чтобы войти в вашу учетную запись, злоумышленнику потребуется ввести не только пароль, но и одноразовый SMS-код, который придет на ваш телефон. Таким образом, вы будете в относительной

безопасности, даже если ваш пароль украдут. Заодно вы вовремя узнаете о том, что пароль попал не в те руки, и сможете оперативно сменить его.



Чтобы включить двухэтапную проверку:

• На главной странице личного кабинета откройте вкладку Настройки-Настройка безопасности. Включить двухэтапную проверку входа. Введите пароль от аккаунта и нажмите «Включить».

Однако мошенники придумали схему получения доступа вне зависимости от наличия двухфакторной аутентификации. Например, **взлом Госуслуг под видом пролонгации абонентского договора с оператором сотовой связи.** Она заключается в том, что гражданину звонит якобы представитель сотового оператора, у которого обслуживается номер телефона гражданина. Мошенники говорят, что номер старый, обслуживается, например, больше десяти лет, и его необходимо "пролонгировать". Иначе номер будет передан новому абоненту. Пролонгировать абонентский номер предлагается через сайт «Госуслуги». Для этого нужно только продиктовать код из пришедшего сообщения.

Если гражданин выполняет все указания звонящего, то у мошенников сразу появляется доступ к его личному кабинету "Госуслуг".

В этой связи **код из СМС и ответ на контрольный вопрос по телефону сообщать нельзя**: настоящий сотрудник Госуслуг никогда не попытается узнать эти данные.

5. Включите вход с помощью электронной подписи

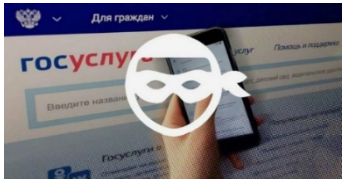
Если вы пользуетесь квалифицированной электронной подписью, можно применять ее и для входа в аккаунт. Этот метод надежнее SMS-кодов: перехватить сообщение с одноразовым кодом проще, чем подделать подпись. •Нажмите на свою аватарку и в открывшемся меню выберите Личный кабинет.

•На главной странице личного кабинета откройте вкладку Настройки.

•Нажмите Настройки безопасности.

•Выберите Включить вход с помощью электронной подписи.

•Введите пароль от аккаунта и нажмите Включить.



ЕСЛИ АККАУНТ ВЗЛОМАЛИ

Шаг 1: Восстановите доступ к учётной записи

1.Восстановите пароль онлайн на Госуслугах, через банк или в центре обслуживания

Шаг 2: Защитите аккаунт

Используйте вход с подтверждением, контрольный вопрос и другие опции для защиты аккаунта

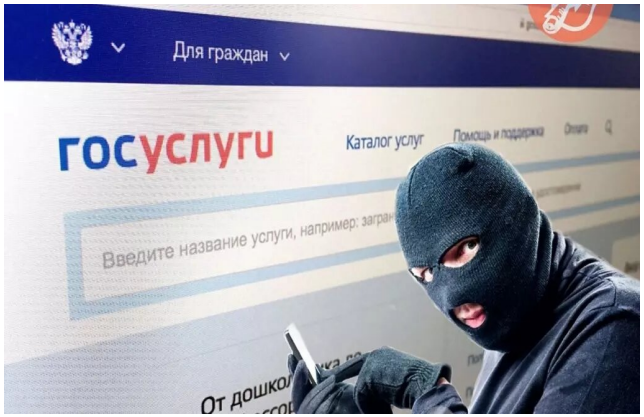
Шаг 3: Определите, где использовалась учётная запись

Шаг 4: Подайте заявление в МВД

Обратитесь в подразделение МВД. Расскажите о взломе и приведите всю информацию, которую знаете. Например, пригодятся время взлома или чужие контактные данные, которые были указаны в профиле

Если вы точно знаете, в какую организацию от вашего имени обратились мошенники, свяжитесь с ней напрямую. Сообщите о взломе и о том, что вы не подавали никаких заявлений и не совершали никаких действий.

ПРОКУРАТУРА РЕСПУБЛИКИ ТЫВА



ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ ВЗЛОМА АККАУНТА «ГОСУСЛУГИ»

г. Кызыл
2024 г.