В соответствии со ст. 159 УК РФ «мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием».

Под финансовой преступностью понимается совокупность преступлений, непосредственно связанных с посягательством на отношения по формированию, распределению, перераспределению и использованию фондов денежных средств (финансовых ресурсов) субъектов экономических отношений. Финансовые преступления могут быть классифицированы по различным основаниям. В зависимости от уровня финансовых отношений, являющегося объектом посягательств, различают: преступления, посягающие на финансовую систему государства (государственные и муниципальные финансы; преступления, посягающие на финансы предприятий. В зависимости от сферы посягательств различают: преступления в сфере налогообложения, преступления на рынке ценных бумаг, преступления в сфере страхового, валютного и кредитного рынков, преступления на рынке товаров и услуг.

За последние годы злоумышленники придумали массу хитроумных способов мошенничества с карточками. Появился даже специальный термин carding. Он обозначает разные виды мошенничества с платежными картами, при которых снятие средств происходит без ведома или подтверждения владельца карты. Причем мошенники постоянно совершенствуют технологии обмана. Так что, если вы не хотите в один прекрасный день лишиться приличной суммы, лучше знать все ловушки заранее.

- Скимминг
Этим термином называют незаконное изготовление дубликата карты. Для этого используется специальное устройство - скиммер: маленькая накладка, которую устанавливают или на сам банкомат, или на платежные терминалы - POS-терминал или импринтер (тот самый, через который «прокатывают» банковскую карту). Скиммер считывает информацию с магнитной ленты карты, а мошенники воспроизводят данные на дубликате. Чтобы узнать пин-код, на панели банкомата монтируется скрытая камера или специальная накладка на клавиатуру, которая запоминает набор цифр.- Фишинг

Проще говоря, нелегальный способ вынудить держателя карты предоставить данные. Это может быть электронное письмо с вирусом. Либо пользователя переводят на фальшивый сайт банка. Еще одна разновидность - злоумышленники используют в качестве прикрытия интернет-магазин, объясняя, что оплата не прошла и для совершения покупки требуется еще раз ввести номер карты, CVV или продиктовать код (ключ) для подтверждения операции.

- Вишинг
Родной брат фишинга - только в этом случае используется телефон. Жертве могут прислать сообщение от имени банка о том, что с его карты пытались незаконно снять средства и попросить перезвонить по указанному номеру, где подставной сотрудник службы безопасности опять же попросит назвать данные карты. Еще один вариант - для звонка используется программа, иммитирующая автоинформатора. Жертва слышит профессионально записанный голос, который, под предлогом проблем в банковской системе, просит уточнить данные по карте – в том числе ПИН-код и кодовое слово. Вводить данные предлагается при помощи набора цифр на телефоне.

- «Ливанская петля»
Мошенники заклеивают с внешней стороны карман для выдачи денег в банкомате. Вы вводите карту, набираете код и ждете, когда появятся банкноты, но ничего не происходит.

Банкомат сообщает, что средства выданы, в то время как деньги застряли внутри. Например, в темноте сложно разглядеть скотч. Пока клиент, забрав карту, освобождает место у банкомата следующему в очереди (как правило, злоумышленнику) и звонит в банк, предприимчивый технолог отклеивает изоленту и забирает деньги.

- Фальшивые банкоматы

Любители чужих денег иногда мыслят масштабно - сами производят фальшивые банкоматы или переделывают старые. Размещаются фальшивки, как правило, в очень людных местах. После того, как вы ввели ПИН-код, на дисплее банкомата появляется сообщение о неисправности машины или о том, что закончились наличные. Вы спокойно получаете назад свою карту, в то время как мошенники уже успели скопировать с магнитной полосы данные счета и его персональный идентификационный номер.

ЭТО ВАЖНО ЗНАТЬ

10 советов владельцам карт

- Старайтесь снимать наличные в банкоматах своего банка и не пользоваться банкоматами в мелких магазинах и аптеках. А если выхода нет, проверьте устройство - нет ли на нем лишних предметов. Если что-то заподозрите, сразу же звоните в банк.

