Как не стать жертвой кибермошенников. О новых мерах защиты денежных средств граждан в банках

Цифровые технологии дают новые возможности и облегчают многие операции с денежными средствами, в том числе провести онлайн-переводы и оплатить покупку товаров, получить государственные услуги через официальные приложения банков и государственных органов.

Вместе с тем в последние годы значительно возросло и количество граждан, которые становятся жертвами мошенников. Технический прогресс играет на руку аферистам. Им достаточно завладеть персональными данными, которые мы сами оставляем в сети «Интернет».

Чтобы обмануть или злоупотребить доверием, мошенники, как правило, используют слабые стороны человека, например, его чрезмерную доверчивость или жажду быстрых и легких денег.

Одной из главных задач кибермошенника является под любым предлогом узнать у гражданина данные банковской карты, ее номер, срок действия, СVV-код (трехзначный номер на обратной стороне карты) и ПИН-код. С этой целью они звонят, представляясь работниками службы безопасности банка или сотрудниками правоохранительных органов, и сообщают о несанкционированном списании денежных средств со счетов, оформлении фейковых кредитов, отправляют смс-сообщения или электронные письма о начислении социальной выплаты, компенсации или кэшбэка, о выигрыше в лотерею, суперскидках в интернет-магазинах, благотворительных сборах и т.п. Потеряв бдительность в таких ситуациях, граждане  теряют денежные средства со своих банковских карт.

В настоящее время преступники активно используют также и другой способ хищения денег путем «вскрытия» личных страниц в социальных сетях, ведения переписки от чужого имени, в результате чего денежные средства переводятся лицу, выступающему от имени пользователя, находящегося в категории «друзей», который якобы просил деньги в долг.

В связи с участившимися случаями хищений денежных средств граждан в банках путем безналичных переводов, органами власти приняты меры правового и организационного характера, направленные на борьбу с такими явлениями.

Банкам или иным операторам по переводу денег предложили новые способы защиты граждан от мошенников.

С целью недопущения операций по переводу денежных средств граждан в отсутствие добровольного согласия, а именно без согласия клиента банка или с согласия, полученного под влиянием обмана или при злоупотреблении доверием, с 25.07.2024 внедряется механизм дополнительной проверки банками операций с указанными признаками. Данные новеллы введены Федеральным законом от 24.07.2023 № 369-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе».

Признаки переводов без добровольного согласия клиента определит Банк России.

 Законодателем предусмотрены возможность приостановки банковских операций при наличии признаков хищений с необходимостью дополнительного подтверждения операции, а также приостановление использования клиентами электронных средств платежа. Сомнительные транзакции будут заморожены на два дня, о чем банк уведомит клиента. За это время человек, находящийся под влиянием злоумышленников, сможет одуматься и не подтверждать перевод. Деньги переведут при условии, если не возникнет иных препятствий.

При этом гражданин в случае утраты электронного средства платежа и (или) его использования без добровольного согласия обязан направить соответствующее уведомление в банк  в предусмотренной договором форме незамедлительно после обнаружения факта утраты электронного средства платежа и (или) его использования без добровольного согласия, но не позднее дня, следующего за днем получения уведомления о совершенной операции.

Банк будет должен возместить деньги клиенту, если средства были переведены на мошеннический счет, который находится в специальной базе Банка России. Это должно быть сделано в течение 30 дней после получения заявления от пострадавшего.

Данные изменения вступят в силу только в июле 2024 года, список мошеннических счетов составляется и актуализируется постоянно на основе информации, полученной от банков и других операторов платежных систем. Так что сообщение в правоохранительные органы и Банк России сведений о счетах мошенников, на которые были направлены деньги, может поспособствовать тому, что другие люди не пострадают.

