**КАК НЕ СТАТЬ**

**ЖЕРТВОЙ МОШЕННИКОВ**

К наиболее типичным способам совершения преступлений с использованием информационно-телекоммуникационных технологий можно отнести следующие.

* Злоумышленники звонят гражданам, представляясь сотрудниками банков, называя их по имени, отчеству, просят сообщить данные банковских карт (номер. CVC(CVV), PIN-коды и т.п.) для предотвращения якобы несанкционированного списания денежных средств либо оформления кредита. Используя эти сведения, получают удаленный доступ к личному кабинету клиента банка и переводят деньги без ведома собственника. При этом, преступники могут использовать программы подмены телефонных номеров, в связи с чем номер входящего звонка определяется у клиента как номер банка, либо как телефон правоохранительных органов.
* Хищения с использованием преступниками интернет - сервисов объявлений «Авито». «Юла» и т.д.. Вводя гражданина в заблуждение относительно своего намерения приобрести или продать товар, в ходе телефонных разговоров, злоумышленники узнают реквизиты банковской карты потерпевшего, при помощи которых списывают денежные средства со счета. В ряде случаев предлагается перейти по ссылкам для перевода денежных средств, после чего «продавец» не предоставляет оплаченный товар и не выходи т на связь.
* Массовая рассылают SMS-сообщения следующего содержания: «Ваша карта заблокирована. Для разблокировки необходимо позвонить по номеру...». Хищения денежных средств у граждан совершаются также путем направления SMS-сообщений о выигрыше, для получения которого необходимо перевести денежные средства на указанный абонентский номер.
* Преступники представляются родственниками либо знакомыми потерпевших, рассказывают, что попали в беседу (стали виновником дорожно-транспортного происшествия, задержаны сотрудниками полиции, срочно требуются деньги на операцию и т.п.) и просят предоставить им денежные средства.
* Злоумышленники взламывают электронную почту, аккаунты в социальных сетях, после чего от имени пользователя рассылают гражданам, сведения о которых имеются в контактах данного лица, просьбы о займе денежных средств. В результате деньги поступают на счет мошенника.

Чтобы не стать жертвой преступников, необходимо следовать определенным правилам:

1. Если получен звонок или сообщение в социальной сети с просьбой о срочной денежной помощи для знакомого или родственника, не стоит принимать решение сразу. Необходимо проверить полученную информацию, связавшись со своими родными и знакомыми.
2. Никогда и никому не сообщайте трёхзначный код на обратной стороне Вашей банковской карты (CVV), это ключ к Вашим деньгам.
3. Нельзя сообщать никому личные сведения, данные банковских карт и СМС- пароли, которые могут быть использованы злоумышленниками для неправомерных действий.
4. Если по телефону Вас просят набрать комбинацию цифр в банкомате, прекратите разговор. Никогда не выполняйте действия с банкоматом «под диктовку» другого человека. даже если он представился работником банка или правоохранительных органов.

 Необходимо помнить, что злоумышленники могут представиться сотрудниками банка, правоохранительного органа, учреждения здравоохранения и обращаться по имени и отчеству. Однако только мошенники будут' просить сообщить реквизиты банковской карты, смс-пароль (код). CVV-код карты. В каждом таком случае необходимо завершить разговор.

Сотрудники банка также не предлагают:

* установить программы удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, для удаления вирусов с мобильного устройства):
* перевести денежные средства на «защищенный счет»;
* включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк.

При необходимости Вы всегда можете связаться с банком по официальному номеру
контактного центра (номер телефона службы поддержки клиента указан на оборотной стороне банковской карты), обратиться в отделение банка или полицию

Если Вы стали жертвой преступника, необходимо незамедлительно обратиться в органы внутренних дел с соответствующим заявлением лично, либо. В заявлении следует максимально подробно рассказать о всех обстоятельствах события. Также следует принять меры к блокировке банковской карты.

