



ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ

Прокуратура Хабаровского края

Прокуратура Охотского района

Охотская ул., д. 1, р. п. Охотск
Хабаровский край, 682480
тел. /факс (42141) 9-20-55
E-mail: oh@phk.hbr.ru

Главам муниципальных образований
Охотского муниципального района

09.09.2020 № 1-16-2020

О направлении информации
для размещения на сайте

Направляю для размещения на официальном интернет-сайте органа местного самоуправления прилагаемую информацию с разъяснением законодательства о мошенничестве с использованием информационно-коммуникационных технологий.

Просим информацию разместить на сайте под рубрикой «Прокурор разъясняет». После размещения информации на сайте прошу **копию скриншота страницы сайта направить** в прокуратуру района электронной почтой.

Приложение: информация 1 файл (в электронном виде).

И.о. прокурора района

А.В. Кузнецов

Соснина О.А.
8(42141)91256

АГ 100467

Мошенничество с использованием информационно-коммуникационных технологий. Как обезопасить себя.

Пластиковая банковская карта в качестве платежного средства является неотъемлемой частью жизни современного человека, во многом заменив наличные деньги и став заманчивой мишенью для злоумышленников ввиду того, что связь с банковским счетом позволяет, получив доступ к карте, завладеть всей суммой, а не небольшим количеством средств, которые обычно хранятся в кошельке. Существует множество способов, дающих возможность распоряжаться средствами с чужой платежной карты.

Мошенник может завладеть чужой банковской картой и ПИН-кодом к ней обманным путем. Также ПИН-код может быть подсмотрен, а карта получена с помощью кражи или грабежа. Кроме этого, ПИН-код может быть снят на микрокамеру, установленную рядом с банкоматом и направленную на устройство ввода. Кодовая комбинация цифр может быть считана 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 в виде подтверждения транзакции посредством СМС-сообщения.

Ответственность за использование чужого доверия с целью завладения средствами, привязанными к платежной карте, предусматривается в ст. 159.3 УК РФ.

Мошенничества совершаются не только с платежными картами, но и с другими типами платежных систем и устройств.

Кошельки платежных систем, например, Киви, привязываются к личному номеру телефона сотового оператора в процессе его регистрации и позволяют пополнять счет любым удобным способом и выполнять перевод средств.

Хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей является мошенничеством в сфере компьютерной информации (ч. 1 ст. 159.6 УК РФ).

Существует множество способов незаконного овладения чужими средствами или данными, являющимися собственностью правообладателя. Например, мошенничество в интернет-магазинах может заключаться в том, что: с покупателя берут предоплату за товар и не выполняют своих обязательств; по факту поставки товар существенно отличается от представленного в предложении на сайте; товар, совпадая по внешнему виду, имеет значительно более низкие эксплуатационные характеристики и вскоре ломается, а взыскать ущерб с продавца не представляется возможным.

Мошенничество с SIM-картами также является одним из видов мошенничества. Приобрести SIM-карту, зарегистрированную на другого

владельца, и сегодня можно буквально на каждом углу. Абоненту достаточно пополнить счет номера. Сюрпризы начинаются потом. Приобретая SIM-карту у дилера, который игнорирует ее регистрацию, пользователь автоматически попадает в зону риска.

Житейский пример: Иван, купивший SIM-карту по дешевке на улице, однажды получил такое СМС-сообщение: "По вашему номеру проходит замена SIM-карты. Если вы не заказывали данную услугу, то срочно обратитесь в наш контактный центр..." Это было последнее СМС-сообщение на его мобильный номер от МТС - через несколько минут SIM-карта отключилась. А дальше Иван обнаружил, что не может зайти на свои страницы в Facebook и "ВКонтакте", в почтовый ящик на "Яндексе". Воспользовавшись привязанным номером телефона, злоумышленники сменили там пароли. Ивану, по незнанию купившему SIM-карту на уличном лотке, теперь предстоит доказывать свои права на аккаунты администрациям Facebook, "ВКонтакте" и "Яндекса". Единственное, что он успел сделать, - связаться с банками и заблокировать счета, к которым также был привязан номер мобильного. Но самое обидное, что восстановить доступ к своему телефонному номеру он вряд ли сможет, ведь формально он ему никогда и не принадлежал.

Большинство абонентов даже не подозревают, как короток путь от их телефонного номера до банковского счета.

Для защиты от 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.

- Выучите ПИН-код наизусть или запишите его на листочек, но храните отдельно от карты.

- Не используйте так называемые зарплатные карты для расчетов в магазинах и оплаты интернет-покупок. Деньги с карточного счета лучше переводить на лицевой либо устанавливать суточные лимиты на все виды совершаемых операций.

- Выбирайте банкоматы, расположенные внутри офисов банков или в охраняемых точках, оборудованных системами видеонаблюдения.

- Не пользуйтесь подозрительными моделями банкоматов. Прежде чем вставить карту в терминал, внимательно осмотрите его (нет ли чего-нибудь подозрительного на клавиатуре или в картоприемнике).

