

### **Как не стать жертвой кибермошенников**

• 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 этим, значительно возросло количество граждан, ставших жертвами мошенников, в данном случае кибермошенников.

Наиболее часто граждан вводят в заблуждение при поступлении телефонных звонков от якобы службы безопасности банков, в связи с несанкционированными списаниями денежных средств со счетов. Полагая, что звонок поступил во спасение их сбережений, они передают преступным элементам сведения о кодах, поступающих в смс-сообщениях, о реквизитах банковских карт (включая CVV-код). В настоящее время преступники активно используют также и другой способ хищения денег путем «вскрытия» личных страниц в социальных сетях («ВКонтакте», «Одноклассниках» и др.), 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 и т.п.

В связи с этим, гражданам необходимо проявлять повышенную бдительность при общении с неизвестными лицами при использовании средств телекоммуникаций. Нельзя никому сообщать (даже работникам банков) реквизиты банковских карт, пароли, коды, пин-коды, CVV-коды, коды из смс-сообщений. При поступлении звонка от сотрудников банка прервать разговор и самим перезвонить в банк. Нельзя передавать банковские карты третьим лицам. Незамедлительно сообщить в банк об утрате банковской карты, мобильного телефона с «привязанной» к номеру

банковской картой или о смене телефонного номера. Не оставлять без присмотра телефоны, с «привязанной» к номеру банковской картой. При заключении сделок купли-продажи, онлайн оплату проводить только с проверенными контрагентами.

### **Хищение денежных средств с банковских карт граждан**

Преступники все чаще при совершении преступлений используют IP-телефонию с полной подменой абонентского номера, серверы, расположенные за пределами территории Российской Федерации, а также телефонные номера и счета в кредитных учреждениях, оформленные на номинальных лиц. Межрегиональный характер преступлений также значительно затрудняет процесс раскрытия преступлений.

В настоящее время одними из самых распространенных способов хищения денежных средств является их хищение с банковской карты владельца.

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

1) бесконтактные, т.е. совершаемые без контакта с потенциальным потерпевшим;

2) контактные, т.е. совершаемые посредством установления контакта злоумышленника с потенциальным потерпевшим (например, путем телефонного звонка или SMS-сообщения).

Чтобы обезопасить себя от действий мошенников, необходимо придерживаться следующих рекомендаций:

- не сообщать конфиденциальные данные карты третьим лицам (срок, CVV-код и ПИН-код);

- подключить услугу СМС-уведомлений для контроля за счётом;

- ПИН-код хранить отдельно от карточки и прикрывать рукой клавиатуру банкомата или терминала в момент его ввода;

- установить расходные лимиты в интернет-банке или мобильном приложении;

- никогда никому не сообщать код из СМС для подтверждения операции, которую клиент не совершал (сотрудники банка не вправе запрашивать данную информацию);

- после выявления факта незаконного списания денег с карты необходимо срочно её заблокировать и обратиться в ближайшее отделение банка.

Дальнейшая процедура включает следующие этапы: Клиент пишет заявление о несогласии с конкретной расходной операцией. Банк проводит служебное расследование по факту хищения средств. В установленные сроки (до 30 дней) владелец карточки уведомляется о решении. Банк может вернуть деньги только в том случае, если пользователь не нарушал правила безопасности, то есть добровольно не сообщал конфиденциальную информацию третьим лицам. Независимо от решения банка, владелец



карточки имеет право обратиться в правоохранительные органы и написать заявление о краже денег.

Ежедневно злоумышленники изобретают новые способы хищения средств с банковских карт, поэтому невозможно предугадать все сценарии развития событий. Однако при соблюдении указанных элементарных мер безопасности любой пользователь сможет предотвратить нанесение ущерба от действий мошенников.

### **Каковы условия перевода работника на постоянную работу в другую местность вместе с работодателем либо к другому работодателю?**

Перевод работника на постоянную работу в другую местность вместе с работодателем либо к другому работодателю допускается только с письменного согласия работника.

Под другой местностью следует понимать местность за пределами административно-территориальных границ соответствующего населенного пункта

(п.16 Постановления Пленума ВС РФ от 17.03.2004 N 2). Перевод на работу из одного населенного пункта в другой даже в пределах одного административного района рассматривается как перевод в другую местность независимо от наличия автобусного или иного регулярного сообщения между этими пунктами. Отказ работника от перевода в другую местность вместе с работодателем является основанием для прекращения с ним трудового договора по п. 9 ст. 77 ТК. На практике имеют место случаи, когда это основание применяется и при отказе работника от перевода вместе с филиалом в другую местность. Суды, если к ним обращаются такие работники с иском о восстановлении на работе, не признают правомерным их увольнение, поскольку работодатель, структурным подразделением которого является филиал, не переезжает в другую местность.

При переводе на работу в другую местность работникам выплачиваются соответствующие компенсации: стоимость проезда самого работника и членов его семьи, стоимость провоза багажа, расходы по устройству на новом месте и др.

По письменной просьбе работника или с его письменного согласия может быть осуществлен перевод работника на постоянную работу к другому работодателю.

Перевод на постоянную работу к другому работодателю влечет за собой изменение одной стороны трудового договора, поэтому он рассматривается ТК как самостоятельное основание прекращения ранее заключенного трудового договора (п. 5 ст. 77 ТК) и в то же время как основание для

заклучения нового. Работнику, в письменной форме приглашенному на работу в порядке перевода от другого работодателя, не может быть отказано в заключении трудового договора в течение месяца со дня увольнения с прежнего места работы (ч. 4 ст. 64 ТК).

В трудовой книжке работника в этом случае производятся записи об увольнении и о приеме на работу с указанием порядка, в котором осуществлено увольнение в связи с переводом - по просьбе работника или с его согласия (см. п. 6.1 Инструкции по заполнению трудовых книжек, утвержденной Минтрудом России).

Независимо от порядка перевода запрещается переводить работника на работу, противопоказанную ему по состоянию здоровья.