

Ежедневно количество зарегистрированных фактов мошеннических действий на территории Алтайского края увеличивается. Зачастую жертвами мошенников становятся люди уже не раз попадавшие на «удочку» преступников. В реалиях пандемии, бдительность граждан снижается, а желание быстрого заработка денежных средств с каждым днем становится все ярче выражена!

Наиболее распространенные схемы мошеннических действий:

### **Покупки в интернете.**

Клиент находит объявление о продаже товара или услуг. Переводит деньги, мошенники перестают выходить на связь.

#### **«Близкий человек попал в беду».**

В соцсетях пишет родственник или друг. Он попал в непростую ситуацию и ему срочно нужны деньги. Так действуют мошенники, взломав аккаунты.

### **Служба безопасности банка.**

Клиенту поступает звонок или SMS с просьбой перезвонить. Мошенники представляются службой безопасности банка, говорят, что зафиксирована попытка списания денег со счета клиента, выясняют данные карты и коды подтверждения и списывают деньги со счета.

### **Продажа в интернете.**

Клиент размещает объявление о продаже товара. Мошенники звонят и узнают данные карты продавца под предлогом необходимости совершить перевод за товар. Далее они списывают деньги с карты, узнав у продавца код подтверждения (якобы он нужен для зачисления). Другой вариант этой схемы — использование подложного сервиса «безопасной сделки» в интернете.

### **Программы удаленного доступа.**

Звонит «служба безопасности банка»: на устройстве клиента обнаружен вирус, необходимо скачать антивирус и сканировать гаджет. Во время сканирования устройство, якобы, нельзя использовать, так как вирус может распространиться дальше. На самом деле клиент скачивает программу удаленного доступа, а во время «проверки» мошенники получают доступ к мобильному банкингу и выводят средства клиента.

### **Безопасный счет.**

Звонок от «службы безопасности»: произошла утечка данных, в ней замешаны сотрудники. Необходимо снять деньги через безопасный банкомат банка-партнера и перевести их на специальный страховочный счет. Другим вариантом этой схемы является сценарий, когда преступники предлагают сразу перевести деньги на счет, не снимая их в банкомате. За причиненные неудобства клиенту предлагается вознаграждение. Мошенники просят не отключать телефонную связь во время операций. Предупреждают, что "банк" не несет ответственность за сохранность денег по условиям обслуживания счета: если их не снять, они могут пропасть.

### **Автоматическая голосовая служба банка.**

Звонок из «банка»: был зафиксирован вход в личный кабинет из другого города или страны. В рамках мер по безопасности необходимо назвать номер карты для идентификации. Мошенники предупреждают, что сейчас поступит код по SMS, но его никому нельзя называть. После чего переключают на голосовую службу. Клиент доверяет голосу робота и вводит код в тональном режиме. Мошенники меняют пароль и логин в его личном кабинете и выводят деньги.

### **МО МВД России «Алейский» предупреждает!**

Чтобы обезопасить себя от мошенников, необходимо соблюдать следующие меры безопасности:

- **Нужно всегда держать в тайне следующие данные: коды из SMS, PIN-код карты, контрольные вопросы, данные карты, включая срок действия и трехзначный код. Нельзя также раскрывать персональные данные: отчество, место и год рождения, данные паспорта.**
- **Если кто-то позвонил сам, не следует ему доверять, даже если он представился сотрудником банка. Нужно перезвонить в банк в случае подозрительного звонка или сообщения от банка.**
- **Не нужно скачивать никакие программы на смартфон по просьбе незнакомцев и тем более предоставлять им доступ к ним.**
- **Не нужно носить записанный пин-код рядом с картой. Лучше подключить оповещения об операциях и настроить лимиты на траты.**
- **Для быстрой связи с банком нужно заранее сохранить его номера в телефоне.**

- Если карта пропала — нужно сразу же связаться с банком, заблокировать карту, проверить операции и обратиться в банк для выпуска карты.
- Если украли деньги со счета — нужно связаться с банком и описать ситуацию. После чего — написать заявление в полицию и отправить в банк талон о принятии заявления
- Если пропал телефон — нужно связаться с банком для блокировки приложения и удаления данных карты со смартфона. Также нужно немедленно обратиться к сотовому оператору для блокировки сим-карты и проверить последние операции.

**При возникновении вышеописанных ситуаций, незамедлительно обращайтесь в дежурную часть по телефону 8-38553-21-333. Будьте бдительны и не попадайтесь на уловки мошенников!!!**