

Хищение денежных средств с банковских карт

В связи с увеличением объемов расчетов по средствам банковских карт, безналичных денежных переводов, участились случаи хищения денежных средств с банковских счетов, а также электронных денежных средств. Злоумышленники используют и применяют составные элементы высоких технологий, как средство, создающее условия для реализации преступного умысла, разрабатывая новые и новые приемы их преступного применения. Повышенную общественную опасность мошенничеству в сфере высоких технологий придает тот факт, что оно совершается с использованием виртуального пространства, средств сотовой связи.

Только в 2020 году в городе Иркутске зарегистрировано 1510 мошенничеств, раскрываемость которых составила 23,9 %, при этом с использованием мобильных средств связи – 1209; путем присвоения и растраты – 55 (57). Следует отметить, что большинство потерпевших показывают, что знали о способах совершения преступлений данной категории, однако полагали, что жертвами мошенников они не станут.

Ответственность за мошенничество с использованием электронных средств платежа, предусмотрена статьей 159.3 Уголовного кодекса Российской Федерации.

Существует несколько способов, дающих возможность преступникам распорядиться средствами с чужой банковской карты:

- мошенник может завладеть чужой банковской картой и ПИН-кодом к ней обманным путем;
- карта может быть похищена тайно или открыто, а ПИН-код может быть подсмотрен; снят на микрокамеру, установленную рядом с банкоматом и направленную на устройство ввода; считан при помощи специальной накладной клавиатуры.

Это не исчерпывающий перечень действий преступников по завладению денежными средствами с использованием кредитной карты.

Узнать информацию об имени держателя, срок окончания действия и SVC-код платежной карты, используемой для покупок и платежей в Интернете, мошенник может на порталах, не снабженных дополнительной защитой (3D-secure) в виде подтверждения транзакции посредством СМС-сообщения.

Кроме того, зачастую мошенники представляются сотрудниками банков и других известных компаний и по телефону обещают своей жертве кредиты под низкий процент, сообщают о совершении платежей по их картам мошенниками, сообщают якобы о выигрыше в конкурсе или о поступлении платежа, который можно получить, произведя определенные действия через банкомат.

В результате указанных действий преступников, неподготовленный человек может запросто остаться без денежных средств на своем банковском счете.

Для защиты от подобных мошенников следует придерживаться некоторых правил:

- никогда и никому, ни при каких обстоятельствах нельзя передавать такие конфиденциальные данные, как логин, пароль или реквизиты вашей банковской карты (секретный код безопасности CVV2, подтверждающий подлинность карты, имя ее владельца, срок действия) и, разумеется, ПИН-код. Кроме того, если банковская карта привязана к номеру сотового телефона с функцией отправки СМС-сообщений с кодом подтверждения операции с картой, нельзя сообщать данный код другим лицам;

- необходимо выбирать банкоматы, расположенные внутри офисов банков или в охраняемых точках, оборудованных системами видеонаблюдения;

- необходимо при вводе ПИН-кода закрывать клавиатуру банкомата рукой;

- при возникновении проблем нельзя пользоваться советами «случайных помощников», лучше сразу позвонить в банк и заблокировать карту. Если карта осталась в банкомате и не известен телефон банка, можно позвонить в компанию, осуществляющую техническое обслуживание банкомата (номер должен быть указан на терминале);

- в случае потери карты или при наличии оснований полагать, что третьи лица узнали ее реквизиты, необходимо срочно обратиться в банк и заблокировать ее;

- необходимо помнить, что банки не рассылают сообщений о блокировке карт, а в телефонном разговоре не выспрашивают конфиденциальные сведения и коды, связанные с картами клиентов;

- необходимо незамедлительно информировать банк, эмитента карты или кредитора, если в банковских отчетах и отчетах по кредитным картам имеются транзакции, которых Вы не совершали. Необходимо отслеживать списания с карты, обращать внимание на те, которые Вы не узнаете или которые подозрительно выглядят;

- не стоит принимать всерьез звонки с предложением малорискованных и высокоприбыльных инвестиций, особенно если оппонент настаивает на немедленном вложении денег, гарантирует высокие прибыли, обещает низкий или вообще отсутствующий финансовый риск;

- нельзя принимать всерьез сообщения о выигрыше или о Ваших высоких шансах выиграть в лотереях, конкурсах или играх, в которых не принимали участие, особенно, если предлагают отправить деньги на оплату «налогов», «сборов» или «таможенных платежей», прежде чем выслать Ваш выигрыш.

Кроме того, есть ряд правил, соблюдение которых поможет сохранить денежные средства при осуществлении платежей или банковских операций с помощью сети Интернет:

- не переходить по ссылкам, указанным в поступивших сообщениях, потому что безопаснее вводить ссылку вручную на уже проверенном сайте в строке браузера.

- обязательно проверять адресную строку, если поступил запрос на повторную авторизацию, чтобы убедиться, на том ли сайте находитесь;

- перед вводом логина и пароля, проверять, защищено ли соединение (наличие перед адресом сайта букв "https" говорит о защищенном соединении);

- всегда проверять источник входящих писем и сообщений, ведь может быть небезопасным даже письмо, присланное лучшим другом, так как его могли также обмануть или взломать телефон, почту, аккаунт;

- не заходить в интернет-банк с чужих компьютеров или телефонов (если пришлось это сделать, то по завершению сессии необходимо нажать "Выход" и очистить кэш-память);

- не вводить без необходимости свои персональные данные, помимо логина и пароля;

- лучше использовать сложный пароль для входа в личный кабинет, а также одноразовые пароли, запрашиваемые банками для подтверждения действий в личном кабинете;

- оперативно уведомлять банк при получении подозрительных сообщений на телефон, не звонить по указанным в них номерам. Также необходимо информировать банк в случае смены номера или утраты SIM-карты;

- установить пароль на телефон и не снимать блокировку с экрана при посторонних лицах;

- до совершения покупки в интернет-магазине необходимо собрать информацию о продавце: физический адрес продавца (не абонентский ящик), его телефон, отзывы в Интернете. В случае негативных отзывов, сведений об обмане и пр., лучше не рисковать;

- игнорировать сообщения с просьбами предоставить личную или финансовую информацию;

- необходимо помнить, что фальшивые письма и фальшивые сайты могут во всем повторять дизайн настоящих, но гиперссылки, скорее всего, будут неправильные, с ошибками или будут отсылать не туда. По этим признакам можно отличить фишинговое письмо от настоящего.

В случае если Вы все же стали жертвой мошенников, Вам необходимо обратиться с заявлением в дежурную часть Межмуниципальное управление МВД России «Иркутское» по адресу: 664007, г. Иркутск, ул. Декабрьских Событий, 23, либо в территориальные отделы полиции МУ МВД России «Иркутское».

Прокуратура г. Иркутска