

«Сотрудники полиции Алтайского края напоминают:

В последнее время участилось количество звонков гражданам от потенциальных мошенников, которые могут представляться:

- сотрудниками правоохранительных органов (полиции, прокуратуры, следственного комитета);
- сотрудниками дежурных частей;
- следователями;
- сотрудниками банков и иных финансовых и кредитных организаций;
- сотрудниками служб безопасности банков;
- сотрудниками портала Государственных услуг;
- представителями брокерских контор, финансовых бирж, фондов, различных инвестиционных компаний;
- представителями медицинских страховых компаний;
- ясновидящими, целителями, магами.

Злоумышленники пользуются различными софтами и программами, позволяющими осуществить замену номера, с которого поступает звонок.

В связи с этим принимающая сторона видит телефоны, похожие или полностью повторяющие горячие линии банков, дежурных частей, иных официальных органов и организаций, которые зачастую могут начинаться с цифр 8-800... или 8-495...

Как правило, звонящий, который представляется сотрудником службы безопасности банка или правоохранительных органов, сообщает о том, что на вашем счете замечены подозрительные операции и для того, чтобы «обезопасить» деньги, нужно перевести их на другой счет или даже оформить кредит на ваше имя, чтобы «вычислить преступника». Нельзя поддаваться на подобные настоятельные просьбы. Необходимо положить трубку и сделать ответный звонок. Ответный звонок позволит попасть на настоящую справочную линию банка, страховой компании или в дежурную часть полиции. Здесь подтверждают, что никто не интересовался вкладами конкретных граждан.

Помимо того, что «на вашем счете замечены подозрительные операции» злоумышленники могут сообщить следующую информацию:

- вы стали обладателем крупного выигрыша, за который нужно заплатить налог;
- ваш родственник (сын, внук) попал в беду (совершил ДТП) и для решения вопроса о не возбуждении уголовного дела или лечения пострадавшего в ДТП нужны деньги;
- вам положена компенсация за ранее приобретенные лекарства и БАДы;
- вы можете приумножить свой капитал в кратчайшие сроки, если доверите свои деньги некоему фонду или биржевому брокеру, согласитесь инвестировать их в тот или иной проект, купить акции предприятия с известным названием;
- вам пишет друг по социальной сети и просит занять денег (как правило, страница взломана, просьбы о займе поступают от злоумышленников)».

Еще одна мошенническая схема связана с противоправными действиями потенциальных мошенников, которые за счет грамотно построенной убедительной беседы, используя методы социальной инженерии и психологические приемы, втираются в доверие и получают от жертвы необходимые персональные данные (номера паспорта, СНИЛС, счетов, банковских карт) и оформляют на ничего не подозревающего гражданина кредиты, которые тут же выводят на подконтрольные счета. Гражданин узнает об этом только тогда, когда банк начинает требовать погашение графика кредитных выплат с процентами. Так могут действовать злоумышленники, которые представляются сотрудниками портала «Государственные услуги».

Стать жертвой мошеннических посягательств может владелец личного кабинета на сайте «Госуслуг». Как правило, злоумышленники представляются сотрудниками портала и просят продиктовать им код из СМС-сообщения.

Причины называют разные: для активации учетной записи, привязки куар-кода к странице или для усиления безопасности. На самом деле аферисты пытаются с помощью граждан получить доступ к их аккаунту, только уже под своим паролем. Все это нужно для того, чтобы получить доступ к персональным данным и от имени зарегистрированных пользователей оформлять кредиты и микрозаймы. Поэтому при подготовке информации, связанной с данной мошеннической схемой необходимо разъяснить, что сотрудники портала «Государственные услуги» никогда не звонят гражданам с подобными просьбами

«Сотрудники полиции Алтайского края обращают внимание, что:

- никогда сотрудники банков или сотрудники служб безопасности банков инициативно не звонят клиентам для того, чтобы выяснить их персональные данные и узнать номера счетов;
- ни в коем случае нельзя никому сообщать номера своих банковских карт в комбинации с CVC- кодом (три цифры с обратной стороны карты);
- категорически нельзя в ответ на подозрительный звонок неизвестного вам лица брать крупные суммы в кредит для того, чтобы перевести их на некий «безопасный счет»;
- в социальных сетях необходимо использовать более сложные, многоступенчатые пароли, чтобы страницу не взломали;
- при продаже-покупке через Интернет нужно внимательно изучать страницу продавца, не пользоваться товарами или услугами продавцов, у которых нет рекомендаций, а аккаунт является недавно зарегистрированной страницей (как правило, это страница-однодневка);
- при покупке товаров через Интернет обращать внимание на то, чтобы не попасть на сайт-двойник, который могут создать злоумышленники. В таком случае вся информация, которую вы вводите для оплаты товара: сумма, номер, срок действия банковской карты, CVC-код – становятся известными посторонним лицам;
- ни при каких обстоятельствах нельзя передавать посторонним лицам сведения о своих счетах и банковских картах, а также не совершать никаких действий со своими картами и вкладами, о которых просят незнакомые лица по телефону, тем более не выполнять никаких действий в банкомате со своей банковской картой под диктовку неизвестного лица».

Целесообразно также акцентировать внимание на следующей рекомендации, адресованной гражданам: «При возникновении любых вопросов либо сомнений необходимо проконсультироваться непосредственно в отделении названного банка, позвонить на горячую линию кредитной организации, уточнить сведения по телефону доверия полиции, обратиться в ближайшую дежурную часть. Будьте бдительны! Не отдавайте свои деньги мошенникам!».

**«Ваш родственник попал в беду»,
целесообразно использовать следующие рекомендации:**

«Сотрудники полиции напоминают простые правила:

- проведите беседы со своими пожилыми родственниками;
- расскажите им об этом виде мошенничества;
- объясните, что прежде всего надо позвонить своим родным и убедиться, что с ними все в порядке, а не отдавать в панике деньги незнакомым людям.

Помните: злоумышленники звонят под видом родственника (сына, внука, дочери и так далее) либо сотрудника правоохранительных органов и сообщают, что близкий человек стал виновником ДТП. Незнакомый голос мошенники объясняют плохой связью, полученной травмой либо, чтобы отвести подозрения, прерывают разговор и передают трубку сотруднику полиции. Далее они просят передать им деньги якобы для возмещения ущерба потерпевшим либо на лечение пострадавшего родственника. Потенциальные преступники также могут сообщить, что эта сумма необходима для того, чтобы уголовное дело не возбуждалось. Аферисты убеждают пожилых людей положить деньги в пакет и передать их курьеру».