Как не стать жертвой мошенничества «сайта Госуслуги».

1. Если вам звонят от лица Госуслуг и просят раскрыть конфиденциальную информацию, например, логин и пароль от учётной записи, не называйте их. **Служба поддержки Госуслуг никогда не запрашивает такие данные**! Положите трубку, зафиксируйте время и номер телефона собеседника, после чего напишите об этом в службу поддержки Госуслуг.

2. Помните, что мошенники могут назвать вас по имени и отчеству, указать дату рождения, серию и номер паспорта — такую информацию легко найти в интернете. Следует насторожиться, если собеседник начинает вас торопить, угрожать вам или доверительным тоном объяснять, что только он может помочь. **Сотрудники «Госуслуги» никогда не звонят без заявки гражданина**

3. Как защитить аккаунт от взлома. Самый действенный способ — создать надёжный пароль, основанный на фразе, которая не содержит личные данные, состоит минимум из 12 букв разного регистра, цифр и специальных символов и которую легко запомнить. **Также нужно обязательно подключить (двойное подтверждение) двухфакторную аутентификацию.**

4. Если у вас подключена двухфакторная аутентификация, то при попытке взлома вам в смс придёт код доступа для подтверждения входа. Это означает, что кто-то пытается войти в аккаунт, используя ваши логин и пароль В такой ситуации следует немедленно сменить пароль, сообщение кому-либо пароля также запрещено!

5. Как понять, что мне пишут мошенники. Обратите внимание, что все письма от Госуслуг приходят от отправителя **no-reply@gosuslugi.ru.** Если письмо пришло с другого адреса, даже очень похожего, это мошенники! Если в письме предлагается перейти по ссылке, чтобы сменить пароль, необходимо убедиться, что вы попали на сайт Госуслуг **gosuslugi.ru.** Если у вас установлен ненадёжный пароль, система может автоматически прислать уведомление. Если в письме сообщается о внезапной выплате или штрафе, прежде чем вводить данные карты, проверьте информацию: сделать это можно на сайте Госуслуг или в личном кабинете. Если информация отсутствует в официальных каналах, значит, это мошенническое письмо.

Как не стать жертвой мошенников, общие рекомендации:

1. Не сообщайте никому и никогда паспортные данные и финансовые сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или СМС-код. Сотрудники банков и государственных структур никогда не запрашивают такую информацию. Не публикуйте ее в социальных сетях, на форумах и каких-либо сайтах в Интернете, а также не храните данные карт и PIN-коды на компьютере или в смартфоне.

2. Если с неизвестного номера звонит сотрудник Центробанка, Госуслуг, правоохранительных органов, государственной организации или банка с сомнительным предложением (например, сообщением о попытке оформления кредита или подозрительной операции от вашего имени, обещанием высокого дохода по вкладу, предложением перевести средства на безопасный счет Центробанка, логина и пароля учётной записи Госуслуги) или по телефону запугивают и требуют быстрых действий с финансами, положите трубку. Если подозреваете, что вам звонит мошенник, позвоните в банк по номеру телефона, указанному на обратной стороне карты или на его сайте, или в контакт-центр ведомства, сотрудником которого представлялся звонящий.

3. Не совершайте каких-либо действий по счету, аккаунту если вам звонят из Центробанка, Госуслуг с просьбой или требованием о переводе денег, в том числе на «защищенный» или «специальный» счет, или с предложением об оформлении кредита. Банк России не открывает счета и не работает с гражданами.

4. По возможности установите антивирус на все устройства и обновляйте его.

5. Совершайте покупки в сети «Интернет» только на проверенных сайтах. Заведите специальную банковскую карту для онлайн-покупок и пополняйте ее ровно на ту сумму, которая нужна для оплаты. При совершении покупок обращайте внимание на наличие в строке браузера рядом с названием сайта значка безопасного соединения (замочка).

6. Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые предлагают, например, пройти опрос, получить какую-либо выплату и тому подобное. Официальные сайты финансовых организаций в поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой.

Это мошенники!

Как не стать жертвой мошенничества «с банковскими картами».

При использовании услуги «Мобильный банк».

В случае потери мобильного телефона с подключенной услугой «Мобильный банк» или мобильным приложением **например:** «Сбербанк Онлайн» следует незамедлительно обратиться к оператору сотовой связи для блокировки SIM-карты и в Контактный центр Банка для блокировки услуги «Мобильный банк» или мобильного приложения **например:** «Сбербанк Онлайн». Если вы потеряли карту или подозреваете, что она украдена, незамедлительно произведите ее блокировку.