- Не стесняйтесь закрывать клавиатуру рукой. При возникновении проблем не пользуйтесь советами "случайных помощников" - сразу звоните в банк и блокируйте карту. Если карта осталась в банкомате и вы не знаете телефон своего банка, позвоните в компанию, осуществляющую техническое обслуживание банкомата. Номер должен быть указан на терминале.

- Если вы потеряли карту или у вас есть основания полагать, что третьи лица узнали ее реквизиты, обратитесь в банк и заблокируйте ее.

- Всегда с подозрением относитесь к сообщениям, в которых вас просят перейти по какой-то ссылке (проверьте, нет ли этой страницы в списке подозрительных). Да и в принципе безопаснее будет вручную ввести ссылку на уже проверенный сайт в строке браузера, чем переходить по ссылке из сообщения.

- Если вас просят заново авторизоваться, обязательно проверяйте адресную строку - на том ли вы сайте находитесь.

- Старайтесь пользоваться последними версиями программного обеспечения, установленными на вашем компьютере или планшете.

- Прежде чем ввести логин и пароль, проверьте, защищено ли соединение. Если перед адресом сайта стоит "https", все в порядке.

- Если сомневаетесь в письме, проверьте его источник.

- Помните, что даже если письмо или сообщение со ссылкой вы получили от лучшего друга, расслабляться нельзя - его тоже могли обмануть. Поэтому ведите себя не менее осторожно, чем при обращении со ссылками, пришедшими из неизвестного источника.

- По возможности не заходите в онлайн-банки и другие подобные сервисы через открытые Wi-Fi-сети в кафе или на улице (за таким Wi-Fi могут стоять мошенники, подменяющие адрес сайта на уровне подключения и перенаправляющие вас на поддельную страницу).

- Заходить в интернет-банк с чужих компьютеров тоже не рекомендуется. Если это все же случилось, по завершении сессии нажмите "Выход" и очистите кэш-память.

- Пользуйтесь антивирусами и своевременно обновляйте их.

- Обнаружив фишинговую операцию, обязательно сообщите о ней в банк (если письмо пришло от имени финансового учреждения) или в службу поддержки социальной сети (если такие ссылки рассылает кто-то из пользователей).

- Без необходимости не вводите никакие свои персональные данные, помимо логина и пароля.

- Придумайте сложный пароль для входа в личный кабинет, а также используйте одноразовые пароли, запрашиваемые банками для подтверждения действий в личном кабинете.

- Не забывайте, что банки не рассылают сообщений о блокировке карт, а в телефонном разговоре не выспрашивают конфиденциальные сведения и коды, связанные с картами клиентов.

- Чтобы уберечь SIM-карту, к которой привязана карта, оперативно уведомляйте банк при получении подозрительных сообщений и ни в коем случае не звоните по указанным в них номерам. Проинформируйте банк, если сменили номер или потеряли SIM-карту. Установите пароль на телефон и не снимайте блок с экрана, если кто-то посторонний наблюдает за вашими действиями. А если SIM-карта оформлена на вас лично, запретите ее замену по доверенности.

- Делая покупки в интернет-магазинах, предварительно узнайте, с кем имеете дело. Попробуйте найти физический адрес продавца (не абонентский ящик) и его телефон. Поищите отзывы в Интернете. Если люди пишут о

неприятном опыте с такими магазинами, вам придется решить, стоит ли рисковать.

- Следите за своими банковскими отчетами и отчетами по кредиткам на предмет списаний с вашей карты, которых вы не узнаете или которые подозрительно выглядят. Позвоните своему банку, эмитенту карты или кредитору, если найдете транзакции, которых вы не совершали.

- Если кто-то связывается с вами с предложением малорискованных и высокоприбыльных инвестиций, воздержитесь. Такие мошенники обычно настаивают на немедленном вложении денег, гарантируют высокие прибыли, обещают низкий или вообще отсутствующий финансовый риск или требуют, чтобы вы срочно выслали наличные.

- Если вы собираетесь делать покупку онлайн, лучше совершать ее, используя кредитную карту с высокой степенью защиты.

- Не отвечайте на сообщения с просьбами предоставить личную или финансовую информацию.

- Не верьте сообщениям, которые рекламируют ваши высокие шансы выиграть в иностранную лотерею или сообщают, что вы уже выиграли. Мошенники будут утверждать, что нужно отправить деньги на оплату "налогов", "сборов" или "таможенных платежей", прежде чем выслать вам ваш выигрыш. Если вы отправите деньги, вы их потеряете.

- Имейте в виду: фальшивые письма и фальшивые сайты могут во всем повторять дизайн настоящих (качество подделки зависит от того, насколько хорошо мошенники знают свою работу), но гиперссылки, скорее всего, будут неправильные - или с ошибками, или вообще будут отсылать не туда. По этим признакам можно отличить фишинговое письмо от настоящего.

Прокуратура Охотского района