Одним из основных видов преступных посягательств в настоящее время являются факты хищения денежных средств с использованием информационно-телекоммуникационных технологий.

При совершении данных преступлений злоумышленники зачастую пользуются доверием граждан, в результате чего потерпевшими самостоятельно осуществляются действия по передаче персональных данных или переводу денежных средств.

Также мошенники представляются с целью получения доступа к персональным данным, управлению банковским счетом или мобильным телефоном как сотрудники банковских или кредитных организаций или правоохранительных органов.

В настоящее время злоумышленники нередко прибегают к такому способу как «дублирование телефонных номеров», т.е. при помощи специального компьютерного обеспечения телефонный номер с которого гражданам поступает звонок, является идентичным официальному номеру банка или правоохранительного органа. В таком случае необходимо руководствоваться правилами, изложенными ниже.

Кроме того, данные преступления относятся к категории трудно раскрываемых ввиду применения злоумышленниками значительных мер конспирации, таких как оформление разовых абонентских номеров на лиц, не осведомленных об использовании их данных для совершения преступления, транзитных банковских счетов и счетов неперсонифицированных интернет-кошельков.

Для того, чтобы не стать жертвой преступников необходимо запомнить и знать определенные правила, в случае :

СОТРУДНИКИ БАНКА И ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ НИКОГДА НЕ ПРОСЯТ СООБЩИТЬ ИМ:

1) ПИН-код и код безопасности, расположенный на оборотной стороне карты;

2) Персональные данные (ФИО, серия, номер паспорта, адрес регистрации);

3) Реквизиты и данные о сроке действия карты;

4) Пароли и коды из СМС-сообщений для подтверждения финансовых операция или их отмены.

В случае, если Вам поступает звонок и собеседник просит предоставить вышеуказанные данные, то необходимо немедленно прекратить разговор и уведомить о звонке банковскую организацию и правоохранительные органы.

СОТРУДНИКИ БАНКА И ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ НИКОГДА НЕ ПРЕДЛАГАЮТ:

1) Установить программы удаленного доступа или сторонние предложения на мобильное устройство и разрешить подключение к ним под предлогом удаления вирусов, помощи в переводе денежных средств и т.д.

2) Перейти по ссылке из СМС-сообщения;

3) Под их руководством перевести для сохранности денежные средства на «защищенный счет».

В рамках телефонного общения сотрудники банковских организаций могут только осуществлять консультации по продуктам и услугам кредитно-финансового учреждения.

КРОМЕ ТОГО, С ЦЕЛЬЮ СНИЖЕНИЯ ПОТЕНЦИАЛЬНОЙ ВОЗМОЖНОСТИ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ НЕОБХОДИМО:

1) Не записывать ПИН-код на бумаге и не хранить рядом с картой, в том числе и в бумажнике;

2) Не вводить данные банковской карты не неизвестных интернет-страницах, а также страницах сомнительного содержания. При осуществлении покупок посредством сети «Интернет» пользоваться общеизвестными ресурсами и магазинами. Учитывать обстоятельство, что объявления о продаже дорогостоящих вещей с необъяснимо высокой скидкой может являться уловкой мошенников.

3) При снятии денежных средств с банкомата принимать меры предосторожности при вводе ПИН-кода на банкомате. Не прислушивайтесь к советам посторонних лиц, предлагающих Вам свою помощь при осуществлений операций в банкоматах;

4) Подключить услугу SMS-оповещений и реагировать на них, в случае поступления сообщения, связанного с несанкционированным списанием денежных средств;

5) Установить лимиты на совершение операций, связанных с переводом денежных средств, которые смогут исключить факт разового списания крупных денежных сумм и

вовремя предотвратить хищение денежных средств;

6) Использовать только официальные приложения банковских организаций, размещенных в магазинах App Store, Google Play, Microsoft Store;

7) В случае поступления звонков с подозрительных номеров либо при наличии сомнений о добропорядочности собеседника, прервите разговор и обратитесь в близлежащий филиал банковской организации лично или по номеру, указанному на банковской карте, чтобы уведомить их о подозрительном звонке;

8) Сотрудники полиции, Следственного комитета РФ, ФСБ России и иных правоохранительных органов **НИКОГДА** даже с целью пресечения противоправных посягательств не будут просить Вас сообщить свои персональные данные или информацию о банковской карте в рамках телефонного звонка, а также не будут просить Вас перевести денежные средства на другой счет.

9) Сотрудники правоохранительных органов **НИКОГДА** не просят перевести денежные средства для «решения вопроса» с целью помощи родственникам или друзьям, попавшим в затруднительное положение и прекращения административного или уголовного производства (например, при совершении ДТП с наличием пострадавших лиц). В таком случае необходимо прекратить разговор и как можно быстрее связаться с лицом, для помощи которому Вас просили перевести денежные средства.

Также необходимо помнить, что у Вас могут быть пожилые родственники или родители, которые являются группой риска при совершении подобных преступных посягательств. Ввиду новизны данного вида преступления, сложности понимания используемых механизмов и схем, а также оказания психологического давления и злоупотребления доверием данные лица наиболее подвержены риску совершения в отношении них преступлений.

Разъясните своим родственникам в доступной форме какие действия им не следует совершать при поступлении телефонных звонков подобного рода, постоянно находитесь на связи с ними, чтобы исключить факты возможного совершения мошеннических действий.

Гражданам необходимо быть бдительными при обращении с банковскими картами и электронными денежными средствами и принимать меры предосторожности. При возникновении малейших подозрений предпринимаемых попыток совершений мошеннических действий следует незамедлительно уведомлять об этом банковскую организацию и правоохранительные органы

Контактная информация

В случае, если в отношении Вас совершены мошеннические действия и Вы стали жертвой злоумышленников, то можете обратиться в ОМВД России по Соль-Илецкому городскому округу по номерам телефонов – 102, 8 (35336) 2-48-02, либо по адресу: г. Соль-Илецк, ул. Вокзальная, д. 119, а также в УМВД России по Оренбургской области по номерам телефонов -8 (3532) 79-02-01, 102, либо по адресу: г. Оренбург, ул. Комсомольская, д. 49

Прокуратура Соль-Илецкого района

Как избежать хищения денежных средств с банковских карт и счетов

2021