ЮРЛОВ И ПАРТНЕРЫ
Адвокатское бюро

КОМУ ВАЖНО:
Физическим лицам

ПРОФИЛАКТИКА ТЕЛЕФОННОГО МОШЕННИЧЕСТВА И КРАЖИ ДОСТУПА К ГОСУСЛУГАМ

В связи с резким ростом телефонного мошенничества в этой рассылке мы поделимся полезными советами, которые помогут вам распознать мошенников, обеспечить защиту своих персональных данных и защитить свои права после несанкционированного доступа к сайту Госуслуг.

1. Что такое мошенничество по краже доступа к Госуслугам?

Мошенничество по краже доступа к сайту Госуслуг является преступлением в сфере компьютерной безопасности – ст. 272.1 УК РФ, а последующее хищение имущества потерпевшего может быть квалифицировано как мошенничество – ст. 159 УК РФ.

!!! Основной признак, что звонят мошенники – просьба сообщить КОД или перейти по ссылке из СМС-сообщения. !!!

Способы получения доверия	
Звонок из органов *под видом сотрудников правоохранительных органов*	указывают на правонарушения, совершенное вами или вашими близкими, просят оказать содействие в раскрытии преступления
Звонок от сотового оператора *под видом работника сотового оператора*	указывают, что в скором времени истекает срок действия договора
Звонок от менеджеров по доставке товаров *под видом работника службы доставки или почтового отделения*	выбирают праздничные дни. Звонят под предлогом получения обратной связи по услуге
Звонок из поликлиники *под видом работника поликлиники*	предлагают перенести или повторно назначить запись к врачу

!!! Действия мошенников всегда нацелены на получение КОДа из СМС-сообщения!!!

2. Последствия утери доступа аккаунта Госуслуг

За 1 час доступа к аккаунту гражданина мошенники смогут:

- оформить несколько кредитных договоров, используя данные с Госуслуг;
- создать усиленную квалифицированную электронную подпись в приложении «Госключ» для заключения иных договоров;
- продать автомобиль посредством электронного договора купли-продажи.

Утеря доступа от аккаунта приводит к раскрытию персональных данных гражданина, включая паспорт, СНИЛС, ИНН, полис ОМС, сведения о движимом и недвижимом имуществе, а также историю всех ваших запросов в гос. органы через портал «Госуслуги».

Чтобы избежать распространения персональных данных необходимо проявлять настороженность при общении с людьми, которые звонят с неизвестных вам номеров или используют скрытие номера.

!!! ПОМНИТЕ !!!

Сотрудники государственных органов в крайне редких случаях звонят по телефону. Госслужащие и представители компаний никогда не станут по телефону требовать информацию из СМС-сообщений и общаться с вами в неподобающей манере.

3. Порядок действий, если мошенники получили доступ к Госуслугам

1. Восстановите пароль / сменить пароль от портала.

2. Установите подтверждение входа через телефон.

3. Совершите выход со всех устройств.

Лучше всего эти шаги выполнить в ближайшем отделении «Мои Документы», т.к. сменить пароль самостоятельно через телефон или почту может оказаться уже невозможно. Сотрудники МФЦ помогут вам быстрее разобраться с этими вопросами в стрессовой ситуации.

4. Посмотрите, где использовалась учётная запись.

Перейдите в *личный кабинет → Профиль → Безопасность → Действия в системе.*

Обращайте внимание на действия, совершенные в отношении кредитных организаций.

5. Проверьте заявления и уведомления за время пока у мошенников был доступ к вашему аккаунту.

Обычно они запрашивают обновление данных электронной трудовой книжки (ЭТК), индивидуального лицевого счёта (ИЛС), 2-НДФЛ, чтобы узнать больше финансовой информации о вас.

6. Убедитесь, что на вас не оформили кредит.

Введите в *поисковой строке запрос «выписка БКИ» → «узнать свое БКИ».*

Необходимо *перейти по ссылке в PDF документе, который вам отправят ответом на запрос → авторизироваться → выполнить запрос отчета кредитной истории.*

7. Подайте заявление в МВД.

Это нужно сделать, даже если в кредитной истории нет неизвестных вам заявок на кредит. Мошенники могут использовать ваши данные позже, если у них останется доступ к учётной записи на Госуслугах. Поданное заявление поможет доказать, например, что кредит или заём оформляли не вы.

Заявление в МВД необходимо подавать лично, сотрудники органов помогут грамотно оформить ваше заявление. При этом нужно получить номер записи в книге учета сообщений о преступлении (КУСП).

8. Обратитесь в банк или МФО, если на вас взяли кредит.

Лучше всего явиться к ним уже после подачи заявления в МВД, т.к. в ином случае банк с большей вероятностью откажет вам в аннулировании кредита.

9. Подайте Жалобу.

Центробанк, Минцифры — если мошенники взяли кредит в банке;

Финансовому уполномоченному — если в микрофинансовой организации.

Если же жалоба не помогла, то необходимо обращаться в суд с заявлением о признании договора недействительным.

4. Самозапрет на кредиты

1 марта 2025 года в силу вступает новый закон, благодаря которому каждый гражданин сможет ввести в отношении себя запрет на заключение кредитных договоров.

Для «включения» механизма будет достаточно зафиксировать специальный запрет в своей кредитной истории через портал «Госуслуги» или в МФЦ. Достаточно заполнить шаблонное заявление, выбрав желаемые условия запрета. Для его снятия также нужно подать заявление. Эта услуга будет бесплатной и неограниченной по числу обращений.

При этом допускается наложение запрета в зависимости от кредитной организации – банк или МФО, а также в зависимости от способа обращения – дистанционно или в офисе.

!!! БУДЬТЕ БДИТЕЛЬНЫ ПРИ ОБЩЕНИИ С НЕЗНАКОМЦАМИ И ЗАЩИЩАЙТЕ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ!!!

23.12.2024 г.
С наилучшими пожеланиями,
Адвокатское бюро «Юрлов и Партнеры»

Контакты:

Старший Партнер Бюро, адвокат
Цепков Владислав Николаевич
v.tsepkov@y-p.ru