Прокуратура
г. Бодайбо

Главам муниципальных образований

28.12.2021 № 1-19-2021

ИНФОРМАЦИЯ
для размещения на официальных сайтах

Заголовок «Прокуратура г. Бодайбо разъясняет, как не оказаться жертвой хищения безналичных денежных средств с банковских карт (счетов)».

Содержание: Прокуратурой города проанализированы факты хищения безналичных денежных средств с банковских счетов граждан с использованием информационно-телекоммуникационных технологий, количество таких фактов динамически растёт из года в год. При этом в большинстве случаев преступления возможно было предотвратить при более бдительной правовой позиции граждан.

Стоит отметить, что мошенники при совершении преступлений пользуются исключительно доверием граждан, вводя их в заблуждение, совершают одно из двух следующих действий:

1. Завладевают данными потерпевших о логине и пароле необходимых для входа в личный кабинет сервиса «мобильный банк», а также обманными путем представляясь либо представителем банка или сотрудником правоохранительного органа спрашивают о ходе пришедшем на номер «900» в смс-сообщении необходимом для входа в «личный кабинет»;

2. Посредством программного обеспечения могут обеспечивать дистанционный вход в сотовый телефон и (или) персональный компьютер. В случае подключения к сотовому телефону программного обеспечения «мобильный банк» и сохраненного логина и пароля, дистанционного могут осуществить вход в данное приложение и совершить несанкционированные собственником противоправные операции, совершив хищение денежных средств;

3. Путем хищения или получения во владение сотового телефона или банковской карты используют их для распоряжения безналичными денежными средствами находящимися на банковском счете привязанном к банковской карте;

4. Путем обмана представляясь работниками правоохранительных органов или банка понуждают к совершению действия связанных с переводом, а следовательно и отчуждений денежных средств с банковского счета собственника на иной банковский счет не принадлежащий собственнику.

Необходимо понимать, что банком специально разработан двухступенчатый вход в мобильный кабинет, на первой стадии которого необходимо введение логина и пароля, а на второй стадии кода из смс-сообщения, что теоретически должно исключать неправомерное списание денежных средств.

Что можно сделать для того, чтобы обезопасить себя от противоправных действий? Первое, осуществлять вход в личный кабинет исключительно на персональном компьютере, исключив вход в «сбербанк онлайн» с сотового телефона. Даже при наличии постороннего входа по отдельности как на персональный компьютер, так и при стороннем подключении перевод денежных средств будет недоступен, при их хранении не на банковской карте, а на сберегательной книжке с которой возможно осуществлять переводы посредством «мобильного банка».

Второе, ни при каких обстоятельствах не сообщать неизвестным лицам представившимся работниками банка и правоохранительных органов код с смс-сообщений и иные персональные данные. Обратите внимание, работники банков и правоохранительных органов не имеют право требовать по телефону сообщать указанные персональные данные и не будут этого делать. Данные сведения могут запрашивать только мошенники.

Последнее время участились случаи изменения номеров сотовых телефонов мошенников, они имеют возможность корректировать свои телефоны под телефоны «900» и т.д.

Поэтому все операции по банковским счетам осуществлять необходимо только лично, не следуя требованиям неизвестных лиц.

Если Вам звонили мошенники или похитили денежные средства, необходимо незамедлительно звонить и сообщать о совершенных противоправных действиях в отдел полиции. Сообщение о преступлении поступившее по телефону также будет зарегистрировано и по нему будут проведена процессуальная проверка. Незамедлительность сообщения необходима для «блокирования» счетов, установления лиц причастных к совершению противоправных действий.

Кроме того, при поступлении звонков от неустановленных лиц помимо запрета сообщения персональных данных, ни в коем случае нельзя совершать действия которые от Вас пытаются добиться мошенники. Обычно от мошенников поступают просьбы перевести денежные средства на безопасный банковский счет или требования об оформлении кредита. Нельзя выполнять требования мошенников, так как, переводя денежные средства со своего счета, Вы фактически своими руками совершаете за преступников противоправные действия и лишаетесь денежных средств. Следует внимательно оценивать действия звонящих неизвестных лиц, не подтверждать какие то голосовые команды (при подключении таких в банке), так как посредствам голосовых команд неизвестные лица также имеют возможность похищать денежные средства.

В сухом остатке, для обеспечения безопасности и целостности безналичный денежных средств на банковских счетах необходимо соблюдать следующие правила:

1. Хранить основную массу денежных средств на счете банковской книжке, а на банковской карте хранить лишь небольшую часть денежных средств необходимую для кратковременных текущих расходов;

2. Пользоваться программным обеспечением «мобильный банк» только на персональном компьютере не сообщая коды из смс-сообщений с номера «900» сторонним лицам, исключив подключение «мобильного банка» с сотового телефона;

3. Использовать различные пароли для входа, как в сотовый телефон, так и на персональный компьютер. Обеспечить хранение паролей в недоступных для посторонних лиц местах, в том числе никому не сообщать эти сведения;

4. Систематически менять логин и пароль в «мобильном банке», сотовом телефоне, персональном компьютере;

5. При утере сотового телефона и (или) сим-карты, банковской карты блокировать ее, обращаясь в банк в этот же день снимать денежные средства с банковского счета «привязанного» к номеру сим-карты или переводить их на другой банковский счет;

6. Исключить пользование своим сотовым телефоном посторонними лицами, имеющими возможность посредством команд смс с номера «900» переводить денежные средства с «привязанного» банковского счета;

7. При сообщении требований о предоставлении кодов с номера «900», логина, пароля, а также персональных данных под видом работника банка или правоохранительных органов (прокуратуры РФ, МВД РФ, СК РФ, МЧС РФ и т.д.), прекращать телефонный разговор с этими лицами;

8. Ни под каким предлогом не совершать никаких действий с банкомата, не брать кредит в банке по требованию неизвестных Вам лиц.

Разъясняю, что уголовная ответственность за вышеуказанные действия предусмотрена двумя статьями Уголовного кодекса РФ.

Квалификация противоправных действий зависит от того, кто совершает противоправные действия, сам потерпевший под давлением и под диктовку третьих (ст. 159 УК РФ – мошенничество, путем обмана), либо путем предоставления злоумышленникам персональных данных, сведений о логине, пароле, коде с смс «900» и иных данных, при помощи которых последние совершают хищение денежных средств (п. «г» ч. 3 ст. 158 УК РФ – кража, то есть тайное хищение денежных средств, совершенная с банковского счета).

И.о. прокурора города

младший советник юстиции А.В. Жагло