Заблокировать банковскую карту можно разными способами:

1. **По телефону горячей линии.**

Универсальный способ. Номер для экстренной связи всегда указан на официальном сайте банка. Лучше заранее сохранить номер горячей линии банка в мобильном телефоне, чтобы не разыскивать его в экстренном случае. Оператор службы поддержки попросит назвать паспортные данные, кодовое слово или СМС-код, который пришлет вам на телефон. После этого он заблокирует карту.

2. **Через мобильное приложение.**

Самый быстрый способ, если у Вас есть доступ к интернету, приложение уже установлено на вашем телефоне и в нем есть опция по блокировке карты.

3. **В интернет-банке.**

Удобно, если у Вас подключен интернет-банкинг и рядом есть компьютер, планшет или смартфон с доступом в интернет. В личном кабинет на сайте банка обычно есть опция «Заблокировать карту». Свое решение надо будет подтвердить кодом из СМС, которое банк вышлет на ваш номер.

4. **По СМС.**

Некоторые банки используют систему СМС-команд. На короткий номер банка надо отправить кодовое слово

(например, «блокировка»). В ответ Вы получите код, который надо снова отправить на номер банка, чтобы подтвердить действие. Но лучше заранее уточнить, предлагает ли ваш банк такую услугу и какие кодовые слова нужно использовать.

5. <u>В отделение банка.</u>

Если вы находитесь рядом с офисом банка или потеряли телефон вместе с картой, пишите заявление о блокировке карты в отделении. Но для этого понадобится паспорт. Сразу после блокировки карты вы можете оставить заявку на выпуск новой. Если будете действовать быстро, у Вас есть шанс вернуть похищенное. Вы можете отменить операцию по карте, которую совершили мошенники. Но сделать это нужно не позднее следующего дня после того, как получите от банка уведомление об операции. Чтобы не дать шанса мошенникам украсть ваши деньги, внимательно отслеживайте все операции по картам. Банк обязан уведомлять вас о всех платежах - в вашем договоре прописано, каким способом он должен это делать.

6. <u>Лучше всего подключить СМС-оповещения.</u>

Отследить операции по карте вы также можете через мобильное приложение или онлайн-банк. Всегда можно получить выписку по счету в отделении банка и иногда через банкомат. Если у вас украли карту, имеет смысл перепроверить все последние платежи. Если вы ведете переписку в социальной сети «В Контакте», мессенджерах «WhatsApp, Telegram, Viber и др., если вы общаетесь с кем-то, используя сайт знакомств, будьте бдительны! Не присылайте незнакомцам ваши личные фото. Вашим доверием могут воспользоваться злоумышленники.

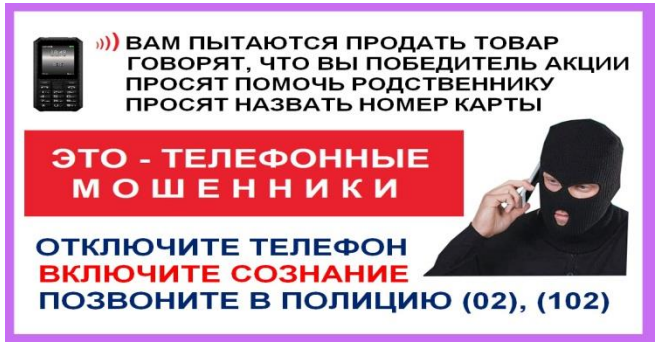
<u>КУДА ОБРАЩАТЬСЯ:</u>

Если вы столкнулись с фактом совершения мошеннических действий или вам стало известно о готовящемся хищении путём обмана - **СРОЧНО ЗВОНИТЕ В ПОЛИЦИЮ <u>по месту совершения преступления!</u>**

<u>Контакты отдела МВД России по г. Северодвинску</u>

г. Северодвинск, ул. Индустриальная, д. 26.
Дежурная часть: 8-(8184)-56-05-58
8-(8184)-56-15-59

<u>Единый номер вызова служб экстренного реагирования:</u> «102» «112» (для дальнейшего соединения с органами правопорядка нажать кнопку «2»)



При бездействии полиции,
Вы вправе обратиться
<u>в прокуратуру г. Северодвинска</u> по адресу:
г. Северодвинск, ул. Торцева, д. 16 А.

Дежурный прокурор:8-921-671-15-49
Наш email: severodvinsk@29.mailop.ru

ПРОКУРАТУРА РАЗЪЯСНЯЕТ

КАК НЕ СТАТЬ ЖЕРТВОЙ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Для хищения денежных средств у граждан злоумышленники используют все более изощренные сценарии.
В результате жители г. Северодвинска страдают от их действий, теряют деньги, которые в некоторых случаях копили годами.

Знания о том, как противостоять мошенничеству, помогут в нужную минуту принять единственно правильное решение.

Прокуратура
г. Северодвинска

2024 г.