Новые схемы и маски мошенников:

Мошенники предлагают пересчитать пенсию из-за неучтенного стажа работы

Злоумышленники звонят пожилым людям и **представляются работниками Социального фонда России (СФР)**. Они сообщают, что размер текущей пенсии можно существенно увеличить, так как будто бы обнаружен неучтенный трудовой стаж. Тех, кто поверил аферистам, приглашают якобы на консультацию в Многофункциональный центр или отделение СФР для решения вопроса. Причем мошенники называют настоящие адреса центров или отделений, которые находятся в городе, где живет потенциальная жертва. Это усыпляет бдительность человека.

По сценарию злоумышленников, для записи на прием человек должен предоставить данные паспорта, СНИЛС, ИНН и назвать код из СМС-сообщения. На деле перечисленные документы и числовой код из сообщения нужны мошенникам для получения доступа к учетной записи человека на портале Госуслуги. Заполучив доступ к ней, они могут беспрепятственно оформить на жертву кредиты или займы.

Что предпринять:

При поступлении такого телефонного звонка прервите разговор. Настоящие сотрудники государственных служб, в том числе Социального фонда России, не звонят с подобными вопросами. По любым социальным вопросам нужно самостоятельно позвонить в единый контактный центр СФР по телефону 8-800-10-000-01 либо обратиться в ближайшее отделение фонда. Никому и никогда не сообщайте личные данные, реквизиты карт, СМС-код, а также логины и пароли от своих аккаунтов

Новые схемы и маски мошенников:

Аферисты обманывают граждан, представляясь **сотрудниками Федеральной службы судебных приставов.**

Они звонят своим потенциальным жертвам и сообщают о наличии исполнительного производства, настаивая при этом на немедленном погашении долга.

Схема новая, неизменным остается одно — попытка добраться до счетов граждан.

Узнавайте информацию через официальные сайты!

Сайт Федеральной службы судебных приставов - http://fssprus.ru.

Либо вы можете получить квитанцию, придя на личный прием к судебному приставу, и оплатить непосредственно по квитанции либо через портал «Госуслуги».

Пожалуйста, будьте бдительны и не передавайте незнакомым людям свои личные данные.

Новые схемы и маски мошенников:

Мошенники представляются работниками **«Почты России»** или же каких-то других почтовых служб**.**

Во время такого звонка, если пользователь сразу не кладет трубку, аферист заявляет о том, что человеку якобы поступила посылка из-за рубежа, за которую требуется перечислить таможенный сбор.

В этом случае многие граждане сообщают мошенникам, что они никакой посылки из-за рубежа не заказывали и не ждали. Тогда аферисты сообщают, что для отмены посылки и для того, чтобы не платить таможенный сбор, необходимо продиктовать код из SMS-сообщения, который придет на телефонный номер абонента.

В действительности же в этот момент на телефонный номер потенциальной жертвы приходит SMS-сообщение с кодом подтверждения.

Однако этот код мошенники запрашивают, чтобы получить доступ к личному кабинету пользователя в онлайн-банкинге или же к аккаунту на портале госуслуг и других популярных сервисов, где содержатся чувствительные данные.

Чтобы не стать жертвой таких киберпреступлений необходимо оставаться максимально бдительными и критически оценивать любые запросы на передачу конфиденциальных данных или персональной информации, которые поступают от неизвестных лиц по телефону, в социальных сетях и мессенджерах.

Представители государственных органов, «Почты России» и других учреждений никогда не будут запрашивать логины, пароли, коды подтверждения из SMS-сообщений и другие идентификационные данные.

Новые схемы и маски мошенников:

Мошенники звонят **от имени сотрудников Федеральной налоговой службы.**

Они сообщают человеку по телефону, что видят неучтенные при расчете налога доходы, и предлагают провести сверку по документу, который уже направили.

Человек у себя документ не находит.

Псевдоналоговик объясняет это рассинхронизацией с порталом Госуслуг и предлагает назвать код из SMS, чтобы исправить ситуацию.

Далее с этой информацией мошенники получают доступ к личной странице Госуслуг и личным данным человека.

Правила:
Как защитить себя от социальной инженерии

Схема действий злоумышленников всегда одинакова: обманным путем они вынуждают человека самостоятельно сообщить данные для входа в личный кабинет банковского приложения, мобильного оператора, Госуслуг и других полезных ресурсов. Чтобы звучать убедительно и воздействовать на эмоциональном уровне, они затрагивают самые актуальные темы.