**Прокуратура напоминает о необходимости проявлять повышенную бдительность при общении с неизвестными лицами при использовании средств телекоммуникаций.**

**Следует придерживаться элементарных правил «кибергигиены», которые позволят сохранить денежные средства:**

- не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам. Даже если ссылка кажется надежной, а телефон верным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера проверяйте в официальных справочниках;

- если вам приходит смс-сообщение о зачислении средств или сообщение, похожее на привычное уведомление банка, а затем звонит якобы «растяпа», который по ошибке зачислил вам деньги и просит вернуть, не спешите ничего возвращать. Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, смс-сообщение - не от вашего банка, а звонил вам злоумышленник. Проверьте состояние вашего счета, закажите выписку в онлайн-банке или позвоните в банк, прежде чем переводить кому-то деньги;

- в любых ситуациях сохраняйте спокойствие и при каких-то сомнениях лучше позвонить и получить консультацию от банковского сотрудника напрямую;

- не сообщайте третьим лицам конфиденциальные данные банковских карт, пароли, коды из смс-сообщения для подтверждения банковской операции, пин-коды, CVV-коды, коды из смс-сообщений. Сотрудникам банка они не нужны, а мошенникам откроют доступ к вашим деньгам;

- не храните данных карт на компьютере и смартфоне;

- для контроля за совершением таких операций желательно подключить услугу смс-уведомлений, а также установить расходные лимиты по карте, за пределами которых перевести со счета денежные средства будет нельзя;

- рекомендуется оформить отдельную банковскую карту для оплаты товара в интернет-магазинах;

- проверяйте информацию. Если вам говорят, будто вы что-то выиграли или с вашей карты случайно списали деньги и нужно назвать свои данные, чтобы остановить операцию, закончите разговор и перезвоните в банк по номеру телефона, указанному на обратной стороне вашей карты;

- если вам сообщают, что у родственников или друзей неприятности, постарайтесь связаться с ними напрямую;

- используйте сложные пароли, состоящие из комбинаций цифр и букв или иных символов, не сообщайте никому свои пароли и личные данные;

 - на аккаунты в мессенджерах установите двойную защиту. На Госуслугах тоже установите двойную аутентификацию. Не переходите по ссылкам и кладите трубку, если в телефоне вам что-то начинают говорить про деньги;

- не передавайте банковские карты третьим лицам;

- не оставляйте без присмотра телефоны с «привязанной» к номеру банковской карты;

- сотрудники правоохранительных органов не вправе получать по телефону данные о банковских счетах, номера банковских карт, коды и пароли;

- воздержитесь от покупок на малоизвестных и подозрительных интернет-сайтах и у лиц, осуществляющих продажу товаров или услуг в социальных сетях, особенно при необходимости внесения полной предоплаты за товар или услуги;

- не переходите по ссылкам, содержащимся в спаме и других подозрительных электронных письмах отправителей, которых вы не знаете;

- никогда не открывайте письма на электронной почте, если не уверены в отправителе;

 - не нажимайте на кнопки, ссылки и баннеры, если не знаете, на какой ресурс они ведут;

- не подключайтесь к сомнительному Wi-Fi, не подключайте чужие USB-носители;

 - не предоставляйте возможность физического доступа к вашим устройствам;

 - проверяйте информацию, прежде чем в нее поверить;

- используйте антивирусные программы;

- ограничьте личную информацию в соцсетях: фотографии, имена и фамилии, родственные связи, места отдыха, домашний адрес, ваш банк, номер телефона и т.д.;

- регулярно проводите беседы с детьми о правилах поведения в интернете, особенно в соцсетях. Ваши дети должны знать о недопустимости любого негативного воздействия на них и необходимости сообщить родителям о подобных инцидентах.

**Куда обращаться за помощью?**

Если все-таки Вы поняли, что стали жертвой мошенника, необходимо сразу заблокировать свою карту, сообщить в банк по «горячей линии» о краже денег и написать в отделение банка заявление о несогласии с операцией (сделать все это необходимо не позднее следующего дня после того, как банк уведомил вас об операции, которую вы не совершали). Если вы соблюдали правила использования карты (не хранили пин-код вместе с картой и никому не сообщали ее данные), то есть шанс вернуть украденные деньги.

Поскольку кража денег - это уголовное преступление, напишите заявление в полицию. Даже если вам кажется, что это незначительное мошенничество, вполне вероятно, что вы поможете обезвредить профессиональную группу кибермошенников.

Важно помнить, что преступление всегда легче предотвратить, чем вернуть похищенное, воспользуйтесь этими советами по предупреждению киберпреступлений, которые позволят вам обезопасить себя и близких от преступных посягательств.

Прокуратура Первомайского района