- Запишите номер call-центра банка в свой мобильный телефон. Если вы потеряете карту или ее украдут, то нужно сразу же позвонить в банк и заблокировать ее.- Нигде не указывайте ваш пин-код. И никому его не сообщайте, даже если вам представились сотрудником безопасности банка. Храните эти 4 цифры лишь в собственной памяти или под кодовым именем в мобильном.

- Установите SMS-оповещение. Услуга стоит недорого - обычно 40 - 60 рублей в месяц. Это поможет держать ваш электронный кошелек под контролем. Вы сразу же узнаете, если по вашей карте будет совершена незаконная операция.

- При оплате через интернет пользуйтесь проверенными сайтами. А также обращайте внимание на строку браузера. Она должна начинаться так: https://, где «s» обозначает, что ваши данные будут передаваться по защищенному каналу связи.

- Никому не говорите трехзначный код, указанный на оборотной стороне карты.

- Не пересылайте данные карты по электронной почте и не запоминайте логины и пароли к своему личному кабинету в онлайн-банкинге у себя на компьютере.

- Если у вас карта с магнитной полосой, лучше перевыпустите ее и получите карту с чипом, она надежнее. По крайней мере, от скиммеров вы точно будете защищены.

- Уточните в вашем банке, используют ли там специальный сервис 3D-Secure. Он позволяет совершать покупки в интернет-магазинах через защищенное соединение. Для подтверждения операции вам должны выслать на телефон одноразовый пароль.

- Если денег на карте много, установите лимиты на единовременное снятие либо на дневной оборот. При необходимости увеличить их не составит труда.

Если вы будете соблюдать эти простые меры, то максимально обезопасите свои деньги, и карточным мошенникам будет сложнее получить доступ к ним.

Наиболее распространенные виды финансовых пирамид: 5 ключевых схем мошенничества!

Сейчас наблюдается третья волна пирамид. Она связана с развитием интернет-сообщества

Финансовые пирамиды в России заявили о себе в 1990-ые годы. Расцвет этого явления был связан с началом приватизации и развитием финансового рынка. Возрождение явления пришлось на годы мирового экономического кризиса – 2008-2009 года. Сейчас наблюдается третья волна пирамид. Она связана с развитием интернет-сообщества.

Различные способы классификации позволяют структурировать пирамиды:

- По охвату деятельности: интернациональные, федеральные, региональные и местные;
- По способу регистрации: реальные и виртуальные;
- По варианту привлечения новых потребителей: централизованные и сетевые.

ЦБ РФ постоянно публикует на своем официальном портале информацию по поводу самых распространенных типов финансовых пирамид. В настоящее время их выделяют пять.

Первый тип. Классический вариант мошенничества. Организации не скрывают того, что они являются финансовыми пирамидами. Свой бизнес они строят за счет вкладчиков, которые вовлекают других участников в проект. Главной мотивацией при этом является то, что людей очень много и всегда найдутся новые, чтобы вступили в проект. Примером таких компаний является «МММ».

Второй тип. Организации, которые представляют себя как аналог современному потребительскому и ипотечному кредитованию. В такие фирмы нередко обращаются люди, получившие отказ в банках и МФО. Процент у них гораздо ниже, чем в банках. При этом деньги выманиваются под предлогом первоначального взноса, который составляет 5-20% от полной суммы кредита.

Третий тип. Мошенники, прикрывающиеся «вывеской» микрофинансовых организаций, кредитных кооперативов и ломбардов. Деньги привлекаются в качестве займов или по средствам реализации различных векселей.

Четвертый тип. Фирмы, предлагающие списать долги по потребительских кредитам. Заемщиков убеждают в том, что они выкупают их долг у банка и МФО. Стоимость такого выкупа составляет около 30% от полной суммы кредита.

Пятый тип. Компании, которые представляют собой псевдоигроков рынка по организации торговли на международном валютном рынке FOREX.

В прошлом году удалось выявить и ликвидировать более 250 финансовых пирамид. Несмотря на это граждане страны потеряли более 2 млрд. рублей!