Мошенники могут представляться сотрудниками социальных служб, медиками, правоохранителями, обещать выигрыш в лотерею или увеличение пенсии, выплаты от государства или выгодный кредит. Такие методы получения доступа к данным называются социальной инженерией.

! Будьте бдительны во время телефонных разговоров. *Не торопитесь. Если диалог кажется вам подозрительным,* прервите звонок. Лучше перезвоните в банк или организацию по номерам, указанным на официальном сайте.

Обратите внимание на способ связи. Для звонков мошенники часто используют мессенджеры. Настоящие представители ведомств и органов власти никогда не будут звонить через WhatsApp или Telegram.

Не сообщайте никому логины и пароли от личных кабинетов. Не говорите никому смс-коды Госуслуг и ответ на контрольный вопрос, который вы используете для восстановления доступа.

Внимательно следите за актуальностью номера, к которому привязан аккаунт.

Используйте сложные пароли, периодически меняйте их. Если сервис позволяет, подключите двухфакторную аутентификацию. На Госуслугах в качестве второго фактора можно выбрать смс-код, одноразовый ТОТР-код и вход по биометрии.

Внимательно изучайте адрес страницы, на которой вводятся данные, чтобы не попасть на фишинговый ресурс.

Единственно верный адрес Госуслуг — gosuslugi.ru.

Госуслуги надежно защищены, и злоумышленник может получить доступ к аккаунту только в том случае, если пользователь сам передаст всю необходимую для входа информацию. На портале есть все инструменты для того, чтобы обезопасить аккаунт. Но нужно бережно относиться к своим данным.

Инструкция:

Если аккаунт на Госуслугах взломали

Шаг 1: восстановите доступ к учетной записи

1. Восстановите пароль онлайн на Госуслугах, через банк или в центре обслуживания.
2. Проверьте, ваши ли номер телефона и почта указаны в личном кабинете.

Шаг 2: защитите аккаунт

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

Шаг 3: определите, где использовалась учетная запись

1. Перейдите в личный кабинет → Безопасность → Действия в системе. Проверьте, не было ли подозрительных действий в учетной записи. Если были, и учетная запись использовалась на Госуслугах, обратитесь в службу поддержки. Если на стороннем ресурсе — в службу поддержки данного ресурса.
2. Выйдите из приложений, в которые вы не заходили: личный кабинет → Безопасность → Моб. приложения.
3. Отзовите разрешения, которые вы не выдавали: личный кабинет → Согласия и доверенности → Разрешения.
4. Проверьте поданные заявления. Это поможет выявить, какие действия хотели совершить мошенники от вашего имени.

Шаг 4: обращение в организацию, в которую обратились мошенники

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.

Шаг 5: 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.

Инструкция:

Как защитить учетную запись на Госуслугах

Подключите дополнительные опции для входа на Госуслуги

1. Перейдите в личный кабинет → Безопасность → Вход в систему.
2. В разделе «Вход с подтверждением» выберите удобный вариант: подтверждение по смс, одноразовому коду или биометрии.
3. В разделе «Контрольный вопрос» переведите переключатель в активное положение и установите вопрос.
4. В разделе «Уведомления о входе» переведите переключатель в активное положение

Как подключить вход с подтверждением

Как настроить контрольный вопрос

Дополнительные меры безопасности

- Используйте уникальный логин и пароль, которые не встречаются на других сайтах.
- Никому не сообщайте ответ на контрольный вопрос и коды из смс, приходящие от отправителя gosuslugi и с номера 0919.
- Внимательно проверяйте адрес сайта.

Единственно верный адрес Госуслуг — gosuslugi.ru. Проверяйте, чтобы в адресной строке не было похожих написаний вроде gossuslugi, gos.uslugi, gosuclugi и других.

- Не переходите по подозрительным ссылкам. Ссылки от Госуслуг обычно ведут в личный кабинет, на конкретную услугу, сайты ведомств.
- Не открывайте присланные файлы, если не уверены в отправителе.

! Письма от Госуслуг приходят с адресов:

no-reply@gosuslugi.ru или no-reply@pos.gosuslugi.ru

- Устанавливайте официальные приложения. Приложение «Госуслуги» можно скачать в RuStore, Google Play, App Store и AppGallery.