Как сохранить денежные средства при осуществлении платежей или банковских операций с помощью сети Интернет

Не переходить по ссылкам, указанным в поступивших сообщениях, безопаснее вводить ссылку вручную на уже проверенном сайте в строке браузера.

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).

Проверять источник входящих писем и сообщений, он может быть небезопасным даже если письмо, от друга, 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. В случае смены номера или утраты SIM-карт информировать банк.

Установить пароль на телефон и не снимать блокировку с экрана при посторонних лицах.

Запретить оператору связи замену SIM-карты по доверенности.

До совершения покупки в интернет-магазине необходимо собрать информацию о продавце: адрес продавца (не абонентский ящик), его телефон, отзывы в Интернете.

Использовать для покупок в Интернете банковскую карту с высокой степенью защиты.

Игнорировать сообщения о предоставлении личной или финансовой информации.

Фальшивые письма и 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 ближайшего к вам отделения полиции.

ИСКИТИМСКАЯ МЕЖРАЙОННАЯ ПРОКУРАТУРА

Как обезопасить себя от действий мошенников по хищению денег с банковских карт?

г. Искитим
2021 г.

В настоящее время довольно распространенным преступлением является мошенничество с использованием электронных средств платежа.

Ответственность за использование чужого доверия с целью завладения средствами, привязанными к платежной карте, предусматривается статьей 159.3 Уголовного кодекса РФ.

Способы распоряжения 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.

Узнать информацию об имени держателя, срок окончания действия и CVC-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.

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

Никогда и никому, ни при каких обстоятельствах нельзя передавать логин, пароль или реквизиты вашей банковской карты (секретный код безопасности CVV2, подтверждающий подлинность карты, имя ее владельца, срок действия) и, разумеется, ПИН-код. 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 необходимо 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.

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