ПРОКУРАТУРА
Российской Федерации

Прокуратура
Ростовской области

Прокуратура Аксайского района

346720, г. Аксай, ул. Гуляева, 109
Тел. (86350) 55-1-66

.02.2025 № 22-159-2025

Главам администраций Аксайского района, Аксайского городского поселения, сельских поселений Аксайского района

Направляются для размещения на официальном сайте администрации статьи для информирования граждан.

Приложение: на л.

Прокурор района
советник юстиции К.К. Артемов

А.С. Бойченко, тел. 8 (863-50) 5-46-96

УТВЕРЖДАЮ

Прокурор Аксайского района

советник юстиции

К.К. Артемов

.02.2025

Разъяснение законодательства о преступлениях, совершаемых с использованием информационно-коммуникационных технологий

В настоящее время в Российской Федерации хищения с использованием средств связи набирают стремительные обороты. Законодатель, пытаясь сдержать рост указанного вида хищений, реагирует на данную ситуацию. Это подтверждается теми изменениями, которые вносятся в уголовное законодательство.

Так, Федеральным законом от 23 апреля 2018 года часть 3 статьи 158 и часть 3 статьи 159.3 УК РФ были дополнены особо квалифицирующим признаком: «деяния, совершенные с банковского счета, а равно в отношении электронных денежных средств». Кроме того, ужесточена санкция за мошенничество с использованием электронных средств платежа: арест на срок до четырех месяцев заменен на лишение свободы на срок до трех лет.

Подчеркивая общественную опасность преступлений, предусмотренных за мошенничество с использованием электронных средств платежа и в сфере компьютерной информации, законодатель снизил пороговое значение крупного размера с одного миллиона пятьсот тысяч рублей до двухсот пятидесяти тысяч рублей, особо крупного – с шести миллионов рублей до одного миллиона рублей.

Все рассматриваемые хищения денежных средств с банковских счетов граждан, совершенных с использованием систем дистанционного банковского обслуживания, можно разделить на две основные группы:

1) бесконтактные, то есть совершаемые без личностного контакта субъекта с потенциальным потерпевшим (преступления, в которых субъект не контактирует с потерпевшим);

2) контактные, то есть совершаемые посредством установления личностного контакта субъекта с потенциальным потерпевшим (например, путем телефонного звонка или SMS-сообщения).

Также хищения денежных средств можно разделить на следующие виды, это когда:

- субъект осуществляет телефонный звонок от лица вымышленных сотрудников банка или службы безопасности и сообщает о необходимости предоставления информации о номере карты, ее владельце, сроке действия, трехзначном коде, указанном на оборотной стороне карты, в связи с

«проведением профилактических работ», «блокированием карты по подозрению в попытке хищения денег» и т.п.;

- субъект просит предоплату за товар или услуги в Интернете;

- субъект сообщает о выигрыше;

- субъект осуществляет телефонный звонок лицу и сообщает, что у его родственника (знакомого) проблемы, например, попал в ДТП, совершил правонарушение и т.п., и предлагает «решить проблему» с помощью внесения на счет злоумышленника определенной денежной суммы.

Следует отметить, что число указанных противоправных деяний продолжает увеличиваться. Высокая степень общественной опасности таких преступлений подтверждается их спецификой – совершить их могут лица, обладающие специальными знаниями и использующие технические средства, именно в криминальных целях, что приводит к нарушению не только права собственности, но и банковской тайны.

Помощник прокурора
Аксайского района А.С. Бойченко

УТВЕРЖДАЮ

Прокурор Аксайского района

старший советник юстиции

К.К. Артемов

.02.2025

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

Пластиковая банковская карта в качестве платежного средства стала 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.

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 счет, либо устанавливать суточные лимиты на все 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 защищенное 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 и 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 выдачу 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 малорисковых и высокодоходных 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 выплатят выигрыш. Если вы отправите деньги, вы их потеряете.

- Имейте в виду: фальшивые письма и фальшивые сайты могут в точности повторять дизайн настоящих (качество подделки зависит от того, насколько хорошо мошенники делают 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.

Помощник прокурора
Аксайского района [illegible]