Как сохранить денежные
ва при осуществлении платежей
нковских операций с помощью
сети Интернет

еходить по ссылкам, указанным
оступивших сообщениях,
нее вводить ссылку вручную на
роверенном сайте в строке
ра.

ять адресную строку, если
ил запрос на повторную
вацию, чтобы убедиться, на том
е находитесь.

вводом логина и пароля,
ять, защищено ли соединение
ие перед адресом сайта букв
говорит о защищенном
ении).

ять источник входящих писем и
ний, он может быть
асным даже если письмо, от
так как его могли также
ть или взломать телефон, почту,

одить в интернет-банк с чужих
теров или телефонов (если
ось это сделать, то по
ению сессии необходимо нажать
" и очистить кэш-память).

одить без необходимости свои
альные данные, помимо логина
я.

использовать сложный пароль
ода в личный кабинет, а также
овые 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.

ПРОКУРАТУРА
ЧЕЛЯБИНСКОЙ ОБЛАСТИ

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

г. Челябинск
2020 г.

астоящее время довольно страненным преступлением ся мошенничество с зованием электронных средств а.

тственность за использование доверия с целью завладения зами, привязанными к ной карте, предусматривается і 159.3 Уголовного кодекса РФ.

обы распоряжения средствами чужой банковской карты:

ник может завладеть чужой ской картой и ПИН-кодом к ней ым путем.

может быть похищена тайно или о, а ПИН-код может быть трен; снят на микрокамеру, зленную рядом с банкоматом и ленную на устройство ввода; при помощи специальной ной клавиатуры.

информацию об имени еля, срок окончания действия и од платежной карты, зуемой для покупок и платежей ернете, мошенник может на ах, не снабженных ительной защитой (3D-secure) в подтверждения транзакции ством СМС-сообщения.

ю мошенники представляются никами банков и других ых 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..